FACULTAD DE INGENIERÍA UNAM
DIVISIÓN DE EDUCACIÓN CONTINUA

CURSOS INSTITUCIONALES

ADMINISTRACIÓN DE REDES

Del 05 al 09 de Agosto de 2002

APUNTES GENERALES

CI-209

SECRETARÍA DE GOBIERNO
AGOSTO DEL 2002

Palacio de Minería, Calle de Tacuba No. 5, Primer piso, Delegación Cuauhtémoc, CP 06000, Centro Histórico, México D F,
APDO Postal M-2285 • Tels: 5521 4021 al 24, 5623.2910 y 5623 2971 • Fax. 5510 0573

INSTALACION Y ADMINISTRACION DE WINDOWS 2000 SERVER

Para diseñar, instalar y poner a punto una red de datos bajo la plataforma Windows 2000 Server es necesario un previo diseño a toda la infraestructura de la red, y por tanto al equipo que la va a soportar, por tanto este manual esta diseñado conforme a las necesidades especificas del curso así, por lo tanto se indicara en ocasiones la instalación paso a paso de algunas de las mas importantes herramientas con las que cuenta el sistema operativo, así como sus requisitos de hardware.

Introducción

El diagrama de la figura 1 ilustra la configuración básica del servidor.

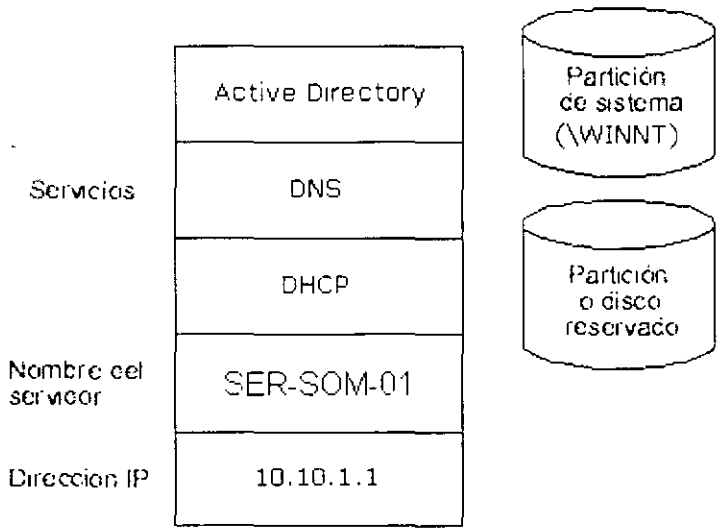


Figura . La configuración del servidor.

Configuración de los discos del servidor

Si desea utilizar un único servidor para la estructura descrita en esta guía, necesita un servidor con dos unidades de disco o con una única unidad pero con dos particiones. (En algunos pasos se requieren servidores adicionales u otros equipos; en la guía específica se habla de tales adiciones.)

El primer disco o partición contiene Windows 2000 y los demás archivos de la infraestructura común, como los paquetes de Windows Installer y los archivos de origen de la aplicación.
El segundo disco o partición está reservado a procedimientos de otras guías detalladas. Así, por ejemplo, contiene las imágenes del sistema operativo de la Guía detallada para la instalación remota del sistema operativo.
Cada disco o partición debe contener varios gigabytes de información y formatearse para el Sistema de archivos de Windows NT (NTFS). En esta guía se incluyen los pasos necesarios para crear y formatear las particiones.

Instalación del servidor

El primer paso del procedimiento de instalación consiste en crear discos de inicio. La instalación comienza después de iniciar el equipo desde estos discos. Éste es el procedimiento utilizado con estas guías, con lo que podrá configurar de nuevo fácilmente las particiones del disco.
Nota: Al configurar particiones y formatear unidades, se destruirán todos los datos de la unidad de disco duro del servidor.

Crear los discos de instalación de Windows 2000

Se necesitan cuatro discos formateados y el disco compacto de Windows 2000 Server. En un equipo que ejecute una versión de 32 bits del sistema operativo Windows:
Inserte el disco compacto de Windows 2000 Server en la unidad de CDROM.
Cuando se le pregunte **¿Desea actualizar a Windows 2000?**, haga clic en **No**.
En la pantalla de presentación del disco compacto de Windows 2000 Server, haga clic en **Examinar este CD**.
Cuando aparezca la lista de carpetas, haga doble clic en la carpeta **BOOTDISK**
Haga doble clic en **MAKEBT32**.
En el símbolo del sistema **Especifique el disquete donde se van a copiar los archivos de imagen**, escriba: **A**.
Inserte el primer disco y presione **ENTRAR**.
Siga las instrucciones para crear los otros tres discos.
Recomendación Etiquete los discos como se le solicita durante el proceso de creación para efectuar la instalación en el orden correcto.
Cierre la carpeta **BOOTDISK** y la pantalla de presentación del disco compacto de Windows 2000.

Iniciar la instalación

El programa de instalación crea las particiones del disco en el equipo que ejecuta Windows 2000 Server, formatea la unidad y copia los archivos de instalación del disco compacto al servidor.

Nota En estas instrucciones se da por supuesto que está instalando Windows 2000 Server en un equipo que no utiliza Windows. Si está actualizando una versión anterior de Windows, algunos pasos de la instalación pueden diferir.

Inserte el disco de instalación número uno de Windows 2000 Server.

Reinicie el equipo. Comenzará entonces la instalación de Windows 2000 Server.

Inserte los otros tres discos de instalación de Windows 2000 Server a medida que lo solicite el programa de instalación de Windows 2000.

En la pantalla **Programa de instalación**, presione **ENTRAR**.

Revise y, si procede, acepte el contrato de licencia presionando **F8**.

Nota Si tiene una versión previa de Windows 2000 instalada en este servidor, debe recibir un mensaje que le pregunta si desea reparar la unidad. Presione ***ESC*** para continuar y no reparar la unidad.

Siga las instrucciones para eliminar todas las particiones del disco existentes. Los pasos exactos variarán según el número y el tipo de particiones que tenga ya el equipo. Siga eliminando particiones hasta que todo el espacio del disco tenga la etiqueta **Espacio sin particiones**.

Cuando todo el disco esté etiquetado como **Espacio sin particiones**, presione **C** para crear una partición en el espacio sin particiones.

Si su servidor tiene una única unidad de disco, divida el espacio en disco disponible a la mitad para tener dos particiones del mismo tamaño. Elimine el **valor predeterminado del espacio total.** Escriba el valor de la mitad de su espacio en disco total en el símbolo del sistema **Crear partición de tamaño (en MB)**. Presione **ENTRAR**. (Si su servidor tiene dos unidades de disco, escriba el tamaño total de la primera unidad en este símbolo del sistema.)

Cuando haya creado la partición **Nueva (sin formato)**, presione **ENTRAR**.

Seleccione **Formatear la partición utilizando el sistema de archivos NTFS** (la selección predeterminada) y presione **ENTRAR**. Retire el disco de la unidad.

El programa de instalación de Windows 2000 formateará la partición y copiará los archivos del disco compacto de Windows 2000 Server a la unidad de disco duro. Se reiniciará el equipo y continuará el programa de instalación de Windows 2000.

Continuar la instalación

Seguidamente se describen los pasos para continuar la instalación con el Asistente para la instalación de Windows 2000 Server.

Aparecerá **Éste es el Asistente para la instalación de Windows 2000**; haga clic en **Siguiente**. Windows 2000 detectará e instalará dispositivos. Esto puede llevar varios minutos y puede que la pantalla parpadee durante el proceso.

En el cuadro de diálogo **Configuración regional**, haga los cambios necesarios para su configuración regional (por lo general, para Estados Unidos no se necesita ninguna) y haga clic en **Siguiente**.

En el cuadro de diálogo **Personalice su *software***, escriba **Sistema .Operativos Modernos** en el cuadro **Nombre** y **UTPBOCAS** en el cuadro **Organización**. Haga clic en **Siguiente**.

Escriba la **Clave del producto** (la encontrará al dorso de la caja del disco compacto de Windows 2000) en los cuadros de texto provistos para ello. Haga clic en **Siguiente**.

En el cuadro de diálogo **Modos de licencia**, seleccione el modo de licencia adecuado para su organización y haga clic en **Siguiente**.

En el cuadro de diálogo **Nombre del equipo y Contraseña del administrador**, escriba el nuevo nombre del equipo **SER-SOM-01** en el cuadro del nombre del equipo y haga clic en **Siguiente**

Recomendación Para facilitar los pasos de estas guías, el cuadro de la Contraseña de administrador se deja en blanco. Esto puede ser peligroso para la seguridad. Siempre que instale un servidor para una red de producción debe establecer una contraseña.

En el cuadro de diálogo **Componentes de Windows 2000**, haga clic en **Siguiente**. Espere a que se instalen los componentes de red. Podría tardar unos minutos.

En el cuadro de diálogo **Configuración de fecha y hora**, corrija si es necesario la fecha y la hora, y haga clic en **Siguiente**.

En el cuadro de diálogo **Configuración de red**, compruebe que está seleccionada la opción **Configuración típica** y haga clic en **Siguiente**.

En el cuadro de diálogo **Dominio del grupo de trabajo o del equipo** está seleccionado **No** de manera predeterminada; haga clic en **Siguiente**.

Nota Llegado a este punto se debe haber especificado un nombre de dominio, pero esta guía utiliza el Asistente para Configurar su servidor con el fin de crear el nombre de dominio posteriormente.

La instalación de Windows 2000 Server continúa con la configuración de los componentes necesarios. Esta operación tarda unos minutos.

Cuando llegue al Asistente **Finalización de la instalación de Windows 2000**, retire el CD-ROM de la unidad y haga clic en **Finalizar**.

Se reiniciará el servidor y se cargará el sistema operativo desde la unidad de disco duro.

Configurar el servidor como controlador de dominio

El Protocolo de configuración dinámica de host (DHCP), el Servicio de nombres de dominio (DNS) y DCPromo (la herramienta de la línea de comandos que crea DNS y Active Directory) pueden instalarse manualmente o mediante el Asistente **Configurar su servidor** de **Windows 2000**. Esta guía emplea el asistente; los procedimientos manuales no están recogidos en ella.

Presione **CTRL-ALT-SUPR** e inicie la sesión en el servidor como **administrador**. Deje en blanco el cuadro de la contraseña.

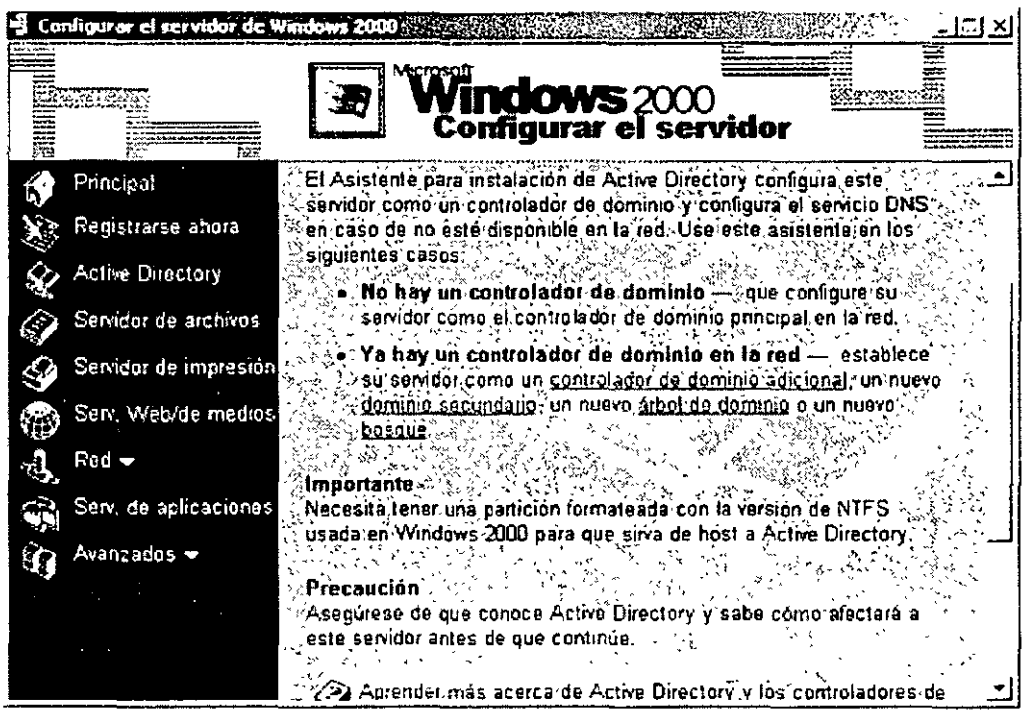
Cuando aparezca la página **Configurar su servidor de Windows 2000**. seleccione **Éste es el único servidor de mi red** y haga clic en **Siguiente**.

Haga clic en **Siguiente** para configurar el servidor como controlador de dominio e instale Active Directory, DHCP y DNS.

En la página **¿Desea poner un nombre a su dominio?**, escriba **utpbocas**.

En el cuadro de nombre de dominio, escriba com. Haga clic en algún lugar de la pantalla fuera del cuadro de texto para ver la Vista previa del nombre del dominio de Active Directory. Haga clic en Siguiente.

Nota Como se muestra en la figura 2, el nombre combinado aparecerá como utpbocas.com en el cuadro **Vista previa del nombre de dominio de Active Directory**. El asistente agregará el punto



(.) al nombre.

Figura 2 Asistente Configurar su servidor

Asistente Configurar su servidor

Haga clic en **Siguiente** para ejecutar el asistente. Cuando se le solicite, inserte el CD-ROM de Windows 2000 Professional. Cuando finalice el asistente se reiniciará la máquina.

El Asistente **Configurar su servidor** instalará DNS y DHCP, y configurará DNS, DHCP y Active Directory. Los valores predeterminados establecidos por el asistente son los siguientes:

Ámbito DHCP:	10.0.0.3-10.0.0.254
Servidor DNS preferido:	127.0.0.1
Dirección IP:	10.10.1.1
Máscara de subred:	255.0.0.0

utpbocas.com es el dominio de Active Directory y el nombre DNS; **utpbocas** es el nombre de dominio de nivel inferior.

Formatear la segunda unidad o partición de disco

Advertencia Al formatear la partición se destruyen todos los datos de la misma. Hágalo sólo si es necesario y asegúrese de seleccionar la partición correcta.

Inicie la sesión en el servidor como Administrador.

Desactive la casilla de verificación **Mostrar esta pantalla al iniciar** en el Asistente **Configurar su servidor** y cierre el asistente.

Haga clic en **Inicio**, seleccione **Programas**, **Herramientas administrativas** y haga clic en **Administración de equipos**. Aparecerá el complemento Administración de equipos.

Haga clic en el signo + que aparece junto a **Almacenamiento**, si la carpeta no está ya expandida.

Haga clic en la carpeta **Administración de discos**.

Haga clic con el botón secundario del *mouse* (ratón) en **espacio no asignado en disco** y haga clic en **Crear partición**.

Aparecerá **Éste es el Asistente para crear partición**. Haga clic en **Siguiente**.

Seleccione **Partición extendida** y haga clic en **Siguiente**.

Haga clic en **Siguiente** para aceptar el tamaño de partición especificado y, después, haga clic en **Finalizar**.

Haga clic con el botón secundario del *mouse* en **Espacio libre** y después haga clic en **Crear unidad lógica**.

Aparecerá **Éste es el Asistente para crear partición**. Haga clic en **Siguiente**.

Seleccione **Unidad lógica** y haga clic en **Siguiente**.

Haga clic en **Siguiente** para aceptar el tamaño de partición especificado.

Acepte la letra de unidad predeterminada; para ello, haga clic en **Siguiente**.

En la página Formatear la partición, acepte los valores predeterminados que usará para el sistema de archivos (el formato NTFS y el tamaño de la partición completa), el tamaño de la unidad de asignación y la etiqueta de volumen. Haga clic en **Siguiente** y, a continuación, en **Finalizar**. Se formateará la unidad o la partición. Esto puede llevar cierto tiempo, dependiendo del tamaño del disco y la velocidad del equipo.

Nota Es posible que reciba un mensaje de error *El volumen está abierto o en uso. La solicitud no puede completarse*. Se trata de un error de temporización porque acaba de crear la partición. Si recibe este mensaje, haga clic en *Aceptar*, vuelva a hacer clic con el botón secundario del *mouse* en la partición y haga clic en *Formatear*. Acepte todos los valores predeterminados y haga clic en *Aceptar*. Recibirá un mensaje de advertencia diciéndole que si continúa con el formateado se borrarán todos los datos. Haga clic en *Aceptar*.

Cuando haya formateado el disco o la partición, cierre el complemento Administración de discos.

Active Directory

Ejemplo de infraestructura de Active Directory

Esta infraestructura común se basa en la compañía ficticia *utpbocas*.

El nombre DNS de utpbocas es *utpbocas.com*, configurado con ayuda del Asistente **Configurar su servidor** en la sección anterior. La figura 2 que aparece a continuación ilustra la infraestructura de ejemplo de Active Directory.

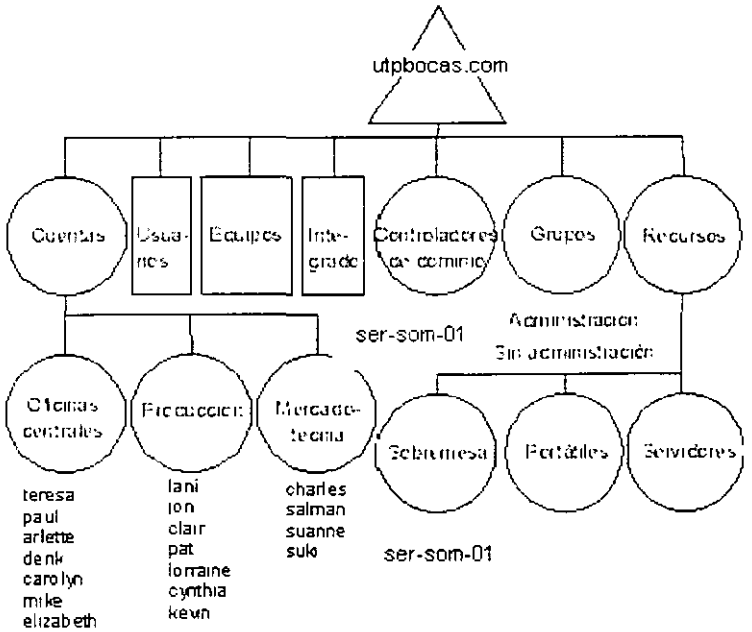


Figura Ejemplo de estructura de AD.

Los aspectos más interesantes son el Dominio (utpbocas.com) y las unidades organizativas (OU) Cuentas, Oficinas centrales, Producción, Mercadotecnia, Grupos, Recursos, Sobremesa, Portátiles y Servidores. Todos están representados por círculos en el diagrama anteriormente citado. Las OU tienen por objeto delegar la administración y aplicar Directiva de grupo; no se trata de ser el simple reflejo de una organización empresarial.

Llenar Active Directory

En esta sección se explica cómo crear manualmente las OU, los usuarios y los grupos de seguridad descritos en el apéndice A de este documento.

Para crear unidades organizativas y grupos

Haga clic en **Inicio**, seleccione **Programas**, **Herramientas administrativas** y haga clic en **Usuarios y equipos de Active Directory**.

Haga clic en el signo + situado junto a **utpbocas.com** para expanderlo Haga clic en **utpbocas.com** para ver su contenido en el panel de la derecha.

En el panel de la izquierda, haga clic con el botón secundario del *mouse* (ratón) en **utpbocas.com**, seleccione **Nuevo** y haga clic en **Unidad organizativa**.

Escriba **Cuentas** en el cuadro de nombre y haga clic en **Aceptar**.

Repita los pasos 3 y 4 para crear las OU **Grupos** y **Recursos**. Estas tres OU aparecerán ahora en el panel derecho.

Haga clic en **Cuentas**, en el *panel de la izquierda*. Sus contenidos se mostrarán ahora en el panel de la derecha (está vacío al principio).

Haga clic con el botón secundario del *mouse* en **Cuentas**, seleccione **Nuevo** y haga clic en **Unidad organizativa**.

Escriba **Oficinas centrales** y haga clic en **Aceptar**.

Repita los pasos 6 y 7 para crear las OU **Producción** y **Mercadotecnia** dentro de **Cuentas**.

Siga el mismo procedimiento para crear **Sobremesa**, **Portátiles** y **Servidores** bajo la OU Recursos.

Cree los dos grupos de seguridad; para ello, haga clic con el botón secundario del *mouse* en **Grupos**, seleccione **Nuevo** y haga clic en **Grupo**. Los dos grupos que se agregarán son **Administración** y **No administración**. La configuración de cada grupo debe ser **Global** y **Seguridad**. Haga clic en **Aceptar** para crear cada grupo.

Para crear cuentas de usuario

En la pantalla de la izquierda, haga clic en el signo + situado junto a la carpeta **Cuentas** para expandirla.

Haga clic en **Oficinas centrales** (bajo **Cuentas**) en la pantalla de la izquierda. Sus contenidos se mostrarán ahora en el panel de la derecha (está vacío al principio).

Haga clic con el botón secundario del *mouse* en **Oficinas centrales**, seleccione **Nuevo** y haga clic en **Usuario**.

Escriba **Teresa** como primer nombre y **Atkinson** como apellido. (Observe que en el cuadro del nombre completo aparece automáticamente el nombre completo.)

Escriba **Teresa** como **Nombre de inicio de sesión de usuario.**

Haga clic en **Siguiente**.

Haga clic en **Siguiente** en la página **Contraseña** para aceptar los valores predeterminados.

Haga clic en **Finalizar**. En la pantalla de la derecha aparecerá ahora Teresa Atkinson como usuario bajo utpbocas.com/Cuentas/Oficinas centrales.

Repita los pasos 2 a 7, agregando los nombres que aparecen en el apéndice A para la OU Oficinas centrales.

Repita los pasos 1 a 8 para crear los usuarios de las OU Producción y Mercadotecnia.

Para agregar usuarios a grupos de seguridad

En el panel de la izquierda, haga clic en **Grupos**.

En el panel de la derecha, haga doble clic en el grupo **Administración**.

Haga clic en la ficha **Miembros** y después en **Agregar**.

Seleccione los usuarios en el panel superior; para ello, mantenga presionada la tecla **CTRL** mientras hace clic en cada nombre. Haga clic en **Agregar** para agregarlos todos de una vez. (Los usuarios que deben ser miembros de este grupo de seguridad aparecen en la lista del apéndice A.) Sus nombres se mostrarán en el panel inferior. Haga clic en **Aceptar**.

Repita los pasos 2 a 4 para agregar miembros al grupo **No administración**.

Cierre el complemento **Usuarios y equipos de Active Directory**.

TABLAS D EFUNCIONES DE WINDOWS 2000 SERVER

FUNCIONES DEL SERVIDOR DE INFRAESTRUCTURA

A medida que las organizaciones instalan más computadoras de escritorio para aumentar la productividad y automatizar el proceso de sus operaciones, buscan formas más eficientes de administrar sus redes y computadoras de escritorio. Windows 2000 Server proporciona un gran número de nuevas funciones, diseñadas para facilitar a las organizaciones la administración de una red de computadoras de escritorio y disminuir los costos de administración.

