



Windows Server® 2008

Por ReparaciondePC.cl

Más manuales en

<http://reparaciondepc.cl/blog/manuales-gratis>

Microsoft®

INDICE

FUNDAMENTOS DE WINDOWS SERVER 2008	9
INTRODUCCIÓN A LA GESTIÓN DE REDES USANDO WINDOWS SERVER 2008.....	10
<i>Evolución de los sistemas operativos Microsoft para Servidores.....</i>	10
CARACTERÍSTICAS GENERALES DEL SERVIDOR MICROSOFT	11
<i>Identificación y acceso a la infraestructura de la red</i>	13
<i>Seguridad y políticas</i>	13
<i>Implementación rápida.....</i>	13
<i>Componentes de Windows Deployment Services</i>	14
<i>Cambios en las características RIS</i>	15
<i>Servidores de administración sencilla</i>	16
<i>Soporte para tareas de oficina.....</i>	18
<i>Soporte para acceso centralizado a las aplicaciones.....</i>	18
<i>Implementación de Servicios y Aplicaciones Web.....</i>	18
<i>Confiabilidad.....</i>	19
<i>Protección de datos</i>	19
<i>Incremento de la productividad con Hyper-V</i>	19
EDICIONES DE WINDOWS SERVER 2008.....	20
EDICIONES DE SERVIDORES SIN HYPER-V.....	21
ROLES DEL WINDOWS SERVER 2008	22
GESTIÓN DE MÁQUINAS VIRTUALES	25
ENTENDERÁ LOS CONCEPTOS DE EQUIPO VIRTUAL	26
<i>Instalar Microsoft Virtual Machine</i>	27
<i>Crear una máquina Virtual.....</i>	28
<i>Agregar o quitar componentes de hardware a la máquina virtual</i>	31
<i>BIOS de la máquina Virtual</i>	32
<i>Utilizando CD o DVD físico</i>	33
<i>Utilizando archivos ISO</i>	34
<i>Apagar equipo virtual</i>	34
TRABAJANDO CON VIRTUAL SERVER.....	35
<i>Requisitos de instalación.....</i>	35
<i>Instalación.....</i>	36
<i>Configurar equipos virtuales.....</i>	38
<i>Iniciar equipos virtuales</i>	40
<i>Crear redes virtuales</i>	41
<i>Gestión de máquinas virtuales.....</i>	41
INSTALACIÓN DE WINDOWS SERVER 2008.....	43
INSTALACIÓN DE WINDOWS SERVER 2008.....	44
<i>Opción de Instalación con Hyper-V</i>	44
<i>Opción de Instalación Básica</i>	44
<i>Activar Hyper-V en una instalación de Servidor Básico.....</i>	45
<i>Dispositivos de hardware recomendados</i>	45
<i>Proceso de Instalación de Windows Server 2008.....</i>	46
<i>Seguridad del servidor</i>	48
<i>Requisitos del sistema.....</i>	48
<i>Compatibilidad.....</i>	49
<i>Licencia del producto</i>	49
<i>Administrar las licencias por volumen.</i>	50
<i>Activación del producto</i>	50
<i>Configuración de sistemas múltiples.....</i>	50



<i>Automatización de las instalaciones de Windows</i>	51
GESTIÓN DE EQUIPO VIRTUAL	57
<i>Liberar el Mouse</i>	57
<i>Enviar teclas Control + Alt + Supr</i>	57
<i>Guardar estado y cerrar equipo virtual</i>	57
<i>Reanudar equipo virtual</i>	58
ROLES DEL SERVIDOR	59
<i>Agregar y/o Quitar roles a un Servidor</i>	59
<i>Tareas de configuración Inicial</i>	60
<i>Comandos a través de la Consola</i>	60

IMPLEMENTACIÓN DE ACTIVE DIRECTORY EN LA INFRAESTRUCTURA DE RED 63

INTRODUCCIÓN A LOS SERVICIOS DE DIRECTORIO.....	64
TERMINOLOGÍA DE ACTIVE DIRECTORY	64
PLANIFICACION DE ESPACIO DE NOMBRES Y DOMINIOS	66
<i>Arboles y bosques</i>	67
<i>Dominios y unidades organizativas</i>	67
<i>Diseño de una estructura de dominios</i>	67
INSTALACIÓN DE ACTIVE DIRECTORY	68
<i>Instalar el Servicio de controlador de dominio</i>	68
<i>Instalar el primer controlador de dominio</i>	69
ACCESO A LAS HERRAMIENTAS PARA GESTIONAR EL ACTIVE DIRECTORY	73
RECONOCIMIENTO DEL ENTORNO DE TRABAJO DE ACTIVE DIRECTORY	74
COPIA DE SEGURIDAD DEL ACTIVE DIRECTORY.....	75
<i>Instalación de la característica de copia de seguridad</i>	75
<i>Realizar copia de seguridad del Estado del Sistema</i>	76
<i>Recuperar el SystemState a partir de una copia de seguridad.</i>	78

VIRTUALIZACIÓN DE SERVIDORES 79

INTRODUCCIÓN A LA VIRTUALIZACIÓN EN WINDOWS SERVER 2008.....	80
REVISIÓN DE ARQUITECTURAS DE 32 Y 64 BITS	81
<i>Entendiendo el tema de Arquitecturas</i>	81
<i>Arquitectura x86</i>	81
<i>Arquitectura x64</i>	82
<i>Relación con la Memoria</i>	83
<i>32 bits contra 64 bits</i>	84
<i>Disponibilidad del Software para x86 y x64</i>	85
<i>Tecnología de virtualización</i>	85
<i>Beneficios de la Virtualización</i>	85
ESCENARIOS DE VIRTUALIZACIÓN	86
<i>Consolidación de Servidores</i>	86
<i>Continuidad del negocio</i>	86
<i>Pruebas y desarrollo</i>	86
<i>Delegaciones remotas</i>	86
CARACTERÍSTICAS DE WINDOWS SERVER VIRTUALIZATION	87
<i>Windows Hypervisor</i>	87
<i>Soporta clientes de 64 bits</i>	87
<i>Soporte para múltiples clientes</i>	87
<i>Migración de las máquinas virtuales</i>	87
<i>Nueva arquitectura de virtualización de dispositivos</i>	87
<i>Manipulación VHD Offline</i>	87
TIPOS DE VIRTUALIZACIÓN	88
<i>Virtualización de Máquinas (Servidores)</i>	88

<i>Virtualización de Máquinas (Puesto de trabajo)</i>	88
<i>Virtualización de Aplicaciones</i>	88
<i>Virtualización de Presentación</i>	88
<i>Virtualización de almacenamiento</i>	88
<i>Virtualización de red</i>	89
INSTALACIÓN DE SISTEMAS VIRTUALIZADOS.....	89
<i>Instalación de la función Hyper-V</i>	89
<i>Iniciar el Administrador Hyper-V</i>	90
<i>Crear equipo Virtual</i>	91
<i>Instalar un Sistema Operativo</i>	93
<i>Actividades para Instalar Windows XP y Linux</i>	94
GESTIÓN DE UNIDADES ORGANIZATIVAS Y USUARIOS.....	95
USO DE UNIDADES ORGANIZATIVAS.....	96
<i>Creación de Unidades organizativas</i>	96
<i>Propiedades de las unidades organizativas</i>	98
<i>Traslado de unidades organizativas</i>	99
<i>Eliminación de Unidades organizativas</i>	100
<i>Elementos disponibles dentro de una OU</i>	101
CREACIÓN DE CUENTAS DE USUARIO	101
<i>Denominación de cuentas de usuario</i>	101
<i>Tipos de cuentas</i>	102
<i>Consideraciones sobre las cuentas de usuario y de sistema:</i>	103
<i>Opciones de las cuentas de usuario</i>	104
<i>Creación de cuentas de usuario de dominio</i>	104
<i>Creación de cuentas de usuario locales</i>	106
ADMINISTRACION DE CUENTAS DE USUARIO	108
<i>Busqueda de cuentas de usuario</i>	108
<i>Deshabilitación de cuentas de usuario</i>	108
<i>Eliminación de cuentas de usuario</i>	109
<i>Traslado de cuentas de usuario</i>	109
<i>Desbloqueo de cuentas de usuario</i>	109
<i>Propiedades de la cuenta de usuario</i>	109
<i>Opciones de cuenta</i>	111
PERFILES DE USUARIO.....	113
<i>Directorio Particular</i>	113
ESTRATEGIAS DE SEGURIDAD A TRAVÉS DE GRUPOS	115
INTRODUCCION A GRUPOS	116
<i>Grupos predeterminados</i>	116
<i>Ámbito de grupo</i>	117
<i>Tipos de grupo</i>	118
<i>Identidades especiales</i>	119
<i>Información sobre creación de grupos</i>	120
NIVELES DE FUNCIONAMIENTO	120
<i>Cambiar el nivel funcional del dominio</i>	121
PLANIFICACION DE ESTRATEGIAS DE GRUPO	122
<i>Determinación de los nombres de grupo</i>	122
IMPLEMENTACIÓN DE GRUPOS.....	124
<i>Creación de grupos</i>	124
GESTIÓN DE RECURSOS COMPARTIDOS	129
ASPECTOS FUNDAMENTALES DEL USO COMPARTIDO DE ARCHIVOS.....	130
COMPARTIR ARCHIVOS DESDE CUALQUIER CARPETA DEL EQUIPO	130
COMPARTIR ARCHIVOS DESDE LA CARPETA PÚBLICA DEL EQUIPO	130



QUÉ MÉTODO DE COMPARTICIÓN SE VA A UTILIZAR	131
OTRAS MANERAS DE COMPARTIR ARCHIVOS.....	131
ESTABLECER PERMISOS PARA CARPETAS COMPARTIDAS.....	132
ESTABLECER PERMISOS EN CARPETAS COMPARTIDAS	132
<i>Para establecer permisos en una carpeta compartida mediante la interfaz de Windows</i>	133
<i>Para especificar permisos de archivos para un usuario mediante una línea de comandos</i>	133
ADMINISTRACIÓN DE PERMISOS PARA CARPETAS COMPARTIDAS.....	134
PERMISOS NTFS	134
PERMISOS SMB.....	135
PERMISOS NFS.....	136
ADMINISTRACIÓN DE UN RECURSO COMPARTIDO EXISTENTE	137
<i>Acceso al Administrador</i>	138
VISUALIZACIÓN Y MODIFICACIÓN DE LAS PROPIEDADES DE UNA CARPETA COMPARTIDA.....	139
<i>Para ver o modificar las propiedades de una carpeta o volumen compartido</i>	139
<i>Consideraciones adicionales</i>	139
DEJAR DE COMPARTIR UN RECURSO	139
<i>Para dejar de compartir una carpeta o un volumen</i>	139
<i>Consideraciones adicionales</i>	140
CREAR UN ACCESO DIRECTO A UNA UNIDAD DE RED (ASIGNAR)	140
<i>Accesos directos a ubicaciones de Internet como sitios web o sitios FTP.</i>	140
COMPARTIR CARPETAS	140

TRABAJANDO CON PERMISOS NTFS..... 143

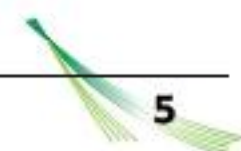
SISTEMA DE ARCHIVOS NTFS.....	144
<i>Comparación de los sistemas de archivos NTFS y FAT</i>	144
NTFS.....	144
FAT32	144
CONVERTIR UN DISCO DURO O PARTICIÓN AL FORMATO NTFS	144
¿QUÉ SON LOS PERMISOS?	145
LO QUE SE DEBE SABER ANTES DE APLICAR PERMISOS A UN ARCHIVO O CARPETA.....	146
<i>Para aplicar permisos a un archivo o carpeta</i>	146
¿EXISTE ALGÚN RIESGO AL APLICAR PERMISOS A UN ARCHIVO O CARPETA?.....	147
¿QUÉ ES EL CIFRADO?	147
¿QUÉ ES EL SISTEMA DE CIFRADO DE ARCHIVOS (EFS)?.....	147
MEDIDAS PARA EVITAR LA PÉRDIDA DE CLAVES DE CIFRADO.....	148
COPIA DE SEGURIDAD DE LAS CLAVES DE CIFRADO	148
PERMISOS DE RECURSO COMPARTIDO Y NTFS EN UN SERVIDOR DE ARCHIVOS	149
<i>Consideraciones adicionales</i>	150
PERMISOS DE ARCHIVOS Y CARPETAS.....	151
<i>Importante</i>	152
CÓMO AFECTA LA HERENCIA A LOS PERMISOS DE ARCHIVOS Y CARPETAS	152
DEFINIR, VER, CAMBIAR O QUITAR PERMISOS ESPECIALES	153
<i>Para definir, ver, cambiar o quitar permisos especiales</i>	153
<i>Precaución</i>	153
DETERMINAR DÓNDE APLICAR PERMISOS.....	154
<i>Importante</i>	154
<i>Cuando la casilla Aplicar estos permisos a objetos y/o contenedores sólo dentro de este contenedor está desactivada</i>	155
<i>Cuando la casilla Aplicar estos permisos a objetos y/o contenedores sólo dentro de este contenedor está activada</i>	155
CONFIGURACIÓN DE SEGURIDAD AVANZADA EN PERMISOS	156
CUOTAS DE DISCO	157
<i>Administración de cuotas</i>	157
<i>Crear una cuota</i>	158

SERVICIOS DE IMPRESIÓN 161

TERMINOLOGÍA EMPLEADA EN LOS SERVICIOS DE IMPRESIÓN	162
INSTALACION DE IMPRESORAS EN EL SERVIDOR.....	162
<i>Para agregar una impresora de red, inalámbrica o Bluetooth</i>	162
<i>Para agregar una impresora local</i>	163
<i>Quitar una impresora</i>	163
CONFIGURACION DE SEGURIDAD DE IMPRESORAS	164
OPCIONES DE LOS SERVIDORES DE IMPRESIÓN	164
<i>Configuracion de puertos</i>	164
IMPRESORAS Y ACTIVE DIRECTORY	165
<i>Publicacion de impresoras</i>	165
DISTRIBUCIÓN DE CONTROLADORES A TRAVÉS DE LA RED	165

FUNDAMENTOS SOBRE DIRECTIVAS DE GRUPO 167

INTRODUCCIÓN A ADMINISTRACIÓN DE DIRECTIVAS DE GRUPO	168
MODIFICAR OBJETOS DE VARIAS DIRECTIVAS DE GRUPO LOCAL.....	168
<i>Para modificar objetos de varias directivas de grupo local</i>	169
<i>Consideraciones adicionales</i>	169
APERTURA DEL EDITOR DE DIRECTIVAS DE GRUPO LOCAL	169
<i>Para abrir el Editor de directivas de grupo local desde la línea de comandos</i>	169
<i>Para abrir el Editor de directivas de grupo local como complemento de MMC</i>	170
CONSOLA DE ADMINISTRACIÓN DE DIRECTIVAS DE GRUPO.....	170
ABRIR GPMC	170
PARA INICIAR GPMC	170
PERSONALIZAR LA INTERFAZ DE USUARIO DE GPMC.....	171
PARA CONFIGURAR LAS OPCIONES DE LA INTERFAZ DE USUARIO	171
CREAR UN OBJETO DE DIRECTIVA DE GRUPO	172
<i>Para crear un objeto de directiva de grupo</i>	172
EDITAR UN OBJETO DE DIRECTIVA DE GRUPO	173
<i>Para editar un objeto de directiva de grupo</i>	173
BUSCAR UN OBJETO DE DIRECTIVA DE GRUPO	173
<i>Para buscar un objeto de directiva de grupo</i>	173
AGREGAR UN DOMINIO	174
<i>Para agregar un dominio en GPMC</i>	174
ESPECIFICAR UN CONTROLADOR DE DOMINIO	175
<i>Para especificar un controlador de dominio</i>	175
AGREGAR UN BOSQUE.....	175
<i>Para agregar un bosque</i>	175
AGREGAR UN SITIO	176
<i>Para agregar un sitio</i>	176
VER, IMPRIMIR Y GUARDAR UN INFORME DE CONFIGURACIÓN DE DIRECTIVA DE GRUPO	176
<i>Para ver, imprimir y guardar un informe de configuración de Directiva de grupo</i>	176
COPIAR UN OBJETO DE DIRECTIVA DE GRUPO.....	177
<i>Para copiar un objeto de directiva de grupo (método de arrastrar y colocar)</i>	177
<i>Para copiar un objeto de directiva de grupo (método de hacer clic con el botón secundario)</i>	177
IMPORTAR LA CONFIGURACIÓN DE UN OBJETO DE DIRECTIVA DE GRUPO	177
<i>Para importar la configuración de un objeto de directiva de grupo</i>	177
TRABAJAR CON TABLAS DE MIGRACIÓN	178
VINCULAR UN OBJETO DE DIRECTIVA DE GRUPO	178
<i>Para vincular un GPO</i>	178
FILTRAR CON GRUPOS DE SEGURIDAD	179
<i>Para filtrar con grupos de seguridad</i>	179
EXIGIR UN VÍNCULO DE OBJETO DE DIRECTIVA DE GRUPO	179
<i>Para exigir un vínculo de objeto de directiva de grupo</i>	179





DESACTIVAR LA CONFIGURACIÓN DE USUARIO O DEL EQUIPO EN UN OBJETO DE DIRECTIVA DE GRUPO	180
<i>Para deshabilitar la configuración de usuario o equipo en un objeto de directiva de grupo.....</i>	180
DESACTIVAR UN VÍNCULO DE OBJETO DE DIRECTIVA DE GRUPO	180
<i>Para deshabilitar un vínculo de objeto de directiva de grupo.....</i>	180
BLOQUEAR HERENCIA.....	181
<i>Para bloquear la herencia.....</i>	181
DETERMINAR EL CONJUNTO RESULTANTE DE DIRECTIVAS	181
<i>Para determinar el conjunto resultante de directivas.....</i>	181
SIMULAR UN CONJUNTO RESULTANTE DE DIRECTIVAS MEDIANTE MODELADO DE DIRECTIVAS DE GRUPO	182
<i>Para simular un conjunto resultante de directivas mediante Modelado de directivas de grupo ..</i>	182
DELEGAR PERMISOS PARA VINCULAR OBJETOS DE DIRECTIVA DE GRUPO	183
<i>Para delegar permisos para vincular objetos de directiva de grupo.....</i>	183

MANTENIMIENTO LA OPERATIVIDAD DEL SERVIDOR..... 185

INTRODUCCIÓN AL MONITOR DE CONFIABILIDAD Y RENDIMIENTO DE WINDOWS.....	186
PARA INICIAR EL MONITOR DE CONFIABILIDAD Y RENDIMIENTO DE WINDOWS.....	186
<i>Vista de recursos.....</i>	186
<i>Monitor de sistema.....</i>	186
<i>Monitor de confiabilidad.....</i>	186
ACCESO A LAS CARACTERÍSTICAS DEL MONITOR DE CONFIABILIDAD Y RENDIMIENTO.....	187
<i>Miembros del grupo Usuarios.....</i>	187
<i>Miembros del grupo Usuarios del monitor de sistema.....</i>	187
<i>Miembros del grupo Usuarios del registro de rendimiento.....</i>	187
USAR EL MONITOR DE CONFIABILIDAD PARA SOLUCIONAR PROBLEMAS	188
<i>Gráfico de estabilidad del sistema.....</i>	188
<i>Visualización de datos históricos.....</i>	188
<i>Informe de estabilidad del sistema.....</i>	188
<i>Eventos de confiabilidad.....</i>	189
<i>Cambios del reloj del sistema.....</i>	189
<i>Instalaciones y desinstalaciones de software.....</i>	189
<i>Errores de aplicación.....</i>	189
<i>Errores de hardware.....</i>	190
<i>Errores de Windows.....</i>	190
<i>Errores varios.....</i>	190
<i>Errores de software.....</i>	191
<i>Errores de hardware.....</i>	191
<i>Perspectiva general.....</i>	191
NUEVAS CARACTERÍSTICAS DEL MONITOR DE CONFIABILIDAD Y RENDIMIENTO DE WINDOWS.....	192
<i>Conjuntos de recopiladores de datos.....</i>	192
<i>Asistentes y plantillas para crear registros.....</i>	192
<i>Vista de recursos.....</i>	192
<i>Monitor de confiabilidad.....</i>	192
<i>Configuración de propiedades unificada para toda la recopilación de datos, incluida la programación.....</i>	193
<i>Informes de diagnóstico fácil de usar.....</i>	193
SUPERVISAR LA ACTIVIDAD DEL SISTEMA CON VISTA DE RECURSOS.....	193
<i>Iniciar Vista de recursos.....</i>	193
<i>Identificar el uso de los recursos en Vista de recursos.....</i>	194
<i>Navegación por vista de recursos.....</i>	194
<i>Detalles de Vista de recursos.....</i>	194
<i>Consideraciones adicionales.....</i>	196
USO DEL MONITOR DE RENDIMIENTO.....	196
<i>Para iniciar el Monitor de rendimiento.....</i>	197
<i>Para conectarse a un equipo remoto con el Monitor de rendimiento.....</i>	197

CONFIGURAR LA PANTALLA DEL MONITOR DE RENDIMIENTO	197
<i>Para configurar la pantalla del Monitor de rendimiento</i>	197
<i>Para guardar la pantalla del Monitor de rendimiento actual como página web</i>	197
<i>Para guardar la pantalla del Monitor de rendimiento actual como imagen</i>	198
<i>Consideraciones adicionales</i>	198
USAR EL MONITOR DE CONFIABILIDAD.....	198
INICIAR EL MONITOR DE CONFIABILIDAD	198
<i>Para abrir el Monitor de confiabilidad en Microsoft Management Console</i>	198
VER EL MONITOR DE CONFIABILIDAD EN UN EQUIPO REMOTO	199
HABILITAR LA RECOPIACIÓN DE DATOS PARA EL MONITOR DE CONFIABILIDAD.....	199
<i>Para habilitar la tarea programada RACAgent</i>	199
DESCRIPCIÓN DEL ÍNDICE DE ESTABILIDAD DEL SISTEMA	200
INTRODUCCIÓN AL PROGRAMADOR DE TAREAS.....	200
DESENCADENADORES Y ACCIONES.....	200
<i>Desencadenadores</i>	201
<i>Configuración del desencadenador</i>	201
CONFIGURACIÓN AVANZADA	204
ACCIONES.....	205
INICIO DE UN PROGRAMA	205
CONFIGURACIÓN DE TAREAS.....	206
<i>Permitir que la tarea se ejecute a petición</i>	206
<i>Ejecutar la tarea de inmediato si se pasó por alto algún inicio programado</i>	206
<i>Si la tarea no se ejecuta, reiniciarla cada: <período de tiempo></i>	206
<i>Detener la tarea si se ejecuta por más: <período de tiempo></i>	206
<i>Hacer que la tarea se detenga si no finaliza cuando se solicite</i>	206
<i>Eliminar la tarea si no está programada para ejecutarse de nuevo después de: <período de tiempo></i>	206
<i>Aplicar la siguiente regla si la tarea ya está en ejecución:</i>	207
INICIAR EL PROGRAMADOR DE TAREAS.....	207
<i>Para ejecutar el Programador de tareas mediante la interfaz de Windows</i>	207
<i>Para ejecutar el Programador de tareas desde la línea de comandos</i>	207



Fundamentos de Windows Server 2008

En este capítulo trataremos:

- Identificará las características de Windows Server 2008
- Conocerá la infraestructura de la red Microsoft

Introducción:

Microsoft Windows Server 2008 está diseñado para ofrecer a las organizaciones la plataforma más productiva para virtualización de cargas de trabajo, creación de aplicaciones eficaces y protección de redes. Ofrece una plataforma segura y de fácil administración, para el desarrollo y alojamiento confiable de aplicaciones y servicios web. Del grupo de trabajo al centro de datos, Windows Server 2008 incluye nuevas funciones de gran valor y eficacia y mejoras impactantes en el sistema operativo base.



Introducción a la gestión de redes usando Windows Server 2008



En la pequeña, mediana y gran organización se necesita control; control concerniente a quién tiene permitido el acceso a los recursos de información de la organización, cómo se verifica la identidad de alguien, qué se le permite hacer, cómo hacer un efectivo control y cómo almacenar los incidentes para una auditoría e incrementar la eficiencia de la infraestructura de red.

Windows Server 2008 proporciona a los profesionales de TI más control sobre sus servidores e infraestructura de red y les permite centrarse en las necesidades críticas del negocio. Capacidades mejoradas en secuencias de comandos y automatización de tareas, como las que ofrece Windows PowerShell, ayudan a los profesionales de TI a automatizar tareas comunes de TI. La instalación y administración basadas en funciones con Administrador del Servidor facilita la tarea de administrar y proteger las múltiples funciones de servidor en una empresa. La nueva consola del Administrador del servidor proporciona un único origen para administrar la configuración del servidor y la información del sistema. El personal de TI puede instalar sólo las funciones y características que sean necesarias, y hay asistentes que automatizan muchas de las tareas de implementación de sistemas que tardan más tiempo. Herramientas mejoradas de administración del sistema, como el Monitor de rendimiento y confiabilidad, ofrecen información sobre sistemas y alertan al personal de TI sobre problemas potenciales antes de que sucedan.

Evolución de los sistemas operativos Microsoft para Servidores

Windows Server 2008 es la nueva versión del SO de Microsoft para SERVIDORES. Es la evolución de Windows Server 2003 sobre el núcleo de Windows Vista, los cambios en el Kernel permiten implementar nuevas funcionalidades a niveles más altos y sacar partido del nuevo Hardware. Posee:

- Gestión de la Memoria (NUMA).
- Windows Hardware Error Architecture (WHEA).
- Seguridad: Protección contra el parcheo del Kernel, Integridad y firmado de código.
- Mejoras Hardware: ACPI3.0, PCI Express y Bios EFI.



Características generales del Servidor Microsoft

Windows Server 2008 tiene las siguientes características generales:

1. Identificación y acceso a la infraestructura de la red
2. Seguridad y políticas
3. Implementación rápida
4. Servidores de administración sencilla
5. Soporte para tareas de oficina
6. Soporte para acceso centralizado a las aplicaciones
7. Implementación de Servicios y Aplicaciones Web
8. Confiabilidad
9. Protección de datos
10. Incremento de la productividad con Hyper-V

Una característica generalmente no suele describir la función principal del servidor. En cambio, describe una función auxiliar o de soporte de un servidor. Un administrador instala típicamente una característica no como la función principal del servidor, pero para aumentar la funcionalidad de un rol instalado. Por ejemplo, Failover Clustering es una característica que los administradores pueden optar por instalar después de la instalación de roles específicos, como el Servicios de Archivo, para hacer el rol de Servicios de Archivo más redundante.

Las siguientes características están disponibles en Windows Server 2008 y se pueden instalar mediante el uso de Server Manager:

Característica	Descripción
Funciones Microsoft .NET Framework 3.0	Microsoft. NET Framework 3.0 combina el poder de .NET Framework 2.0 APIs con las nuevas tecnologías para la construcción de aplicaciones que ofrecen atractivas interfaces de usuario.
BitLocker Drive Encryption	BitLocker Drive Encryption ayuda a proteger los datos en caso de pérdidas, robos, o retiro inadecuado de los ordenadores con la encriptación de todo el volumen.
Extensiones de Servidor BITS	Servicio de Transferencia Inteligente en Segundo plano (BITS) las Extensiones de Servidor permiten un servidor para recibir los archivos cargados por los clientes que utilizan BITS.
Kit de Administración Connection Manager	Kit de administración Connection Manager (CMAK) genera los perfiles Connection Manager.
Desktop Experience	Desktop Experience incluye características de Windows Vista®, tales como Windows Media Player, temas de escritorio, y gestión de fotografías.
Gestión de Políticas de Grupo	La Gestión de Políticas de Grupo hace más fácil de entender, desplegar, gestionar y solucionar problemas de implementaciones de Políticas de Grupo.



Característica	Descripción
Internet Printing Client	Internet Printing Client le permite usar HTTP para conectarse y hacer uso de las impresoras que se encuentran en los servidores de impresión de la Web.
Internet Storage Name Server (iSNS)	Internet Storage Name Server (iSNS) proporciona servicios de hallazgo para redes de área de almacenamiento Internet Small Computer System Interface (iSCSI).
LPR Port Monitor	Line Printer Remote (LPR) Port Monitor permite a los usuarios que tienen acceso a ordenadores basados en UNIX para imprimir en dispositivos conectados a ellos.
Message Queuing	Message Queuing (Mensaje en Cola) proporciona la entrega de mensajes garantiza, un enrutamiento eficaz, seguridad, y mensajería basada en prioridades entre aplicaciones

Algunas otras características se enumeran a continuación (consulte la web de Microsoft para mayor información)

- Multipath I / O
- Peer Name Resolution Protocol
- qWave
- Asistencia remota
- Herramientas de Administración de Servidor Remoto
- Removable Storage Manager
- RPC sobre HTTP Proxy
- Servicios para NFS
- SMTP Server
- Storage Manager para SANs
- Servicios TCP/IP Simples
- Servicios SNMP
- Subsistema para Aplicaciones basadas en UNIX
- Cliente Telnet
- Servidor Telnet
- Trivial File Transfer Protocol (TFTP) Client
- Failover Clustering
- Equilibrio de la carga en la red
- Windows Server Backup
- Administrador de Recursos del Sistema Windows
- Servidor WINS
- Servicio de Wireless LAN
- Base de Datos Interna de Windows
- Windows PowerShell
- Servicio de Activación de Procesos Windows

Identificación y acceso a la infraestructura de la red



Es necesario proveer de una identidad para acceso a la infraestructura de red. Esta información permitirá acceder a los recursos de la red. Para controlar quién, a qué hora y cómo accederá a dichos recursos se efectúa a través de una Identity y un Access Management (IDA).

Todas las organizaciones necesitan un IDA para proveer servicios de administración de la información acerca de los usuarios y computadoras, haciendo disponibles los recursos y controlando el acceso a ellos, simplificando el uso de las herramientas que permiten hacerlo, protegiendo la información sensible de la empresa adecuadamente.

Seguridad y políticas



Hacer que los usuarios y los equipo estén conectados a la red no asegura el acceso, es necesario utilizar estándares de seguridad, o mecanismos tales como: Group Policy y autenticación a través de Active Directory, o la nueva plataforma Network Access Protection (NAP).

NAP provee una plataforma para que cualquiera conectado a la red pase por un conjunto de políticas de seguridad antes de ingresar a la infraestructura de red.

Network Policy and Access Services (NPAS) en Windows Server® 2008 incluye las tecnologías necesarias para establecer redes privadas virtuales (VPN), conexiones de acceso bajo demanda y accesos inalámbricos con protección 802.11. Con NPAS se pueden definir y aplicar políticas para la autenticación del acceso a la red, autorización y control de salud del cliente remoto.

En Windows Server 2008 el control del acceso y seguridad de red se hace aplicando diversas tecnologías y protocolos, como el **Servidor de Política de Red** (NPS, Network Policy Server), el servicio **Routing and Remote Access Service** (RRAS), **Health Registration Authority** (HRA), y el protocolo **HCAP** (Host Credential Authorization Protocol).

Se puede implementar NPS como un servidor y proxy RADIUS (Remote Authentication Dial-in User Service), y como servidor de políticas de protección de acceso a la red (NAP, Network Access Protection). NAP permite asegurarse de que las máquinas que se conectan a la red cumplen con las directivas corporativas en materia de salud y seguridad establecidas en la organización

Implementación rápida

Windows Deployment Services (WDS) permite una implantación y adopción rápida de los sistemas operativos Windows: Se puede utilizar para instalar máquinas nuevas a partir de una instalación basada en red. Esto supone que no hay que estar presente físicamente en cada máquina y que no hay necesidad de instalar el sistema operativo directamente desde un CD o un DVD.



Componentes de Windows Deployment Services

Se organizan en tres categorías:

- **Componentes de servidor:**

Entre los que se incluye un servidor de PXE (Pre-Boot Execution Environment) y TFTP (Trivial File Transfer Protocol) para el arranque del sistema cliente desde la red y las primeras fases de carga e instalación de un sistema operativo. Además incluye una carpeta compartida y un repositorio de imágenes donde se almacenan imágenes de arranque, imágenes de instalación y archivos que se necesitan durante el arranque en red. También hay una capa de red, un componente multicast y otro de diagnósticos.

- **Componentes de cliente:**

Entre los que se encuentra una interfaz gráfica de usuario (GUI) que se ejecuta dentro del Entorno de Preinstalación de Windows (Windows PE). Cuando un usuario selecciona una imagen del sistema operativo, los componentes de cliente se comunican con los del servidor para instalar esa imagen.

- **Componentes de gestión:**

Estos componentes son un conjunto de herramientas para la administración del servidor, de las imágenes de sistema operativo y de las cuentas de máquina de la red.

Cambios en las características RIS

Windows Deployment Services para Windows Server 2008 introduce una serie de modificaciones con respecto a las características de RIS en versiones previas del sistema operativo. Además existen también modificaciones sobre Windows Deployment Services que se pueden instalar en máquinas que ejecutan Windows Server 2003.

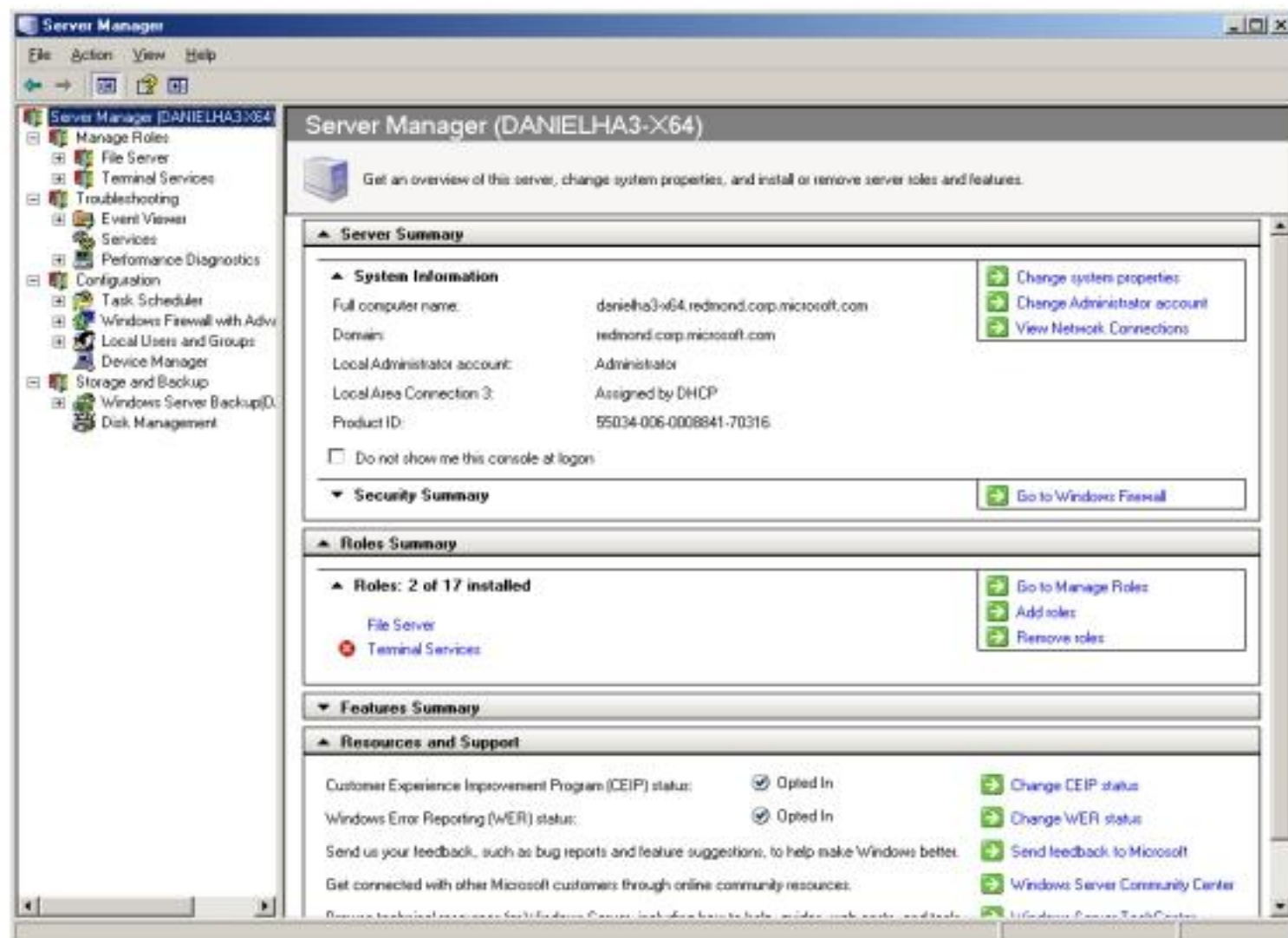
CAMBIOS CON RESPECTO A RIS	CAMBIOS CON RESPECTO A WDS SOBRE WINDOWS SERVER 2003
<ul style="list-style-type: none"> • Nueva interfaz gráfica de usuario que permite seleccionar y desplegar imágenes y que además sirve para administrar los componentes de servidor y cliente de Windows Deployment Services. • Windows PE es el sistema operativo de arranque. • Instalación basada en imágenes con archivos de imágenes de Windows (.WIM). • Posibilidad de transmitir datos e imágenes mediante multicast. • Posibilidad de transmitir datos e imágenes mediante multicast en un servidor aislado (instalando el Transport Server). • Servidor PXE extensible y con mejor rendimiento. • Nuevo formato del menú de arranque para seleccionar imágenes de instalación. • Posibilidad de desplegar Windows Vista y Windows Server 2008. 	<ul style="list-style-type: none"> • Posibilidad de transmitir datos e imágenes mediante multicast. • Posibilidad de transmitir datos e imágenes mediante multicast en un servidor aislado. • No soporta imágenes de RISEUP o pantallas de OSChooser. • Servidor TFTP mejorado. • Capacidad para arranque desde la red de máquinas x64 con EFI (Extensible Firmware Interface). • Informes de métrica de instalaciones.

Cabe resaltar que llegar a este punto ha tenido todo un proceso a través de varios años, tal como se aprecia a continuación.