Nueva función	Descripción	Beneficio
SERVICIOS DE DIRECTORIO		
Protocolo ligero de acceso a directorio (LDAP)	Las versiones 2 y 3 de LDAP están implementadas para el acceso de cliente	Esto permite sincronización e interoperabilidad entre multiples sistemas operativos y directorios
Denominación estandar	Los usuarios y las aplicaciones se ven afectados por el formato de nombre que se utiliza en los servicios de directorio. Si un usuario o aplicaciones necesita encontrar o utilizar algo, ese usuario o aplicacion debe saber el nombre o alguna propiedad del objeto a fin de localizarlo Existen numerosas formas comunes para nombres en directorios, definidas por estándares formales y *de facto*, y Active Directory soporta muchos de estos formatos incluyendo Nombres URL de HTTP, URLs LDAP y Nombres X 500, asi como Nombres UNC	Este soporte ampliado para numerosos formatos de nombres permite a los usuarios y a las aplicaciones utilizar el formato con el que estan más familiarizados al acceder a Active Directory A continuación, se explican algunos de estos formatos
Desarrollado a partir de DNS	DNS es el servicio de directorio que se utiliza más en el mundo DNS es el servicio localizador utilizado en Internet y en la mayoria de las intranets privadas Un servicio localizador se utiliza para convertir un nombre, por ejemplo, MyMachine Myco Com, en una dirección TCP/IP	Ya que DNS está diseñado para escalar a sistemas muy grandes (soporta a Internet en su totalidad), al tiempo que se conserva lo suficientemente "ligero" para utilizarse en un sistema con sólo unas cuantas computadoras, las organizaciones pueden estar seguras de que el servicio de directorio de Windows 2000 Server escalará en una forma que satisfaga sus necesidades

Nueva función	Descripción	Beneficio
Interfaz de servicio de Active Directory (ADSI)	ADSI obtiene las capacidades de los servicios de directorio de diferentes proveedores de red para presentar un solo conjunto de interfaces de servicio de directorio, a fin de administrar los recursos de la red ADSI es un conjunto de interfaces de programación ampliables fáciles de utilizar que pueden usarse para escribir aplicaciones a fin de acceder y administrar lo siguiente: • Active Directory • Cualquier directorio basado en LDAP • Otros servicios de directorio en una red del cliente, incluyendo NDS	Esto simplifica en gran medida el desarrollo de aplicaciones habilitadas con directorio, así como la administracion de sistemas distribuidos Los desarrolladores y administradores utilizan este unico conjunto de interfaces de servicio de directorio para enumerar y administrar los recursos en un servicio de directorio, sin importar que ambiente de red contiene a ese recurso
Esquema ampliable	Active Directory proporciona a los desarrolladores y administradores la capacidad de ampliar el esquema de directorio y crear nuevas propiedades y objetos	Los desarrolladores pueden utilizar esta función de amplitud a fin de crear sus propias estructuras de datos en el directorio para las aplicaciones por lo que el directorio se utiliza como un almacén de datos Además los usuarios en la red pueden publicar informacion importante en el directorio para que otros puedan encontrar fácilmente esta informacion
Catálogo global	Otro nuevo concepto en Active Directory es el catálogo global (GC). El catalogo global alberga todos los objetos de todos los dominios en el directorio de Windows 2000 Server y un subconjunto de propiedades de cada objeto	Diseñado para alto rendimiento. GC permite a los usuarios encontrar fácilmente un objeto, sin importar dónde se encuentre en el arbol, al tiempo que busca por atributos seleccionados.
Duplicacion multimaster	Con la duplicación multimaster, pueden hacerse cambios en cualquier controlador de dominio en el dominio Entonces, el controlador de dominio duplica los cambios en sus socios de duplicacion	Utilizar la duplicación multimaster da como resultado una disponibilidad al 100 por ciento del directorio para cambios, incluso si los controladores de dominio unicos no estan disponibles Además, al proporcionar varias copias del directorio a través de multiples servidores, el directorio de Windows 2000 Server es capaz de escalar hasta satisfacer las necesidades de la empresa

Nueva función	Descripción	Beneficios
Compatibilidad con versiones anteriores	Windows 2000 Server soporta un ambiente combinado de controladores de dominio Active Directory de Windows 2000 Server y controladores de dominio Windows NT Server 4 0 Los clientes con versiones anteriores pensarán que están accediendo a controladores de domino Windows NT Server 4 0.	Esta compatibilidad al 100 por ciento con versiones anteriores permite que las empresas migren sus controladores de dominio primero y después sus clientes, o que migren una combinacion de servidores y clientes Nunca hay un punto en el proceso de migración que requiera una migración masiva a la nueva versión del sistema operativo en los servidores o clientes Así mismo, nunca es necesario poner todo un domino fuera de linea para migrar los controladores de domino o clientes
SEGURIDAD		
Administrador de configuraciones de seguridad	El Administrador de configuraciones de seguridad proporciona una configuracion de seguridad de un solo paso y una herramienta de análisis para Windows 2000 Server Permite la configuracion de varias especificaciones de registro donde la seguridad es importante, controles de acceso en archivos y claves de registro, así como configuración de seguridad de los servicios del sistema	El Administrador de configuraciones de seguridad es una tecnología que "se define una vez y se aplica varias veces", y que permite a los administradores de red definir configuraciones de seguridad como una plantilla, y después aplicarla a computadoras seleccionadas en una operación
Autenticación *Kerberos*	La Version 5 del protocolo de autenticación *Kerberos* reemplaza a NTLM como el protocolo de seguridad principal para acceso a recursos dentro o a traves de dominios de Windows 2000 Server	El soporte total para la Version 5 del protocolo *Kerberos* proporciona un solo acceso rapido a los recursos empresariales basados en Windows 2000 Server, así como a otros ambientes que soportan este protocolo
PPTP/L2TP	PPTP/L2TP proporciona soporte para redes privadas virtuales Permite que las empresas utilicen Internet como una red privada virtual a fin de lograr comunicaciones seguras y autenticadas	Permite a los usuarios remotos conectarse a su empresa utilizando Internet Esto a su vez les brinda la capacidad de reemplazar líneas arrendadas costosas y utilizar Internet
Servidor de certificados de claves públicas	El servidor de certificados de claves públicas basado en X 509 y la integración con Active Directory permite el uso de certificados de claves públicas para autenticación	El Servidor de certificados de claves publicas integrado en Windows 2000 Server es para organizaciones que desean emitir certificados de claves públicas a sus usuarios sin depender de los servicios CA comerciales

Nueva función	Descripción	Beneficio
Infraestructura de tarjetas inteligentes	Las tarjetas inteligentes proporcionan almacenamiento resistente a alteración para proteger claves privadas, números de cuenta contraseñas y otras formas de información personal	Las tarjetas inteligentes son un componente clave de la infraestructura de claves públicas que Microsoft esta integrando a la plataforma Windows porque las tarjetas inteligentes mejoran las soluciones basadas solo en software como la autenticación de clientes firmas unicas, almacenamiento seguro y administracion del sistema
Protocolo de seguridad IP	IPSEC soporta autenticacion a nivel de red, integridad de datos y encriptación Se integra a la seguridad inherente del sistema operativo de Windows 2000 Server a fin de proporcionar la plataforma ideal para salvaguardar las comunicaciones de intranet e Internet	La Administracion de seguridad IP de Microsoft rige las comunicaciones seguras de extremo a extremo Una vez que un administrador ha implementado la seguridad IP para una empresa las comunicaciones se aseguran en forma transparente no se requiere capacitacion o interacción alguna del usuario

SERVICIOS DE ADMINISTRACION

Windows 2000 Server proporciona un conjunto amplio de servicios de administración y una gama de herramientas integradas fáciles de utilizar La infraestructura de administración está conformada por una variedad de servicios diferentes que en conjunto hacen que Windows 2000 Server sea el mejor ambiente a partir del cual desarrollar herramientas de administración y llevar a cabo operaciones administrativas. Windows 2000 Server ofrece una variedad de herramientas en sí, pero también son importantes las herramientas que se proporcionan a través de Systems Management Server y de terceros. La infraestructura de administración es lo suficientemente sofisticada para soportar dicha variedad de herramientas.

Nueva función	Descripción	Beneficio
INTERFACES DE ADMINISTRACION		

Nueva función	Descripción	Beneficio
Microsoft Management Console	Microsoft Management Console (MMC) proporciona a los administradores de sistemas una consola común para visualizar las funciones de red y utilizar herramientas administrativas MMC muestra en pantalla consolas que alojan programas llamados *snap-ins*, que proporcionan la funcionalidad necesaria para administrar la red	MMC reduce el costo total de propiedad para el escritorio. La delegación de tareas, agrupación logica de herramientas y procesos, y la administración a través de una sola interfaz permite a los administradores de sistemas organizar mejor sus herramientas y tareas, asi como simplificar la administracion remota
Herramienta de migracion de servicio de directorio de Microsoft (*snap-in* de MMC)	La Herramienta de migración de servicio de directorio de Microsoft proporciona una arquitectura para descubrir los recursos NetWare moldearlos fuera de línea y migrarlos a Active Directory Esta función incluye lo siguiente Descubrimiento de todas las propiedades NetWare de usuarios, y grupos para uniones y NDS Migración rudimentaria de archivos Exportación a Active Directory	Esta herramienta de migración asegura que el servicio de directorio no se dañara inadvertidamente durante la migracion, porque la copia fuera de linea en la máquina local se puede manipular, cambiar y actualizar tan seguido como sea necesario antes de migrar Los administradores pueden intentar diferentes escenarios de "por si acaso" a fin de encontrar el diseño que funcione mejor para su red y llevar a cabo la migración en etapas destinadas a minimizar las interrupciones Este enfoque fuera de linea también puede utilizarse a fin de proporcionar instantáneas de historial del directorio que pueden compararse con otras actualizaciones para ver como ha crecido o cambiado el directorio a través del tiempo
Administracion de computadora (*snap-in* de MMC)	El *snap-in* de Administración de computadora es una herramienta para configurar la computadora del administrador Esta diseñado para que funcione con una sola computadora, y todas sus funciones se pueden utilizar desde una computadora remota, lo que permite que un administrador solucione problemas y configure una maquina desde cualquier otra computadora en la misma red	El *snap-in* de Administración de computadora es una carpeta de Herramientas administrativas o una caja de Herramientas remota. No sólo proporciona acceso a las herramientas básicas de Windows 2000 Server (visualizacion de eventos, creación de componentes compartidos, administración de dispositivos, y demás), sino que también descubre dinámicamente qué servicios de servidor y aplicaciones hay para administrar

Nueva función	Descripción	Beneficio
Administracion de discos (*snap-in* de MMC)	El *snap-in* de Administración de discos es una herramienta gráfica para administrar discos que reemplaza al Administrador de discos Soporta particiones, unidades logicas y los nuevos volumenes dinámicos Contiene menues de accesos rapidos y asistentes para simplificar la creación de volumenes, así como inicializar y actualizar discos	Esta herramienta permite que los administradores lleven a cabo tareas administrativas como la creacion, ampliación, duplicacion de un volumen o incluso agregar discos todo sin reiniciar el sistema o interrumpir a los usuarios
Administracion de los servicios del sistema (*snap-in* de MMC)	Esta herramienta le permite detener iniciar, poner en pausa y continuar los servicios en computadoras locales y remotas Reemplaza a la aplicación Panel de control de servicios en versiones anteriores de Windows 2000 Server	Esta funcion permite que el servicio SCM administre problemas comunes del usuario Por ejemplo, cuando un servicio falla puede reiniciarlo automaticamente, ejecutar un *script* o archivo exe, o incluso reiniciar el servidor
Administrador de dispositivos y Asistente de hardware (*snap-in* de MMC)	El Administrador de dispositivos es un *snap-in* de Microsoft Management Console que le permite configurar dispositivos y recursos en su computadora	Agregar nuevo hardware cambiar propiedades de dispositivos desconectar o expulsar dispositivos y resolver conflictos de hardware son sólo unas de las operaciones que pueden realizarse con el Asistente de hardware
Política de grupo	La interfaz de instalación de aplicaciones las opciones de política destinadas a computadoras y usuarios, y los *scripts* se encuentran en un *snap-in* de Microsoft Management Console (MMC) llamado Política de grupo (GP) El *snap-in* GP es responsable de administrar las configuraciones de la Política de grupo a medida que se aplica a un sitio, dominio o unidad organizacional determinado	La administracion basada en politicas automatizará tareas como actualizaciones de sistemas operativos instalación de aplicaciones, perfiles de usuarios y bloqueo del sistema de escritorio.
Windows Scripting Host (WSH)	Windows 2000 Server soporta la ejecución directa de *scripts* desde la interfaz o el indicador de comandos. Este soporte se proporciona a traves de Windows Scripting Host (WSH), una herramienta extremadamente flexible con soporte integrado para *scripts* en Visual Basic y Java y una arquitectura independiente de lenguaje	Windows Scripting Host permite a los administradores y/o usuarios ahorrar tiempo al automatizar muchas de las acciones de las interfaces, como la creacion de un acceso rapido, conexión a un servidor de red, desconexión desde un servidor de red etc
Programador de tareas	El Programador de tareas proporciona una interfaz accesible para el usuario a fin de programar aplicaciones Esta interfaz es la misma en Windows 95 y Windows 2000 Server, a excepción de las funciones de seguridad adicionales en Windows 2000 Server	Con el Programador de tareas es posible invocar cualquier *script*, programa o documento en cualquier momento o intervalo, diariamente o una vez al año, y en eventos como arranque del sistema, conexion de usuario o inactividad del sistema
INSTALACION EN COMPUTADORA		

Nueva función	Descripción	Beneficio
Instalación remota de sistema operativo	Utilizando una tecnología de arranque remoto basada en estándares (PXE), una PC puede conectarse automáticamente a Windows 2000 Server e instalar Windows 2000 Professional	El servicio de Instalación remota de sistema operativo puede utilizarse para configurar simplemente una nueva computadora, actualizar una computadora a Windows 2000 Server o volver a formatear e instalar el sistema operativo en una máquina existente
TECNOLOGIAS INTELLIMIRROR		
Administración de datos del usuario	Los usuarios pueden conectarse a cualquier PC basada en Windows 2000 Professional en la red corporativa y siempre tendrán acceso a sus datos, aplicaciones y preferencias de computadora Así mismo, los usuarios pueden utilizar recursos clave fuera de línea basados en red y locales, que automáticamente se sincronizarán después de reconectarse a la red	Los datos del usuario siempre están disponibles y la vista del usuario del ambiente computacional es consistente, sin importar si la computadora cliente está conectada a la red Ademas, se evita la pérdida o falla de los datos del usuario en la máquina local
Instalación y mantenimiento de software	El administrador puede especificar un conjunto de aplicaciones que siempre estarán disponibles a un usuario o grupo de usuarios Si una aplicación requerida no está disponible cuando se necesita, se instalará automáticamente Así mismo, se soportan la actualización de autoreparación y la eliminación de aplicaciones.	Los administradores de informática pueden instalar y mantener aplicaciones para cualquier usuario o grupo de usuarios con sólo unos pasos, sin necesidad de intervención del usuario o sin "visitar" ningún escritorio.
Administración de configuraciones del usuario	Administración centralizada y control de computadoras de escritorio, con la capacidad de asegurar las configuraciones de escritorio	Con la tecnología de administración IntelliMirror, las configuraciones de los usuarios se duplican en la red y los administradores pueden definir ambientes computacionales específicos para usuarios y computadoras
Memoria cache del lado del cliente	La memoria cache del lado del cliente sincroniza transparentemente los datos entre una red y una máquina local Esto da como resultado un método fácil de utilizar para usuarios remotos a fin de que puedan sincronizarse con la red	Con la memoria caché del lado del cliente los datos siempre están disponibles y la vista de los usuarios del ambiente computacional es consistente, sin importar si la computadora cliente esta conectada a la red
INSTRUMENTACION		

Nueva función	Descripción	Beneficio
Instrumentacion de administración de Windows	La Instrumentacion de administracion de Windows proporciona soporte total de sistema operativo integrado para una administracion uniforme del sistema y de las aplicaciones con base en el Modelo de información común (CIM) adoptado por Desktop Management Task Force como parte de su iniciativa de Administracion de empresas basada en Web (WBEM)	La Instrumentacion de administracion Windows simplifica la instrumentacion de controladores y aplicaciones lo que significa mayor control, ofrece el potencial de disminuir los costos de propiedad a traves de un ambiente mejor administrado y brinda información detallada y ampliable consistente a traves de diferentes productos de distribuidores

Nueva función	Descripción	Beneficio
SERVICIOS DE TERMINAL		
Soporte a clientes múltiples	Ofrece la GUI de Windows a usuarios de Terminales basadas en Windows y escritorios heredados, incluyendo Win16, Macintosh y UNIX, así como escritorios basados en interfaces de programación de aplicaciones Win32 (La conectividad a máquinas Macintosh y maquinas basadas en UNIX requiere accesorios adicionales de terceros)	Los clientes pueden utilizar hardware heredado.
Soporte de desconexion de *roaming*	Soporta la capacidad de los usuarios de salirse de una sesion sin desconectarse	Esto permite a los usuarios dejar una sesión activa, o en ejecucion, mientras se desconectan y despues reconectarse a la sesión existente desde otra maquina o en otro momento.
Soporte de conexión multiple	Soporta múltiples sesiones de conexion simultánea desde escritorios diferentes	Esto permite que los usuarios se conecten a numerosos Terminal Servers o a uno solo varias veces para llevar a cabo numerosas tareas o ejecutar múltiples sesiones en un solo escritorio
Soporte a sistemas de archivos distribuidos	El soporte es para conectarse a un componente compartido Dfs	Esto permite que los clientes alberguen componentes compartidos Dfs de Terminal Server

Nueva función	Descripción	Beneficio
Administración de servicios de terminal y Administración a control remoto	La Herramienta de administración de servicios de terminal se utiliza para consultar y administrar sesiones de Terminal Server, así como usuarios y procesos en Terminal Servers Cualquier usuario de Servicio de terminal con privilegios administrativos y acceso a las utilidades administrativas en Terminal Server puede administrar remotamente a Terminal Server	Entre sus funciones, la utilidad puede • Desconectar una sesión • Enviar un mensaje a una sesión o usuario • Restablecer una sesion • Mostrar en pantalla el estado de conexion de la sesion • Mostrar en pantalla la información de cliente de la sesion • Mostrar en pantalla los procesos del usuario del sistema • Terminar un proceso
Configuración de servicios de terminal	Crea, modifica y elimina sesiones y configuraciones de sesiones en su Terminal Server	Entre sus funciones, la Configuración de conexión puede • Configurar una nueva conexión • Administrar permisos para una conexión • Agregar usuarios y grupos a listas de permiso • Controlar las especificaciones de fin de temporizacion y de desconexión
Integración con el monitor de rendimiento de Windows 2000 Server	Permite que un administrador monitoree fácilmente el rendimiento del sistema de Terminal Server	Al utilizar el Monitor de rendimiento con los Servicios de terminal, los administradores de red pueden • Monitorear el uso del procesador por sesión de usuario • Monitorear la asignación de memoria por sesión de usuario • Monitorear el uso de memoria localizada e intercambio por sesión de usuario
Fin de temporización configurable de inactividad	Los administradores pueden configurar cuándo finalizar sesiones debido a inactividad	Esta funcion permite la reducción de carga del servidor
Niveles múltiples de codificación	Los administradores tendran la opción de configurar transmisiones de datos entre Terminal Server y los Clientes de Terminal Server	Esto permite que los administradores encripten todos o parte de los datos transmitidos entre el cliente y el servidor en tres niveles diferentes, dependiendo de sus necesidades de seguridad

Nueva función	Descripción	Beneficio

Nueva función	Descripción	Beneficio
HERRAMIENTAS DE CONFIGURACION Y RESOLUCION DE PROBLEMAS		
Recuperacion avanzada del sistema (ASR)	La Recuperacion avanzada del sistema (ASR) integra los componentes de respaldo, restablecimiento, reparacion y recuperación en una solución unificada y totalmente nativa de Windows 2000 Server	ASR permite que los usuarios guarden un estado completo de su sistema, y proporciona una forma de restablecer ese estado para fines de recuperacion de desastre
Administrador de componentes opcionales	Para soportar la instalación de componentes opcionales, la instalación de Windows 2000 Server ahora proporciona un mecanismo que permite que cualquier numero de componentes adicionales se agrupen en un módulo de instalación, y se instalen durante o después de la configuración del sistema	Windows 2000 Server soporta la capacidad de integrar componentes opcionales a fin de permitir que los integradores de sistemas personalicen instalaciones de componentes adicionales de terceros
Configuracion de modo seguro	Ahora Windows 2000 Server soporta una pantalla de opciones de modo seguro que puede accederse desde el cargador de arranque inicial a traves de la tecla F8.	El modo seguro evita que el sistema operativo no pueda arrancarse despues de instalar un controlador de terceros "con fallas" o una aplicación que utiliza controladores de modo *kernel* (especialmente filtros de sistemas de archivos)
Duplicacion de disco	La configuración incluye un mecanismo para OEMs, VARs y administradores de sistema a fin de duplicar o "clonar" totalmente los sistemas instalados en circunstancias controladas (por ejemplo hardware identico y algunas configuraciones de dominio)	Los clientes corporativos que instalan miles de escritorios y servidores Windows 2000 Server en hardware identico en ambientes computacionales homogéneos desean la capacidad de personalizar una sola maquina y después "clonar" el disco duro de la misma en los otros escritorios de la empresa
Asistente de incompatibilidad de controlador	Este asistente de resolucion de problemas detecta y advierte al usuario si ciertas aplicaciones/componentes instalados provocarán que falle la actualización o si los componentes no funcionaran después de que se termina la actualizacion	En caso de que se reporte una incompatibilidad, el usuario puede ser dirigido automaticamente a un sitio Web creado por el OEM/Proveedor independiente de software que proporcione mayor información o una solucion para el problema, o el usuario puede proporcionar un disco suministrado por el OEM/ Proveedor independiente de software para solucionar la aplicación incompatible.