Servidores de administración sencilla

Windows Server® 2008 facilita la tarea de gestión y la obtención de múltiples roles de servidor en una empresa con la nueva consola de Server Manager. Server Manager en Windows Server 2008 proporciona una única fuente para la gestión de la identidad de un servidor e información del sistema, mostrando el estado del servidor, identificación de problemas con el rol de configuración de servidor, y la gestión de todas los roles instalados en el servidor.



Server Manager sustituye varias características incluidas en Windows Server® 2003, incluido Administre su Servidor, Configure su Servidor, y Agregar o Quitar componentes de Windows.

Server Manager también elimina el requisito de que los administradores ejecuten el Asistente de Configuración de Seguridad antes de desplegar servidores; los roles de servidor se configuran con las opciones de seguridad recomendadas por defecto, y están dispuestos a desplegar tan pronto como estén adecuadamente instalados y configurados.

¿Qué hace Server Manager?



Server Manager es una ampliación de Microsoft Management Console (MMC) que le permite ver y gestionar virtualmente la totalidad de la información y las herramientas que afectan la productividad de su servidor. Los comandos en Server Manager permiten instalar o quitar roles de y características de servidor, y aumentar los roles ya instalados en el servidor mediante la adición de los servicios de rol.

Server Manager hace más eficiente la administración del servidor al permitir a los administradores a hacer lo siguiente mediante el uso de un único instrumento:

- Ver y hacer cambios en los roles y características de servidor instalados en el servidor.
- Realizar tareas de gestión relacionadas con el ciclo de vida operacional del servidor, como inicializar o detener servicios, y gestión local de cuentas de usuario.
- Realizar tareas de gestión relacionadas con el ciclo de vida operacional de roles instalados en el servidor.
- Determinar el estado del servidor, identificar eventos críticos, y analizar y solucionar problemas o fracasos de configuración.
- Instalar o quitar roles, servicios del rol, y características utilizando una línea de comandos de Windows.

¿Quién estaría interesado en Server Manager?

Server Manager está diseñado para proporcionar el mayor beneficio a cualquiera de los siguientes tipos de profesionales de TI:

- Un administrador de TI, planificador o analista que está evaluando Windows Server 2008
- Una empresa IT planificadora o diseñadora
- Uno adoptador temprano de Windows Server 2008
- Un arquitecto IT que es responsable de la gestión y seguridad informática en toda una organización

¿Hay alguna consideración especial?

Antes de utilizar Server Manager, se recomienda que se familiarice con las funciones, terminología, requisitos, y las tareas de gestión de día a día de cualquiera de los roles que desea instalar en su servidor.



Server Manager se instala por defecto como parte del Windows Server 2008 el proceso de configuración. Para utilizar Server Manager, deberá iniciar una sesión en el equipo como miembro del grupo Administradores en el equipo local.

Soporte para tareas de oficina

Sería excelente si todos sus servidores estén instalados en una sola localización de modo que usted pudiera protegerlos y tenerlos bajo su mirada. Desafortunadamente, la empresa de hoy consiste en un conjunto de jefaturas corporativas y una gran cantidad de sucursales alejadas, dispersadas alrededor del globo. Aunque usted sea el responsable de dichos servidores no podrá administrarlos físicamente, y estarán en las manos de usuarios con poca o ninguna experiencia en manejo de servidores.

Windows Server 2008 tiene varias tecnologías que ayudan a controlar estos servidores. Los controladores de dominio Read-Only (RODCs) son un nuevo tipo de controlador del dominio que recibe una copia inalterable de la base de datos del Directorio Activo. Si usted combina RODCs con la característica del cifrado de BitLocker primero introducida en Windows Vista, no tendrá que preocuparse de robos de información o manipulación indebida por parte de una persona en la ubicación física de los servidores.

Soporte para acceso centralizado a las aplicaciones

Dar soporte a los usuarios móviles puede ser una tarea difícil. Aunque las tecnologías de red privadas virtuales (VPN) han hecho el acceso alejado más simple, dando los usuarios remotos acceso completo a su red interna a través de Internet, no son a menudo la mejor solución. Con las mejoras en el Terminal Services en Windows Server 2008, sin embargo, los usuarios (tanto remotos como los de la red) pueden tener acceso seguro a los Servidores de Terminal y tener la misma clase de experiencia como si estuvieran trabajando localmente desde una máquina conectada a la red empresarial.

El Terminal Services Gateway (TS Gateway) deja a usuarios remotos con seguridad a través su cortafuego y tiene acceso a los servidores terminales que funcionan en su red corporativa.

Implementación de Servicios y Aplicaciones Web

¿Su organización provee de aplicaciones y servicios a sus clientes? ¿Es la web una manera de vivir para su negocio? Las nuevas características y mejoras en Internet Information Services 7.0 van a satisfacer las necesidades de usted y sus clientes.

Internet Information Services se originó de acuerdo a la siguiente secuencia histórica:

- 1996
 - V1 con Windows NT 4.0
 - V2 & V3 en subsiguientes Service Packs
- 1997
 - V4 como parte del NT 4 Option Pack
- 2000
 - V5 incluido por defecto en Windows 2000

- 2001
 - Marzo 2001: #1 en Internet Site Share
 - Otoño 2001: Code Red y Nimda
- 2003
 - V6 incluido en Windows Server 2003

La gestión del servidor Web se simplifica gracias a Internet Information Services 7.0, una potente plataforma de publicación Web para aplicaciones y servicios. Esta plataforma modular dispone de una interfaz de gestión simplificada y orientada a tareas, un control más preciso sobre todos los sites, mejoras en la seguridad y una gestión integrada del estado de salud para Servicios Web. Internet Information Server (IIS) 7 y .NET Framework 3.0 se complementan para conseguir una plataforma completa de aplicación que conecta a los usuarios entre sí y con sus datos, permitiéndoles visualizar, compartir y actual sobre la información

Confiabilidad

Windows Server 2008 es el sistema operativo Windows Server más flexible y robusto creado hasta la fecha. Con sus nuevas tecnologías y funcionalidades, como Server Core, PowerShell, Windows Deployment Services o las tecnologías avanzadas de red y cluster, Windows Server 2008 se constituye como la plataforma Windows versátil y fiable que necesita para responder a las necesidades de su empresa y los requisitos de sus actividades y aplicaciones. El Gestor del Servidor (Server Manager) agiliza la configuración y puesta en servicio del sistema, simplificando el mantenimiento posterior de los roles de servidor gracias a una consola de gestión unificada.

Protección de datos

Windows Server 2008 es la versión de Windows Server más segura que se haya creado nunca. Incorpora una amplia serie de mejoras para la seguridad y refuerzo del sistema operativo, como Network Access Protection (NAP), Gestión de Derechos Federados (Federated Rights Management) y el Controlador de Dominio en modo "read-only" (solo lectura) que aportan un nivel desconocido hasta ahora de protección para la red, los datos y la empresa. Windows Server 2008 ofrece una mayor protección contra fallos e intrusiones para los servidores, la red, los datos y las cuentas de usuario. Network Access Protection permite aislar ordenadores que no cumplen con las políticas de seguridad establecidas para su organización, con medidas como la restricción del acceso a la red, comprobación de estado y resolución de deficiencias.

Incremento de la productividad con Hyper-V

Virtualización de múltiples sistemas operativos (Windows, Linux y otros) sobre un mismo servidor: con las tecnologías de virtualización incorporadas dentro del sistema operativo y gracias a unas políticas de licencia más sencillas y flexibles, ahora es más fácil que nunca aprovechar al máximo todos los beneficios y ahorros que permite la virtualización. Windows Server 2008 le aporta la flexibilidad necesaria para crear un Datacenter ágil y dinámico, capaz de responder con eficacia ante los cambios en las necesidades de su negocio.






Ediciones de Windows Server 2008




















































A continuación se describe las diferentes Ediciones de Windows Server 2008

Edición	Descripción
Windows Server 2008 Standard	Windows Server 2008 es el sistema operativo más robusto creado hasta la fecha. Incorpora capacidades de virtualización (ediciones de 64 bits) y Web mejoradas, y está diseñado para aumentar la fiabilidad y flexibilidad de las infraestructuras de servidor, reduciendo a la vez los costes y el tiempo de soporte.
Windows Server 2008 Enterprise	Windows Server 2008 Enterprise es una plataforma de nivel corporativo para aplicaciones críticas de negocio. La disponibilidad del sistema se ve aumentada mediante funcionalidades como el cluster y la adición de procesadores en caliente.
Windows Server 2008 Datacenter	Windows Server 2008 Datacenter es una plataforma de nivel corporativo para aplicaciones críticas de negocio y virtualización a gran escala sobre servidores de todo tipo. La disponibilidad del sistema se ve incrementada gracias a cluster y particionamiento dinámico del hardware. Permite reducir los costes de infraestructura mediante la consolidación de aplicaciones facilitada por derechos de licencia de virtualización ilimitados. Escala desde 2 a 64 procesadores.
Windows Web Server 2008	Esta edición está diseñada como servidor Web especializado exclusivamente. Windows Web Server 2008 es una plataforma sólida de funcionalidades Web basada en las tecnologías de última generación que introduce Windows Server 2008.
Windows Server 2008 For Itanium-Based Systems	Windows Server 2008 para sistemas basados en Intel Itanium es una edición optimizada para entornos a gran escala de bases de datos, aplicaciones de línea de negocio o de otro tipo, donde se requiere una alta disponibilidad y la capacidad de escalar hasta a 64 procesadores para responder a las necesidades de las organizaciones y de las soluciones de misión crítica.
Windows Server 2008 Sin Hyper-V	Disponible en ediciones Standard, Enterprise y Datacenter

Ediciones de Servidores sin Hyper-V

Para aquellos clientes que no necesitan virtualización, también están disponibles las ediciones Standard, Enterprise y Datacenter de Windows Server 2008 sin la tecnología Hyper-V.

Indicador:  = No disponible  = Función parcial  = Función completa

Rol de Servidor	Enterprise	Datacenter	Standard
Servicios de Dominio del Directorio Activo			
Servidor de Aplicaciones			
Servidor DHCP			
Servidor DNS			
Servicios Web (IIS)			
Servidor de Impresión			
Hyper-V ¹			
Servicios de Dominio restringidos del Directorio Activo			
Servicios de Gestión de Derechos del Directorio Activo			
Servidor de Fax			
Servicios UDDI			
Servicios de Despliegue de Windows			
Servicios de Certificados del Directorio Activo			 ²
Servidor de Archivos			 ³
Servidor de Accesos y Políticas de Red			 ⁴
Terminal Services			 ⁵
ADFS (Active Directory Federation Services)			

¹ Para clientes que no necesitan virtualización existen ediciones Standard, Enterprise y Datacenter de Windows Server 2008 editions sin tecnología Hyper-V.

² Limitado a la creación de Autoridades de Certificación—no incluye otras funcionalidades de ADFS (NDES, Online Responder Service). Consulte la documentación del rol ADCS en TechNet para más información.

³ Limitado a una raíz DFS independiente.

⁴ Limitado a 250 conexiones RRAS, 50 conexiones IAS y 2 Grupos de Servidor IAS.

⁵ Limitado a 250 conexiones de Gateway de Terminal Services.



Roles del Windows Server 2008

Un rol del servidor describe la función principal del servidor. Los administradores pueden optar por dedicar todo un servidor para un rol, o instalar múltiples roles del servidor en un único equipo. Cada rol puede incluir uno o más servicios del rol, u opcionalmente instalar elementos del rol. Los siguientes roles están disponibles en Windows Server 2008 y puede ser instalados y administrados usando Server Manager:

Nombre del Rol	Descripción
Servicios de Dominio Active Directory	Active Directory Domain Services (AD DS) almacena información sobre usuarios, computadoras, y otros dispositivos de la red. AD DS ayuda a los administradores de seguridad a gestionar esta información.
Servidor de Aplicación	El Servidor de Aplicación proporciona una solución completa para la organización y gestión de aplicaciones empresariales distribuidas de alto rendimiento.
Dynamic Host Configuration Protocol (DHCP) Server	El Protocolo de Configuración Dinámica de Servidores permite asignar, o arrendar, direcciones IP a computadoras y otros dispositivos que estén habilitados como clientes DHCP.
Servidor DNS	Sistema de nombres de dominio (DNS) proporciona un método estándar para asociar los nombres con las direcciones numéricas de Internet.
Servicios de Archivo	Los Servicios de Archivo proporcionan las tecnologías para la administración de almacenamiento, repetición de archivos, gestión de nombres distribuido, búsqueda rápida de archivo, y racionalizar el acceso de los clientes a los archivos.
Política de Red y Servicios de Acceso	Con los Servicios de Acceso a la Red, usted puede desplegar servidores VPN, servidores de acceso telefónico, enrutadores, y acceso inalámbrico protegido 802.11.
Servicios de Impresión	Los Servicios de Impresión permiten la administración de servidores de impresión e impresoras.
Servidor Web (IIS)	El servidor Web (IIS) permite el intercambio de información en la Internet, una Intranet, o una extranet. Se trata de una plataforma unificada que integra Web IIS 7.0, ASP.NET, y Windows Communication Foundation.
Hyper-V	Hyper-V proporciona los servicios que usted puede utilizar para crear y gestionar máquinas virtuales y sus recursos. Cada máquina virtual opera en un entorno de ejecución aislado. Esto le permite ejecutar múltiples sistemas operativos simultáneamente. Disponible únicamente en ediciones de 64bits, por el momento.

Windows Deployment Services	Usted puede utilizar Windows Deployment Services (Servicios de Desplazamiento de Windows) para instalar y configurar remotamente el sistema operativo Microsoft® Windows en equipos con Pre-boot Execution Environment (PXE) boot ROMs..
Fax Server	El Servidor de Fax envía y recibe faxes, y le permite administrar los recursos del fax como trabajos, configuración, informes, y dispositivos de fax en el equipo o en la red.
Servicios de Certificado Active Directory®	Servicios de Certificado Active Directory® proporciona servicios personalizables para la creación y gestión de certificados de clave pública usados en software de sistemas de seguridad que emplean tecnologías de clave pública.
Servicios de Federación Active Directory	Active Directory Federation Services (AD FS) proporciona la tecnología Web single-sign-on(SSO) para la autenticación de un usuario para múltiples aplicaciones Web utilizando una sola cuenta de usuario.
Active Directory Lightweight Directory Services	Organizaciones que tienen aplicaciones que requieren un directorio para almacenar los datos de la aplicación puede utilizar Active Directory Services Lightweight Directory (AD LDS, Servicios de Directorio Ligero) como el almacén de datos. AD LDS permite múltiples instancias de AD LDS simultáneamente en un único servidor, independientes para abastecer múltiples aplicaciones.
Active Directory Rights Management Services (AD RMS)	Active Directory Rights Management Services (AD RMS, Servicios de Administración de Derechos) es una tecnología de protección de la información que trabaja con AD RMS aplicaciones habilitadas para ayudar a salvaguardar la información digital de uso no autorizado.
Universal Description, Discovery, and Integration (UDDI) Services	Los servicios UDDI proporcionan capacidades de Descripción Universal, Descubrimiento e Integración (UDDI) para compartir información acerca de los servicios Web dentro de la intranet de una organización, entre socios de negocios en una extranet, o en la Internet.
Servicios Terminales	Los Servicios Terminales proporcionan tecnologías que permiten a los usuarios el acceso a programas basados en Windows que son instalados en un servidor terminal. Los usuarios pueden conectarse a un servidor terminal para ejecutar programas en ese servidor.



Preguntas de Repaso

1. Investigación:
 - a. Averigüe en qué consiste la característica WHEA.
 - b. En qué beneficia la Gestión de Memoria (NUMA) al Windows Server 2008
 - c. Describa la ventaja de trabajar con Clusters
 - d. Averigüe 3 características nuevas que se han incorporado en Windows Server 2008 respecto a Windows Server 2003
2. Mencione al menos 3 características que no son soportadas en Windows Server 2008 Estándar que sí lo son en Windows Server 2008



Gestión de máquinas virtuales

En este capítulo trataremos:

- Instalará Virtual PC para administrar servidores virtuales
- Instalará Virtual Server para el manejo de los servidores virtuales

Introducción:

Con Microsoft® Virtual PC 2007, y también con Virtual Server 2005 puede crear y ejecutar uno o más equipos virtuales, cada uno con su propio sistema operativo, en un solo equipo físico. Esto le proporciona la flexibilidad de poder usar distintos sistemas operativos en un único equipo físico.



Introducción sobre Equipos Virtuales

Microsoft Virtual PC permite crear uno o más equipos virtuales, cada uno con su propio sistema operativo, en un solo equipo físico. El equipo virtual emula un equipo estándar basado en la arquitectura x86, con todos los componentes de hardware básicos excepto el procesador. Cada equipo virtual funciona como un equipo físico independiente, utilizando hardware emulado y el procesador del equipo físico. Como cada equipo virtual tiene su propio sistema operativo, puede ejecutar diversos sistemas operativos simultáneamente en un solo equipo.

En el diagrama se ilustran los distintos niveles y componentes de Virtual PC cuando se ejecuta en el sistema operativo host.



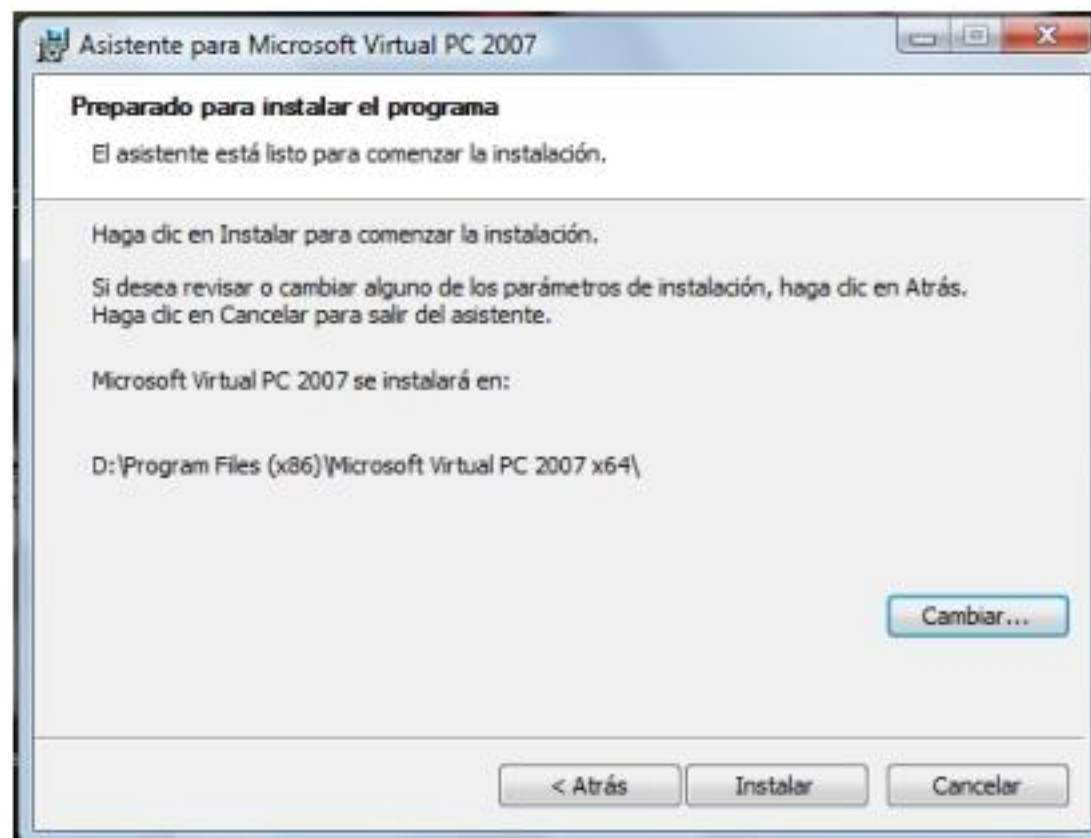
Arquitectura de Virtual PC 2007

❖ Exclusivo en Virtual PC 2007:

- Usa solamente una CPU del host
 - Una sola thread para todas las VMs
- Una única unidad de CD
- Soporte a NAT
- Network a través del adaptador de (Loopback) del host
- Tarjeta de sonido (VM)
- Compartición de carpetas
- Drag-and-drop

Instalar Microsoft Virtual Machine

1. Busque la carpeta en la que está almacenado el paquete de instalación. Haga doble clic en **Setup**.
2. Cuando aparezca el Asistente InstallShield para Microsoft Virtual PC, haga clic en **Siguiente**.
3. En el cuadro de diálogo **Contrato de licencia**, lea el contrato y haga clic en **Acepto los términos del contrato de licencia**. A continuación, haga clic en **Siguiente**.
4. En el cuadro de diálogo **Información del usuario**, escriba el nombre del usuario y la organización que correspondan, escriba la clave de producto de Virtual PC y, a continuación, realice una de las acciones siguientes:
 - Para instalar Virtual PC para cualquier usuario del equipo, haga clic en **Cualquier persona que use este equipo** y, a continuación, haga clic en **Siguiente**.
 - Para instalar Virtual PC para su uso exclusivo, haga clic en **Sólo para mí (nombre de usuario)** y, a continuación, haga clic en **Siguiente**.
5. En el cuadro de diálogo Preparado para instalar el programa, realice una de las acciones siguientes:
 - Para instalar Virtual PC en la carpeta predeterminada, C:\Archivos de programa\Microsoft Virtual PC, haga clic en **Instalar**.
 - Para instalar Virtual PC en una ubicación diferente, haga clic en **Cambiar**. En el cuadro de diálogo **Cambiar la carpeta de destino actual**, vaya a la ubicación en la que desea instalar Virtual PC, haga clic en **Aceptar** y, a continuación, haga clic en **Instalar**.



6. Cuando aparezca el cuadro de diálogo Asistente InstallShield finalizado, haga clic en **Finalizar**.

Importante

- Si instala Virtual PC mediante el Escritorio remoto, el proceso de instalación finaliza la sesión remota. Esto se produce cuando se vuelve a generar la pila de red después de instalar los controladores de red de Virtual PC. Cuando finalice la sesión, espere unos segundos y vuelva a establecer la conexión remota.

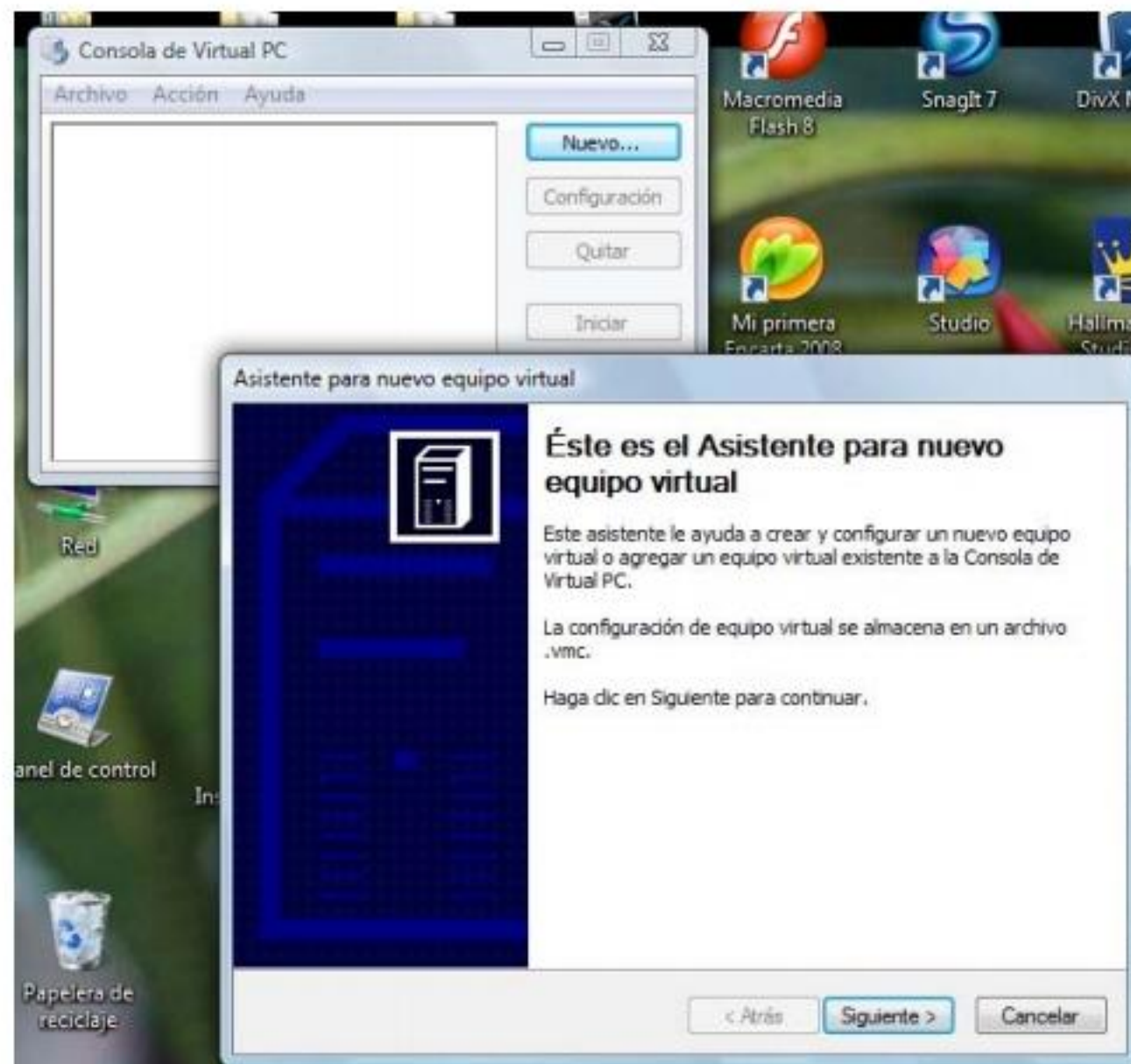


Crear una máquina Virtual

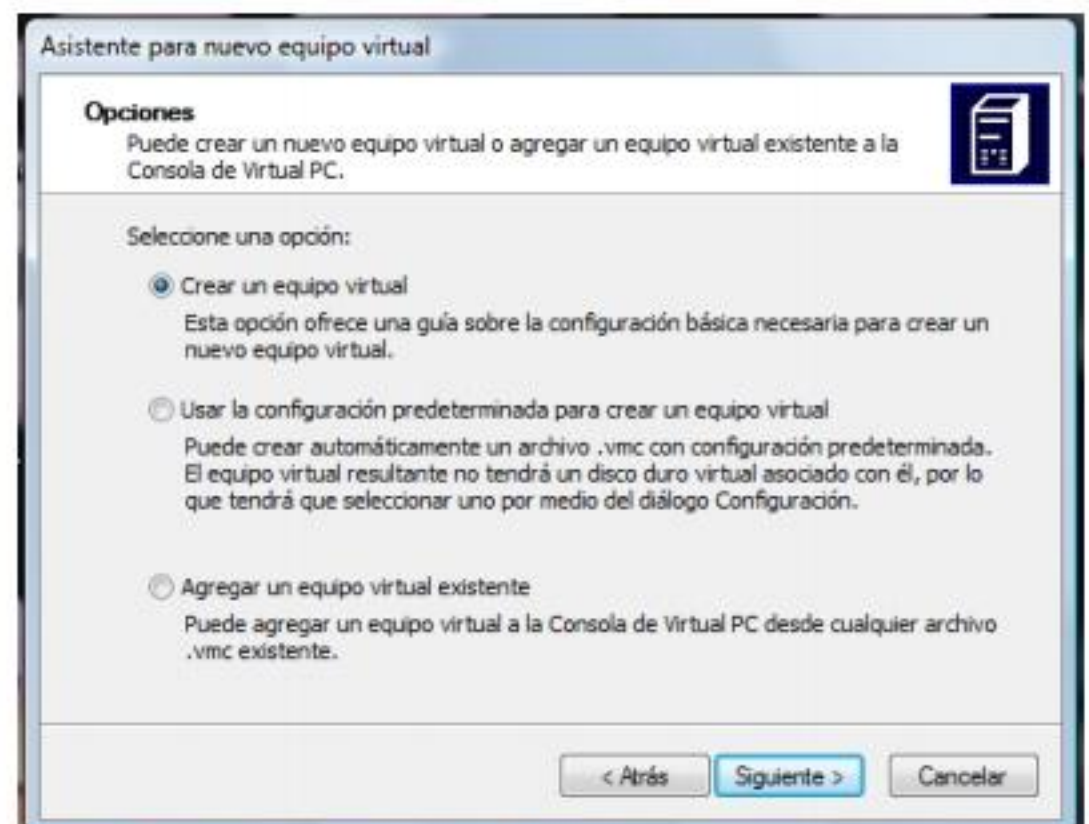
1. Abra la **Consola de Virtual PC** haga clic en Inicio, Todos los Programas.



2. En la **Consola de Virtual PC**, haga clic en **Nuevo**.

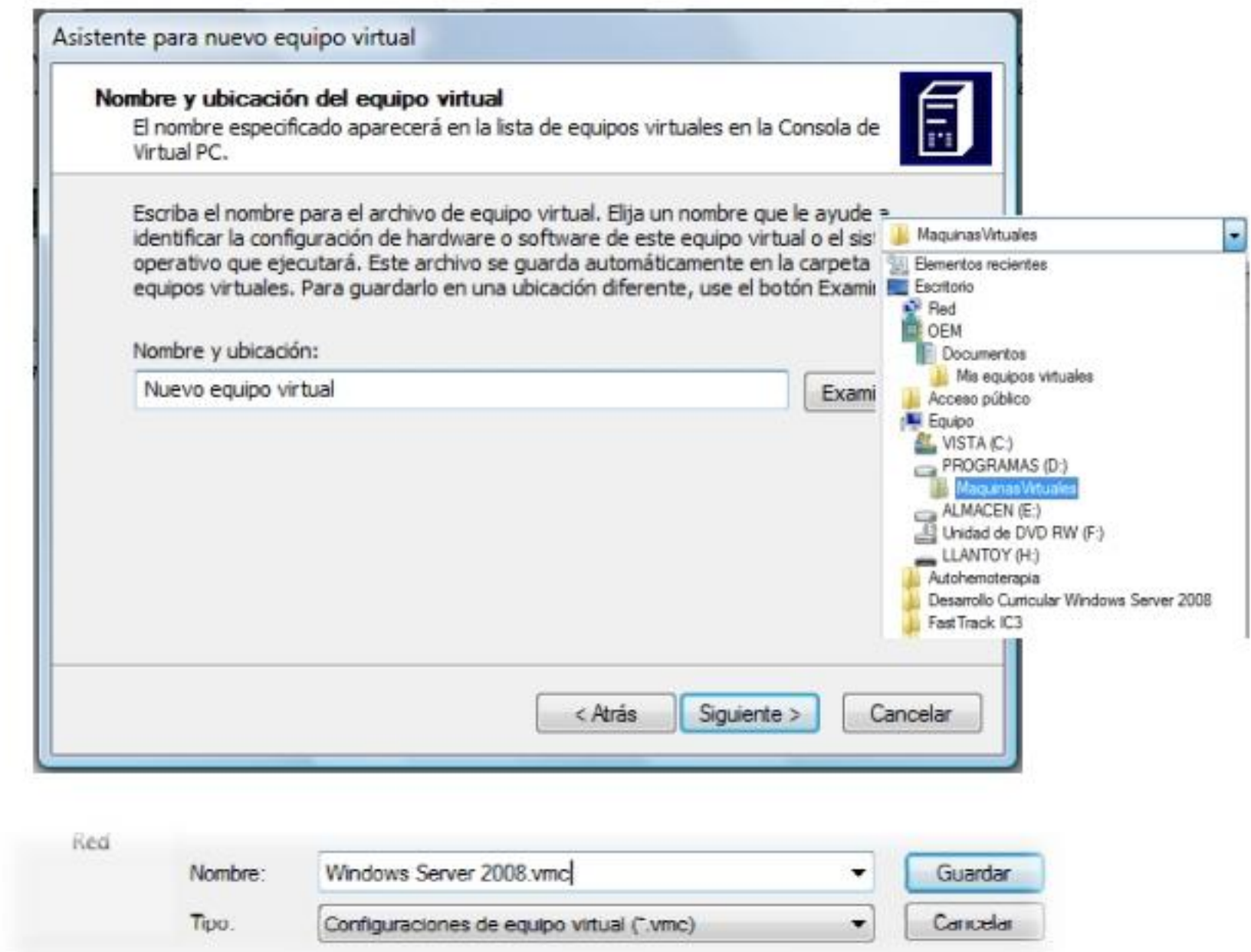


3. En el cuadro de diálogo **Asistente para nuevo equipo virtual**, haga clic en **Siguiente**.
4. En el cuadro de diálogo **Opciones**, haga clic en **Crear un equipo virtual** y, a continuación, haga clic en **Siguiente**.



5. En el cuadro de diálogo **Nombre y ubicación del equipo virtual**, escriba un nombre para el nuevo equipo virtual y, a continuación, haga clic en **Siguiente**.

De forma predeterminada, el asistente crea un nuevo archivo de configuración de equipo virtual (.vmc) y una nueva carpeta (con el mismo nombre) en la subcarpeta Mis equipos virtuales de la carpeta Mis documentos. Si desea almacenar la nueva carpeta y el nuevo archivo de configuración en una ubicación diferente, escriba la ruta de acceso completa a dicha ubicación o haga clic en **Examinar** para buscarla.



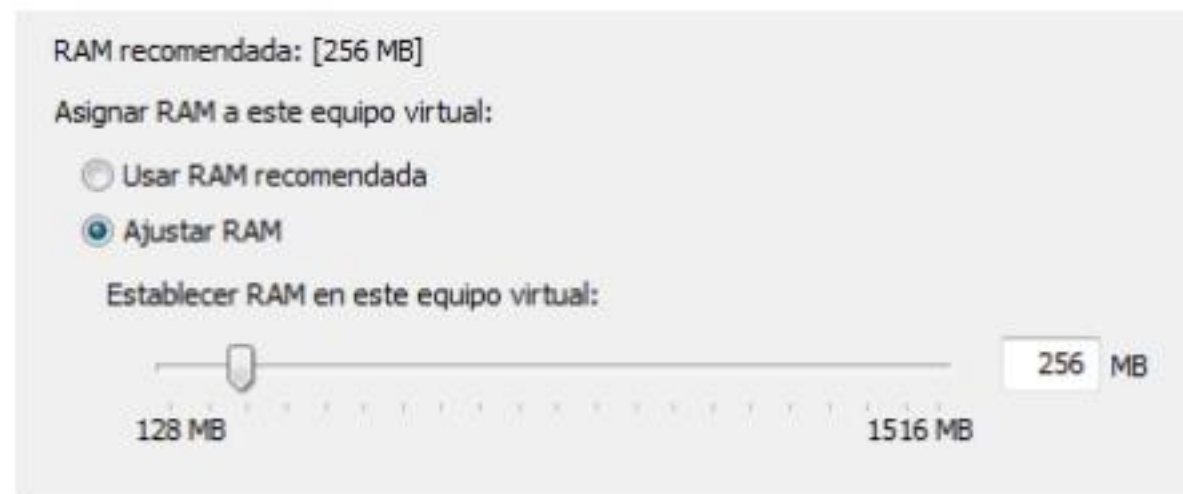
6. En el cuadro de diálogo **Sistema operativo**, en la lista **Sistema operativo**, seleccione el sistema operativo que desea ejecutar en este equipo virtual o haga clic en **Otro** si el sistema operativo no figura en la lista y, a continuación, haga clic en **Siguiente**.



7. En el cuadro de diálogo **Memoria**, realice una de las acciones siguientes:
 - o Para aceptar la asignación de memoria recomendada, haga clic en **Usar RAM recomendada** y, a continuación, haga clic en **Siguiente**.



- o Si desea modificar la asignación de memoria recomendada, haga clic en **Ajustar RAM** y mueva el control deslizante o escriba el número de megabytes que desea para cambiar el valor de configuración; a continuación, haga clic en **Siguiente**.

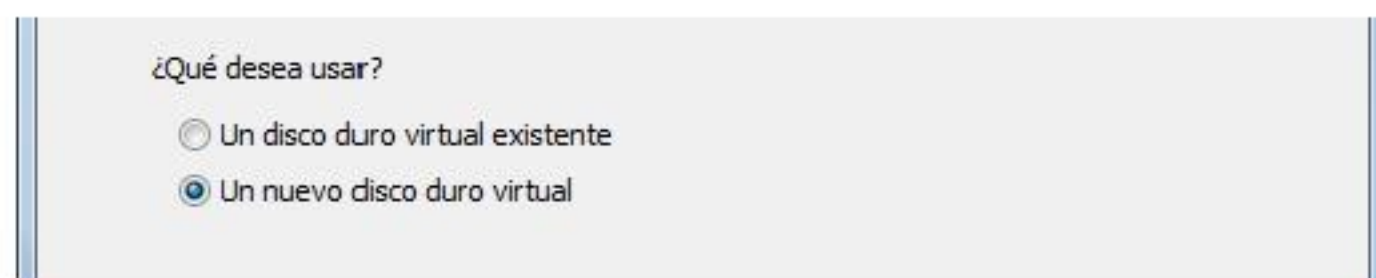


8. En el cuadro de diálogo **Disco duro virtual**, realice una de las acciones siguientes:

Para utilizar un disco duro creado previamente

1. Haga clic en **Un disco duro virtual existente** y, a continuación, haga clic en **Siguiente**.
2. En el cuadro de diálogo **Ubicación del disco duro virtual**, escriba el nombre de un archivo de disco duro virtual existente (.vhd).
3. Active o desactive la casilla de verificación **Habilitar discos para deshacer** y, a continuación, haga clic en **Siguiente**.