WINDOWS 2000 SERVER INSTALACION, COMPONENTES Y CONFIGURACION

Nueva función	Descripción	Beneficio
Asistente de configuración de servidor	Ahora, Windows 2000 Server puede configurarse automáticamente para un número de escenarios de uso diferentes Servidor Active Directory; Servidor de operación en red, Servidor de archivos, Servidor de impresión, Servidor Web y Servidor de *clustering*	Para cada escenario, la configuración solo instala los servicios importantes, por ejemplo, el escenario del Servidor Active Directory configura al servidor como un controlador de dominio e instala los servicios AD y DNS
Instalación automatizada	La instalacion automatizada es el medio a través del cual los OEMs, administradores en empresas, VARs y otros usuarios pueden instalar Windows 2000 Server y los componentes opcionales, por ejemplo, *Clustering*, Active Directory etc , sin la interacción de ningún usuario con la computadora	Esto permite instalaciones personalizadas más rapidas del sistema operativo
Consola de comandos de reparación	Esta utilidad permite que un usuario autorizado lea/escriba volumenes NTFS utilizando los Discos flexibles de arranque de Windows 2000 Server y, por lo tanto, copie archivos, inicie/pare servicios de, y repare el sistema Asi mismo, es posible reparar el Registro de arranque maestro/sector de Arranque y los volúmenes de formato/fdisk	En anteriores versiones no habia una forma sancionada de Microsoft para acceder a un volumen NTFS a menos que se iniciara Windows 2000 Server Sin embargo, en algunos casos, esto era imposible si un archivo de sistema critico estaba dañado o faltaba La única solución era llevar a cabo una instalacion paralela de Windows 2000 Server o ejecutar el proceso de reparacion, siendo ambos procesos muy tardados A menudo, debido a esto, los administradores instalaban Windows 2000 en FAT, porque siempre podian acceder al volumen utilizando un disco flexible DOS
Introducion de Service Pack	Ahora, los administradores pueden introducir fácilmente los medios de Service Pack en el sistema operativo base, es decir, los usuarios no necesitan reinstalar SP's después de instalar nuevos componentes Los Service Packs entregan actualizaciones (soluciones de errores y algunas veces funciones) al sistema operativo base En Windows NT Server 4 0, esto provocaba un problema porque a veces cuando el estado del sistema cambiaba (por ejemplo, se instalaba RAS), el SP tenia que reaplicarse.	Los administradores pueden aplicar un Service Pack a un componentes compartido de instalación, para que cuando se ejecute la Configuración de modo de texto, se utilicen las claves de registro y archivos adecuados del SP (por ejemplo, INFs/archivos actualizados), y para cuando se ejecute la configuración de modo GUI, se invoquen las DLL's adecuadas de Service Pack para llevar a cabo cualquier trabajo adicional Como resultado, cuando el usuario necesite agregar un nuevo componente (por ejemplo, RAS), se utilizan los archivos y entradas de registro adecuados (SP y/o Sistema operativo base)

Nueva función	Descripción	Beneficio
Soporte de disco dinámico	Permite actualizaciones e instalaciones sin problemas en volumenes de disco dinamico (por ejemplo, volumenes que no requieren rearranque para implementar cambios a la configuracion)	Un volumen de disco dinámico es cualquier disco dividido por el Administrador de disco logico (que contiene una partición de sistema de 4 MB al final del disco físico) lo que permite que el volumen se amplie y configure para tolerar fallas

FUNCIONES DEI SERVIDOR DE ARCHIVOS E Impresión

Las organizaciones están utilizando sistemas operativos de servidor para diferentes necesidades comerciales Uno de los usos más populares de un sistema operativo de servidor es proporcionar servicios para impresión, publicación e información compartida. Desde la entrada al mercado de Windows 2000 Server, las organizaciones han aprovechado las funciones ricas de archivos e impresión. A medida que las tecnologías de Internet como HTML y los medios de flujos se han popularizado, las organizaciones están considerando publicar y compartir en estos nuevos formatos Windows 2000 Server es una plataforma con servicios integrados para archivos compartidos e impresión, servidores Web y medios de flujos.

Administración de servicios de archivos	El *snap-in* de MMC de Administracion de servicios de archivos permite a los usuarios crear componentes compartidos y administrar las sesiones y conexiones en computadoras locales o remotas Reemplaza la funcionalidad que se encontraba anteriormente en la aplicación de Panel de control del sistema Además de sus capacidades remotas, también permite que el usuario cree componentes compartidos para cualquiera de los servicios de archivos instalables que se ofrecen en Microsoft: Servicios de archivos e impresión para Macintosh y Servicios de archivos e Impresión para NetWare	Al utilizarse con el Sistema de archivos distribuidos (Dfs), esta herramienta podria utilizarse para conectar componentes compartidos en toda la empresa en un solo espacio de nombre logico, es decir, los usuarios se conectan a un recurso para acceder a todos los recursos publicados dentro de cualquier volumen Dfs Asi mismo, podría utilizarse con la herramienta de Administración de directorio a fin de publicar un componente compartido como un Objeto de volumen en Active Directory que los usuarios pudieran consultar fácil y rápidamente en busca de recursos y componentes compartidos disponibles.

FUNCIONES DEl SERVIDOR DE ARCHIVOS E IMPRESION

Nueva función	Descripción	Beneficio
Integración de Active Directory	Windows 2000 Server proporciona un objeto de impresora estándar para Active Directory Utilizando este objeto, las organizaciones pueden publicar impresoras en Active Directory para que sean compartidas a través de la red	Esto proporciona a los usuarios una forma fácil de buscar impresoras a través de la red Los usuarios pueden encontrar atributos basados en impresora como capacidades (PostScript, color, papel tamaño oficio, etc.) y la ubicacion almacenada en Active Directory
Protocolo de impresión de Internet (IPP)	IPP es el estándar de Internet más reciente que permite que los usuarios impriman directamente a una URL, visualicen el estado de la impresora utilizando un explorador, e instalen controladores de una URL	Los usuarios podrán imprimir fácilmente documentos a través de intranet e Internet Por ejemplo, un usuario puede imprimir un documento a color en www colorprinter kinkos com/
Impresión de alta disponibilidad	Las organizaciones pueden aprovechar los servicios de *cluster* en Windows 2000 Advanced Server & DataCenter Server para desarrollar servidores de impresión altamente disponibles	Esto proporciona a los usuarios el nivel más alto de disponibilidad de servidor de impresión
Interfaz mejorada y simplificada	Utilizando el nuevo soporte *Plug and Play*, el asistente mejorado de impresión adicional y las especificaciones simplificadas de dispositivo, los usuarios pueden configurar una impresora con Windows 2000 Server en forma mucho mas fácil que antes	Estas funciones hacen que la instalacion y configuración de impresoras para la estación de trabajo y el servidor sean directas, por ejemplo, ya no es necesario que los usuarios sepan sobre modelos de controlador, lenguajes de impresora o puertos

Funciones de publicación Web

Nueva función	Descripción	Beneficio
ADMINISTRACION MEJORADA		
Configuración y actualización integradas	Internet Information Server se instala como un servicio de operación en red de Windows 2000 Server Los clientes con cualquier versión existente de Windows NT Server 3.51 o 4 0 se actualizarán automaticamente a los nuevos servicios Web en Windows 2000 Server. Además, si los clientes están actualizando Windows 9x o Windows NT Workstation con PWS, también se actualizarán Así mismo, los usuarios de Windows 9x y PWS se actualizarán durante la actualizacion de Windows 9x a Windows 2000 Professional	Facilita a los clientes aprovechar las nuevas funciones y servicios de Windows 2000 Server e IIS

Nueva función	Descripción	Beneficio
Contabilidad de procesos	Proporciona información sobre como los sitios Web utilizan los recursos de la CPU en el servidor La Contabilidad de procesos se habilita y personaliza por sitio	Los administradores de sistemas y desarrolladores de aplicaciones pueden utilizar esta función para determinar el uso de la CPU Los Proveedores de servicios de Internet (ISPs) pueden utilizar esta información para determinar que sitios están utilizando en forma desproporcionadamente alta de los recursos de la CPU o que puedan tener *scripts* o procesos CGI que funcionen mal Los administradores de informática pueden utilizar esta información para cobrar los costos de alojar un sitio Web y/o aplicación a la división adecuada dentro de una compañía
Regulación de CPU	Al aprovechar el Objeto de trabajo en Windows 2000 Server, los administradores pueden limitar la cantidad de tiempo de procesamiento de la CPU que una aplicación o sitio Web tiene permitido utilizar durante un tiempo predefinido	Las organizaciones que ejecutan múltiples sitios Web en una computadora o que ejecutan otras aplicaciones en la misma computadora como su servidor Web, pueden limitar la cantidad de tiempo que las aplicaciones fuera de proceso de un sitio Web tienen para utilizar el procesador Esto asegura que el tiempo de procesador este disponible para otros sitios Web o aplicaciones no Web
Dominios de usuarios multiples	Cuando se centralizan múltiples sitios Web en Windows 2000 Server, los administradores pueden proporcionar un espacio de nombre único para cada sitio	Esto proporciona a los profesionales de informática la capacidad de alojar multiples sitios Web en un solo servidor al tiempo que ofrecen dominios separados de usuarios para cada sitio Cada dominio de usuarios puede ser administrado en forma segura por el administrador de sitio asignado
Asistente de certificación	La seguridad SSL es un requerimiento cada vez más común para los sitios Web que proporcionan comercio electrónico y acceso a información comercial sensible El nuevo Asistente SSL facilita la configuración de sitios Web habilitados con SSL en Windows 2000 Server	Al utilizar el Asistente de certificación, los administradores pueden configurar y mantener fácilmente la encriptación SSL y la autenticación de certificado de cliente en un sitio Web basado en Windows 2000 Server
Asistente de permiso	El Asistente de permiso guía a los administradores a través de las tareas de configurar permisos y acceso autenticado en un sitio Web IIS	Esto facilita significativamente la configuración y administración de sitos Web que requieren acceso autenticado a su contenido

Nueva función	Descripción	Beneficio
Bloc de tareas MMC	IIS aprovecha totalmente las capacidades del bloc de tareas en Microsoft Management Console Los administradores se encuentran con una lista de tareas que pueden realizarse en cada nodo u objeto bajo el *snap-in* IIS Por ejemplo, si un usuario tiene un servidor seleccionado bajo el *snap-in de* MMC IIS, el bloc de tareas mostrará en pantalla asistentes para crear nuevos sitios Web y FTP.	Esto facilita increiblemente la administración de un servidor IIS Los administradores simplemente seleccionan la tarea que desean realizar y un asistente los guia a traves de los pasos
Scripts mejorados de administración de lineas de comandos	IIS incluye *scripts* adicionales que pueden ejecutarse desde la linea de comandos para automatizar las tareas de administracion comunes del servidor Web	Desde la linea de comandos, los administradores pueden crear *scripts* personalizados que automatizan la administracion de IIS.
SOPORTE PARA LOS ESTANDARES DE LA INDUSTRIA MAS RECIENTES		
Soporte para WebDAV	Autoría y Versiones distribuidas (DAV) es una extension del estándar HTTP 1.1 para exponer un medio jerarquico de almacenamiento de archivos, como un sistema de archivos, a través de una conexión HTTP	Al utilizar DAV, los autores remotos pueden accesar facilmente recursos en el sistema de archivos a través de HTTP Con la implementacion IIS de DAV, los usuarios pueden permitir a los autores remotos, editar, buscar o eliminar archivos y directorios en el servidor
Carpetas Web	El soporte para las Carpetas Web permite que los usuarios naveguen a un servidor que cumple con la Autoría y Versiones distribuidas (DAV) y vean el contenido (si cuentan con los permisos adecuados) como si fuera parte del mismo espacio de nombre que el del sistema local. Los usuarios pueden arrastrar y cortar archivos, recuperar/modificar información de propiedad de archivos y llevar a cabo otras tareas relacionadas con el sistema de archivos	El soporte para las Carpetas Web permite que los usuarios mantengan una apariencia y experiencia consistente mientras navegan entre el sistema local de archivos, una unidad conectada a red y un sitio Web de Internet. Por ejemplo, hace posible llevar a cabo el equivalente de un comando DIR en un recurso HTTP y recuperar toda la información necesaria para llenar una vista de Microsoft Windows Explorer
Autenticacion de compendio	La autenticación de compendio ofrece las mismas funciones que la autenticación básica, pero implica una forma diferente de transmitir las credenciales de autenticación La autenticación básica envia contraseñas a través de Internet en la forma de texto simple El compendio soluciona esto al confundir la contraseña en el cable	Los usuarios con exploradores que soportan la Autenticación de compendio se autentican así mismos en un servidor IIS sin comprometer sus credenciales de conexión

Nueva función	Descripción	Beneficio
Compresion HTTP	Es la integracion del protocolo de compresión HTTP estandar en la industria La Compresion HTTP comprime y almacena en la memoria caché los archivos estáticos y opcionalmente realiza compresión a solicitud de archivos generados dinámicamente	Proporciona transmision mas rapida de paginas entre el servidor Web y los clientes habilitados con compresión Esto es útil en escenarios donde el ancho de banda es limitado, pero existen recursos disponibles en el servidor para realizar la compresion Las versiones 4 y 5 de Internet Explorer soportan los métodos de compresión utilizados en Windows 2000 Server
Reinicio FTP	Si un usuario es interrumpido mientras descarga un archivo grande desde un sitio FTP, la proxima vez que descargue el archivo, iniciará desde donde el usuario lo dejó	Esto proporciona un enfoque mucho mas fácil y menos tardado a los usuarios que descargan información desde Internet.
SITIOS WEB DINAMICOS MAS FACILES DE CREAR *(Nota: En la sección Servicios de aplicaciones es posible encontrar mayor información sobre las aplicaciones Web)*		
Mejoras de rendimiento	ASP sin *Scripts*— Los archivos ASP que no contienen *scripts* del lado del servidor se procesan como si fueran paginas HTML estaticas Control de flujo — En lugar de redireccionar solicitudes que requieren un viaje redondo al cliente y que impactan el rendimiento, los desarrolladores Web pueden transferir solicitudes directamente a un archivo asp, sin abandonar nunca el servidor Objetos mejorados de rendimiento — IIS proporciona versiones actualizadas con rendimiento mejorado de componentes instalables populares. Auto ajuste — IIS ahora detecta cuando las solicitudes de ejecucion son bloqueadas por recursos externos y automáticamente proporciona mas hilos para ejecutar simultáneamente solicitudes adicionales y continuar así el procesamiento normal.	El rendimiento es importante para crear e instalar soluciones empresariales rentables en la red Las mejoras continuas de rendimiento en IIS proporciona a las organizaciones una solucion mas rentable para crear e instalar aplicaciones empresariales en Web
Manejo de errores	Los desarrolladores pueden redireccionar errores a una pagina ASP que muestra en pantalla información útil, como la descripcion de un error o el numero de linea en un archivo asp donde ocurrio el error	Al utilizar las capacidades de manejo de errores, los desarrolladores pueden invertir menos tiempo en escribir procedimientos usuales de manejo de errores y mas tiempo en enfocarse en la lógica comercial de sus aplicaciones

Nueva función	Descripción	Beneficio
Scriptlets de servidor	Al utilizar *Scriptlets* de servidor, los desarrolladores pueden encapsular *scripts* comunes, como aquellos utilizados para el acceso a base de datos o generacion de contenido, convirtiéndolos en componente reutilizables accesibles desde cualquier archivo asp o programa Los *Scriptlets* pueden tambien incorporarse en programas escritos en lenguajes de programacion que cumplen con COM, como Microsoft VBScript o Microsoft Visual J++	Al utilizar *scriptlets*, los desarrolladores pueden aprovechar lenguajes de *scripts* faciles de utilizar para convertir sus procedimientos de *scripts* lógicos empresariales en componentes COM reutilizables que pueden usarse en aplicaciones Web, así como en otros programas que cumplen con COM

Funciones de los servicios de medios de Windows

Nueva función	Descripción	Beneficio
SERVICIO DE SERVIDOR		
Distribución a traves del protocolo HTTP	Sirve un flujo *unicast* a través de HTTP hacia otro Windows 2000 Server y servidor basado en medios	Facilita la entrega de flujos a traves de *firewalls* sin abrir un puerto especifico en el *firewall*.
Autenticación de distribución *proxy*	Si un usuario se encuentra a un reto *proxy*, el servidor le ofrecera la oportunidad de introducir su ID y contraseña	Seguridad de *firewall*
Reducción, cambio de flujo	Entrega el flujo con base en el audio y regula el video con base en velocidades de conexion de cliente a 28.8 Kbps y 56 Kbps	Calidad de flujo mejorada a través de la conexión de cliente
Reenvío UDP	Si faltan paquetes UDP, el servidor reenvía los paquetes perdidos.	Mejor calidad de medio al utilizar el protocolo UDP
Limitación de conexiones de cliente por punto de publicacion	Limita el número de clientes que estan conectados a un punto de publicación.	Mejor administración en servidores centralizados a fin de maximizar clientes para un punto de publicación especifico, magnifico para escenarios de facturación
Limitación de ancho de banda total por punto de publicacion	Limita el ancho de banda por punto de publicación.	Mejor administración en servidores centralizados a fin de maximizar clientes para un punto de publicación especifico
Salida para formato de archivo W3C	La salida registra eventos con base en la informacion estadistica de cliente.	Las herramientas estandar de análisis pueden leer fácilmente información de monitoreo.
Reporte y análisis de uso basados en analista	Integración con Site Server para hacer reportes con las bitacoras de Medios de Windows	Mejora la integración con Site Server para reportar el uso

Nueva función	Descripción	Beneficio
Modelo de autorizacion conectable	Los clientes pueden autorizar la reproduccion de contenido de flujo especifico con aplicaciones personalizadas. (Abrir API en SDK)	Habilita cualquier aplicacion habilitada de comercio para trabajar con los flujos de Medios Windows
Modelo de notificación conectable	Cada vez que un cliente reproduce, pone pausa, se detiene y demás, el servidor puede indicar lo que el cliente esta haciendo con el contenido. (Abrir API en SDK)	Esto es magnífico para las compañías que centralizan el contenido y que desean saber el tiempo que un cliente permanece conectado y tambien es optimo para facturacion
Ejemplos de autorización de servidor comercial y notificación de eventos	Ejemplos de autorización pre-desarrollados para que los clientes los utilicen	Es mas facil para los clientes familiarizarse con el uso de la autorización
Modelo de autenticación conectable	Utilice su propia base de datos de autenticación personalizada. (Abrir API en SDK).	Puede utilizar los Servicios de medios Windows con su base de datos de autenticacion existente
Seguridad por punto de publicación	Restringe el acceso a grupos de archivos o eventos en tiempo real a traves de la seguridad en los puntos de publicación	Es uno de los nuevos niveles de seguridad que hace posible proporcionar mayor información sensible al contenido para individuos específicos
NTLM utilizando autenticación BASIC	Los administradores pueden restringir el acceso con base en la ID y contraseña del usuario	Mayor seguridad en el servidor para conceder o negar el acceso a contenido
Membresía utilizando autenticación BASIC	Los administradores pueden restringir el acceso con base en la ID y contraseña del usuario	Mayor seguridad en el servidor para conceder o negar el acceso a contenido
Distribución a traves del protocolo HTTP	Sirve a una estacion a través del protocolo HTTP hacia otros Servidor de medios de Windows 2000 Server	Facilita la entrega de flujos a traves de *firewall* sin abrir un puerto específico en el *firewall*.
Autenticación de distribución *proxy*	Si se enfrenta a un reto *proxy* el servidor ofrecera la ID y contraseña de usuario. Solicitará autenticación *proxy* entre Servidores de medios	Proporciona mejor seguridad entre Servidores de medios
Recolección *multicast* sin conexión	Cuando recibe un *multicast*, el cliente utilizara el protocolo HTTP para registrar información estadística de cliente en un servidor Web HTTP	Mejor acceso a la información de cliente en una recolección *multicast* sin conexión
Tres asistentes con funciones completas	El asistente Bajo solicitud para contenido almacenado El asistente de *Unicast* en tiempo real para contenido en tiempo real. El asistente para *Multicast* para transmisiones *multicast*	Simplifica la configuración para crear escenarios complejos

Del Sistema de archivos y almacenamiento

Nueva función	Descripción	Beneficio

Nueva función	Descripción	Beneficio
MEJORAS AL SISTEMA DE ARCHIVOS		
Mejoras NTFS	Windows 2000 Server incluye una version mejorada del sistema de archivos NTFS que ofrece soporte para encriptacion de archivos, la capacidad de agregar espacio en disco a un volumen NTFS sin volver a arrancar, monitoreo de vinculos distribuidos y cuotas de disco por usuario para monitorear y limitar el uso de espacio en disco (descrito posteriormente con mayor detalle), asi como muchas otras mejoras de rendimiento.	Los descriptores de seguridad pueden almacenarse una vez pero tener referencias en varios archivos, lo que ahorra espacio en disco El soporte nativo para propiedades como flujos NTFS permite consultas mas rápidas Descomprimir y volver a comprimir datos de archivo cuando se transmiten a traves de una red puede evitarse, reduciendo la sobrecarga de la CPU en el servidor.
Sistema de encriptación de archivos	La Encriptación del sistema de archivos de Windows 2000 Server (NTFS) proporciona protección para datos importantes. Puede habilitarse por archivo o por directorio La tecnología de encriptación utilizada se basa en claves públicas y se ejecuta como un servicio de sistema integrado lo que hace que sea facil de administrar, difícil de atacar y transparente para el usuario	En la versión anterior de Windows 2000 Server alguien con acceso físico a un sistema podia evitar las funciones de seguridad integradas del sistema operativo utilizando una herramienta para leer las estructuras en disco del sistema de archivos (NTFS) de Windows 2000 Server
Monitoreo de vínculos distribuidos	Windows 2000 Server proporciona un Servicio de monitoreo de vínculos distribuido que habilita las aplicaciones de cliente a fin de monitorear las fuentes de vínculos que han sido movidas	El Monitoreo de vínculos distribuidos ayuda a resolver accesos rapidos y vínculos OLE a archivos residentes en NTFS que han sufrido un cambio de nombre y/o ruta
Cuotas de disco	Windows 2000 Server y Windows 2000 Professional soportan cuotas de disco destinadas a volúmenes formateados para la versión NTFS (volúmenes NTFS) Puede utilizar las cuotas de disco para monitorear y limitar el uso del espacio en disco	Para cada objeto en un disco, puede establecer una cuota así como políticas y definir acciones que se ejecutarán cuando se exceda cierto nivel de tolerancia
Archivos dispersos	El soporte a archivos dispersos permite que una aplicación cree archivos enormes sin comprometer realmente espacio en disco para cada byte.	Al utilizar archivos dispersos, NTFS sólo asignará espacio en disco físico a las partes del archivo escritas Algunas aplicaciones interesantes incluyen matrices dispersas y colas de espera circulares
MEJORAS DE ALMACENAMIENTO		
Servicio de almacenamiento remoto (RSS)	Los Servicios de almacenamiento remoto (RSS) monitorean automaticamente la cantidad de espacio disponible en el disco duro local Cuando el espacio libre en su disco duro principal disminuye abajo del nivel necesario, RSS automáticamente elimina datos locales que han sido copiados al almacenamiento remoto, proporcionando el espacio en disco libre necesario	Ya que los discos ópticos y cintas eliminables son menos costosas por megabyte (MB) que los discos duros, esto puede ser una forma economica de proporcionar almacenamiento máximo y rendimiento local optimo

Nueva función	Descripción	Beneficio
Administrador de almacenamiento eliminable (RSM)	RSM presenta una interfaz comun a cambiadores robóticos y bibliotecas de medios, habilita múltiples aplicaciones para compartir bibliotecas locales y unidades de cinta o disco, y controla medios eliminables dentro de un solo sistema de un solo servidor.	La Administración de disco ha sido mejorada en Windows 2000 Server al permitir que los administradores lleven a cabo tareas en linea sin apagar el sistema o apagar o interrumpir a los usuarios
Nueva utilidad de respaldo	Seagate Software está proporcionando la actualización de Respaldos de Windows 2000 Server que ahora esta centrada en los medios en lugar de en las cintas e incluye una nueva interfaz de usuario con asistentes de respaldo y restablecimiento, hojas de propiedad y acceso a Entorno de red	La Utilidad de respaldo de Windows 2000 Server ayuda a proteger datos contra perdida accidental debido a fallas en los medios de hardware o almacenamiento Esta versión permite que los usuarios respalden datos para una gran variedad de medios de almacenamiento, como unidades de cinta, unidades externas de disco duro, discos Zip, CD-ROMs de grabación y unidades lógicas
Utilidad de defragmentación de disco	Windows 2000 Server y Windows 2000 Professional soportan la capacidad de defragmentar volúmenes de disco, que están formateados como FAT, FAT32 y NTFS	Segura y compatible con todos los tipos de disco, esta nueva utilidad de defragmentación opera mientras el sistema está encendido y funcionando, y los discos están en uso activo
SISTEMA DE ARCHIVOS DISTRIBUIDOS		
Sistema de archivos distribuidos (Dfs)	El Sistema de archivos distribuidos (Dfs) de Microsoft implementa un solo espacio de nombre para recursos desiguales de sistema de archivos en un sitio Un Dfs está organizado como una estructura jerarquica de volumenes lógicos, independiente de la ubicación fisica del recurso	El Sistema de archivos distribuidos (Dfs) de Microsoft para Windows 2000 Server es un componente de servidor de red que facilita a los usuarios encontrar y administrar datos en la red Dfs facilita la creación de un solo arbol de directorio que incluya multiples servidores de archivos y archivos compartidos en un grupo, division o empresa

FUNCIONES DE OPERACION EN RED Y SERVIDOR DE COMUNICACIONES

Impulsadas por Internet, las comunicaciones basadas en red se han convertido en la espina dorsal del comercio, asociaciones e información compartida. Las comunicaciones permiten nuevas oportunidades a los negocios para unirse globalmente y expandir sus mercados. A fin de adaptarse a las condiciones rápidamente cambiantes, la compañía siempre debe estar conectada a nivel interno y con sus socios comerciales.