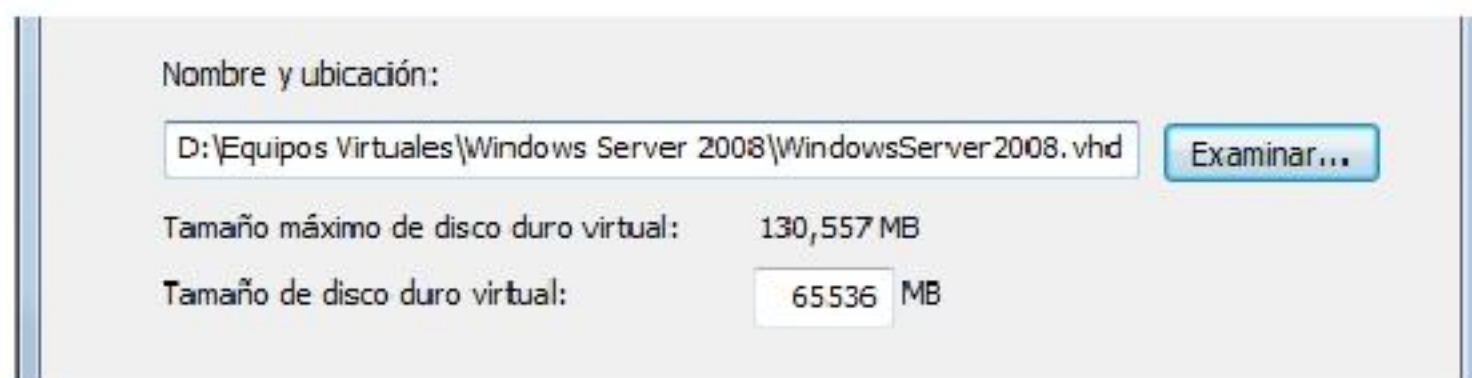
De forma predeterminada, el asistente buscará el archivo de disco duro virtual en la carpeta Mis documentos. Si el archivo que desea utilizar está en otra carpeta, escriba la ruta de acceso completa a dicha carpeta o haga clic en **Examinar** para buscarla.



Para crear un disco duro virtual para este equipo virtual:

4. Haga clic en **Un nuevo disco duro virtual** y, a continuación, haga clic en **Siguiente**.
5. En el cuadro de diálogo **Ubicación del disco duro virtual**, escriba un nombre para el nuevo archivo de disco duro virtual y, a continuación, haga clic en **Siguiente**.

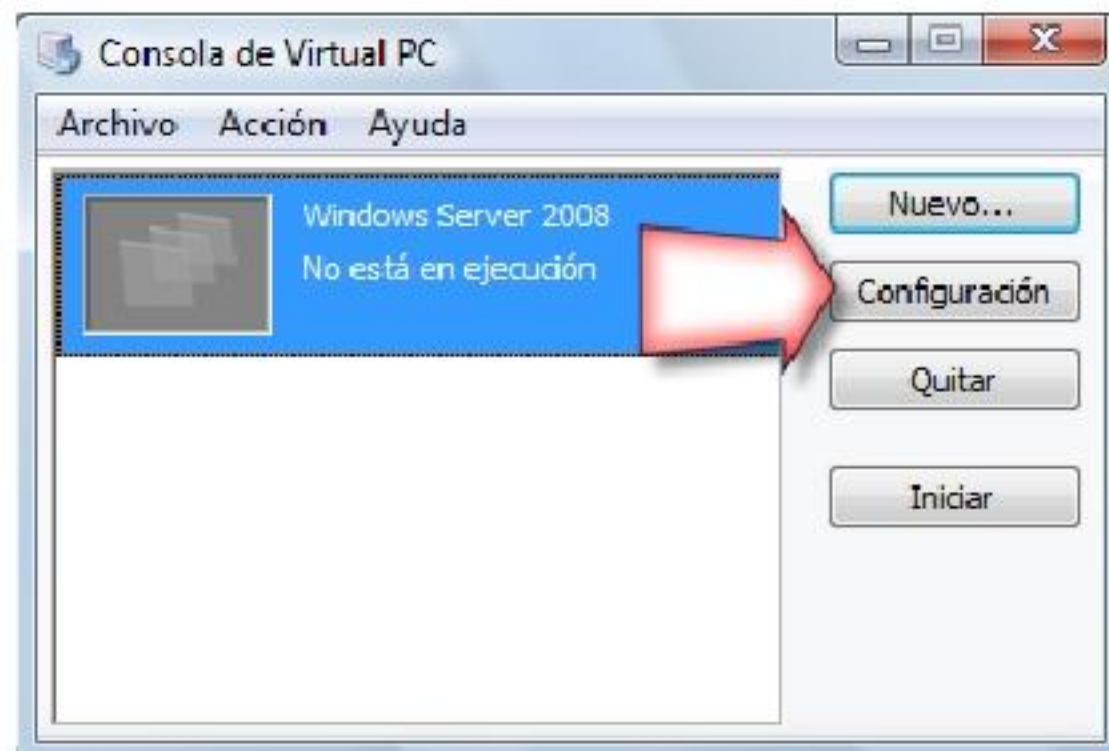
De forma predeterminada, el asistente crea un nuevo archivo de disco duro virtual en la carpeta que contiene el archivo del equipo virtual. Si desea crear el nuevo archivo en una ubicación diferente, escriba la ruta de acceso completa a dicha ubicación o haga clic en **Examinar** para buscarla.



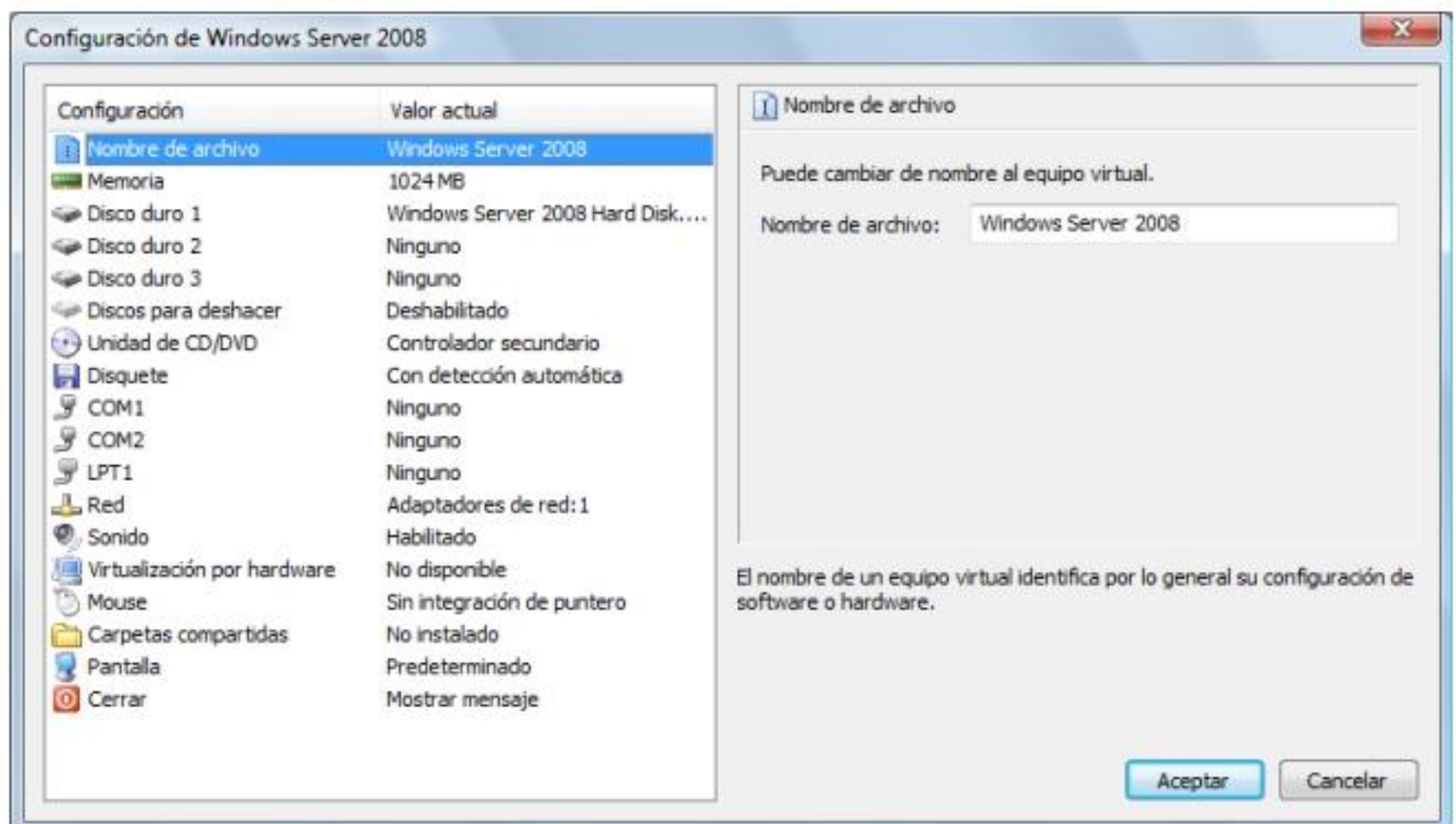
En el cuadro de diálogo **Finalización del Asistente para nuevo equipo virtual**, haga clic **Finalizar**.

Agregar o quitar componentes de hardware a la máquina virtual

1. Seleccione la máquina virtual en la ventana de consola y haga clic en **Configuración**.



2. Active o modifique las opciones del cuadro siguiente



BIOS de la máquina Virtual

Toda máquina virtual también posee un BIOS que permite configurar las opciones de booteo, y otros.

1. Seleccione la máquina Virtual y haga clic en Iniciar.



2. Debe pulsar la tecla suprimir al iniciar la máquina virtual y observará la siguiente pantalla



- Desplácese hasta el menú Boot usando las flechas direccionales y configúrelo tal como aparece a continuación:



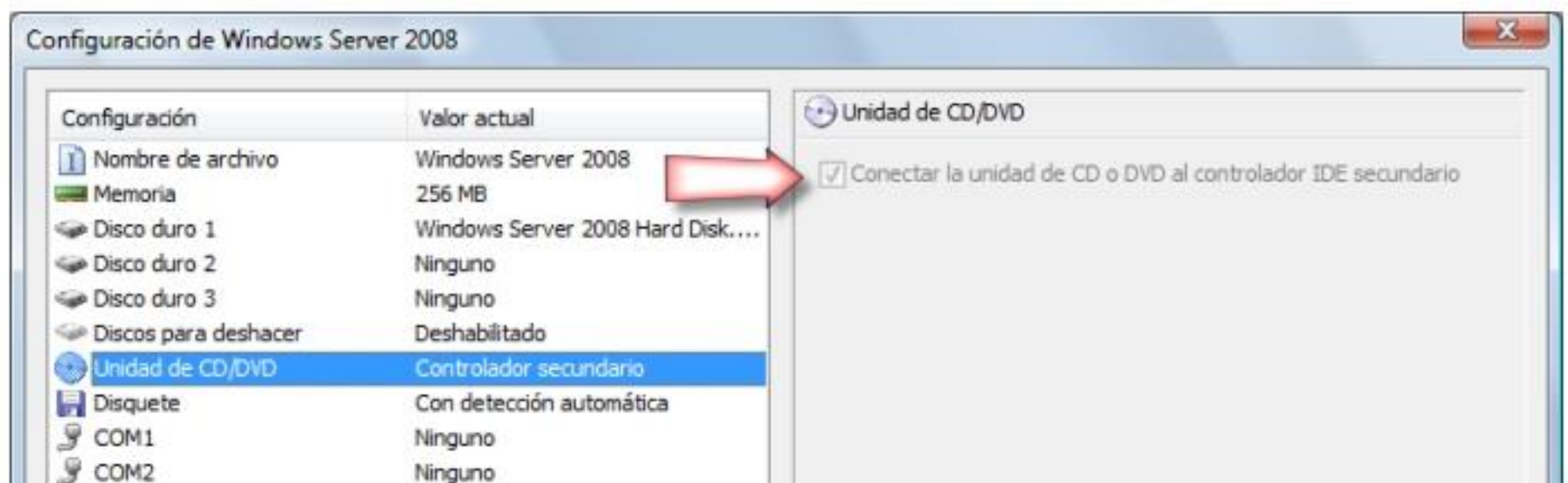
- Pulse la tecla Esc y luego F10, seguido de un Enter.



- Tenga a la mano el CD o DVD de instalación del nuevo Sistema Operativo

Utilizando CD o DVD físico

- Verifique que las propiedades de la máquina virtual esté configurado para acceder a la lectora.

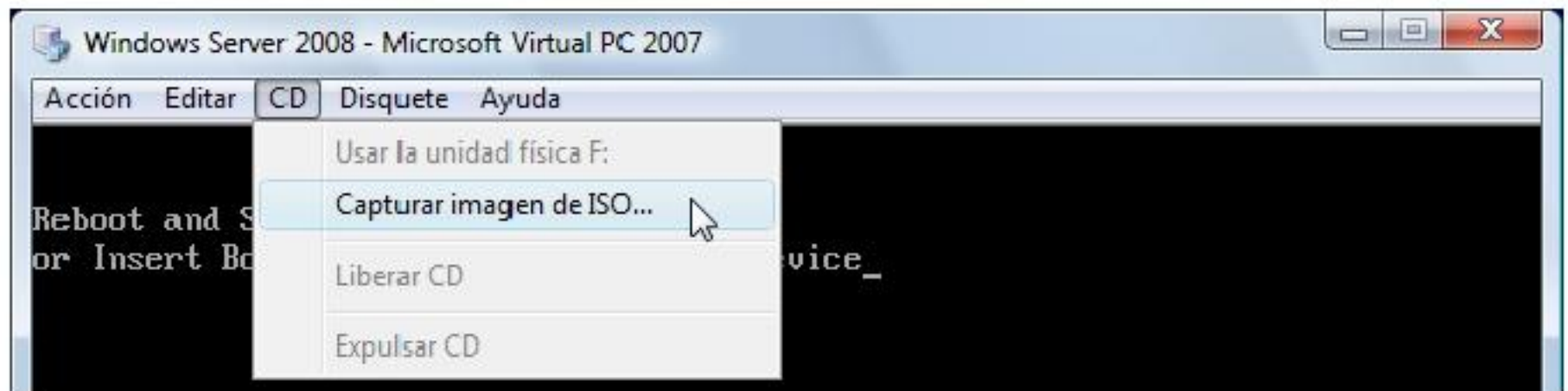


- Inserte el disco (CD o DVD) físico en la Unidad CD-DVD
- Espere a que boote e inicie la instalación

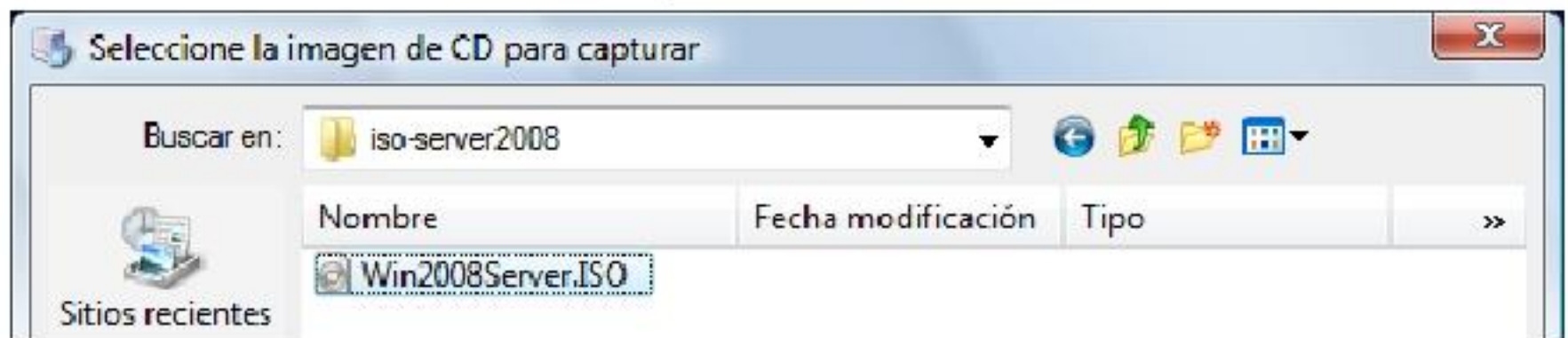
Utilizando archivos ISO

Otros métodos de instalación de un nuevo sistema operativo es utilizando un archivo de imagen (*.iso). Existen diferentes programas que convierten el contenido de un CD o DVD en un archivo de imagen.

1. Inicie la máquina virtual y luego haga clic en el menú CD.
2. Seleccione Capturar imagen de ISO...



3. Seleccione el archivo de imagen

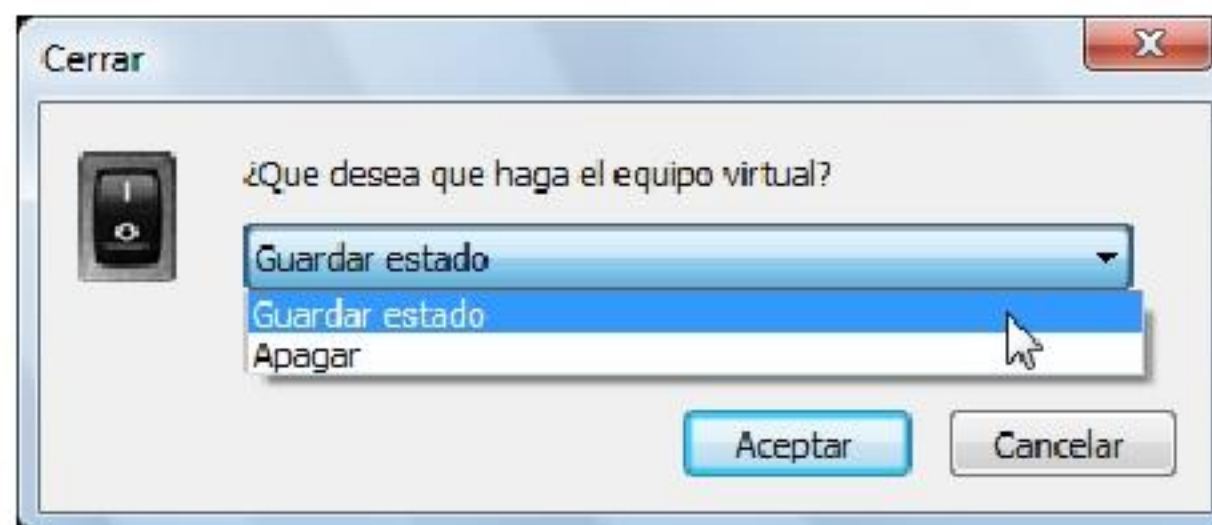


4. Haga clic en Abrir y espere a que inicie el proceso de instalación

Apagar equipo virtual

Aunque inicie un proceso de instalación, usted podrá apagar la máquina virtual en cualquier momento, incluso si el sistema operativo ya está en funcionamiento, podrá apagarlo congelando la sesión para una posterior restauración.

1. Haga clic en el botón cerrar de la ventana de la máquina virtual.



2. Seleccione Guardar estado y haga clic en Aceptar.

La opción Apagar, equivale a desconectar la alimentación eléctrica de una computadora.

Trabajando con Virtual Server

Requisitos de instalación

Para instalar Virtual Server 2005 R2 necesita, una computadora basada en x86 con un procesador de 550 MHz o uno superior (se recomienda 1 GHz) con caché L2, como los procesadores de cualquiera de las siguientes familias:

- Intel—Xeon o Pentium
- AMD—AMD64 o Athlon

Puede ejecutar Virtual Server en servidores con múltiples procesadores. Virtual Server 2005 Standard Edition puede ejecutarse en servidores con un máximo de cuatro procesadores. Virtual Server 2005 Enterprise Edition puede ejecutarse en servidores con más de cuatro procesadores. El número máximo de procesadores para Virtual Server 2005 R2 Enterprise Edition lo determina el sistema operativo host.