Nueva función	Descripción	Beneficio

Nueva función	Descripción	Beneficio
WINDOWS 2000 PROFESSIONAL Y WINDOWS 2000 SERVER		
Mejoras TCP/IP	TCP/IP de Microsoft ha sido actualizado para Windows 2000 Server a fin de incluir numerosas mejoras de rendimiento para operación en red dentro de ambientes LAN y WAN de alto ancho de banda	El soporte a ventanas grandes mejora el rendimiento de TCP/IP cuando existen grandes cantidades de datos "en proceso" o desconocidas entre dos *hosts* conectados durante un periodo prolongado
Seguridad IP (IPSec)	El protocolo de Seguridad IP es un estandar propuesto por IETF para encriptar el tráfico IP Windows 2000 Server integra muy bien IPSec con la administración de políticas del sistema a fin de reforzar la encriptación entre sistemas, en forma transparente para el usuario final IPSec puede utilizarse para comunicaciones privadas y de Red privada virtual. Para los protocolos de túnel o que no sean IP o para asignación dinámica de direcciones IP en VPNs, debe utilizarse L2TP o PPTP	Los clientes pueden tener comunicaciones seguras con encriptación y administradas por politica de grupo que salvaguarden la información que se envia a través de las redes Ya que IPSec está integrada en el sistema operativo, es mas facil de configurar y administrar que las soluciones agregadas Asi mismo, todo el tráfico puede encriptarse, en lugar de solo el tráfico entre dispositivos de red como enrutadores y cajas de encriptacion
Protocolo de tunel de nivel 2 (L2TP)	El Protocolo de túnel de nivel 2 es una especificación de borrador IETF para encapsular y transmitir tráfico que no es IP a través de redes TCP/IP Utiliza IPSec para encriptación opcional y asignación dinamica de direcciones IP destinadas a la administracion simplificada de VPNs	Los clientes tienen la opcion de utilizar este estandar reciente para soportar protocolos IP asi como a protocolos que no son IP (como IPX o AppleTalk) a través de conexiones de Red privada virtual basadas en IPSec
Protocolo de tunel de punto a punto (PPTP)	El Protocolo de túnel de punto a punto es un protocolo definido de multiples proveedores que ha sido ampliamente adoptado para utilizarse en la creacion de soluciones de operación en Red privada virtual Como L2TP, PPTP ofrece servicios de túnel para soportar protocolos que no sean TCP/IP PPTP utiliza MPPE para servicios de encriptación y es compatible con el soporte VPN previo disponible para versiones anteriores de Windows PPTP es una buena alternativa para IPSec y L2TP destinados a organizaciones que no desean instalar y administrar una infraestructura de claves públicas para VPNs	Los clientes tienen la opcion de utilizar una VPN simple compartida basada en confidencialidad para evitar los gastos asociados con mantener infraestructuras de claves públicas. Esto también protege las inversiones existentes en PPTP como una solucion VPN PPTP proporciona encriptación eficiente de software y es una opcion VPN adecuada para procesadores Pentium 486 y anteriores
H 323	H.323 es un estandar ITU para realizar llamadas de multimedia a través de redes IP Este protocolo es soportado como parte del sistema operativo de Windows 2000 Server y es accesible a traves de APIs estandar telefónicas	Las aplicaciones Windows que utilizan H.323 interoperaran con otras aplicaciones y servicios basados en H 323 en otras plataformas

Nueva función	Descripción	Beneficio
TCP/IP mejorado	El Protocolo de control de transmisión/Protocolo de Internet es la serie de protocolos estandar de Internet Engineering Task Force (IETF) para transportar trafico a traves de Internet La implementacion TCP/IP de Microsoft cumple los requerimientos para *hosts* de Internet (RFC 1122 y RFC 1123). que es la especificacion que enumera los requerimientos para implementaciones de sistemas de *hosts* de la serie de protocolos de Internet El TCP/IP de Windows 2000 Server incluye soporte para redes de alta velocidad (RFC 1323) y soporte para Confirmaciones selectivas (SACK) a fin de lograr un mejor rendimiento en redes con pérdidas como ISP y redes inalambricas	El soporte TCP/IP basado en estandares significa que Windows 2000 Server se conecta facilmente a Internet e interopera con la variedad más amplia posible de soluciones de operacion en red de terceros
IPX/SPX	El Intercambio de paquetes de Internet/Intercambio de paquetes en secuencia son los protocolos heredados y de propietario que se utilizan con NetWare de Novell	El soporte IPX conserva la inversión en redes NetWare heredadas al facilitar la integración de ambientes NetWare con Windows 2000 Server
AppleTalk	AppleTalk es el protocolo de propietario heredado que se utiliza para comunicaciones a Apple Macintosh anteriores Apple ha establecido desde entonces TCP/IP como el protocolo de red preferido para los sistemas Macintosh y soporta los archivos compartidos a través del Protocolo de archivos Apple a traves de TCP/IP Con Windows 2000 Server. los clientes ahora tienen la opción de mantener el uso de AppleTalk o reemplazarlo con el Protocolo de archivos Apple a traves de TCP/IP	El Soporte de AppleTalk protege la inversión en sistemas Macintosh anteriores al brindar la opción de dar soporte a computadoras Macintosh mas antiguas sin cambiar el cliente Los sistemas Macintosh mas recientes pueden utilizar TCP/IP para reducir la complejidad de administrar múltiples protocolos de red a fin de soportar clientes Macintosh
Protocolo de punto a punto (PPP)	El Protocolo de punto a punto es un estandar IETF para conexiones de multiprotocolos de marcación El protocolo soporta la asignación dinamica de direcciones IP para sistemas remotos	PPP permite que los sistemas basados en Windows 2000 Server se conecten directamente a Internet o a otros servicios de marcacion con modems sin tener que agregar otro software
SEGURIDAD, ENCRIPTACION Y AUTENTICACION DE PLATAFORMAS DE OPERACIÓN EN RED		

Nueva función	Descripción	Beneficio
CHAP, MS-CHAP, PAP	El Protocolo de prueba de autenticación de intercambio de señales es un estándar IETF comúnmente utilizado para la autenticación de usuarios a traves de conexiones de Protocolo de punto a punto (PPP) El CHAP de Microsoft es una variación del CHAP utilizado para autenticar usuarios con base en el Módulo de acceso de seguridad de (SAM) de Windows 2000 Server e incluye soporte para el cambio de contraseñas MS-CHAP proporciona encriptacion transparente y automática e intercambio de claves. El Protocolo de autenticación de contraseñas proporciona autenticación de contraseñas de texto claro El protocolo es soportado para integridad, pero debido a inquietudes de seguridad, no se recomienda su uso.	Sus sistemas trabajan fuera de caja con los protocolos de autenticación utilizados con mayor frecuencia por ISPs
Protocolo de autenticacion ampliable (EAP)	EAP proporciona ampliación de los métodos de autenticación utilizados para PPP A través del uso de las APIs EAP, los Proveedor independiente de software s pueden suministrar nuevos módulos de autenticación de cliente y servidor para tarjetas token, tarjetas inteligentes, hardware biométrico, sistemas de contraseñas únicas, etc	Permite que servicios de autenticacion mas firmes se agreguen a las conexiones de marcación y VPN a fin de aumentar la seguridad de conexión
Soporte de tarjeta inteligente (EAP-TLS)	El módulo EAP integrado soporta la autenticación de certificados de claves públicas basados en tarjeta inteligente para conexiones de marcación y VPN Funciona con cualquier tarjeta inteligente certificada de Windows	Funciona fuera de caja con la mayoría de las tarjetas inteligentes para simplificar la integración de servicios de autenticación más firmes
Servicios de encriptación RC4	Soporte integrado para encriptacion RC4 de 40 y 128 bits para conexiones de marcación y VPN utilizando la Encriptación de punto a punto de Microsoft La generacion y regeneración iniciales de claves se manejan sin la intervención del usuario	Brinda a los clientes una opcion para encriptación firme comprobada sin los gastos y esfuerzo de una infraestructura de claves públicas
Cliente RADIUS — RFC 2138	Ahora, una PC de servidor que ejecuta Windows 2000 Server puede actuar como un cliente RADIUS para un servidor RADIUS, proporcionando opciones ampliadas de autenticación RADIUS (Servicio de usuario de marcacion de autenticacion remota) es un protocolo de autenticación de marcación y responsabilidad normalmente utilizado por los proveedores del servicio de Internet	Proporciona una opcion para que Windows autentique usuarios basandose en una base de datos de usuarios externa

Nueva función	Descripción	Beneficio
Servidor RADIUS	Servidor de autenticacion de Internet, es un servidor RADIUS de funciones completas Soporta la autenticacion y responsabilidad RADIUS Almacena la información en Active Directory, o en una base de datos local para el servidor IAS Ofrece una interfaz gráfica intuitiva para la mayoria de los atributos comúnmente necesarios, más una opción de entrada totalmente ampliable para todos los atributos especificos al proveedor Utiliza los mecanismos de Acceso del usuario basados en politicas (politicas y perfiles)	Permite que las cuentas de usuarios se conserven centralmente dentro de Active Directory al tiempo que permite que los sistemas no basados en Windows 2000 Server autentiquen con base en Windows 2000 Server
Filtracion de paquetes IP	El servicio de enrutamiento soporta una variedad de funciones de filtración de paquetes de entrada y salida Estas funciones de filtracion de paquetes proporcionan una medida importante de seguridad de red Las opciones de filtracion incluyen lo siguiente, puerto TCP, puerto UDP, ID de protocolo IP, tipo ICMP, código ICMP dirección fuente y dirección destino	Proporciona un metodo a nivel basico para bloquear ciertos tipos de trafico y evitar que entren a una red a fin de aumentar la seguridad
Filtracion de paquetes IPX	El servicio de enrutamiento soporta un nivel similar de filtración de paquetes para paquetes IPX A continuacion, se encuentra una lista de opciones de filtración de paquetes IPX direccion fuente, nodo fuente, *socket* fuente, dirección destino, nodo destino, *socket* de destino y tipo de paquete	Proporciona un metodo a nivel básico para evitar tráfico NetWare en partes de una red.
ADMINISTRACION DE DENOMINACION Y DIRECCIONES DE PLATAFORMAS DE OPERACION EN RED		
DNS Dinamico	DNS Dinamico es un estandar IETF para registros de actualización dinámica en servidores de Sistema de nombres de dominio para reflejar cambios o adiciones en correlaciones de direccion a nombre Windows 2000 Server incluye una implementación de servidor de DNS Dinámico que se integra con DHCP y Active Directory Asi mismo, proporciona soporte de DNS Dinámico para implementaciones que no sean de Windows 2000 Server	DNS Dinámico reduce los costos de administracion de red al disminuir la necesidad de editar y duplicar manualmente la base de datos DNS cada vez que ocurre un cambio en la configuracion de un cliente DNS La integracion de Active Directory elimina el requerimiento de mantener una infraestructura de duplicación separada sólo para DNS El soporte para los protocolos de actualización DNS de IETF permite la interoperabilidad con ambientes DNS existentes e implementaciones de DNS Dinamico de terceros.

Nueva función	Descripción	Beneficio
DHCP con soporte de DNS Dinámico	El Protocolo dinámico de configuración de *Host* (DHCP) proporciona costos menores de propiedad para las redes IP porque asigna dinámicamente direcciones IP a PC's u otros recursos conectados a una red IP El servidor DHCP de Windows 2000 Server se integra con DNS Dinámico y Active Directory para simplificar la administración de direcciones y reflejar dinámicamente las asignaciones de direcciones	Esta es una mejora dramática en el ahorro de tiempo y dinero en comparación con la asignación manual de direcciones IP utilizables
Servicio de localizador de informacion (ILS)	ILS proporciona un registro dinámico para los servicios especificos de aplicaciones El marcador de Windows 2000 Server utiliza ILS para programar y localizar llamadas en conferencia basadas en red	Permite a los usuarios de las aplicaciones encontrar y conectarse a servicios dinámicos cuando mas de una direccion IP es necesaria para la conexion
WINS	El Servicio de nombres de Internet de Windows proporciona una resolución de nombre para dirección destinada a las solicitudes de cliente NetBIOS	Proporciona una forma *Plug and Play* para clientes basados en Windows a fin de encontrar servicios basados en Windows en una red enrutada Conserva la inversión en clientes Windows existentes. Así mismo, brinda administración escalable de espacios de nombres NetBIOS
CALIDAD DE SERVICIO DE PLATAFORMAS DE OPERACION EN RED		
Calidad de servicio diferenciada (diff-serve)	Habilita aplicaciones de misión crítica (como SAP o correo electronico) y aplicaciones de multimedia a fin de obtener la calidad de servicio necesaria de la red. También permite que los administradores de red manejen el impacto de estas aplicaciones en los recursos de red Interopera con RSVP.	Permite que las clases especificadas de aplicaciones obtengan un mejor servicio a traves de las conexiones de red y de las partes diff-serve de las redes corporativas internas
Servicio de control de admisión	Los administradores pueden controlar la cantidad de ancho de banda que las aplicaciones pueden reservar con base en la política configurada en Active Directory	Las redes que instalan ACS pueden evitar el exceso de funcionamiento de la red a través del video de alto ancho de banda de larga ejecución. Los recursos de la red pueden asignarse a aplicaciones de alto valor como telefonía IP
LANs 802 1p de IEEE clasificadas por prioridad	Permite la clasificación por Prioridad del tráfico LAN Windows 2000 Server ha integrado el soporte QoS que permite que el tráfico de red que atraviesa por LANs 802 1p obtenga servicios clasificados por prioridad Este soporte esta integrado con el Servicio de control de admisión, RSVP y Servicios diferenciados	Permite un mejor servicio de red para aplicaciones que no pueden tolerar la pérdida o demora de paquetes, como las aplicaciones de audio y las que son de misión crítica
RSVP	Habilita aplicaciones (básicamente de multimedia) para obtener la calidad de servicio necesaria de la red También permite que los administradores de red manejen el impacto de estas aplicaciones en los recursos de red Interopera con diff-serv.	Mejora el rendimiento de las aplicaciones de latencia y sensibles al ancho de banda en redes locales (por ejemplo, aplicaciones de flujo continuo de multimedia como el audio o video a través de la red)

FUNCIONES DEL SERVIDOR DE APLICACIONES

Procesadores más rápidos, *buses* más amplios y veloces, así como modelos de memoria muy grandes se combinarán para ampliar significativamente la variedad de problemas que pueden ser solucionados por las aplicaciones de Windows 2000 Server. Durante los próximos 18 meses, podemos esperar que el rendimiento computacional masivo y el ancho de banda I/O observado de máquinas de imágenes de un solo sistema aumenten significativamente, tal vez hasta cinco veces.

Nueva función	Descripción	Beneficio
RENDIMIENTO MEJORADO Y CAPACIDAD DE ESCALACION PARA APLICACIONES		
Arquitectura de memoria empresarial	Las memorias físicas mayores a 4GB en plataformas Alpha de Compaq e Intel (IA-32) Dependiendo de la plataforma, es posible soportar tamaños de memoria principal física de hasta 64 GB	Utilizar el direccionamiento de 64 bits de procesadores permite que las aplicaciones que realizan procesamiento de transacciones o apoyan decisiones en grandes conjuntos de datos mantengan mas datos en la memoria para rendimiento altamente mejorado
Capacidad de escalación SMP mejorada	Microsoft ha enfocado sus esfuerzos de desarrollo, prueba y ajuste para la capacidad de escalacion SMP en Windows 2000 Advanced Server.	Windows 2000 Server ha sido optimizado para un numero cada vez mas grande de servidores SMP de ocho vías de precios competitivos basados en procesadores RISC aun más rápidos y Arquitectura Intel
Soporte I_2O	La arquitectura I_2O utiliza un procesador dedicado con su propia memoria para descargar procesamiento I/O de las CPU(s) principales Esto da como resultado un rendimiento mayor y utilizacion menor de la CPU	I_2O evita que el *host* se encargue de tareas I/O que interrumpen significativamente mejorando en gran medida el rendimiento I/O en aplicaciones de alto ancho de banda como el video conectado en red, *groupware* y procesamiento de cliente/servidor
I/O de Distribucion/Recoleccion	I/O de Distribucion/Recoleccion es un tipo especial de I/O de alto rendimiento disponible a través de las funciones ReadFileScatter y WriteFileScatter Win32	Permite rendimiento I/O mas alto cuando los datos de aplicación se localizan en ubicaciones de memoria no contiguas, y los datos necesitan escribirse para una ubicación contigua de archivo

Nueva función	Descripción	Función
Clasificación de alto rendimiento	Optimiza el rendimiento de la clasificacion comercial de grandes grupos de datos	Esta clasificacion normalmente se utilizara a fin de preparar datos para su carga en aplicaciones *data-warehouse* y *data-mart* y para preparar operaciones grandes de lote y de impresion sensible a la clasificación
Equilibrio de cargas de red	El Equilibrio de cargas de red equilibra y distribuye las conexiones de cliente (conexiones TCP/IP) a través de servidores múltiples que escalan el rendimiento de los servicios TCP/IP, como servidores Web, *Proxy* o FTP, así como aseguran su alta disponibilidad	A medida que los servicios de Internet se han vuelto esenciales para llevar a cabo las operaciones diarias en todo el mundo, necesitan poder manejar un gran volumen de solicitudes de cliente sin crear demoras contraproducentes Al escalar el rendimiento utilizando el Equilibrio de cargas de red, puede agregar hasta 32 servidores Windows 2000 a su *cluster* para afrontar la demanda que se coloca en estos servicios
MAYOR CONFIABILIDAD Y DISPONIBILIDAD PARA APLICACIONES		
Objeto de trabajo	Windows 2000 Server continúa una extensión para el modelo de proceso llamado un trabajo. Los objetos de trabajo pueden nombrarse, compartirse y son seguros, y controlan atributos de los procesos asociados con ellos La función básica de un objeto de trabajo es permitir que grupos de procesos sean administrados y manipulados como una unidad	A menudo, los ISPs alojan multiples sitios Web no relacionados en un solo servidor y, por lo tanto, necesitan tener una forma de monitorear los recursos que un sitio dinámico utiliza Los ISPs podrían utilizar el objeto de trabajo para explicar el uso de la CPU de las aplicaciones Web y establecer límites a la cantidad de CPU que una aplicación Web puede utilizar

Nueva función	Descripción	Beneficio
Servicios de *clustering*	El *clustering* en Windows 2000 Advanced Server y DataCenter Server permite que dos servidores se conecten a un "*cluster*" para disponibilidad mas alta y mejor administracion de los recursos del servidor Los servicios de *clustering* monitorean la condición de las aplicaciones estandar y servidores, y pueden recuperar automaticamente datos y aplicaciones de misión crítica debido a muchos tipos comunes de fallas Las nuevas mejoras incluyen el soporte a Active Directory, el soporte para conexiones de red de marcacion con alta disponibilidad, servicios de sistema adicionales pendientes de *clusters* (DHCP, WINS, Dfs) y soporte de actualización de instalación	El soporte de *clustering* permite la entrega de niveles mayores de servicio a usuarios al tiempo que se logra un mayor control sobre la administracion de recursos de servidor críticos Los *clusters* de Windows 2000 Advanced Server y DataCenter Servers aprovechan las plataformas de PC estandar en la industria y la tecnologia de red existente hoy en dia El modelo de controlador de varios niveles de Windows 2000 Server permite que Microsoft agregue soporte rápidamente para tecnología de *clustering* de alto rendimiento de fines especiales (por ejemplo, interconexiones de baja latencia) a medida que los proveedores de hardware introducen al mercado soluciones de *clustering* especializadas
Menos rearranques del servidor	A fin de mejorar la configuracion y mantenimiento del hardware y software, muchas funciones que requerían un rearranque en Windows NT Server 4.0 ya no se necesitan en Windows 2000 Server, como la ampliación de un volumen de almacenamiento, configuracion de protocolos de red y reconfiguracion de especificaciones en PCI y otro hardware PnP	Menos rearranques para tareas de mantenimiento comunes significa que los usuarios pueden estar listos y trabajando por periodos más prolongados Windows 2000 Advanced Server y DataCenter Server también soportan ahora las actualizaciones de instalación que permiten que el mantenimiento planeado tome lugar con tiempo muerto e interrupciones mínimos para los usuarios

WINDOWS 2000 SERVER: DIRECTORIO ACTIVO

Introducción a Active Directory

Un directorio es una estructura jerárquica que almacena información acerca de los objetos existentes en la red. Un servicio de directorio, como Active Directory, proporciona métodos para almacenar los datos del directorio y ponerlos a disposición de los administradores y usuarios de la red. Por ejemplo, Active Directory almacena información acerca de las cuentas de usuario (nombres, contraseñas, números de teléfono, etc.) y permite que otros usuarios autorizados de la misma red tengan acceso a esa información.

Antes de examinar detalladamente Active Directory, debe familiarizarse con la siguiente información:

- Servicio de directorio
- Información general acerca de los dominios
- Introducción a los bosques y árboles de dominio
- Relaciones de confianza entre dominios
- Unidades organizativas
- Introducción a los sitios y servicios de Active Directory
- Grupos
- Introducción al esquema de Active Directory
- Funciones de servidor

Servicio de directorio

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

- Un almacén de datos, también conocido como directorio, que almacena información acerca de los objetos de Active Directory. Estos objetos incluyen normalmente recursos compartidos como servidores, archivos, impresoras y las cuentas de usuario y de equipo de red. Para obtener más información acerca del almacén de datos de Active Directory, consulte Almacén de datos del directorio.