1. CD-ROM o unidad de DVD
2. Se recomienda un monitor Super VGA (800 x 600) o uno con mayor resolución.
3. Sistema operativo host. La versión de 32 bits de cualquiera de los siguientes sistemas operativos:
 - a. Microsoft Windows Server™ 2003, Standard Edition
 - b. Microsoft Windows Server 2003, Enterprise Edition
 - c. Microsoft Windows Server 2003, Datacenter Edition
 - d. Microsoft Windows® Small Business Server 2003
 - e. Microsoft Windows XP Professional
4. Se requiere el componente World Wide Web Service de Internet Information Services (IIS) en la computadora que ejecuta el Sitio Web de Administración.

Importante:

Debería utilizar Microsoft Windows XP Professional como sistema operativo host sólo en un entorno que no sea de producción.

Con respecto a los requisitos de memoria y de espacio en el disco rígido, consulte el siguiente cuadro para determinar lo mínimo que requiere el sistema operativo host. Estos requisitos son sólo indicaciones generales. Debe consultar la documentación del producto provista con cada sistema operativo para conocer los requisitos específicos.

Sistema operativo host	Mínimo de RAM	Espacio mínimo en el disco rígido
Windows Small Business Server 2003, Standard Edition	256 MB	4 GB
Windows Small Business Server 2003, Premium Edition	512 MB	4 GB
Windows Server 2003, Standard Edition	256 MB	2 GB
Windows Server 2003, Enterprise Edition	256 MB	2 GB
Windows Server 2003, Datacenter Edition	512 MB	2 GB



Instalación

1. Descargue desde la web de Microsoft la última versión de Virtual Server. Realizaremos una instalación sobre un host Windows XP o superior.
2. Ejecute el programa de instalación, haga clic en **Instalar Microsoft Virtual server 2005 R2**.
3. Haga clic en Instalar Microsoft Virtual Server 2005 R2
4. Ahora, debemos aceptar los términos del contrato de licencia y hacemos clic en Siguiente.
5. Ingrese la información del usuario y la organización, en nuestro caso ingresaremos Usuario: PNI y Organización: SENATI. Notará que ya aparece una Clave de producto por defecto e inalterable. Ahora haga clic en Siguiente.


Nombre de usuario:

Organización:

6. Seleccionamos **Completa** y hacemos clic en Siguiente

Elija el tipo de instalación.

Completa
Se instalarán todas las características del programa.



7. Recibiremos la siguiente advertencia en el caso de Windows XP por la versión de IIS instalada. Simplemente haga clic en Siguiente.

Microsoft
Virtual Server 2005 R2
Enterprise Edition

Configurar componentes

La versión instalada de los Servicios de Internet Information Server (IIS) no permite el uso de varios sitios Web. El sitio Web de administración de Virtual Server se agregará como un directorio virtual al sitio predeterminado.

Puerto del sitio Web:

8. Habilite la excepción para que Virtual Server pueda trabajar a través del Firewall.

Para tener acceso remoto a Virtual Server a través de un firewall, se necesita una configuración adicional. Si utiliza Firewall de Windows, el programa de instalación agregará entradas de excepción para permitir el funcionamiento correcto. Si usa un producto de firewall distinto, vea la Guía del administrador de Virtual Server para obtener detalles sobre cómo configurar el firewall para usarlo con Virtual Server.

Habilitar excepciones de Virtual Server en Firewall de Windows

9. Ahora estamos listos para el proceso de copia de los archivos del software Virtual Server. Haga clic en Instalar.

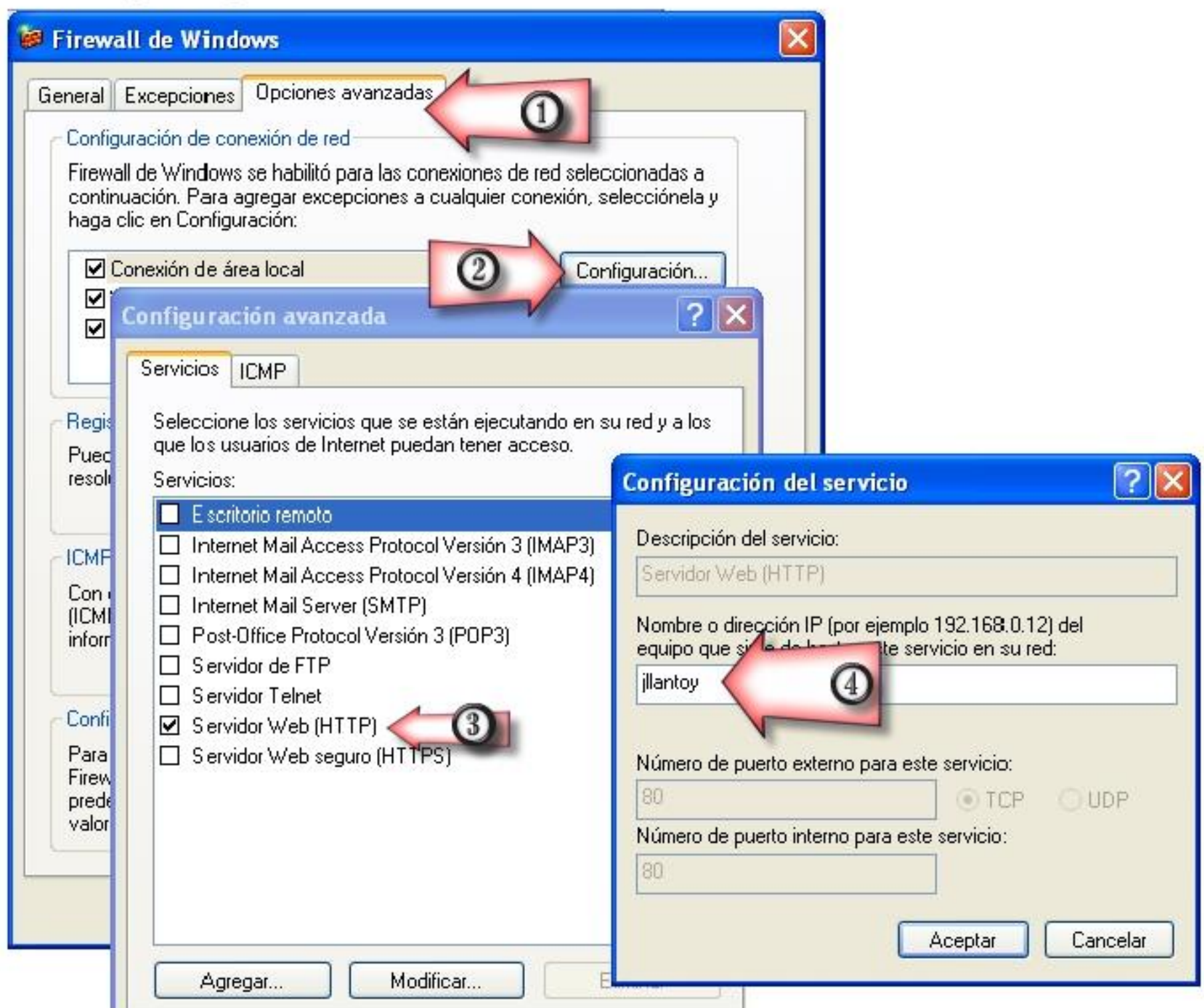
10. El proceso de instalación debe desarrollarse con total normalidad, espere.
11. Luego del proceso de instalación haga clic en Finalizar
12. Se cargará la información sobre Virtual Server.
13. Ahora podrá usar el Sitio Web de administración para acceder a las máquinas virtuales.

Nota:

1. El equipo Host debe tener IIS instalado y debe estar habilitado como Servidor Web en el Firewall.
2. La Instalación del IIS debe realizarse antes de Instalar Virtual Server.
3. La configuración del equipo como servidor web puede realizarse después, incluso, aunque es recomendable hacerlo antes de Instalar Virtual Server.

Configuración del equipo como Servidor Web.

1. Siga la siguiente secuencia.





Configurar equipos virtuales

1. En la primera pantalla se mostrará los datos del equipo host. Haga clic en Crear de la Sección Máquinas Virtuales.

Microsoft Virtual Server 2008

IP del Sitio web para administrar las máquinas virtuales

Exploración
Estado principal
Administrador de Virtual Server

Máquinas virtuales
Crear
Agregar

Estado de 192.168.0.235
Vista remota Nombre de la máquina virtual Estado
No se ha di

Sucesos recientes de 192.168.0.235

Tipo	Fecha y hora	Categoría	Mensaje
------	--------------	-----------	---------

2. Observará que aparece una Sección: Crear máquina virtual. Escriba la Ruta donde guardará la máquina virtual y el nombre del archivo. Defina también la cantidad de RAM, disco duro (Capacidad y Tecnología) y el adaptador de Red. Tome como **ejemplo la configuración** mostrada a continuación:

Crear máquina virtual

Nombre de la máquina virtual
Escriba un nombre de archivo de máquina virtual para crear una máquina virtual en su propia carpeta, que se guardará en la carpeta de configuración predeterminada tal como se especifica en la página [Rutas de búsqueda de Virtual Server](#). Para crear una máquina virtual en otra ubicación, proporcione una ruta de acceso completa.

Nombre de la máquina virtual: D:\Equipos Virtuales\WindowsServer2008

Memoria
La cantidad de memoria puede comprender entre 4 y 1828 MB (se recomienda un máximo de 1645 MB).
Memoria de la máquina virtual (en MB): 512

Disco duro virtual
Para instalar un sistema operativo en esta máquina virtual, conecte un disco duro virtual nuevo o existente a ella. Un disco duro virtual es un archivo .vhd almacenado en el disco duro físico que contiene el sistema operativo invitado, las aplicaciones y los archivos de datos.

Crear un nuevo disco duro virtual
Esta opción crea un disco duro virtual de expansión dinámica sin formato en el mismo directorio que el archivo de configuración de la máquina virtual. El tamaño máximo permitido es 127 GB para discos IDE y 2040 GB para discos SCSI.

Tamaño: 30 Unidades: GB Bus: IDE

Utilizar un disco duro virtual existente
Ubicación: Ninguna
Nombre de archivo (.vhd):
Bus: IDE

Conectar un disco duro virtual más tarde (ninguno)

Adaptador de red virtual
Una máquina virtual está preconfigurada con un adaptador de red Ethernet que puede conectarse a una red virtual.
Conectado a: Red Virtual Clase Redes

3. Ahora haga clic en Crear. Observará la siguiente página descriptiva.

Estado de "Windows Server 2008"

Windows Server 2008 ▶ Haga clic en la miniatura para encender esta máquina virtual

Estado de la máquina virtual	Desactivado
Tiempo de ejecución	n/d
Utilización de CPU física	n/d
Latido	n/d
E/S de disco	n/d

4. Adicionalmente se describe las características de hardware asignadas a la máquina virtual, tal como se aprecia a continuación, y además podrá cambiar las propiedades de memoria, disco, CD/DVD, adaptador de red, etc.

Estado de "Windows Server 2008"

Windows Server 2008 ▶ Haga clic en la miniatura para encender esta máquina virtual

Estado de la máquina virtual	Desactivado
Tiempo de ejecución	n/d
Utilización de CPU física	n/d
Latido	n/d
E/S de disco	n/d
E/S de red	n/d
Sistema operativo invitado	n/d
Virtual Machine Additions	Información de Additions no disponible
Archivo .vmc	D:\Equipos Virtuales\Windows Server 2008.vmc

Configuración de "Windows Server 2008"

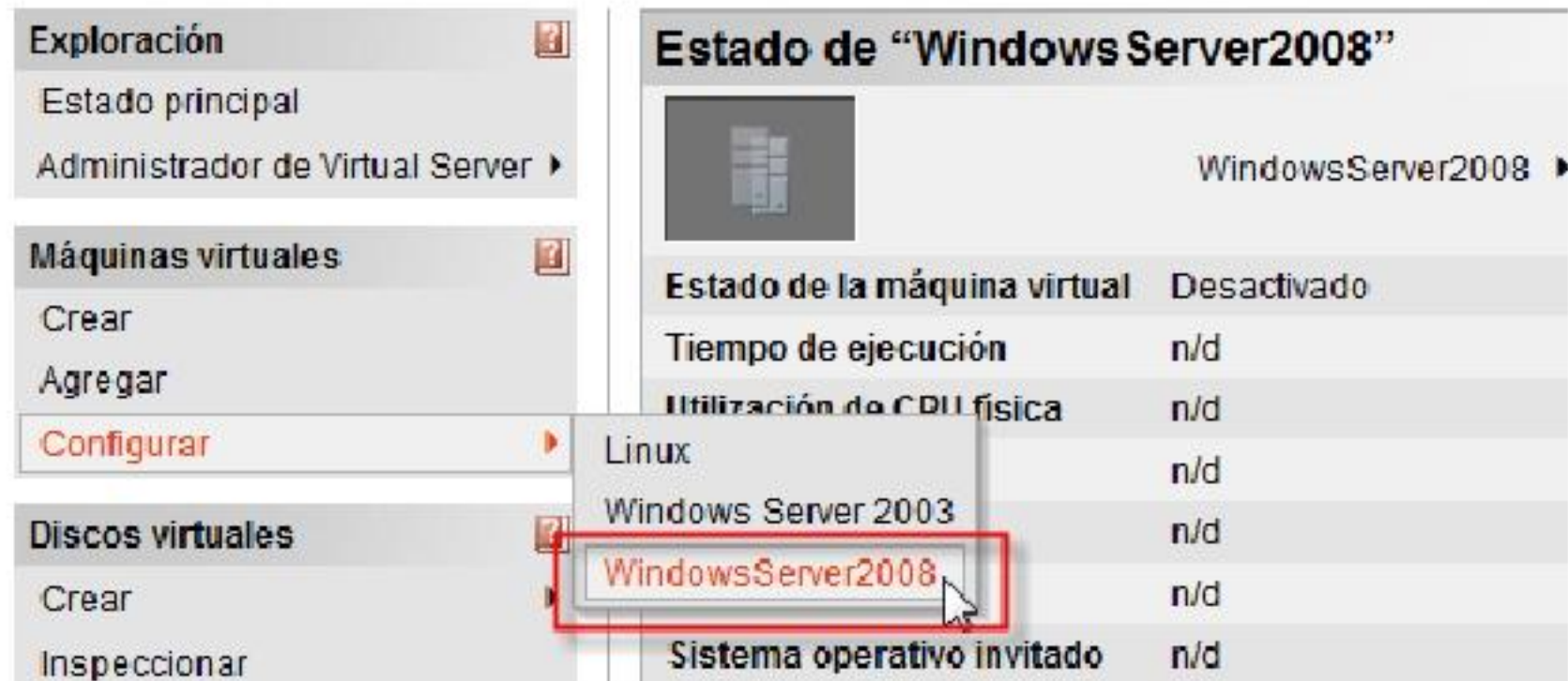
Propiedades generales		"Windows Server 2008"
Cuando se inicia Virtual Server:		No encender nunca la máquina virtual automáticamente
Cuando se detiene Virtual Server:		Guardar estado
Virtual Machine Additions		La información de Virtual Machine Additions no está disponible
Memoria		512 MB
Discos duros		1 disco duro virtual instalado; Los discos para deshacer están deshabilitados
Disco duro virtual 1		Conectado al canal principal (0) Archivo del disco duro virtual "Windows Server 2008.vhd" El tamaño máximo es 40 GB; Actualmente ampliado a 82.5 KB
CD o DVD		1 unidad de CD o DVD virtual instalada
Unidad de CD o DVD virtual 1		Conectado al canal secundario (0) Unidad del host "E"
Adaptadores SCSI		No hay ningún adaptador SCSI virtual instalado
Adaptadores de red		1 adaptador de red virtual instalado
Adaptador de red virtual 1		Conectado a "External Network (Broadcom NetXtreme Gigabit Ethernet for hp)" Dirección Ethernet (MAC) actual: 00-03-FF-F8-F5-4B



Iniciar equipos virtuales

Ahora vamos a iniciar una máquina virtual, pero en el próximo capítulo aprenderemos a instalar un Sistema Operativo.

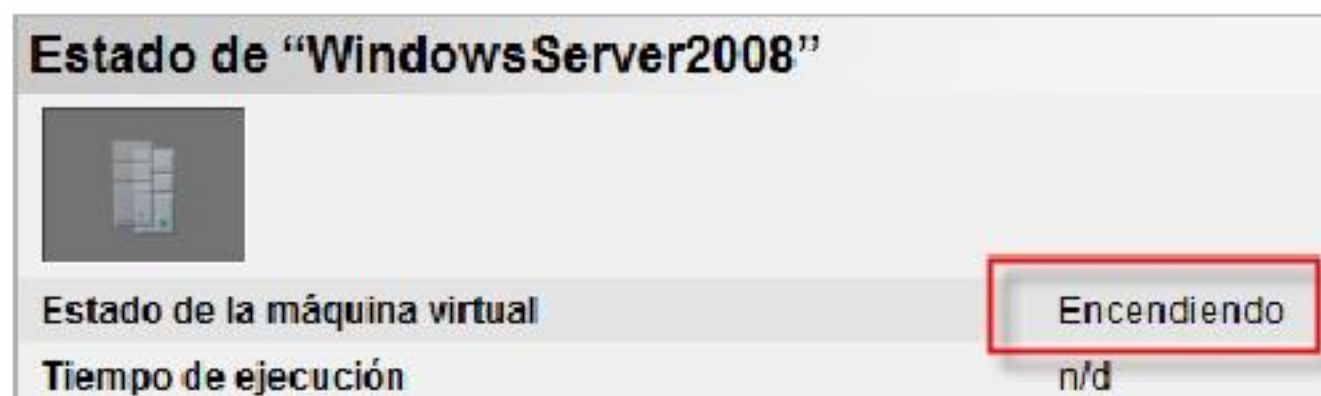
1. Haga clic en la Sección Máquinas virtuales y seleccione Configurar, luego Windows Server 2008 (Si hay más equipos virtuales se mostrarán en la lista)



2. Ahora haga Señale WindowsServer2008 y luego haga clic en encender.



3. Observará un indicador de Encendiendo, debemos esperar hasta que el menú muestra la opción "Control Remoto". A continuación mostramos el indicador.



4. Luego de unos segundos debe aparecer un menú con la opción "Control Remoto", señale la opción WindowsServer2008. El equipo está listo.



Crear redes virtuales

Una red virtual incluye una o varias máquinas virtuales configuradas para tener acceso a recursos de red locales o externos. Una red virtual es independiente de todas las demás redes virtuales existentes. Microsoft® Virtual Server 2005 admite un número ilimitado de redes virtuales; además puede conectar un número ilimitado de máquinas virtuales a una red virtual.

1. En el panel de exploración, en **Redes virtuales**, haga clic en **Crear**.



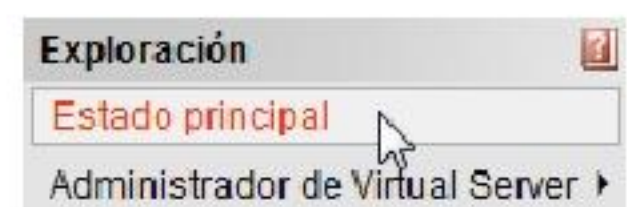
2. En **Nombre de red virtual**, escriba un nombre para la red virtual.
3. En **Adaptador de red en el equipo físico**, seleccione el adaptador que desea utilizar o seleccione **Ninguno (sólo invitados)**.
4. En **Adaptadores de red virtuales desconectados**, active la casilla de verificación **Conectado** de los adaptadores de red virtuales que desee conectar a la red virtual que está creando.
5. En **Notas de red virtual**, escriba notas que ayuden a administrar esta red virtual y, después, haga clic en **Aceptar**.



Gestión de máquinas virtuales

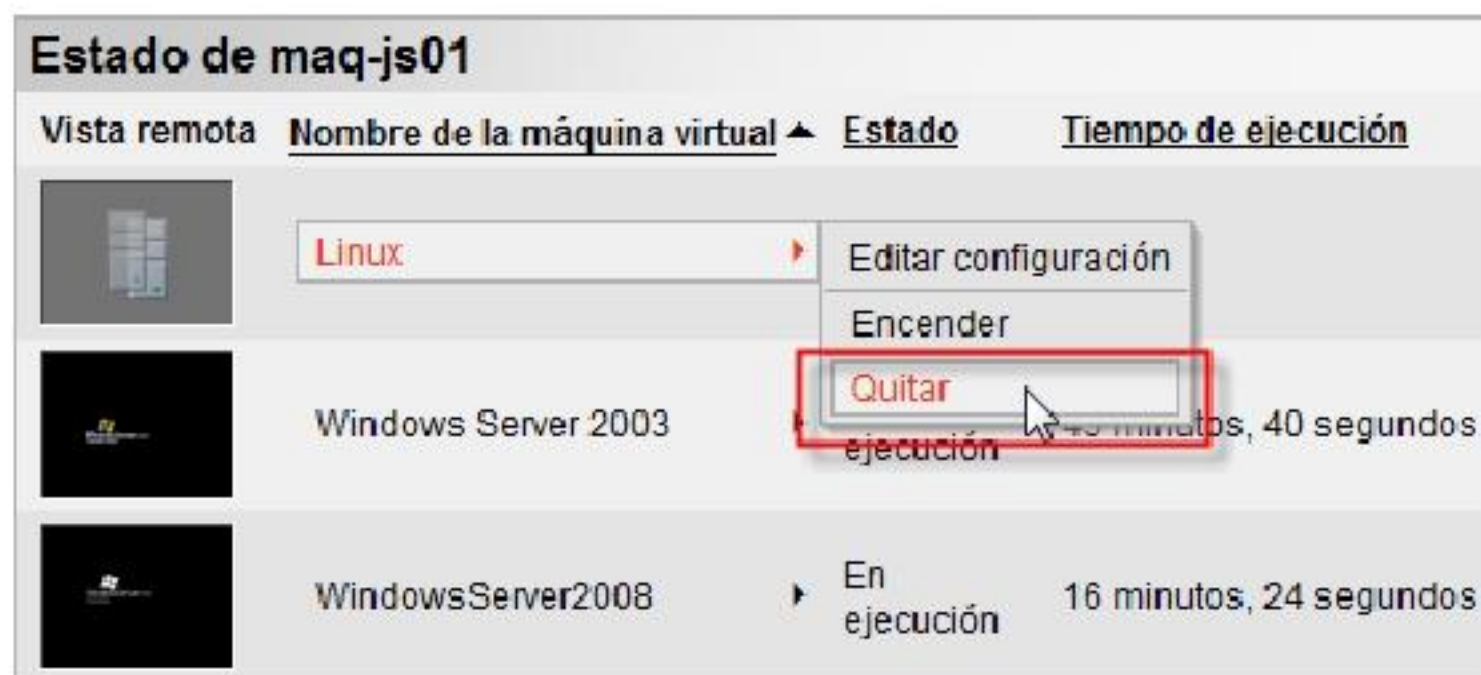
En las tareas de Gestión de máquinas veremos:

1. **Estado.** Muestra las máquinas virtuales que se han creado en el sistema host, y permite realizar tareas específicas sobre ellas.
2. **Apagar.** Las máquinas virtuales puede apagarse en cualquier momento, incluso antes de hacer control remoto sobre ellas. Y para ello señale el nombre del Sistema operativo, y seleccione Apagar.





3. **Quitar.** Para quitar un equipo virtual debe realizar los siguientes pasos
 - a. Debe apagar la máquina virtual, en caso contrario no aparecerá el comando Quitar, tal como se aprecia en la imagen superior.
 - b. Señale el nombre del Sistema Operativo y seleccione Quitar.



Preguntas de Repaso

1. Investigación:
 - a. Qué proceso se debe realizar para utilizar una máquina virtual de Virtual PC 2007 en Virtual Server 2005.
 - b. Otros programas de virtualización de terceros crean máquinas virtuales, como por ejemplo VMWare, describa el proceso para convertir una máquina virtual de VMWare en Virtual Server 2005.
2. Indique el proceso para crear una máquina virtual a partir de una máquina física.
3. Preparar una máquina virtual para los siguientes sistemas operativos. Tenga mucho cuidado de la cantidad de recursos de RAM y Disco duro que asignará a cada equipo.
 - a. Windows 98
 - b. Windows XP
 - c. Fedora 8.0
 - d. Windows Server 2008



Instalación de Windows Server 2008

En este capítulo trataremos:

- Familiarizarse con el procedimiento de instalación del Servidor
- Entenderá la terminología empleada en la gestión del Servidor.
- Instalará Windows Server 2008

Introducción:

Ahora nos concentraremos en el proceso a seguir para instalar el Sistema operativo para redes, Windows Server 2008.



Instalación de Windows Server 2008

Opción de Instalación con Hyper-V

Windows Server 2008 Hyper-V solamente está disponible en la edición x64 de Windows Server 2008 Enterprise Release Candidate 1 (RC1). Necesitará una instalación limpia de la edición x64 de Windows Server 2008 Enterprise RC1 en su sistema host. Hyper-V no puede activarse en sistemas que se ejecutan sobre máquinas virtuales.

Hyper-V no funciona sobre arquitectura una arquitectura de 32bits. Aunque sí se puede ejecutar sobre una arquitectura x86 de 64bits.

Aparte de los requisitos del sistema para Windows Server 2008, Hyper-V requiere un procesador basado en x64, virtualización asistida por hardware y protección de ejecución de datos por hardware. Para la versión beta se han probado un máximo de 16 procesadores lógicos.

Opción de Instalación Básica

La opción de Instalación Básica del servidor del sistema operativo Microsoft Windows Server 2008 es una nueva alternativa de instalación de Windows Server 2008. Esta modalidad permite disponer de un entorno mínimo para la ejecución de ciertos roles de servidor con lo que se reducen los requisitos de mantenimiento y gestión y la superficie de ataque que afectan a otros roles de servidor. La Instalación Básica de Servidor soporta los roles siguientes:

KEY: = No disponible = Función parcial/limitada = Función completa

Rol de Servidor	Enterprise	Datacenter	Standard	Web	Itanium
Servidor Web (IIS)					
Servidor de Impresión					
Hyper-V ¹					
Servicios de Directorio Activo de Dominio					
Servicios de Directorio Restringidos para AD					
Servidor DHCP					
Servidor DNS					
Servidor de Archivos					

¹ Para clientes que no necesitan virtualización, las ediciones Standard, Enterprise y Datacenter de Windows Server 2008 están disponibles sin la Tecnología Hyper-V.

² Limitado a una raíz DFS independiente.

Activar Hyper-V en una instalación de Servidor Básico

1. Si está actualizando un servidor que ejecuta una versión anterior a la RC1 de Windows Server 2008 deberá hacer copia de seguridad de los archivos necesarios de Windows Server antes de empezar. Deben completarse todos los pasos indicados en la preinstalación antes de seguir.
2. Si está actualizando desde una pre-release anterior o una versión beta de Windows Server 2008, desde Windows Server 2003 o desde Windows 2000 Server, seleccione la opción de instalación completa cuando instale Windows Server 2008 RC1.
3. Asegúrese de que dispone de virtualización asistida por hardware antes de instalar. Si ha tenido que introducir cambios en la configuración del BIOS para habilitar ciertas funciones de hardware, debe realizar un ciclo completo de apagado y encendido antes de empezar con la instalación.
4. Escriba "Start /w ocsetup Microsoft-Hyper-V" para habilitar el rol de Hyper-V.
5. Reinicie el sistema cuando se le indique en pantalla

Nota: Se recomienda no activar ningún otro rol de Windows Server 2008 en el sistema host si se activa Hyper-V en dicho equipo.

Para confirmar la instalación del rol Hyper-V, abra la consola MMC de Server Manager, expanda el nodo "Roles" y seleccione "Hyper-V". Compruebe que hay dos servicios activos: "vhdsvc" y "vmms".

Importante: Una vez reiniciado el sistema, inicie sesión con la misma cuenta utilizada anteriormente para instalar el rol de Hyper-V.

Dispositivos de hardware recomendados

Hyper-V estará soportado en una gran variedad de dispositivos de hardware compatibles con x64 en la versión RTM. Para la versión beta se han probado los siguientes dispositivos de hardware y son los que se recomiendan para realizar las pruebas con esta versión. Puede ser necesario actualizar la versión de BIOS del hardware de servidor para poder utilizar diversas funcionalidades. El uso de otras plataformas de hardware puede ocasionar algún tipo de incompatibilidad. La lista completa de dispositivos de hardware soportados se hará pública para la RTM de Hyper-V.

Fabricante	Modelo	Procesador
HP	Proliant DL585	AMD
HP	Proliant DL385 G2	AMD
HP	Proliant DL580 G4	Intel
HP	Proliant DL380 G5	Intel
Dell	PowerEdge 6850	Intel
Dell	PowerEdge 6950	AMD F2 Opteron 8212, con BIOS 1.1.2 o posterior
Dell	PowerEdge 2950	Intel, con BIOS 1.3.7 o posterior
Fujitsu	TX300 S3	Intel



Fabricante		Modelo		Procesador
Fujitsu Computers	Siemens	TX300 S3		Intel
NEC		Express 120Ri-2	5800	Intel

Proceso de Instalación de Windows Server 2008

1. Inserte el CD de Instalación de Windows Server.
2. Encienda la máquina Virtual
3. Espere un momento y haga clic en Control Remoto del Administrador de la Máquina Virtual. Observará la pantalla de bienvenida, luego seleccione las opciones de Idioma y distribución de teclado. Haga clic en Siguiente:

“WindowsServer2008” Remote Control

Remote Control

Instalar Windows

Windows Server 2008

Idioma que va a instalar: Español

Formato de hora y moneda: Español (España, internacional)

Teclado o método de entrada: Español

Especifique el idioma y las preferencias adicionales y después haga clic en Siguiente

Copyright © 2007 Microsoft Corporation. Reservados todos los derechos.

Ayuda y soporte técnico

Instalación de esta versión de Windows Server 2008

Este documento proporciona información acerca de la instalación del sistema operativo Windows Server® 2008. Asimismo, proporciona información que puede usar para solucionar problemas que pueden darse durante la instalación.

La instalación se desarrolla en varias fases. Se le pedirá que proporcione cierta información básica y, a continuación, el programa de instalación copiará archivos y reiniciará el equipo. Al finalizar, el programa de instalación presentará el menú Tareas de configuración inicial, que puede usar para adaptar la configuración del servidor a sus necesidades en particular.

Información de preinstalación

4. Si desea puede leer la ayuda en Qué debe saber antes de instalar Windows.

5. Ahora haga clic en **Instalar ahora**.
6. Luego de esperar un momento nos permitirá seleccionar el Sistema operativo a instalar.


Seleccione el sistema operativo que desea instalar.

Sistema operativo	Arquitectura	Fecha de mo...
Windows Server 2008 Standard (instalación completa)	X86	19/01/2008
Windows Server 2008 Enterprise (instalación completa)	X86	19/01/2008
Windows Server 2008 Datacenter (instalación completa)	X86	19/01/2008
Windows Server 2008 Standard (instalación Server Core)	X86	19/01/2008
Windows Server 2008 Enterprise (instalación Server Core)	X86	19/01/2008
Windows Server 2008 Datacenter (instalación Server Core)	X86	19/01/2008

Descripción:
Esta opción ejecuta la instalación completa de Windows Server. Esta instalación incluye la interfaz de usuario en su totalidad y admite todas las funciones del servidor.

7. Active la casilla **Acepto los términos de licencia**. Haga clic en siguiente.
8. Haga clic en **Personalizada (avanzada)**.
9. Puede crear particiones del disco en el siguiente cuadro. **Siguiente**.

¿Dónde desea instalar Windows?

Nombre	Tamaño total	Espacio disp...	Tipo
 Espacio sin asignar en el disco 0	30.0 GB	30.0 GB	

Actualizar Opciones de unidad

Cargar controlador

10. A continuación se indicará el progreso de la tarea de instalación, espere.

Instalando Windows...

Ésta es toda la información que se necesita en este momento. El equipo se reiniciará varias veces durante la instalación.

- Copiando archivos (0%) ..**
- Expandir archivos
- Instalar características
- Instalar actualizaciones
- Completar instalación

Instalando Windows...

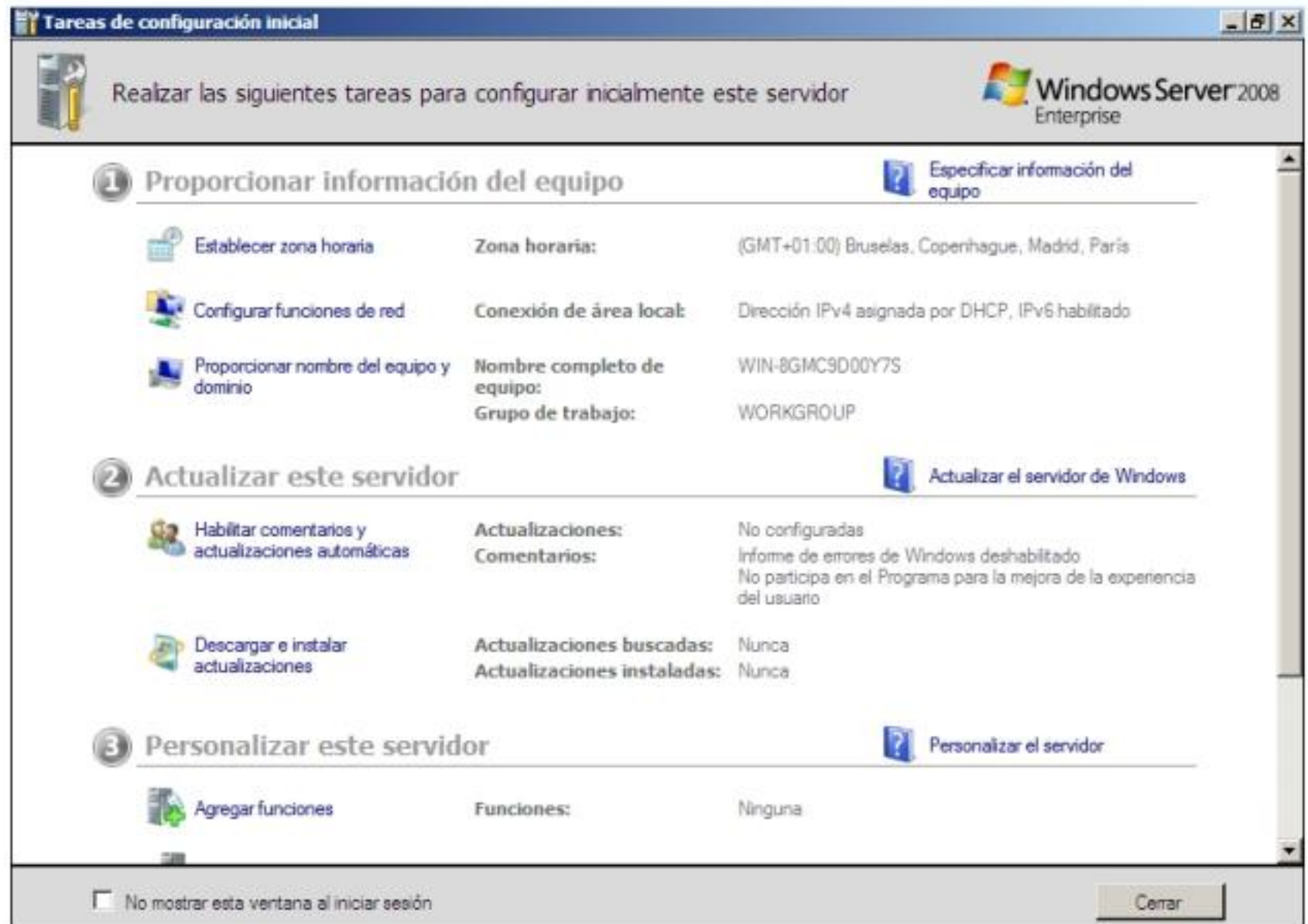
Ésta es toda la información que se durante la instalación.

- ✓ Copiando archivos
- ✓ Expandir archivos
- ✓ Instalar características
- ✓ Instalar actualizaciones
- Completar instalación .**

11. Observará el avance a través de verificaciones que aparecen en pantalla.



12. Para concluir, solicitará que ingrese la contraseña para el Administrador. Ingrése la dos veces y Acepte. Luego se confirmará el cambio de contraseña.
13. El sistema iniciará y mostrará Tareas de configuración inicial.



Seguridad del servidor

¿Los usuarios y las computadoras que conectan con su red de acuerdo con los requisitos de la política de la seguridad de su compañía? ¿Hay manera de hacer cumplir dicha política? Sí, hay. Además de mecanismos de aplicación estándares de la política tales como autenticación de la política de grupo y del Active Directory, el Windows Server 2008 también incluye la nueva plataforma de la protección del acceso de red (NAP). NAP proporciona una plataforma que ayuda en la seguridad de las computadoras del cliente.

Requisitos del sistema

Los requisitos reales variarán en función de la configuración del sistema y de las aplicaciones y características que decida instalar. Es posible que sea necesario espacio disponible en disco adicional si va a instalar a través de una red. Para obtener más información, consulte: Sitio del producto Windows Server 2008, por eso la siguiente tabla sólo es una información referencial.

Componente	Requisito
Procesador	<ul style="list-style-type: none"> •Mínimo: 1 GHz •Recomendado: 2 GHz •Óptimo: 3 GHz o más Nota: Windows Server 2008 para sistemas basados en Itanium precisa un procesador Intel Itanium 2.

Componente	Requisito
Memoria	<ul style="list-style-type: none"> • Mínimo: 512 MB de RAM • Recomendado: 1 GB de RAM • Óptimo: 2 GB de RAM (instalación completa) o 1 GB de RAM (instalación de Server Core) o más • Máximo (sistemas de 32 bits): 4 GB (Standard) o 64 GB (Enterprise y Datacenter) • Máximo (sistemas de 64 bits): 32 GB (Standard) o 2 TB (Enterprise, Datacenter y sistemas basados en Itanium)
Espacio en disco disponible	<ul style="list-style-type: none"> • Mínimo: 8 GB • Recomendado: 40 GB (instalación completa) o 10 GB (instalación de Server Core) • Óptimo: 80 GB (instalación completa) o 40 GB (instalación de Server Core) o más <p>Nota: los equipos con más de 16 GB de RAM requerirán más espacio en disco para la paginación, para la hibernación y para los archivos de volcado</p>
Unidad	Unidad de DVD-ROM
Pantalla y periféricos	<ul style="list-style-type: none"> • Super VGA (800 x 600) o monitor con una resolución mayor • Teclado • Mouse de Microsoft o dispositivo señalador compatible

Compatibilidad

Para averiguar si el hardware es compatible con Windows Server 2008, debe utilizar la opción **asesor de actualización de Windows Vista**. En la web Site de Microsoft aparecerá un enlace a esta herramienta.