- Un conjunto de reglas, el esquema, que define las clases de objetos y los atributos contenidos en el directorio, las restricciones y los límites en las instancias de estos objetos así como el formato de sus nombres. Para obtener más información acerca del esquema, consulte Introducción al esquema de Active Directory.

- Un catálogo global que contiene información acerca de cada uno de los objetos del directorio. Esto permite a los usuarios y administradores encontrar información del directorio con independencia de cuál sea el dominio del directorio que realmente contiene los datos. Para obtener más información acerca del catálogo global, consulte Catálogo global.

- Un sistema de índices y consultas, para que los usuarios o las aplicaciones de red puedan publicar y encontrar los objetos y sus propiedades. Para obtener más información acerca de cómo consultar el directorio, consulte Buscar información del directorio.

- Un servicio de replicación que distribuye los datos del directorio por toda la red. Todos los controladores de dominio de un dominio participan en la replicación y contienen una copia completa de toda la información del directorio de sus dominios. Cualquier cambio en los datos del directorio se replica en todos los controladores de dominio del dominio. Para obtener más información acerca de la replicación de Active Directory, consulte Metas y estrategias de la replicación.

- Integración con el subsistema de seguridad para asegurar el proceso de inicio de sesión en la red así como control de acceso tanto de las consultas de datos del directorio como de las modificaciones de los datos. Para obtener más información acerca de la seguridad de Active Directory, consulte Modelo de seguridad.

- Para sacarle el mayor provecho a Active Directory, el equipo que tiene acceso a Active Directory a través de la red debe ejecutar el software de cliente correcto. En equipos que no ejecutan el software de cliente de Active Directory, el directorio aparecerá igual que un directorio de Windows NT. Para obtener más información acerca del software de cliente, consulte Clientes de Active Directory.

Información general acerca de los dominios

Un dominio constituye un límite de seguridad. El directorio incluye uno o más dominios, cada uno de los cuales tiene sus propias directivas de seguridad y relaciones de confianza con otros dominios. Los dominios ofrecen varias ventajas

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

Los dominios son las unidades de replicación. Todos los controladores de dominio de un dominio determinado pueden recibir cambios y replicarlos a los demás controladores del dominio.

Un único dominio puede abarcar varias ubicaciones físicas distintas o sitios. Al utilizar un solo dominio se simplifican mucho las tareas administrativas.

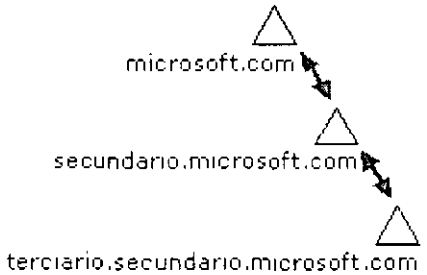
Para obtener más información acerca de los dominios, consulte Descripción de los dominios, Denominación de cuentas y dominios y Planear la estructura de dominios.

Introducción a los bosques y árboles de dominio

Varios dominios forman un bosque. Los dominios también pueden combinarse en estructuras jerárquicas denominadas árboles de dominio.

Árboles de dominio

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

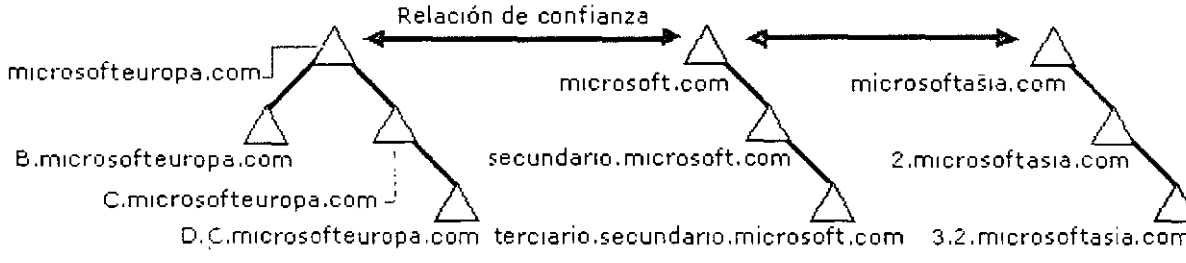


Todos los dominios que comparten el mismo dominio raíz forman un *espacio de nombres contiguo*. Esto significa que el nombre de un dominio secundario consta del nombre de ese dominio secundario más el nombre del dominio principal. En esta ilustración, secundario.microsoft.com es un dominio secundario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

Los dominios de Windows 2000 que forman parte de un árbol están unidos entre sí mediante relaciones de confianza transitivas y bidireccionales. Dado que estas relaciones de confianza son bidireccionales y transitivas, un dominio de Windows 2000 recién creado en un bosque o árbol de dominio tiene establecidas inmediatamente relaciones de confianza con todos los demás dominios de Windows 2000 en ese bosque o árbol de dominio. Estas relaciones de confianza permiten que un único proceso de inicio de sesión sirva para autenticar a un usuario en todos los dominios del bosque o del árbol de dominio. Sin embargo, esto no significa que el usuario, una vez autenticado, tenga permisos y derechos en todos los dominios del árbol de dominio. Dado que un dominio es un límite de seguridad, los derechos y permisos deben asignarse para cada dominio.

Bosques

Un bosque está formado por varios árboles de dominio. Los árboles de dominio de un bosque no constituyen un espacio de nombres contiguo. Por ejemplo, aunque dos árboles de dominio (microsoft.com y microsoftasia.com) pueden tener ambos un dominio secundario denominado "soporte", los nombres DNS de esos dominios secundarios serán soporte.microsoft.com y soporte.microsoftasia.com. Es evidente que en este caso no existe un espacio de nombres contiguo.



Sin embargo, un bosque no tiene ningún dominio raíz propiamente dicho. El dominio raíz del bosque es el primer dominio que se creó en el bosque. Los dominios raíz de todos los árboles de dominio del bosque establecen relaciones de confianza transitivas con el dominio raíz del bosque. En la ilustración, microsoft.com es el dominio raíz del bosque. Los dominios raíz de los otros árboles de dominio (microsofteuropa.com y microsoftasia.com) tienen establecidas relaciones de confianza transitivas con microsoft.com. Estas relaciones de confianza son necesarias para poder establecer otras entre todos los árboles de dominio del bosque. Para obtener más información, consulte Relaciones de confianza entre dominios.

Todos los dominios de Windows 2000 de todos los árboles de dominio de un bosque comparten las siguientes características:

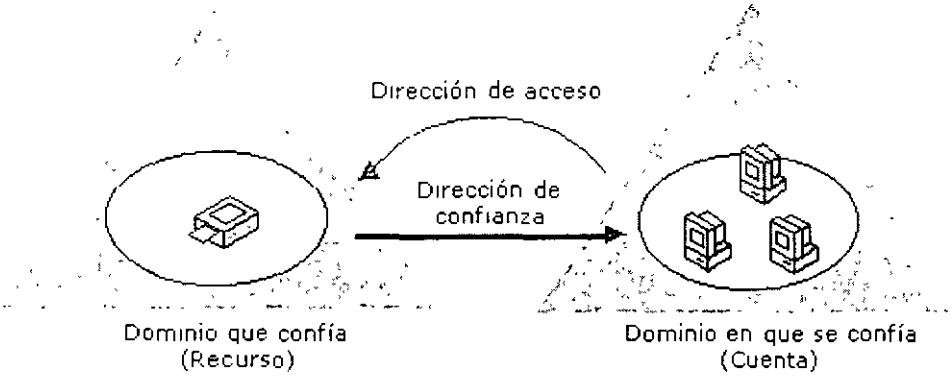
- Relaciones de confianza transitivas entre los dominios
- Relaciones de confianza transitivas entre los árboles de dominio
- Un esquema común

- Información de configuración común
- Un catálogo global común

Al utilizar bosques y árboles de dominio se obtiene la flexibilidad que ofrecen los sistemas de espacios de nombres contiguos y no contiguos. Esto puede ser útil, por ejemplo, en el caso de compañías que tienen divisiones independientes que necesitan conservar sus propios nombres DNS. Para obtener más información acerca de los bosques y árboles de dominio, consulte Descripción de los bosques y árboles de dominio.

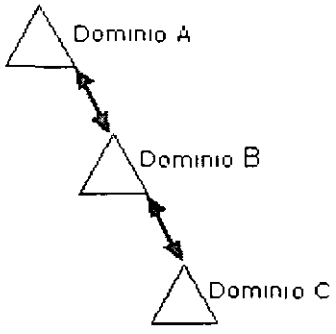
Relaciones de confianza entre dominios

Una confianza de dominio es una relación establecida entre dos dominios que permite a un controlador de dominio autenticar a los usuarios de otro dominio. Todas las relaciones de confianza entre dominios tienen lugar entre dos dominios: el dominio que confía y el dominio en el que se confía.



En la primera ilustración, las confianzas se indican mediante una fecha, que señala al dominio en el que se confía.

En versiones anteriores de Windows, las confianzas se limitaban a los dos dominios implicados en la confianza y la relación de confianza era de un solo sentido. En Windows 2000, todas las confianzas son transitivas y de dos sentidos. Los dominios de una relación de confianza confían el uno en el otro de forma automática.



Como se muestra en la ilustración, esto supone que si el dominio A confía en el dominio B y éste confía en el dominio C, los usuarios del dominio C, cuando se les concedan los permisos correspondientes, podrán tener acceso a los recursos del dominio A.

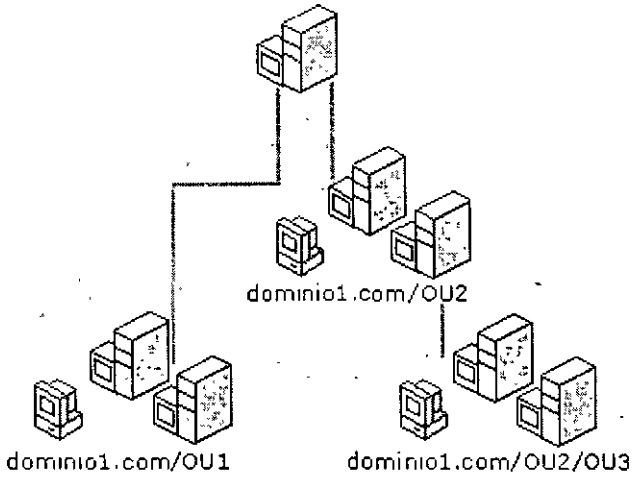
Para obtener más información acerca de las confianzas de dominio, consulte Descripción de las confianzas de dominio y Confianzas de dominio explícitas.

Nota: Cuando un controlador de dominio autentica a un usuario, no implica el acceso a ningún recurso de ese dominio. Esto sólo viene determinado por los derechos y permisos que el administrador del dominio concede a la cuenta de usuario para el dominio que confía. Para obtener más información, consulte Autenticación.

Unidades organizativas

Un tipo de objeto de directorio especialmente útil contenido en los dominios es la unidad organizativa. Las unidades organizativas son contenedores de Active Directory en los que puede colocar usuarios, grupos, equipos y otras unidades organizativas. Una unidad organizativa no puede contener objetos de otros dominios.

Una unidad organizativa es el ámbito o unidad más pequeña a la que se pueden asignar configuraciones de Directiva de grupo o en la que se puede delegar la autoridad administrativa. Con las unidades organizativas, puede crear contenedores dentro de un dominio que representan las estructuras lógicas y jerárquicas existentes dentro de una organización. Esto permite administrar la configuración y el uso de cuentas y recursos en función de su modelo organizativo. Para obtener más información acerca de la configuración de la Directiva de grupo, consulte Directiva de grupo.



Dominio de Windows 2000

Como se muestra en la ilustración, las unidades organizativas pueden contener otras unidades organizativas. La jerarquía de contenedores se puede extender tanto como sea necesario para

modelar la jerarquía de la organización dentro de un dominio. Las unidades organizativas le ayudarán a disminuir el número de dominios requeridos para una red.

Puede utilizar unidades organizativas para crear un modelo administrativo que se puede ampliar a cualquier tamaño. A un usuario se le puede conceder autoridad administrativa sobre todas las unidades organizativas de un dominio o sobre una sola de ellas. El administrador de una unidad organizativa no necesita tener autoridad administrativa sobre cualquier otra unidad organizativa del dominio. Para obtener más información acerca de cómo delegar la autoridad administrativa, consulte Delegar la administración.

Para obtener más información acerca de las unidades organizativas, consulte Planear la estructura de unidades organizativas y Delegar la administración.

Introducción a Sitios y servicios de Active Directory

Active Directory utiliza la replicación con múltiples servidores principales, lo que permite a cualquier controlador de dominio de Windows 2000 del bosque responder a las solicitudes, incluso a aquellas que suponen modificaciones realizadas por los usuarios en el directorio.

Si cuenta con un pequeño grupo de equipos bien conectados, la selección arbitraria de un controlador de dominio puede no causar ningún problema. Sin embargo, en una estructura que incluya una red de área extensa (WAN) puede ser extremadamente ineficaz que un usuario de Toledo, por ejemplo, intente autenticarse en controladores de dominio de Nueva York mediante una conexión telefónica. Sitios y servicios de Active Directory puede mejorar la eficiencia de los servicios de directorio en la mayor parte de los casos gracias al uso de sitios.

La información acerca de la estructura física de la red se proporciona mediante la publicación de sitios en Active Directory con Sitios y servicios de Active Directory. Active Directory utiliza esta información para determinar de qué forma debe replicarse la información de directorio y deben tratarse las solicitudes de servicio.

Los equipos se asignan a sitios en función de su ubicación en una subred o en un conjunto de subredes conectadas entre sí. Las subredes constituyen una forma sencilla y eficaz para representar agrupamientos en la red, de la misma forma que los códigos postales agrupan direcciones de forma conveniente. Las subredes tienen un formato que facilita el envío al directorio de información física relacionada con la conectividad de red. Al tener todos los equipos en una o varias subredes conectadas entre sí también se refuerza la norma de que todos los equipos de un sitio tienen que estar interconectados, ya que los equipos de la misma subred tienden a tener mejores conexiones que una selección cualquiera de equipos de la red.

Los sitios facilitan:

- **Autenticación**. Cuando los clientes inician una sesión con una cuenta de dominio, el sistema de inicio de sesión realiza primero la búsqueda de controladores de dominio que se encuentren en el mismo sitio que el cliente. Al intentar usar primero los controladores de dominio del sitio del cliente, el tráfico de red es sólo local, por lo que se aumenta la eficiencia del proceso de autenticación.

- **Replicación.** La información de directorio se replica tanto dentro de los sitios como entre ellos. Active Directory replica esa información con mayor frecuencia dentro de un sitio que entre sitios distintos. Este sistema permite ofrecer información de directorio actualizada teniendo en cuenta las limitaciones que impone el ancho de banda disponible en la red.

Puede personalizar la forma en que Active Directory replica la información con vínculos a sitios para especificar de qué forma están conectados los distintos sitios. Active Directory usa la información acerca de la manera en que se conectan los sitios para generar objetos de conexión que proporcionan un sistema de replicación muy eficiente y tolerante a errores.

Debe proporcionar información acerca del costo de un vínculo a sitios, los períodos en que el vínculo está disponible y la forma en que debe usarse. Active Directory utiliza esta información para determinar qué vínculo a sitios debe usarse para replicar la información. Al personalizar los programas de replicación de forma que ésta tenga lugar en los períodos más adecuados, como en las horas de baja utilización de la red, se aumenta su eficiencia.

Normalmente, se usan todos los controladores de dominio para intercambiar información entre los sitios, sin embargo puede tener un mayor control sobre la replicación si especifica un servidor cabeza de puente para la información que debe replicarse entre sitios. Establezca un servidor cabeza de puente cuando disponga de un servidor que desee dedicar a la replicación entre sitios, en lugar de utilizar cualquier servidor que esté disponible. También puede establecer un servidor cabeza de puente cuando su implementación use servidores proxy, por ejemplo, para enviar y recibir información a través de un servidor de seguridad.

- **Otros servicios que proporciona Active Directory**. Hay otra información, como enlaces y configuraciones de servicios, que puede estar disponible a través del directorio, lo que facilita la administración y el uso de los recursos de la red y aumenta su eficiencia. Los sitios ayudan a estructurar y optimizar la distribución de información de los servicios, con lo que hay disponible información actualizada para los clientes y se distribuye de forma eficiente a través de la red.

Grupos

Los grupos son objetos de Active Directory o de equipos locales que pueden contener usuarios, contactos, equipos y otros grupos. Los grupos se utilizan para:

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

Existen dos clases de grupos:

- Grupos de seguridad
- Grupos de distribución

Los grupos de seguridad se utilizan para recopilar usuarios, equipos y otros grupos en unidades más fáciles de administrar. Los administradores deben asignar los permisos para recursos (archivos compartidos, impresoras, etc.) a un grupo de seguridad, no a usuarios individuales. Así los permisos se asignan una vez al grupo en lugar de varias veces a cada usuario individual. Cada cuenta que se agrega al grupo recibe automáticamente los permisos y derechos definidos para ese grupo. Al trabajar con grupos en lugar de usuarios individuales se simplifica el mantenimiento y la administración de la red.

Los grupos de distribución sólo se pueden utilizar como listas de distribución de correo electrónico. No pueden utilizarse para filtrar configuraciones de Directiva de grupo. Los grupos de distribución no tienen ninguna función relacionada con la seguridad.

A diferencia de los grupos, las unidades organizativas se utilizan para crear colecciones de objetos en un solo dominio, no para asignar la pertenencia a grupos. La administración de una unidad organizativa y de los objetos que contiene puede delegarse en un administrador individual o en un grupo. Para obtener más información acerca de las unidades organizativas, consulte Unidades organizativas y Planear la estructura de las unidades organizativas.

Los objetos Directiva de grupo se pueden aplicar a sitios, dominios y unidades organizativas, pero nunca a los grupos. Un objeto Directiva de grupo es una colección de valores de configuración que afectan a usuarios y equipos. La pertenencia a un grupo se utiliza para filtrar los objetos Directiva de grupo que afectarán a los usuarios y equipos del sitio, dominio o unidad organizativa. Para obtener más información acerca de la Directiva de grupo, consulte Descripción de la Directiva de grupo.

Para conocer más detalles acerca de los grupos y cómo utilizarlos, consulte Descripción de los grupos.

Introducción al esquema de Active Directory

El esquema de Active Directory es el conjunto de definiciones que describen las clases de objetos y los tipos de información acerca de dichos objetos que se pueden almacenar en Active Directory. Las definiciones se almacenan como objetos para que Active Directory pueda administrar los objetos del esquema con las mismas operaciones de administración de objetos utilizadas para administrar el resto de los objetos del directorio.

Hay dos tipos de definiciones en el esquema: atributos y clases. Los atributos y las clases también se conocen como objetos del esquema o metadatos.

Los atributos se definen independientemente de las clases. Cada atributo sólo se define una vez y se puede utilizar en múltiples clases. Por ejemplo, el atributo Descripción se utiliza en muchas clases, pero se define una vez en el esquema, lo que asegura la coherencia.

Las clases, también conocidas como clases de objetos, describen los posibles objetos del directorio que se pueden crear. Cada clase es una colección de atributos. Al crear un objeto, los atributos almacenan la información que describe el objeto. La clase Usuario, por ejemplo, está compuesta de muchos atributos, entre ellos Dirección de red, Directorio principal, etc. Cada objeto en Active Directory es una instancia de una clase de objeto.

Con Windows 2000 Server se proporciona un conjunto de clases y atributos básicos. Los programadores y los administradores de la red con experiencia puede extender dinámicamente el esquema mediante la definición de nuevas clases y atributos para las clases existentes. Active Directory no permite la eliminación de objetos del esquema, sin embargo, los objetos se pueden marcar como desactivados, lo que proporciona muchas de las ventajas de la eliminación. Extender el esquema es una operación avanzada que puede tener consecuencias adversas. Antes de extender el esquema, consulte la Lista de comprobación: antes de extender el esquema.

La estructura y el contenido del esquema son controlados por el controlador de dominio que mantiene la función de servidor principal de operaciones de esquemas. Una copia del esquema se replica en todos los controladores de dominio del bosque. El uso de este esquema común asegura la integridad y coherencia de los datos en todo el bosque. Para obtener más información acerca del servidor principal de esquemas, consulte Operaciones de un solo servidor principal.

La forma recomendada de extender el esquema de Active Directory es mediante programación, a través de las Interfaces de servicios de Active Directory (ADSI, *Active Directory Service Interfaces*) descritas en el Kit del programador de software de Windows 2000 (*Windows 2000 Software Developer's Kit*). Para obtener información detallada acerca de cómo extender el esquema mediante

programación, consulte el Manual del programador de Active Directory en el sitio Web de Microsoft (http://www.microsoft.com/) y el sitio Web del Grupo de trabajo de ingeniería de Internet (IETF, *Internet Engineering Task Force*) (http://www.ietf.org/).Las direcciones Web pueden cambiar, de forma que es posible que no pueda conectar con el sitio o sitios Web mencionados aquí. Para el desarrollo y las pruebas, también puede ver y modificar el esquema de Active Directory con el complemento Esquema de Active Directory, que se incluye con las Herramientas de administración de Windows 2000 en el disco compacto de Windows 2000 Server. Para obtener más información, consulte Administrar servidores remotamente.

Funciones de servidor

Windows 2000 Server puede desempeñar varias funciones. Puede cambiar fácilmente entre las diversas funciones de Windows 2000 Server para adaptarlo a las necesidades de su organización.

Para obtener más información acerca de las funciones de Windows 2000 Server y de cómo cambiarlas, consulte:

- Controladores de dominio
- Servidores miembro
- Servidores independientes
- Cambiar las funciones de servidor

Controladores de dominio

Un controlador de dominio es un equipo donde se ejecuta Windows 2000 Server que se ha configurado con el Asistente para instalación de Active Directory. El Asistente para instalación de Active Directory instala y configura los componentes que proporciona el servicio de directorio de Active Directory a usuarios y equipos de red. Los controladores de dominio almacenan datos del directorio y administran las interacciones entre el usuario y el dominio, como los procesos de inicio de sesión, la autenticación y las búsquedas de directorio.

Un dominio puede tener uno o varios controladores de dominio. Una organización de pequeño tamaño que utiliza una sola red de área local (LAN) es posible que solamente necesite un dominio con dos controladores de dominio para obtener la mayor disponibilidad y tolerancia a los errores. Una organización grande con muchas ubicaciones de red necesitará uno o varios controladores de dominio en cada ubicación para el mismo fin.

Active Directory admite la replicación con múltiples servidores principales de datos del directorio entre todos los controladores de dominio del dominio. Sin embargo, algunos cambios no se pueden realizar de esta manera, de modo que sólo un controlador de dominio, llamado el servidor principal

de operaciones, acepta solicitudes para dichos cambios. En cualquier bosque de Active Directory, hay al menos cinco funciones diferentes de servidor principal de operaciones que se asignan a uno o varios controladores de dominio. Para obtener más información acerca de los servidores principales de operaciones, consulte Operaciones de un solo servidor principal.

Los controladores de dominio de Windows 2000 Server proporcionan una extensión de las capacidades y funciones de los controladores de dominio de Windows NT Server 4.0. La replicación con múltiples servidores principales de Windows 2000 Server sincroniza los datos del directorio de cada controlador de dominio, lo que asegura la coherencia de la información a lo largo del tiempo. Este tipo de replicación es una evolución del modelo que usa un controlador principal de dominio y un controlador de reserva utilizado en Windows NT Server 4.0, en el que sólo un servidor, el controlador principal del dominio, tenía una copia de lectura y escritura del directorio.

Servidores 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 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 de Active Directory 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 de los servidores 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*).

Para obtener más información acerca de los controladores de dominio, consulte Controladores de dominio.

Servidores independientes

Un servidor independiente es un equipo que ejecuta Windows 2000 Server y que no es miembro de ningún dominio de Windows 2000. Si se instala Windows 2000 Server como miembro de un grupo de trabajo, ese servidor es un servidor independiente.

Los servidores independientes pueden compartir recursos con otros equipos de la red, pero no disfrutan de ninguna de las ventajas que proporciona Active Directory.

Cambiar las funciones de un servidor

Los servidores de un dominio pueden tener una de las dos funciones siguientes: controlador de dominio o servidor miembro.

Si cambian las necesidades del entorno informático, puede ser aconsejable cambiar la función de algún servidor. Mediante el Asistente para instalación de Active Directory puede promover un servidor miembro y convertirlo en un controlador de dominio, o degradar un controlador de dominio a servidor miembro.

DESCRIPCIÓN DE ACTIVE DIRECTORY

Active Directory es una implementación de los protocolos de nombres y directorio estándar de Internet. Utiliza un motor de bases de datos para procesar las transacciones y es compatible con diversos estándares de interfaces de programación de aplicaciones. Esta sección trata·

- Descripción de los dominios
- Descripción de los bosques y árboles de dominio
- Denominación de cuentas y dominios
- Descripción de las relaciones de confianza entre dominios
- Relaciones de confianza explícitas entre dominios
- Sitios
- Cuentas de usuarios y equipos de Active Directory
- Descripción de la Directiva de grupo
- Descripción de la integración con DNS
- Descripción de los grupos
- Servicio de directorio de Active Directory

Descripción de los dominios

Un dominio ofrece las siguientes ventajas:

- Organizar objetos.

Al utilizar unidades organizativas en un dominio es más fácil administrar las cuentas y recursos del dominio.

- Publicar recursos e información acerca de los objetos del dominio.

Al utilizar varios dominios, puede cambiar el tamaño del servicio de directorio Active Directory para ajustarlo a sus necesidades de publicación y administración del directorio.

Un dominio sólo almacena información acerca de los objetos ubicados en ese dominio: por lo tanto, al crear varios dominios se divide o segmenta el directorio para atender mejor a un conjunto dispar de usuarios.

- Aplicar un objeto Directiva de grupo al dominio consolida la administración de los recursos y de la seguridad.

Un dominio define un ámbito o una unidad de directiva. Un objeto Directiva de grupo establece cómo se tiene acceso, se configuran y utilizan los recursos del dominio. Estas directivas se aplican sólo en el dominio, no en varios dominios. Para obtener más información acerca de cómo aplicar objetos Directiva de grupo, consulte Descripción de la Directiva de grupo.

- Delegar la autoridad de administrador elimina la necesidad de tener varios administradores con autoridad administrativa global.

Al usar la autoridad delegada junto con los objetos Directiva de grupo y la pertenencia a grupos se pueden asignar a un administrador derechos y permisos para administrar objetos en todo un dominio, o en una o varias unidades organizativas del dominio. Para obtener más información acerca de cómo delegar el control administrativo, consulte Delegar la administración.

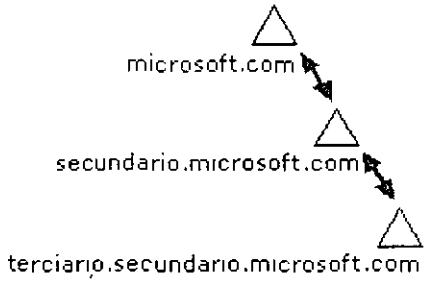
Para obtener más información acerca de los grupos, consulte Descripción de los grupos.

Como un dominio es un límite de seguridad, los permisos administrativos sobre un dominio están limitados a ese dominio de forma predeterminada. Por ejemplo, un administrador que tiene permisos para establecer directivas de seguridad en un dominio no tiene automáticamente la autoridad para establecer directivas de seguridad en otro dominio del directorio.

Para crear un dominio, debe promover uno o más equipos que ejecuten Windows 2000 Server a controladores de dominio. Un controlador de dominio proporciona servicios de directorio de Active Directory a usuarios y equipos de la red, almacena datos del directorio y administra las operaciones entre usuarios y dominios, incluidos los procesos de inicio de sesión, la autenticación y las búsquedas en el directorio. Cada dominio debe tener al menos un controlador de dominio.

Para obtener más información acerca de los controladores de dominio, consulte Controladores de dominio. Para promover un equipo Windows 2000 Server a controlador de dominio, consulte Instalar un controlador de dominio.

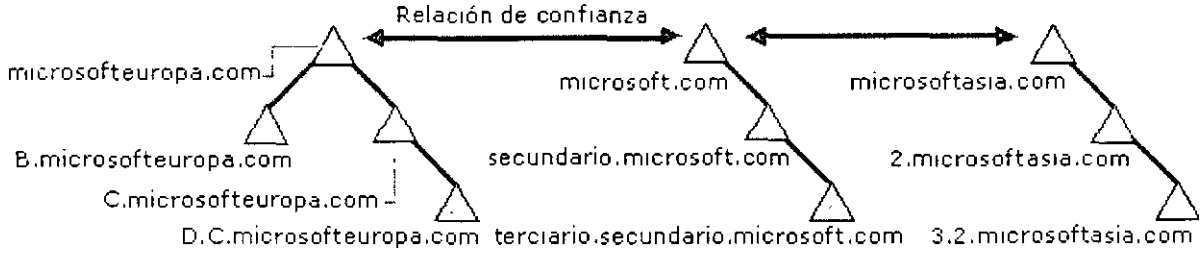
Descripción de los bosques y árboles de dominio



Cada dominio del directorio se identifica mediante un nombre DNS de dominio y necesita uno o más controladores de dominio. Si la red necesita más de un dominio, se pueden crear varios fácilmente.

Uno o más dominios que comparten un esquema y un catálogo global comunes se conocen como bosque. Si varios dominios del bosque tienen nombres DNS de dominio contiguos, como muestra la primera ilustración, esa estructura se denomina árbol de dominio.

Si, como muestra la segunda ilustración, los diversos dominios no tienen nombres DNS de dominio contiguos, se dice que forman árboles de dominio independientes dentro del bosque. Un bosque puede contener uno o más árboles de dominio. El primer dominio de un bosque se conoce como dominio raíz del bosque.



Un dominio se crea al instalar el primer controlador de dominio. Durante la instalación del primer controlador de dominio, el Asistente para la instalación de Active Directory utiliza la información que usted proporciona para instalar el controlador de dominio y crear el dominio en el contexto de relaciones (si existen) con otros dominios y controladores de dominio. Ese contexto puede ser el del primer dominio en un nuevo bosque, el primer dominio en un nuevo árbol de dominio o un dominio secundario en un árbol de dominio ya existente.

Después de instalar el primer controlador de dominio de un dominio, puede instalar controladores de dominio adicionales para aumentar la tolerancia a errores y la disponibilidad del directorio.

Nombres de dominio

Los dominios que forman un único árbol de dominio comparten un espacio de nombres contiguo (jerarquía de nombres). Aplicando los estándares de DNS, el nombre completo de un dominio que forma parte de un espacio de nombres contiguo es el nombre de ese dominio seguido de los nombres de los dominios principal y raíz, en el formato de caracteres con puntos (.). Por ejemplo, un dominio cuyo nombre NetBIOS es "secundario2" que tiene un dominio principal denominado principal.microsoft.com, tendrá el nombre DNS completo secundario2.principal.microsoft.com.

Los árboles de dominio asociados en un bosque comparten el mismo esquema de Active Directory y la información de duplicación y configuración del directorio, pero no comparten un espacio de nombres de dominio DNS contiguo.

La combinación de bosques y árboles de dominio ofrece opciones flexibles para asignar nombres a los dominios. En el directorio se pueden incluir espacios de nombres DNS contiguos y no contiguos.

Para obtener más información acerca de Active Directory y DNS, consulte Sistema de nombres de dominio (DNS, *Domain Name System*).

Relaciones de confianza

En los equipos que ejecutan Windows 2000, la autenticación de cuentas entre dominios es posible gracias a relaciones de confianza bidireccionales y transitivas basadas en el protocolo de seguridad Kerberos V5.

Las relaciones de confianza se crean automáticamente entre dominios adyacentes (dominio principal y secundario) cuando se crea un dominio en un árbol de dominios. En un bosque, se crea automáticamente una relación de confianza entre el dominio raíz del bosque y el dominio raíz de cada árbol de dominio que se agrega al bosque. Dado que esas relaciones de confianza son transitivas, los usuarios y equipos pueden autenticarse en cualquier dominio del bosque o del árbol de dominios.

Al actualizar a Windows 2000 un dominio Windows que ejecuta una versión anterior a Windows 2000, se conservan las relaciones de confianza unidireccionales existentes entre ese dominio y otros dominios. Entre ellas se incluyen todas las relaciones de confianza establecidas con dominios que ejecutan versiones anteriores a Windows 2000. Si instala un nuevo dominio Windows 2000 y desea establecer relaciones de confianza con dominios que ejecutan versiones anteriores a Windows 2000, deberá crear relaciones de confianza externas con esos dominios.

Para obtener más información acerca de las relaciones de confianza, consulte Relaciones de confianza entre dominios. Para obtener más información acerca de las relaciones de confianza externas, consulte Relaciones de confianza externas.

Denominación de cuentas y dominios

Los nombres de dominio de Active Directory suelen coincidir con el nombre DNS completo del dominio. Sin embargo, para asegurar la compatibilidad con versiones anteriores, cada dominio tiene también un nombre previo a Windows 2000 que se utilizará cuando se ejecuten sistemas operativos anteriores a Windows 2000.

El nombre de dominio anterior a Windows 2000 se puede utilizar para iniciar sesión en un dominio de Windows 2000 desde equipos en los que se ejecutan sistemas operativos anteriores a Windows 2000 mediante el formato *nombreDeDominio\nombreDeUsuario*. También se puede utilizar este formato para iniciar sesión en un dominio de Windows 2000 desde equipos en los que se ejecuta

Windows 2000. Asimismo, los usuarios pueden iniciar sesión en equipos en los que se ejecute Windows 2000 mediante el nombre principal del usuario asociado a sus cuentas de usuario.

Cuentas de usuario

En Active Directory, cada cuenta de usuario tiene un nombre de inicio de sesión de usuario, un nombre de inicio de sesión de usuario de sistema anterior a Windows 2000 (nombre de cuenta de administrador de cuentas de seguridad) y un sufijo de nombre principal de usuario. El administrador escribe el nombre de inicio de sesión de usuario y selecciona el sufijo de nombre principal de usuario cuando crea la cuenta de usuario. Active Directory sugiere un nombre de inicio de sesión de usuario de sistema anterior a Windows 2000 a partir de los primeros 20 bytes del nombre de inicio de sesión de usuario. Los administradores pueden cambiar el nombre de inicio de sesión de sistema anterior a Windows 2000 siempre que lo deseen.

En Active Directory, cada cuenta de usuario tiene un nombre principal de usuario que se basa en la RFC 822 de IETF, *Estándar para el formato de los mensajes de texto de Internet ARPA* (*Standard for the Format of ARPA Internet Text Messages*) El nombre principal de usuario está compuesto por el nombre de inicio de sesión de usuario y el sufijo del nombre principal de usuario, que se unen mediante el signo @.

Nota: No agregue el signo @ al nombre de inicio de sesión de usuario ni el sufijo del nombre principal de usuario. Active Directory lo agrega automáticamente cuando crea el nombre principal de usuario. No será válido ningún nombre principal de usuario que contenga más de un signo @.

La segunda parte del nombre principal de usuario, al que se hace referencia como el sufijo del nombre principal de usuario, identifica el dominio en el que se encuentra la cuenta de usuario. El sufijo del nombre principal de usuario puede ser el nombre de dominio DNS, el nombre DNS de cualquier dominio del bosque, o puede tratarse de un nombre alternativo creado por un administrador y usado sólo para iniciar sesiones. No es necesario que este sufijo del nombre principal sea un nombre DNS válido.

En Active Directory, el sufijo predeterminado del nombre principal de usuario es el nombre DNS del dominio raíz del árbol de dominios. En la mayoría de los casos, se trata del nombre de dominio registrado como dominio de empresa en Internet. Al usar nombres alternativos de dominio como sufijo del nombre principal de usuario, es posible proporcionar una seguridad adicional al iniciar una sesión y simplificar los nombres usados para iniciar sesiones en otro dominio del bosque.

Por ejemplo, si su organización usa un árbol de dominios profundo, organizado por departamento y región, los nombres de dominio pueden llegar a ser muy largos. El sufijo del nombre principal de usuario predeterminado para un usuario de ese dominio podría ser *ventas.costaoeste.microsoft.com*. El nombre de inicio de sesión de un usuario en ese dominio sería

usuario@ventas.costaoeste.microsoft.com. La creación del sufijo de nombre principal de usuario "microsoft" permitiría que el mismo usuario iniciara una sesión mediante el nombre de inicio de sesión *usuario@microsoft.com*, que es mucho más sencillo. Para obtener más información acerca de las cuentas de usuario, consulte Cuentas de equipos y usuarios de Active Directory y Nombres de objetos de Active Directory.

Mediante Dominios y confianzas de Active Directory, puede agregar o quitar sufijos de nombre principal de usuario. Para obtener instrucciones, consulte Agregar sufijos de nombre principal de usuario.

Cuentas de equipo

Cada cuenta de equipo creada en Active Directory tiene un nombre completo relativo, un nombre de equipo de Windows 2000 (nombre de cuenta de administración de seguridad), un sufijo DNS principal, un nombre de host y un nombre principal de servicio. El administrador escribe el nombre del equipo cuando crea la cuenta del equipo. Este nombre de equipo se utiliza como nombre completo relativo LDAP.

Active Directory sugiere un nombre de inicio de sesión de usuario de sistema anterior a Windows 2000 a partir de los primeros 15 bytes del nombre completo relativo. El administrador puede cambiar el nombre de inicio de sesión de sistema anterior a Windows 2000 siempre que lo desee.

De forma predeterminada, el sufijo DNS adopta el nombre DNS completo del dominio al que se une el equipo. El nombre de host DNS se crea a partir de los 15 primeros caracteres del nombre completo relativo y el sufijo DNS principal. Por ejemplo, el nombre de host DNS del equipo que se une al dominio *miDominio.microsoft.com* y que tiene el nombre completo relativo *CN=MiPC1234567890*, sería *miPC12345 miDominio.microsoft.com*.

Para obtener más información, consulte Nombres de objetos de Active Directory y Cuentas de equipos y usuarios de Active Directory.

El nombre principal de servicio se crea a partir del nombre de host DNS. El nombre principal de servicio se utiliza durante la autenticación mutua entre el cliente y el servidor de un servicio determinado. El cliente buscará un nombre de equipo a partir del nombre principal del servicio al que intenta conectarse.

Los administradores pueden cambiar la forma en que se crea el nombre principal del servicio. Esta modificación de seguridad permite que un equipo utilice sufijos DNS primarios distintos de los del dominio al que se une este equipo. Esta misma modificación permite que Active Directory utilice más de los 15 primeros bytes del nombre completo relativo cuando se crea el nombre principal del servicio.

Los equipos con estos nombres modificados registrarán correctamente los nombres en el DNS, pero se precisa un procedimiento adicional para habilitar un registro correcto de los atributos de nombre de host DNS (nombreHostDns) y nombre principal del servicio (NombrePrincipalDeServicio) del objeto del equipo en Active Directory.

Precaución

- Si se modifica así la seguridad predeterminada, existe la posibilidad de que un equipo unido al dominio seleccionado pueda ser controlado por un usuario malintencionado y que pueda anunciarse con un nombre distinto mediante el atributo de nombre principal de servicio

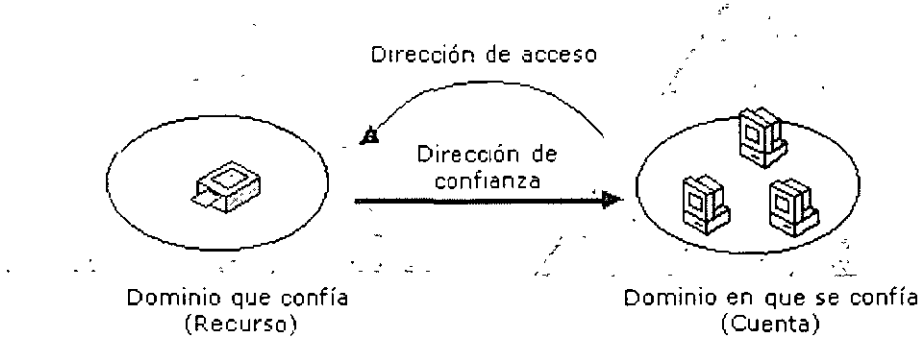
Para obtener más información, consulte Permitir que un equipo utilice un nombre DNS distinto.

Descripción de las confianzas entre dominios

Una confianza entre dominios es una relación que se establece entre dominios y que permite a los usuarios de un dominio ser autenticados por un controlador de dominio de otro dominio. Las solicitudes de autenticación siguen una *ruta de confianza*.

Ruta de confianza

Una ruta de confianza es la serie de relaciones de confianza que deben seguir las solicitudes de autenticación entre dominios. Para que un usuario pueda tener acceso a un recurso de otro dominio, la seguridad de Windows 2000 debe determinar si el dominio que confía (el dominio que contiene el recurso al que el usuario intenta obtener el acceso) tiene una relación de confianza con el dominio en el que se confía (el dominio donde inicia la sesión el usuario). Para determinarlo, el sistema de seguridad de Windows 2000 calcula la ruta de confianza entre un controlador de dominio del dominio de confianza y un controlador de dominio del dominio en el que se confía. En la ilustración, las rutas de confianza aparecen indicadas mediante flechas que muestran la dirección de la confianza.



Todas las relaciones de confianza entre dominios tienen lugar entre dos dominios: el dominio que confía y el dominio en el que se confía. Una relación de confianza entre dominios se caracteriza porque puede ser:

- Bidireccional
- Unidireccional
- Transitiva
- Intransitiva

Confianza unidireccional

Una confianza unidireccional es una sola relación de confianza, en la que el dominio A confía en el dominio B. Todas las relaciones unidireccionales son intransitivas y todas las intransitivas son unidireccionales. Las solicitudes de autenticación sólo se pueden transmitir desde el dominio que confía al dominio en el que se confía. Esto significa que si el dominio A tiene una confianza unidireccional con el dominio B y éste la tiene con el dominio C, el dominio A no tiene una relación de confianza con el dominio C.

Un dominio de Windows 2000 puede establecer una confianza unidireccional con:

- Los dominios de Windows 2000 de un bosque diferente
- Los dominios de Windows NT 4.0
- Los territorios de MIT Kerberos V5. Consulte Autenticación de Kerberos V5.

Debido a que todos los dominios de Windows 2000 de un bosque están vinculados mediante una confianza transitiva, no es posible crear confianzas unidireccionales entre dominios de Windows 2000 pertenecientes al mismo bosque. Para obtener más información, consulte Confianzas de dominio explícitas.

Confianza bidireccional

Todas las confianzas entre dominios de un bosque de Windows 2000 son confianzas transitivas bidireccionales.

Cuando se crea un nuevo dominio secundario, automáticamente se crea una confianza transitiva bidireccional entre el nuevo dominio secundario y el dominio principal. En una confianza bidireccional, el dominio A confía en el dominio B y el dominio B confía en el A. Esto significa que las solicitudes de autenticación se pueden transmitir entre dos dominios en ambas direcciones.

Para crear una confianza bidireccional intransitiva, debe crear dos confianzas unidireccionales entre los dominios implicados. Para obtener más información, consulte Confianzas de dominio explícitas.

Confianza transitiva

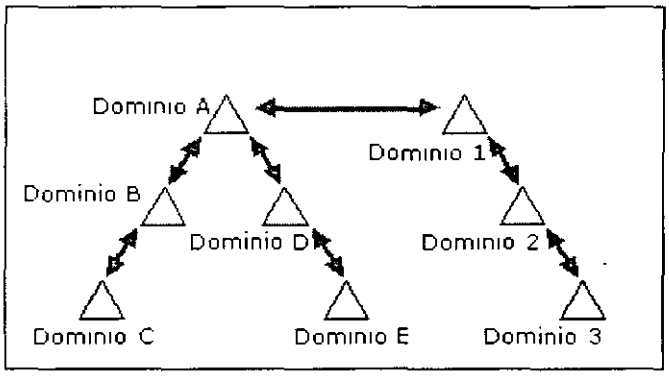
Todas las confianzas entre dominios de un bosque de Windows 2000 son transitivas. Las relaciones de confianza transitiva son siempre bidireccionales. Ambos dominios de la relación confían el uno en el otro.

Una relación de confianza transitiva no está limitada por los dos dominios de la relación. Siempre que se crea un nuevo dominio secundario, implícitamente (es decir, automáticamente) se crea una relación de confianza transitiva bidireccional entre el dominio principal y el nuevo dominio secundario. De esta forma, las relaciones de confianza transitivas fluyen hacia arriba a través del árbol de dominios a medida que éste se forma, con lo que se crean relaciones de confianza transitivas entre todos los dominios del árbol de dominios.

Cada vez que se crea un árbol de dominios en un bosque, se forma una relación de confianza transitiva bidireccional entre el dominio raíz del bosque y el nuevo dominio (la raíz del nuevo árbol de dominios). Si no se agrega ningún dominio secundario al dominio nuevo, la ruta de confianza está entre este nuevo dominio raíz y el dominio raíz del bosque. Si se agregan dominios secundarios al dominio nuevo, con lo que se crea un árbol de dominios, la confianza fluye hacia arriba a través del árbol de dominios hasta el dominio raíz del árbol de dominios y, de este modo, se extiende la ruta de confianza inicial creada entre la raíz del dominio y el dominio raíz del bosque. Si el nuevo dominio agregado al bosque es un solo dominio raíz, es decir, no tiene dominios secundarios, o un árbol de dominios, la ruta de confianza se extiende desde el dominio raíz del bosque hasta cualquier otro dominio raíz del bosque. De esta forma, las relaciones de confianza transitivas fluyen a través de todos los dominios del bosque. Las solicitudes de autenticación siguen estas rutas de confianza y de este modo las cuentas de cualquier dominio del bosque se pueden autenticar en cualquier otro. Con un solo proceso de inicio de sesión, las cuentas que poseen los permisos adecuados pueden tener acceso a los recursos en cualquier dominio del bosque.

Esta ilustración muestra cómo las relaciones de confianza transitivas fluyen a través de todos los dominios del bosque.

Bosque de Windows 2000



Puesto que el dominio 1 tiene una relación de confianza transitiva con el dominio 2 y éste la tiene con el dominio 3, los usuarios del dominio 3 (una vez obtenidos los permisos necesarios) pueden tener acceso a los recursos del dominio 1. Y, puesto que el dominio 1 tiene una relación de confianza transitiva con el dominio A y los otros dominios del árbol de dominios del dominio A la tienen con el dominio A, los usuarios del dominio B (una vez obtenidos los permisos necesarios) pueden tener acceso a los recursos del dominio 3.

Igualmente, puede crear de forma explícita (manualmente) confianzas transitivas entre los dominios de Windows 2000 del mismo árbol o bosque de dominios. Estas relaciones de confianza de acceso directo se pueden utilizar para acortar la ruta de confianza en árboles o bosques de dominios grandes y complejos. Para obtener más información, consulte Confianzas de dominio explícitas.

Nota: Las confianzas transitivas sólo pueden existir entre dominios de Windows 2000 del mismo bosque. Debido a la necesidad de este flujo de confianzas, no es posible tener relaciones intransitivas entre dominios del mismo bosque de Windows 2000.

Confianza intransitiva

Una confianza intransitiva está limitada por los dos dominios de la relación y no fluye a cualquier otro dominio del bosque. En la mayor parte de los casos, debe crear las confianzas intransitivas explícitamente. Consulte Confianzas de dominio explícitas.

Nota: Todas las relaciones de confianza entre los dominios de Windows 2000 y los de Windows NT son intransitivas. Al actualizar Windows NT con Windows 2000, todas las confianzas existentes en Windows NT permanecen intactas. En un entorno en modo mixto, todas las confianzas de Windows NT son intransitivas.

De forma predeterminada, las confianzas intransitivas son unidireccionales, aunque también se puede crear una relación bidireccional si se crean dos unidireccionales. Todas las relaciones de confianza establecidas entre dominios de Windows 2000 que no pertenecen al mismo bosque son intransitivas.

En resumen, las confianzas intransitivas son la única forma de relación de confianza posible entre:

- Un dominio de Windows 2000 y un dominio de Windows NT
- Un dominio de Windows 2000 de un bosque y un dominio de Windows 2000 de otro
- Un dominio de Windows 2000 y un territorio de MIT Kerberos V5. Consulte Autenticación de Kerberos V5

Protocolos de confianza

Windows 2000 autentica usuarios y aplicaciones mediante el uso de dos protocolos: Kerberos V5 o NTLM. El protocolo Kerberos V5 es el predeterminado para equipos donde se ejecuta Windows 2000 y para aquellos que tienen instalado el software de cliente de Windows 2000. Si alguno de los equipos implicados en una transacción no admite Kerberos V5, se utilizará el protocolo NTLM.

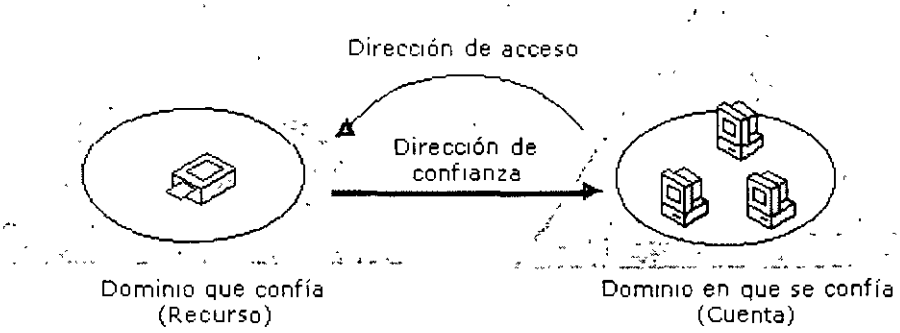
Con este protocolo, el cliente solicita un vale a un controlador de dominio de su dominio de cuenta para el servidor del dominio que confía. Este vale es emitido por un intermediario en el que confían el cliente y el servidor. El cliente presenta este vale de confianza al servidor del dominio que confía para proceder a su autenticación. Para obtener más información, consulte Autenticación de Kerberos V5.

Cuando un cliente intenta obtener acceso a recursos de un servidor de otro dominio con la autenticación NTML, el servidor que contiene el recurso debe ponerse en contacto con un controlador de dominio del dominio de cuenta del cliente para comprobar las credenciales de la cuenta.

Relaciones de confianza explícitas entre dominios

Las confianzas explícitas son relaciones de confianza que crean los propios usuarios. en lugar de crearse automáticamente durante la instalación de un controlador de dominio. Para crear y administrar confianzas explícitas utilice Dominios y confianzas de Active Directory. Hay dos clases de confianzas explícitas: las externas y las de acceso directo. Las confianzas externas permiten la autenticación de usuarios en un dominio fuera de un bosque. Las confianzas de acceso directo acortan la ruta de una confianza en un bosque complejo.

Confianzas externas



Las confianzas externas crean relaciones de confianza con dominios que se encuentran fuera del bosque. La ventaja de crear confianzas externas radica en permitir la autenticación de usuarios en un dominio que no abarcan las rutas de confianza de un bosque. Todas las confianzas externas son intransitivas y de un solo sentido, como se muestra en la ilustración. Puede combinar dos confianzas de un sentido para crear una relación de confianza de dos sentidos.

Importante

- En dominios de modo mixto, las confianzas externas se deben eliminar siempre desde un controlador de dominio de Windows 2000. Las confianzas externas en dominios de Windows NT 4.0 ó 3.51 pueden eliminarlas administradores autorizados en los controladores de dominio de Windows NT 4.0 ó 3.51. No obstante, sólo se puede eliminar el lado de confianza de la relación en controladores de dominio de Windows NT 4.0 ó 3.51. El lado que confía de la relación (creado en el dominio de Windows 2000) no se elimina y, aunque no estará operativo, la confianza seguirá mostrándose en Dominios y confianzas de Active Directory. Para quitar completamente la confianza, deberá eliminarla de un controlador de dominio de Windows 2000 en el dominio que confía.

Si se elimina por equivocación una confianza externa de un controlador de dominio de Windows NT 4.0 ó 3.51, deberá volver a crearla desde cualquier controlador de dominio de Windows 2000 en el dominio que confía.

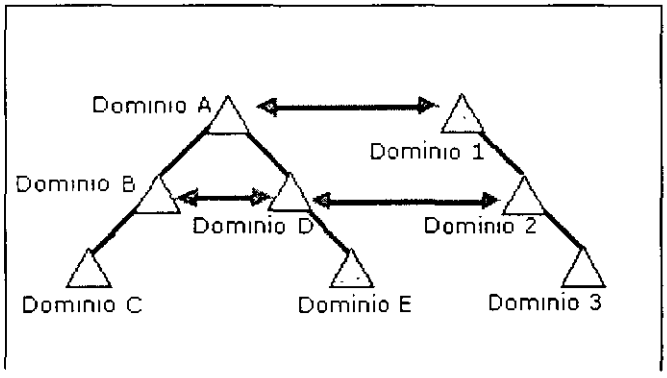
Confianzas de acceso directo

Para que un controlador de dominio de otro dominio pueda conceder a una cuenta acceso a determinados recursos, Windows 2000 debe determinar si el dominio que contiene los recursos deseados, el dominio de destino, tiene una relación de confianza con el dominio en el que se encuentra la cuenta, el dominio de origen. Para averiguarlo, en el caso de dos dominios de un bosque, Windows 2000 calcula una ruta de confianza entre los controladores de los dominios de origen y de destino. Una ruta de confianza es la serie de relaciones de confianza de dominio que

debe atravesar la seguridad de Windows 2000 para pasar las solicitudes de autenticación entre dos dominios cualesquiera. Calcular y atravesar una ruta de confianza entre árboles de dominio de un bosque complejo puede llevar tiempo, que se puede reducir con las confianzas de acceso directo.

Las confianzas de acceso directo son confianzas transitivas de dos sentidos que permiten acortar la ruta en un árbol complejo. Se crean de forma explícita entre dominios de Windows 2000 del mismo bosque. Una confianza de acceso directo es una optimización del rendimiento que acorta la ruta de confianza que la seguridad de Windows 2000 utiliza en la autenticación. El uso más efectivo de las confianzas de acceso directo se produce entre dos árboles de dominio de un bosque.

Bosque de Windows 2000



Como se muestra en la ilustración, puede crear una confianza de acceso directo entre dominios del nivel medio de dos árboles de dominio para acortar la ruta de confianza entre dos dominios de Windows 2000 de un bosque y optimizar el proceso de autenticación de Windows 2000.

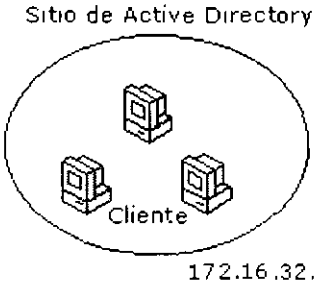
Nota: Si es necesario, puede crear varias confianzas de acceso directo entre dominios de un bosque.

Crear confianzas explícitas

Para crear una confianza exxplícita, debe conocer los nombres de dominio y una cuenta de usuario con permiso para crear confianzas en cada dominio. A cada confianza se le asigna una contraseña que debe conocer el administrador de ambos dominios de la relación. Para obtener instrucciones acerca de cómo establecer una confianza explícita, consulte Para crear una confianza de dominio explícita.

Para obtener más información acerca de las confianzas de dominio, consulte Descripción de las confianzas de dominio. Para obtener más información acerca del proceso de autenticación, consulte Autenticación.

Sitios



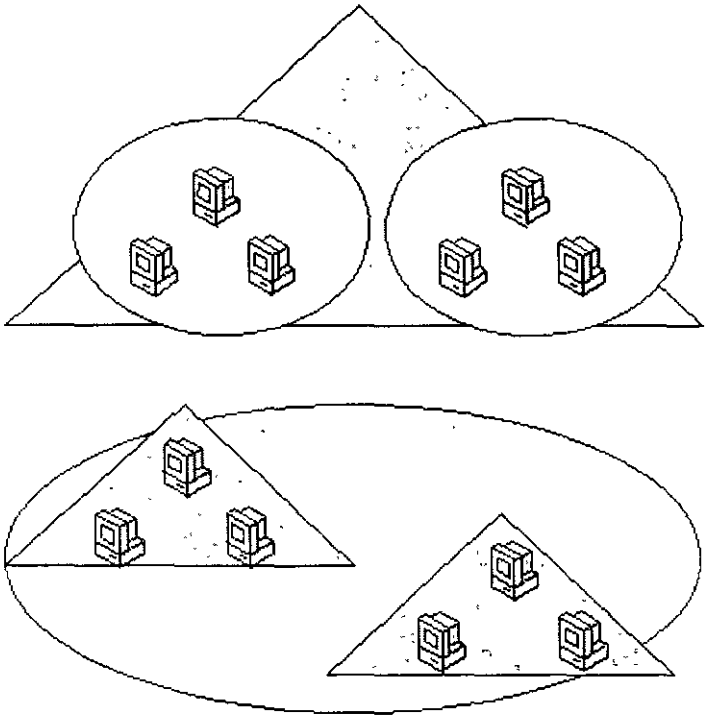
Por comodidad, piense en los sitios como si estuvieran definidos por un conjunto de equipos en una o varias subredes IP. Este planteamiento es correcto porque, para el intercambio eficaz de la información del directorio los equipos de un sitio tienen que estar conectados correctamente, una característica típica de los equipos dentro de una subred. Si un sitio comprende varias subredes, éstas deben estar también conectadas correctamente por el mismo motivo. Las redes de área extensa (WAN) deben emplear múltiples sitios. Si no lo hacen, la atención de las solicitudes o la replicación de información del directorio a través de las WAN puede ser muy poco eficiente.

Para obtener más información acerca de lo que significa que los equipos estén conectados correctamente, consulte Ancho de banda.

¿Cómo se relacionan los sitios con los dominios?

Los sitios asignan la estructura física de la red mientras que los dominios, normalmente, asignan la estructura lógica de la organización. La estructura lógica y la estructura física son independientes la una de la otra, lo que tiene las siguientes consecuencias:

- No es necesaria ninguna correlación entre la estructura física de la red y su estructura de dominios.
- Active Directory permite que haya múltiples dominios en un solo sitio así como múltiples sitios en un solo dominio.



- No es necesaria ninguna conexión entre espacios de nombres de sitios y de dominios.

¿Cómo se utilizan los sitios?

Sitios y servicios de Active Directory permite especificar la información de los sitios. Active Directory utiliza esta información para determinar el mejor modo de utilizar los recursos de las red disponibles. Esto aumenta la eficacia de los siguientes tipos de operaciones:

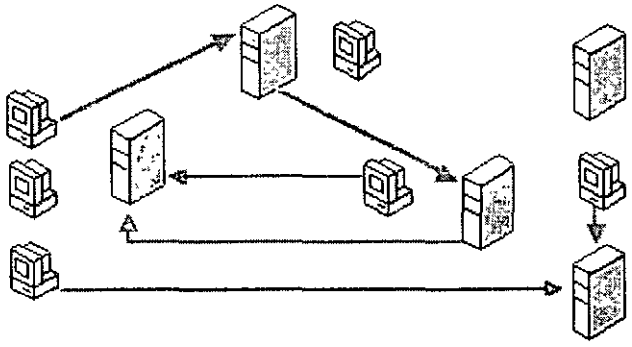
- Solicitudes de servicio

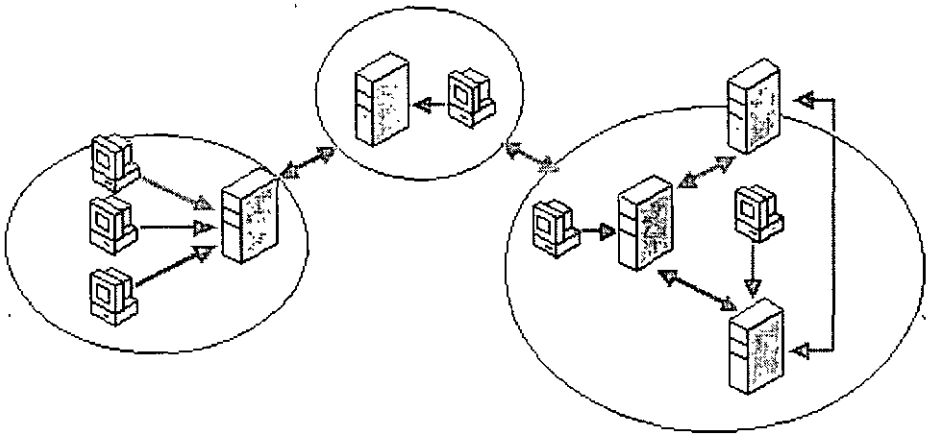
Cuando un cliente solicita un servicio a un controlador de dominio, éste la dirige a un controlador de dominio del mismo sitio, si hay alguno disponible. La selección de un controlador de dominio que esté conectado correctamente con el cliente que formuló la solicitud facilita su tratamiento.

- Replicación

Los sitios optimizan la replicación de información del directorio. La información de configuración y de esquema del directorio se distribuye por todo el bosque y los datos del dominio se distribuyen entre todos los controladores de dominio del dominio. Al reducir la replicación de forma estratégica, igualmente se puede reducir el uso de la red. Active Directory replica información del directorio dentro de un sitio con mayor frecuencia que entre sitios. De esta forma, los controladores de dominio mejor conectados, es decir, aquellos que con más probabilidad necesitarán información especial del directorio, son los que primero reciben las replicaciones. Los

controladores de dominio de otros sitios reciben todos los cambios efectuados en el directorio, pero con menor frecuencia, con lo que se reduce el consumo de ancho de banda de red.





Si una implementación no se organiza en sitios, el intercambio de información entre controladores de dominio y clientes puede ser caótico. Los sitios mejoran la eficacia del uso de la red.

La pertenencia a un sitio se determina de manera diferente para controladores de dominio que para clientes. Un cliente determina en qué sitio está cuando se activa, de modo que la ubicación de su sitio con frecuencia se actualizará dinámicamente. La ubicación del sitio de un controlador de dominio se establece por el sitio al que pertenece su objeto servidor en el directorio, de modo que ésta será coherente a no ser que el objeto servidor del controlador de dominio se mueva intencionadamente a un sitio distinto. Si un controlador de dominio o un cliente tiene una dirección que no está incluida en ningún sitio, el cliente o el controlador de dominio está contenido dentro del sitio inicial creado (Primer sitio predeterminado). Toda la actividad se controla entonces como si la actividad del cliente o del controlador de dominio fuera un miembro del Primer sitio predeterminado, sin tener en cuenta la dirección IP o la ubicación de subred reales. Por lo tanto, todos los sitios siempre tendrán un controlador de dominio asociado, ya que el controlador de dominio más próximo se asocia a sí mismo a un sitio que no tiene ningún controlador de dominio (a menos que se elimine el Primer sitio predeterminado).

Cuentas de usuario y de equipo de Active Directory

Las cuentas de usuario y de equipo de Active Directory representan una entidad física como una persona o un equipo. Las cuentas de usuario y de equipo (así como los grupos) se denominan principales de seguridad. Los principales de seguridad son objetos de directorio a los que se asignan automáticamente identificadores de seguridad. Los objetos con identificadores de seguridad pueden iniciar sesiones en la red y tener acceso a los recursos del dominio. Una cuenta de usuario o de equipo se utiliza para:

- Autenticar la identidad del usuario o equipo.
- Autorizar o denegar el acceso a los recursos del dominio.
- Administrar otros principales de seguridad.
- Auditar las acciones realizadas con la cuenta de usuario o de equipo.

Por ejemplo, a las cuentas de usuario y de equipo que son miembros del grupo Administradores de empresa se les concede automáticamente permiso para iniciar sesiones en todos los controladores de dominio del bosque.

Las cuentas de usuario y de equipo se agregan, deshabilitan, restablecen y eliminan con Usuarios y equipos de Active Directory.

Cuando se establece una confianza entre un dominio de Windows 2000 de un bosque específico y un dominio de Windows 2000 que se encuentra fuera de ese bosque, se puede conceder a los principales de seguridad del dominio externo el acceso a los recursos del bosque. Active Directory crea un objeto de "principal de seguridad externo" para representar cada principal de seguridad del dominio de confianza externo. Estos principales de seguridad externos pueden convertirse en miembros de grupos locales del dominio, que pueden tener miembros de dominios que se encuentran fuera del bosque. Para obtener más información acerca de confianzas, consulte Confianzas de dominios.

Active Directory crea los objetos de directorio para los principales de seguridad externos y no se deben modificar manualmente. Para ver los objetos de principales de seguridad externos, habilite Características avanzadas en Usuarios y equipos de Active Directory. Para obtener información acerca de cómo habilitar Características avanzadas, consulte Ver características avanzadas.

Cuando se establece una confianza entre un dominio de Windows 2000 de un bosque específico y un dominio de Windows 2000 que se encuentra fuera de ese bosque, se puede conceder a los principales de seguridad del dominio externo el acceso a los recursos del dominio interno. Active Directory crea un objeto de "principal de seguridad externo" en el dominio interno para representar

cada principal de seguridad del dominio de confianza externo. Estos principales de seguridad externos pueden convertirse en miembros de grupos locales en el dominio interno. (Los grupos locales de dominios pueden tener miembros de otros dominios que se encuentran fuera del bosque). Para obtener más información acerca de confianzas, consulte Confianzas de dominios.

Cuentas de usuario de Active Directory

Una cuenta de usuario de Active Directory permite que un usuario inicie sesiones en equipos y dominios con una identidad que se puede autenticar y autorizar para tener acceso a los recursos del dominio. Cada usuario que se conecta a la red debe tener su propia cuenta de usuario y su propia contraseña única. Las cuentas de usuario también se pueden usar como cuentas de servicio para algunas aplicaciones.

Windows 2000 proporciona cuentas de usuario predefinidas que se pueden usar para iniciar una sesión en un equipo donde se ejecuta Windows 2000. Estas cuentas predefinidas son:

- Cuenta Administrador
- Cuenta Invitado

Las cuentas predefinidas son cuentas de usuario predeterminadas, diseñadas para permitir que los usuarios inicien una sesión en un equipo local y tengan acceso a sus recursos. Su objetivo principal es iniciar una sesión y configurar inicialmente un equipo local. Cada cuenta predefinida tiene una combinación diferente de derechos y permisos. La cuenta de administrador tiene los derechos y permisos más amplios mientras que la cuenta de invitado los tiene limitados.

Si un administrador de red no modifica ni deshabilita los derechos y permisos predeterminados de la cuenta, cualquier usuario o servicio podría usarlos para iniciar una sesión en una red mediante la identidad Administrador o Invitado. Para obtener la seguridad que proporciona la autenticación y autorización de usuarios, cree una cuenta de usuario individual para cada usuario que participe en la red, mediante Usuarios y equipos de Active Directory. Cada cuenta de usuario, incluidas las cuentas de administrador y de invitado, se puede agregar a los grupos de Windows 2000 para controlar los derechos y permisos asignados a la cuenta. Al usar las cuentas y grupos apropiados para la red se garantiza que los usuarios que se conectan a una red se puedan identificar y sólo puedan tener acceso a los recursos permitidos.

Opciones de las cuentas de usuario de Active Directory

Cada cuenta de usuario de Active Directory tiene varias opciones relativas a la seguridad que determinan cómo alguien que ha iniciado una sesión con esa cuenta de usuario en particular se autentica en la red. Algunas de estas opciones son específicas de las contraseñas:

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión

- El usuario no puede cambiar la contraseña
- La contraseña nunca caduca
- Almacenar contraseña utilizando cifrado reversible

Estas opciones se explican por sí mismas, excepto **Almacenar contraseña utilizando cifrado reversible**. Si hay usuarios de equipos Apple que inician sesiones en la red de Windows 2000, seleccione esta opción para sus cuentas de usuario.

Seleccione la opción **Cuenta deshabilitada** para evitar que los usuarios inicien una sesión con la cuenta seleccionada. Algunos administradores usan cuentas deshabilitadas como plantillas para cuentas de usuario comunes.

Puede usar las opciones restantes para configurar información específica de la seguridad para cuentas de usuario de Active Directory:

- La tarjeta inteligente es necesaria para un inicio de sesión interactivo.
- Se confía en la cuenta para su delegación.
- La cuenta es importante y no se puede delegar.
- Usar tipos de cifrado DES para esta cuenta.
- No requerir autenticación previa Kerberos.

Seleccione la opción La tarjeta inteligente es necesaria Para un inicio de sesión interactivo para almacenar de forma segura claves públicas y privadas, contraseñas e información personal de otro tipo para esta cuenta de usuario. Debe haber un lector de tarjetas inteligentes conectado al equipo de usuario y deben tener un número de identificación personal (PIN) para poder conectarse a la red.

Seleccione la opción Se confía en la cuenta Para su delegación para dar a un usuario la capacidad de asignar responsabilidades para la administración de una parte del espacio de nombres del dominio a otro usuario, grupo u organización.

Seleccione la opción **La cuenta es importante y no se puede delegar** si esta cuenta no se puede asignar para su delegación por parte de otra cuenta.

Seleccione la opción **No requerir autenticación previa Kerberos** si la cuenta usa otra implementación del protocolo Kerberos. No todas las implementaciones o distribuciones del protocolo Kerberos utilizan esta característica. El Centro de distribución de claves Kerberos utiliza vales de concesión de vales para obtener la autenticación de red en un dominio. La hora a la que dicho centro emite un vale de este tipo es importante para el protocolo Kerberos. Windows 2000

utiliza otros mecanismos para sincronizar la hora, de forma que la opción de autenticación previa de Kerberos funcione correctamente.

Seleccione la opción Usar tipos de cifrado DES Para esta cuenta si tiene que usar el Estándar de cifrado de datos (DES, *Data Encryption Standard*). DES admite varios niveles de cifrado, entre los que se incluyen MPPE estándar (40 bits), MPPE estándar (56 bits), MPPE de alto nivel (128 bits), DES IPSec (40 bits), DES IPSec de 56 bits y Triple DES IPSec (3DES). Para obtener más información acerca de cualquiera de estos tipos de cifrado, consulte la Ayuda de Windows 2000.

Cuentas de equipo

Todos los equipos donde se ejecuta Windows 2000 o Windows NT que se unen a un dominio tienen una cuenta de equipo. Las cuentas de equipo son similares a las cuentas de usuario y ofrecen un medio para autenticar y auditar el acceso a la red de los equipos y el acceso a los recursos del dominio. Cada equipo conectado a la red debería tener su propia cuenta de equipo única. Las cuentas de equipo también se crean mediante Usuarios y equipos de Active Directory.

Nota: Los equipos donde se ejecuta Windows 98 o Windows 95 no tienen las características de seguridad avanzadas de aquellos equipos donde se ejecuta Windows 2000 o Windows NT, y no se les puede asignar cuentas de equipo en dominios de Windows 2000. Sin embargo, en dominios de Active Directory es posible conectarse a una red y usar equipos con Windows 98 y Windows 95. Para obtener más información, consulte Clientes de Active Directory.

Descripción de la Directiva de grupo

La configuración de la Directiva de grupo influye en las cuentas de usuario y de equipo y se puede aplicar a sitios, dominios o unidades organizativas. Se puede utilizar para configurar opciones de seguridad, administrar aplicaciones, administrar la apariencia del escritorio, asignar secuencias de comandos y redirigir carpetas desde equipos locales a ubicaciones de red.

A continuación se muestran algunos ejemplos de cómo se puede utilizar la configuración de la Directiva de grupo.

- Establecer la longitud mínima de la contraseña y la cantidad máxima de tiempo que una contraseña tendrá validez. Esto se puede configurar para un dominio entero.

- Los administradores pueden instalar automáticamente una aplicación en cada equipo de un dominio en particular o en todos los equipos asignados a un grupo determinado de un sitio específico. Por ejemplo, podría instalar automáticamente Microsoft Outlook en cada equipo del dominio y Microsoft Excel sólo en aquellos equipos que pertenecieran al grupo Contabilidad de un sitio en particular.

- Las secuencias de comandos de inicio y cierre de sesión exclusivas se pueden asignar a las cuentas de usuario de cada unidad organizativa.
- Si los miembros de un grupo determinado utilizan con frecuencia equipos diferentes, los administradores pueden instalar las aplicaciones necesarias en cada uno de estos equipos.
- La carpeta Mis documentos de cualquier usuario se puede redirigir a una ubicación de red. Los usuarios pueden entonces obtener acceso a sus documentos desde cualquier equipo de la red.

Para obtener más información acerca de la Directiva de grupo, consulte Directiva de grupo.

Descripción de la integración con DNS

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

- . DNS es un servicio de resolución de nombres.

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

- Active Directory es un servicio de directorio

Proporciona un depósito de información y servicios para poner la información a disposición de usuarios y aplicaciones. Los clientes de Active Directory envían consultas a los servidores de Active Directory por medio del Protocolo Lightweight de acceso a directorios (LDAP, *Lightweight Directory Access Protocol*). Un cliente de Active Directory consulta DNS con el fin de encontrar un servidor de Active Directory. Active Directory necesita DNS para funcionar.

Active Directory utiliza DNS como un servicio localizador, que resuelve nombres de dominios, sitios y servicios de Active Directory en una dirección IP. Para iniciar una sesión en un dominio de Active Directory, un cliente de Active Directory consulta a sus servidores DNS configurados la dirección IP del servicio LDAP que se ejecuta en un controlador de dominio para un dominio específico. Para obtener más información de cómo los clientes de Active Directory necesitan DNS, consulte Clientes de Active Directory.

Requisitos de los servidores DNS para Active Directory

Para que Active Directory funcione adecuadamente, los servidores DNS deben proporcionar compatibilidad con los registros de recursos de Ubicación de servicios (SRV) descritos en el documento RFC 2052, *Un registro de recursos de DNS para especificar la ubicación de servicios*

(SRV DNS) (A DNS RR for specifying the location of services (DNS SRV)). Los registros de recursos SRV asignan el nombre de un servicio al nombre de un servidor que ofrece ese servicio. Los clientes y los controladores de dominio de Active Directory utilizan registros SRV para determinar las direcciones IP de los controladores de dominio. Aunque no es un requisito técnico de Active Directory, se recomienda encarecidamente que los servidores DNS proporcionen compatibilidad con las actualizaciones dinámicas de DNS descritas en el documento RFC 2136, *Observaciones acerca del uso de componentes del espacio de direcciones de clase A dentro de Internet (Observations on the use of Components of the Class A Address Space within the Internet)*.

El servicio DNS de Windows 2000 permite el uso tanto de registros SRV como de actualizaciones dinámicas. Si se está utilizando un servidor DNS que no es de Windows 2000, compruebe que al menos admita el registro de recursos SRV. Si no es así, debe actualizarse con una versión que admita el uso de registros de recursos SRV. Por ejemplo, los servidores DNS de Windows NT Server 4.0 deben actualizarse con el Service Pack 4 o posterior para admitir registros de recursos SRV. Un servidor DNS que admite registros SRV pero que no permite las actualizaciones dinámicas debe actualizarse con el contenido del archivo Netlogon.dns creado por el Asistente para instalación de Active Directory cuando se promueve un servidor de Windows 2000 Server a controlador de dominio. El archivo Netlogon.dns se describe en la sección siguiente.

Servidores DNS y el Asistente para instalación de Active Directory

De forma predeterminada, el Asistente para instalación de Active Directory intenta encontrar un servidor DNS con autoridad para el dominio que se está configurando de su lista de servidores DNS configurados que acepte una actualización dinámica de un registro de recursos SRV. Si lo encuentra, todos los registros adecuados para el controlador de dominio se registran automáticamente con el servidor DNS una vez reiniciado el controlador de dominio.

Si no se encuentra un servidor DNS que pueda aceptar actualizaciones dinámicas, bien debido a que el servidor DNS no es compatible con ellas o a que no están habilitadas para el dominio, se llevan a cabo los siguientes pasos para asegurar que el proceso de instalación se complete con el registro necesario de los registros de recursos SRV:

1. El servicio DNS se instala en el controlador de dominio y se configura automáticamente con una zona basada en el dominio de Active Directory.

   Por ejemplo, si el dominio de Active Directory que eligió para el primer dominio del bosque era ejemplo.microsoft.com, se agrega una zona cuya raíz está en el nombre de dominio DNS de ejemplo.microsoft.com y se configura para utilizar el servicio DNS en el nuevo controlador de dominio.

2. Se crea un archivo de texto que contiene los registros de recursos DNS adecuados para el controlador de dominio.

El archivo llamado Netlogon.dns se crea en la carpeta %systemroot%\System32\config y contiene todos los registros necesarios para guardar los registros de recursos del controlador de dominio. El servicio Netlogon de Windows 2000 utiliza Netlogon.dns para admitir Active Directory en servidores DNS que no son de Windows 2000.

Si está utilizando un servidor DNS que admite el registro de recursos SRV pero que no admite actualizaciones dinámicas (como un servidor DNS de UNIX o un servidor DNS de Windows NT Server 4.0), puede importar los registros de Netlogon.dns en el archivo de la zona principal adecuada con el fin de configurar manualmente la zona principal en ese servidor para que admita Active Directory.

DESCRIPCIÓN DE LOS GRUPOS

Tipos de grupos

Hay dos tipos de grupos en Windows 2000:

- Grupos de seguridad
- Grupos de distribución

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

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

Para obtener los procedimientos específicos de administración de grupos, consulte Administrar grupos.

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

Convertir grupos de seguridad en grupos de distribución y viceversa

Un grupo de seguridad puede convertirse en un grupo de distribución, y viceversa, en cualquier momento, sólo si el dominio está en modo nativo. No se pueden convertir grupos si el dominio está en modo mixto.

Para obtener información detallada acerca de estos procedimientos, consulte Convertir un grupo a otro tipo de grupo.

Ámbito de un grupo

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

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

- Los grupos de ámbito global pueden tener como miembros grupos y cuentas sólo del dominio en el que se ha definido el grupo y se les pueden conceder permisos en cualquier dominio del bosque. Los grupos de ámbito global se denominan grupos globales

- Los grupos con ámbito local de dominio pueden tener como miembros los grupos y cuentas de un dominio de Windows 2000 o Windows NT, y sólo se pueden utilizar para conceder permisos en un dominio. Los grupos con ámbito local de dominio se denominan grupos locales de dominio.

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

La siguiente tabla resume el comportamiento de los diversos ámbitos de grupo.

Ámbito universal	Ámbito global	Ámbito local de dominio
En los dominios de modo nativo, puede tener como miembros cuentas de cualquier dominio, grupos globales de cualquier dominio y grupos universales de cualquier	En los dominios de modo nativo, puede tener como miembros cuentas del mismo dominio y grupos globales del mismo dominio.	En los dominios de modo nativo, puede tener como miembros cuentas, grupos globales y grupos universales de cualquier dominio, así como grupos locales del mismo dominio.

dominio.		
En los dominios de modo nativo, no se pueden crear grupos de seguridad de ámbito universal.	En los dominios de modo nativo, puede tener como miembros cuentas del mismo dominio.	En los dominios de modo nativo, puede tener como miembros cuentas y grupos globales de cualquier dominio.
Los grupos se pueden incluir en otros grupos (cuando el dominio es de modo nativo) y se les pueden asignar permisos en cualquier dominio	Los grupos se pueden incluir en otros grupos, y se les pueden asignar permisos en cualquier dominio.	Los grupos se pueden incluir en otros grupos locales de dominio y se les pueden asignar permisos sólo en el mismo dominio.
No se puede convertir en un grupo de otro ámbito.	Se puede convertir en un grupo de ámbito universal, siempre y cuando no sea miembro de otro grupo que tenga ámbito global.	Se puede convertir en un grupo de ámbito universal, siempre y cuando no tenga como miembro otro grupo de ámbito local de dominio.

Cambiar el ámbito de un grupo

Al crear un nuevo grupo éste se configura de forma predeterminada como grupo de seguridad de ámbito global, independientemente del modo del dominio actual. Aunque el cambio de ámbito de un dominio no está permitido en los dominios de modo mixto, se pueden realizar las siguientes conversiones en los dominios de modo nativo:

- **Global a universal**. Sin embargo, esta conversión sólo se permite si el grupo no es miembro de otro grupo de ámbito global.
- **Dominio local a universal**. Sin embargo, el grupo que se convierte no puede tener como miembro otro grupo de ámbito local de dominio.

Para obtener información detallada acerca de estos procedimientos, consulte Para cambiar el ámbito de un grupo.

Grupos integrados y predefinidos

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

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

Grupos integrados

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

- Operadores de cuentas
- Administradores
- Operadores de copia de seguridad
- Invitados
- Operadores de impresión
- Replicador
- Operadores de servidores
- Usuarios

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

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

Derecho de usuario	Permite	Grupos a los que está asignado este derecho de forma predeterminada
Tener acceso a este equipo desde la red	Conectar con el equipo a través de la red.	Administradores, Todos, Usuarios avanzados
Hacer copias de seguridad de archivos y carpetas	Hacer copias de seguridad de archivos y carpetas. Este derecho prevalece sobre los permisos de los archivos y carpetas.	Administradores, Operadores de copia de seguridad
Saltarse la comprobación de	Pasar de una carpeta a otra para tener acceso a los archivos, aún en el caso de	Todos

recorrido	que el usuario no tenga premiso de acceso a las carpetas de archivos principales.	
Cambiar la hora del sistema	Establecer la fecha y hora del reloj interno del equipo.	Administradores, Usuarios avanzados
Crear un archivo de paginación	Este derecho no tiene ningún efecto.	Administradores
Depurar programas	Depurar diversos objetos de nivel inferior, por ejemplo, subprocesos.	Administradores
Forzar el apagado desde un sistema remoto	Cerrar un equipo remoto.	Administradores
Aumentar la prioridad de una programación	Aumentar la prioridad de ejecución de un proceso.	Administradores, Usuarios avanzados
Cargar y descargar controladores de dispositivo	Instalar y quitar controladores de dispositivo.	Administradores
Inicio de sesión local	Iniciar una sesión en el equipo a través de su teclado.	Administradores, Operadores de copia de seguridad, Todos, Invitados, Usuarios avanzados y Usuarios
Administrar los registros de auditoría y seguridad	Especificar los tipos de acceso a recursos (por ejemplo, acceso a archivos) que deben incluirse en la auditoría, y ver y borrar el registro de seguridad. Este derecho no permite a un usuario establecer la directiva de auditoría del sistema. Los miembros del grupo Administradores siempre pueden ver y borrar el registro de seguridad.	Administradores
Modificar las variables de entorno del firmware	Modificar las variables de entorno del sistema que se almacenan en la memoria RAM no volátil de los equipos que admiten este tipo de configuración.	Administradores

Perfilar el rendimiento de un proceso individual	Realizar un análisis de rendimiento (muestreo de rendimiento) en un proceso.	Administradores, Usuarios avanzados
Perfilar el rendimiento del sistema	Realizar un análisis de rendimiento (muestreo de rendimiento) en el equipo.	Administradores
Restaurar archivos y carpetas	Restaurar copias de seguridad de archivos y carpetas. Este derecho prevalece sobre los permisos de los archivos y directorios.	Administradores, Operadores de copia de seguridad
Apagar el sistema	Cerrar el sistema Windows 2000.	Administradores, Operadores de copia de seguridad, Todos, Usuarios avanzados y Usuarios.
Tomar posesión de archivos y otros objetos	Tomar posesión de archivos, carpetas, impresoras y otros objetos del equipo (o conectados a él). Este derecho prevalece sobre los permisos que protegen esos objetos. Para obtener más información acerca de los permisos de archivos y carpetas, consulte Permisos de carpetas compartidas.	Administradores

Grupos predefinidos

Los grupos predefinidos incluidos en la carpeta Usuarios de Usuarios y equipos de Active Directory son los siguientes:

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

- Administradores de empresa
- Administradores de Directiva de grupo
- Administradores de esquema

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

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

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

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

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

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

Identidades especiales

Además de los grupos de las carpetas Integrados y Usuarios, Windows 2000 Server incluye varias identidades especiales. Por comodidad, esas identidades se denominan normalmente grupos. Estos grupos especiales no tienen ninguna pertenencia específica que se pueda modificar, pero pueden representar a distintos usuarios en distintos momentos, dependiendo de las circunstancias. Los tres grupos especiales son:

- Todos

Representa a todos los usuarios actuales de la red, incluidos invitados y usuarios de otros dominios. Cada vez que un usuario inicia una sesión en la red, se agrega automáticamente al grupo Todos.

- Red

Representa a los usuarios que tienen acceso en ese momento a un recurso dado a través de la red (a diferencia de los usuarios que tienen acceso a ese mismo recurso tras haber iniciado una sesión localmente en el equipo en el que está ubicado el recurso). Cada vez que un usuario tiene acceso a un recurso a través de la red, se agrega automáticamente al grupo Red.

- Interactivo

Representa a todos los usuarios que tienen iniciada actualmente una sesión en un equipo determinado y tienen acceso a un recurso ubicado en ese equipo (a diferencia de los usuarios que tienen acceso al recurso a través de la red). Cada vez que un usuario tiene acceso a un recurso dado del equipo en el que ha iniciado una sesión, se agrega automáticamente al grupo Interactivo.

Aunque se pueden asignar derechos y permisos sobre recursos a las identidades especiales, no es posible modificar o ver la pertenencia a dichas identidades especiales. Las identidades especiales no se ven cuando se administran grupos y no pueden colocarse en ningún grupo. Los ámbitos de grupo no se aplican a las identidades especiales. Estas identidades especiales se asignan automáticamente a los usuarios cuando inician una sesión o tienen acceso a un recurso determinado.

Grupos en servidores Windows 2000 Professional e independientes

Algunas características de los grupos, como los grupos universales, el anudamiento de grupos y la distinción entre grupos de seguridad y grupos de distribución, sólo existen en los controladores de dominio y servidores miembros de Active Directory. Las cuentas de grupo de los servidores Windows 2000 Professional y Windows 2000 Server independientes funcionan de igual forma que en Windows NT 4.0.

- Localmente sólo se pueden crear grupos locales en el equipo.

- En un equipo, sólo se pueden asignar permisos a un grupo local creado en ese mismo equipo.

Un equipo Windows 2000 Professional que se une a un dominio de Windows 2000 obtiene ventajas adicionales del dominio. Se pueden mostrar los grupos globales y universales del dominio, así como los grupos globales y universales de todos los dominios del bosque. Puede asignar permisos en el equipo local a esos grupos, o incluirlos en grupos del equipo local.

Anidar grupos

Mediante el anidamiento, puede agregar un grupo como miembro de otro grupo. Puede anidar grupos para consolidar la administración de grupos al aumentar el número de cuentas de miembro afectadas y para reducir el tráfico de replicación que causan los cambios de pertenencia de los grupos.

Las opciones de anidamiento dependen de que el dominio esté en modo nativo o en modo mixto. En los grupos de los dominios de modo nativo o en los grupos de distribución de dominios de modo mixto, la pertenencia se determina de la siguiente forma:

- Los grupos de ámbito universal pueden tener como miembros: cuentas, cuentas de equipo, otros grupos de ámbito universal y grupos de ámbito global de cualquier dominio.
- Los grupos de ámbito global pueden tener como miembros: cuentas del mismo dominio y otros grupos de ámbito global del mismo dominio.
- Los grupos de ámbito local de dominio pueden tener como miembros: cuentas, grupos de ámbito universal y grupos de ámbito global, todos ellos de cualquier dominio. También pueden tener como miembros otros grupos de ámbito local de dominio pertenecientes al mismo dominio.

En los dominios de modo mixto, los grupos de seguridad sólo pueden tener los siguientes tipos de miembros:

- Los grupos de ámbito global sólo pueden tener cuentas como miembros.
- Los grupos de ámbito local de dominio pueden tener como miembros cuentas y otros grupos de ámbito global.

Los grupos de seguridad de ámbito universal no se pueden crear en dominios de modo mixto ya que el ámbito universal sólo se puede utilizar en los dominios de Windows 2000 de modo nativo.

Grupos y modos de dominio

La siguiente tabla resume el efecto que tienen los modos de dominio en los grupos. Para obtener más detalles, consulte Tipos de grupos, Ámbito de un grupo y Anidar grupos.

Dominios de modo nativo	Dominios de modo mixto
Los grupos de seguridad y los grupos de distribución pueden tener un ámbito universal.	Sólo los grupos de distribución pueden tener un ámbito universal.
Está permitido el anidamiento de grupos	En los grupos de seguridad, el anidamiento de grupos

completos.	está limitado a los grupos con ámbito local de dominio cuyos grupos miembros sean de ámbito global (norma de Windows NT 4.0). En los grupos de distribución está permitido el anidamiento de grupos completos.
Los grupos se pueden convertir a voluntad de grupos seguridad a grupos de distribución y viceversa. Los grupos que son de ámbito global o local de dominio se pueden convertir en grupos de ámbito universal.	No se permite la conversión de grupos.

En los dominios de modo nativo y de modo mixto, los contactos y cuentas pueden ser miembros de cualquier grupo.

Cómo afectan los grupos al rendimiento de la red

Cuando un usuario inicia una sesión en una red de Windows 2000, el controlador de dominio de Windows 2000 determina a qué grupo pertenece el usuario. Windows 2000 crea un testigo de seguridad y lo asigna al usuario. El testigo de seguridad incluye el Id. de la cuenta de usuario y el Id. de seguridad de todos los grupos de seguridad a los que pertenece el usuario. La pertenencia a grupos puede afectar al rendimiento de la red a través de:

- Los efectos en el inicio de sesión
- La replicación de grupos de ámbito universal
- El ancho de banda de la red

Efectos en el inicio de sesión

La generación del testigo de seguridad es un proceso prolongado; por ello, cuanto mayor sea el número de grupos de seguridad a los que pertenece el usuario, más tiempo se necesita para generar el testigo de seguridad de ese usuario y más tiempo tardará ese usuario en iniciar una sesión en la red. La importancia de este efecto depende del ancho de banda de la red y de la configuración del controlador de dominio que se ocupa del proceso de inicio de sesión.

A veces, puede que desee crear un grupo sólo para propósitos de correo electrónico, sin tener la intención de utilizarlo para asignar derechos y permisos a sus miembros. Para mejorar el rendimiento en los inicios de sesión, esos grupos se deben crear como grupos de distribución, no como grupos de seguridad. Así se reduce el tamaño del testigo y el tiempo que se tarda en

generarlo, ya que los grupos de distribución se pasan por alto cuando Windows 2000 genera el testigo de seguridad del usuario durante el proceso de inicio de sesión.

Replicación de un grupo universal

Los cambios a los datos almacenados en el catálogo global se replican en todos los catálogos globales del bosque. Los grupos que tienen un ámbito universal *y sus miembros* están incluidos en el catálogo global. Siempre que cambia un miembro de un grupo de ámbito universal, toda la pertenencia al grupo debe replicarse en todos los catálogos globales del bosque o el árbol de dominios.

Los grupos de ámbito global o local de dominio también se incluyen en el catálogo global, pero no se incluyen sus miembros. Esto reduce el tamaño del catálogo global y reduce enormemente el tráfico de duplicación necesario para mantener actualizado el catálogo global. Puede mejorar el rendimiento de la red si utiliza grupos de ámbito global o local de dominio para los objetos del directorio que cambian con frecuencia.

Ancho de banda de la red

El testigo de seguridad de cada usuario se envía a todos los equipos a los que tiene acceso el usuario para que el equipo de destino pueda determinar si el usuario tiene los permisos o derechos necesarios en ese equipo al comparar todos los Id. de seguridad contenidos en el testigo con los permisos enumerados para los recursos de ese equipo. El equipo de destino también comprueba si cualquiera de los Id. de seguridad del testigo pertenecen a uno de los grupos locales del equipo de destino.

Cuanto mayor sea el número de grupos a los que pertenece el usuario, mayor será el tamaño de su testigo de seguridad. Si la red tiene un gran número de usuarios, los efectos que tienen esos testigos de seguridad de gran tamaño en el ancho de banda de la red y en la capacidad de proceso del controlador del dominio pueden ser significativos.

Por ejemplo, supongamos que un dominio determinado contiene 500 recursos de archivos compartidos, cada uno con su asignación correspondiente a un grupo de ámbito local de dominio al que se ha concedido acceso de lectura. Si la mayor parte de los usuarios tienen acceso de lectura a muchos de los recursos compartidos, se agregarán aproximadamente 500 Id. de seguridad a los testigos de la mayor parte de los empleados. Esto puede llevar mucho tiempo y agregar una cantidad considerable de tráfico de datos a la red.