En versiones anteriores la información de compatibilidad se encontraba en un archivo de texto denominado **Lista de compatibilidad de hardware (HLC)**, ahora toda la información se consulta desde la página web.

Consulte la ayuda del Sistema para buscar la palabra **HCL**.

También puede buscar compatibilidad con el software ya instalado. En la página web de **Windows Marketplace** encontrará miles de productos de software y hardware diferentes que funcionan con Windows Server 2008.

Esta modalidad permita ejecutar programas escritos para versiones anteriores de Windows. La mayoría de programas que funcionan en Windows XP también funcionan en esta versión de Windows Server 2008.

Licencia del producto

Una licencia de software otorga al usuario derecho legal a utilizar un software. Por cada programa de software de Microsoft que se utiliza, se otorga una licencia al usuario y ésta se documenta en el Contrato de Licencia de Usuario Final (CLUF). Un usuario de software, necesita una licencia. El acuerdo de licencia da al usuario el derecho de utilizar el software.

El software está protegido por la ley de derechos de autor, que establece que el producto no puede copiar sin autorización del dueño de derechos de autor.



Hay maneras diferentes de adquirir una licencia de Software Microsoft:

1. Producto Empaquetado (Caja): Licencia, CD-Rom y documentación en un paquete
2. Original Equipment Manufacturer (OEM): licencia para software preinstalado en un PC nuevo
3. Licencia por Volumen.

Los programas de Licencia por Volumen ofrecen tres soluciones:

1. **Licencia Microsoft (L)**. Proporciona los derechos de uso de una versión específica de un producto.
2. **Software Assurance (SA)**. Proporciona, para una licencia sobre la que se adquiere los derechos de actualización a las nuevas versiones lanzadas durante el periodo de vigencia del acuerdo.
3. **Licencia & Software Assurance Package (L&SA)**. Combina los beneficios de una licencia Microsoft y Software Assurance en un sólo paquete.

Administrar las licencias por volumen.

El seguimiento y la administración de licencias es una fuente típica de problemas. Por ese motivo se han desarrollado herramientas online para la administración de licencias. Son portales seguros, protegidos con contraseña, en los que se pueden efectuar todas las operaciones necesarias, que permiten ver fácilmente sus propios acuerdos, pedidos, información clave de productos, etc.

Para acceder a las herramientas de administración de licencias puede usar uno de los siguientes enlaces:

Open Multilicencia <https://eopen.microsoft.com>

Select & Enterprise Agreement <http://licensing.microsoft.com>

Activación del producto

Volume Activation 2.0 se ha diseñado para automatizar y administrar el proceso de activación de ediciones por volumen de Windows Vista y Windows Server 2008 y al mismo tiempo abordar los problemas de administración de claves y piratería asociados a las claves de licencia por volumen. Volume Activation 2.0 elimina el uso de claves de producto en el momento de instalación del software y permite una mejor protección y administración de sus claves de producto mediante herramientas de administración de activación nuevas y mejoradas. Además, Volume Activation 2.0 también puede servir como punto de partida para administrar los activos de software de un modo más efectivo.

Configuración de sistemas múltiples

Al respecto cabe mencionar que los sistemas múltiples se crean instalando uno a uno los sistemas operativos en orden de antigüedad, desde el más antiguo hasta el más moderno.

También debe considerar que en un entorno de producción, no es común instalar sistemas múltiples.

Este método difiere de la virtualización en que no crea sistemas que puedan ejecutarse simultáneamente, más bien, funciona uno u otro, pero no ambos al mismo tiempo.

Considere además que algunos Sistemas Operativos solo se pueden instalar en Particiones con formatos específicos como FAT32, NTFS u otros.

Algunos Sistemas Operativos deben instalarse necesariamente en Particiones primarias, mientras que otros pueden instalarse, además, en Unidades lógicas.

Linux debe instalarse, siempre, en último lugar.

Se recomienda que instale Windows Server 2008 en una partición independiente del sistema operativo anterior. Al hacerlo, conservará el acceso al otro sistema operativo. Para obtener los mejores resultados, se recomienda que inicie el programa de instalación desde Windows (en lugar de arrancar desde el DVD del producto) y que realice una instalación (limpia) personalizada en una partición separada.

Automatización de las instalaciones de Windows

Este proceso es conocido como Instalación desatendida. Con el nuevo asistente de instalación, se agrupa ahora toda la funcionalidad relacionada, con lo cual se simplifica el proceso y se ahorra tiempo durante la implementación. La instalación desatendida en Windows Server 2008 no requiere jamás una respuesta a ninguna solicitud de interfaz de usuario, con lo que se simplifica aún más las instalaciones remotas. Esto permite también la instalación de AD DS en una instalación de Server Core. Para garantizar que un servidor DNS recientemente instalado opera correctamente, el DNS se configura automáticamente para la configuración de cliente DNS, reenviadores y sugerencias de raíz, según sea necesario basado en las opciones de instalación seleccionadas.

Tengo a mano una instalación base en un archivo VHD para levantar rápidamente con Virtual Server o Virtual PC y empezar a testear funcionalidades que va encontrando.

Tener una imagen procesada con SysPrep evita los posibles problemas de tener los SID duplicados en una red y permite realizar un entorno de laboratorio lo más cercano a lo que puede ser el entorno de producción.

Vamos a considerar a continuación las características de Automated Installation Kit y de como el Setup de Windows 2008/Vista maneja la información provista en los archivos de instalación desatendida.

De preferencia tenga una instalación 100% desatendida, así lo único que haremos es copiar el VHD a una nueva carpeta, o crear un disco Diferencial sobre esa base y listo.

Paso 1 - Descarga e Instalación de Windows AIK

Descargue una copia de Automated Installation Kit for Windows Vista SP1 and Windows 2008 e instálelo para poder utilizar el Windows System Imaging Manager.

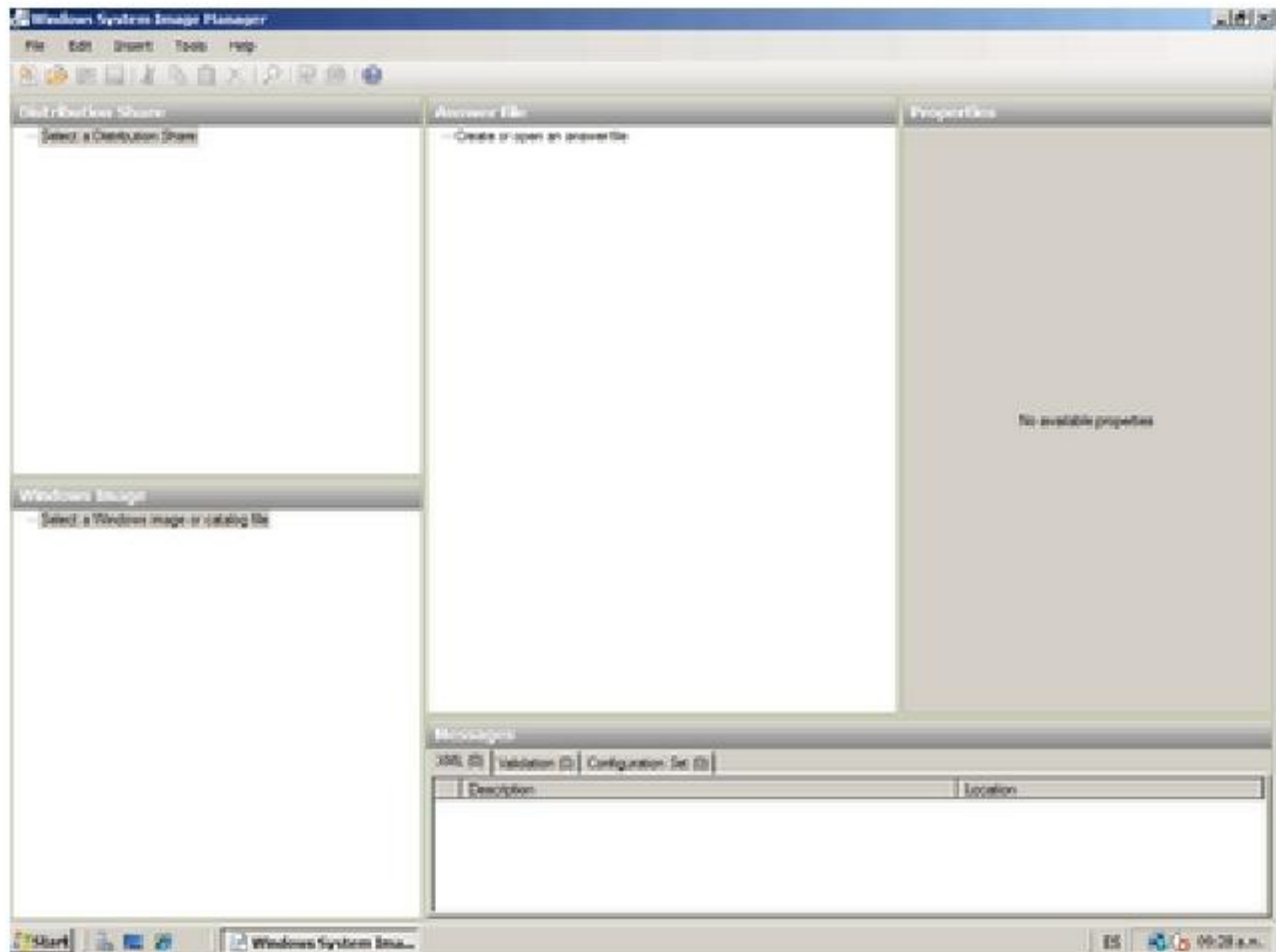
Paso 2 – Tenga el DVD de Windows Server 2008

Dentro del DVD se encuentra un archivo llamado Install.wim, dentro de la carpeta \Sources\ - dependiendo de qué DVD sea (RTM, OEM, etc) puede contener la imagen de la instalación de todas las versiones de Windows 2008 (Estándar, Enterprise, Datacenter, y sus versiones Core, etc) Ese archivo debe copiarse a un volumen para que nos permita generar el catálogo y así poder agregar funciones a nuestra instalación desatendida.

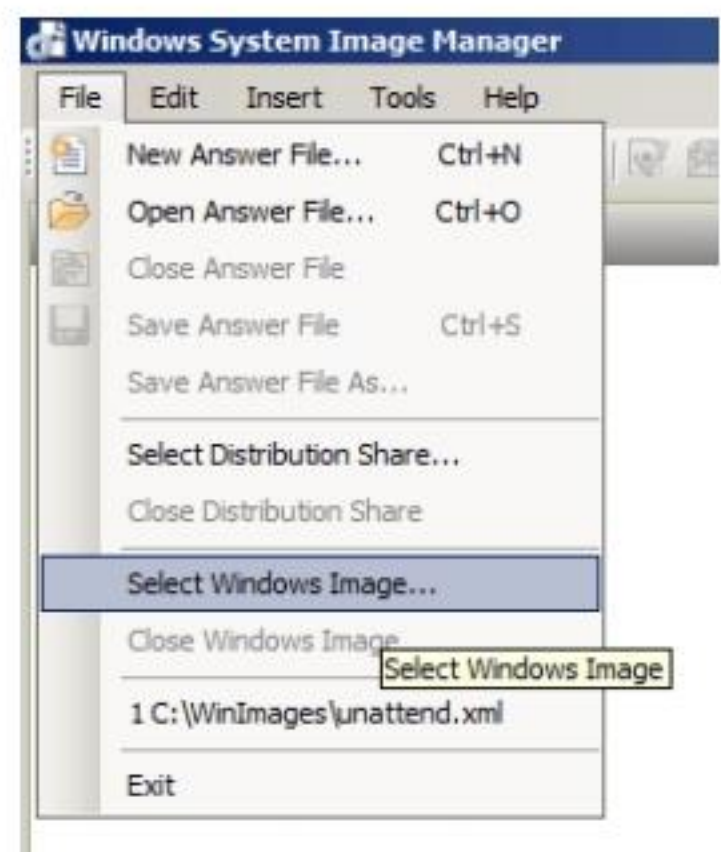


Paso 3- Armar el Catálogo con Windows System Imaging Manager

Abrir el Windows SIM desde Inicio\Todos los Programas\Microsoft Windows AIK\Windows System Image Manager.



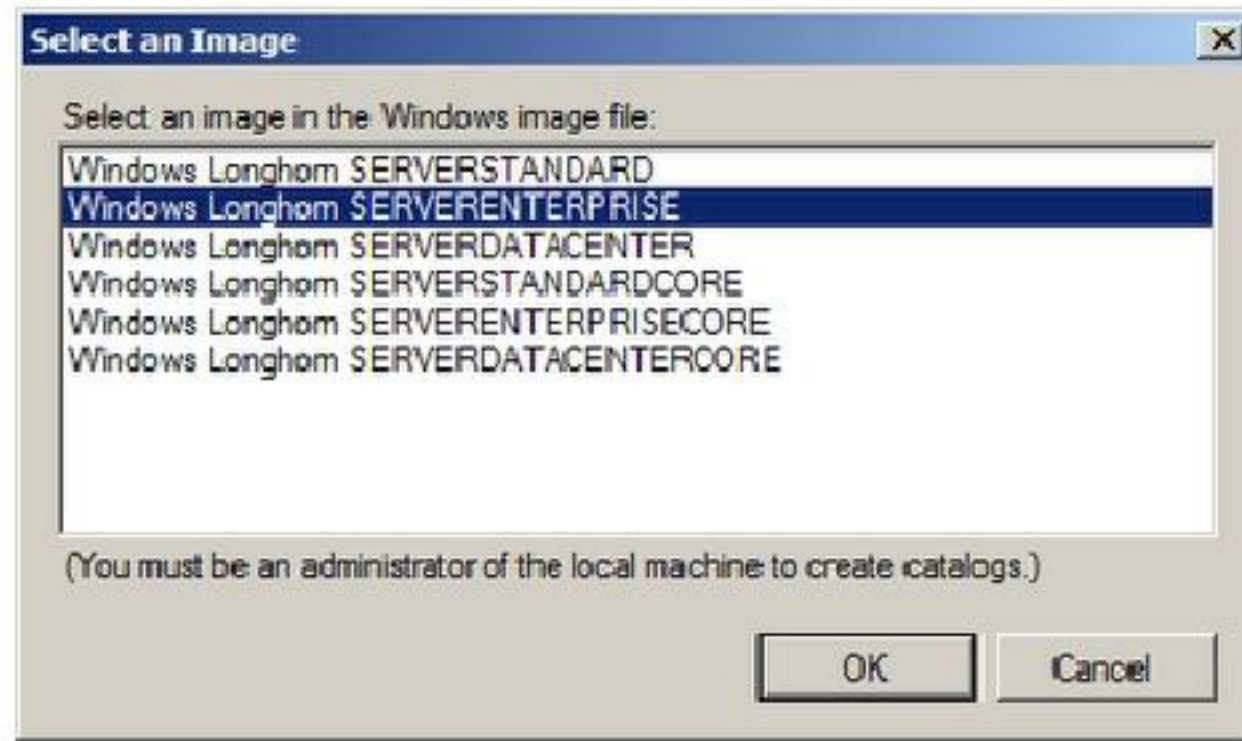
Desde el Menú *File*, seleccionar la opción *Select Image* - esto abrirá un cuadro de diálogo en donde solicitará que se seleccione un archivo de Imagen. Seleccionar el archivo de Imagen que se copió en el punto anterior. Dentro de la imagen están contenidas todas las versiones que se pueden instalar con ella. En este caso selecciono Enterprise porque la imagen que voy a preparar es un Windows Server 2008 Enterprise Edition.



Paso 4 - Crear un nuevo archivo de instalación desatendida.

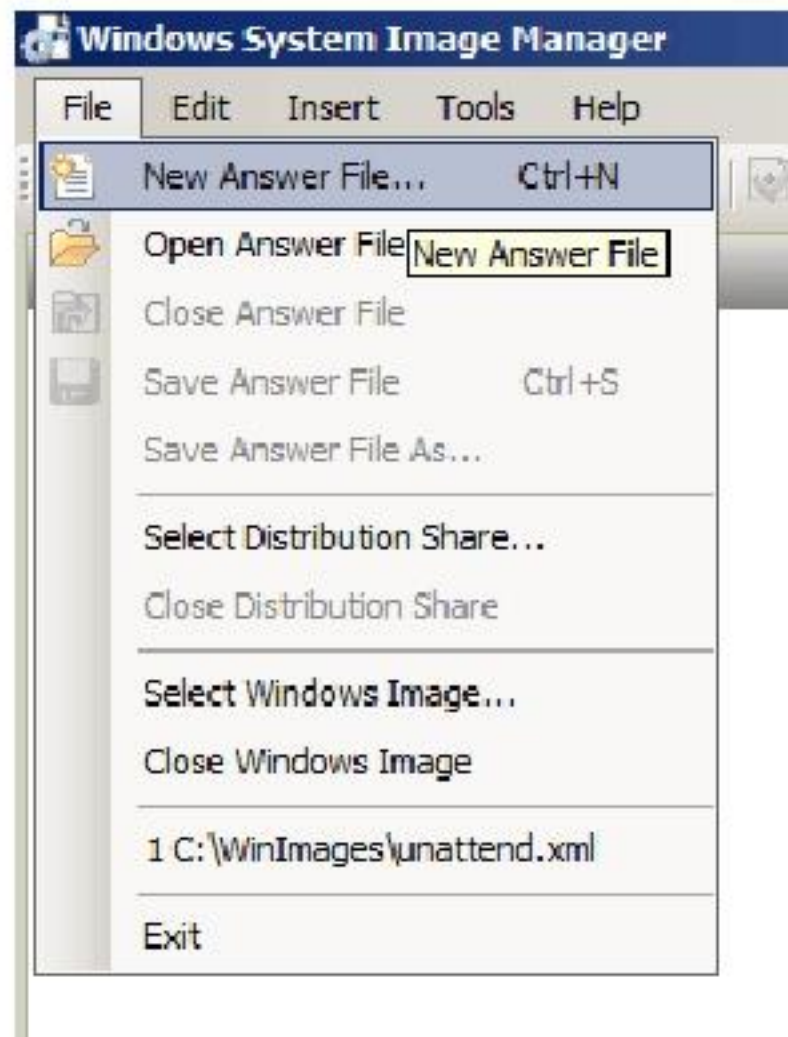
Desde el menú *File* selecciona la opción *New answer File...* - también se puede hacer click con botón derecho sobre *Create or Open an Answer File* y seleccionar la opción *New answer File...*

Esto abrirá un contenedor con los componentes (en donde se ven listadas las Fases de instalación) y un apartado para agregar paquetes. Este archivo no podrá ser guardado hasta que no sea agregada al menos una opción.



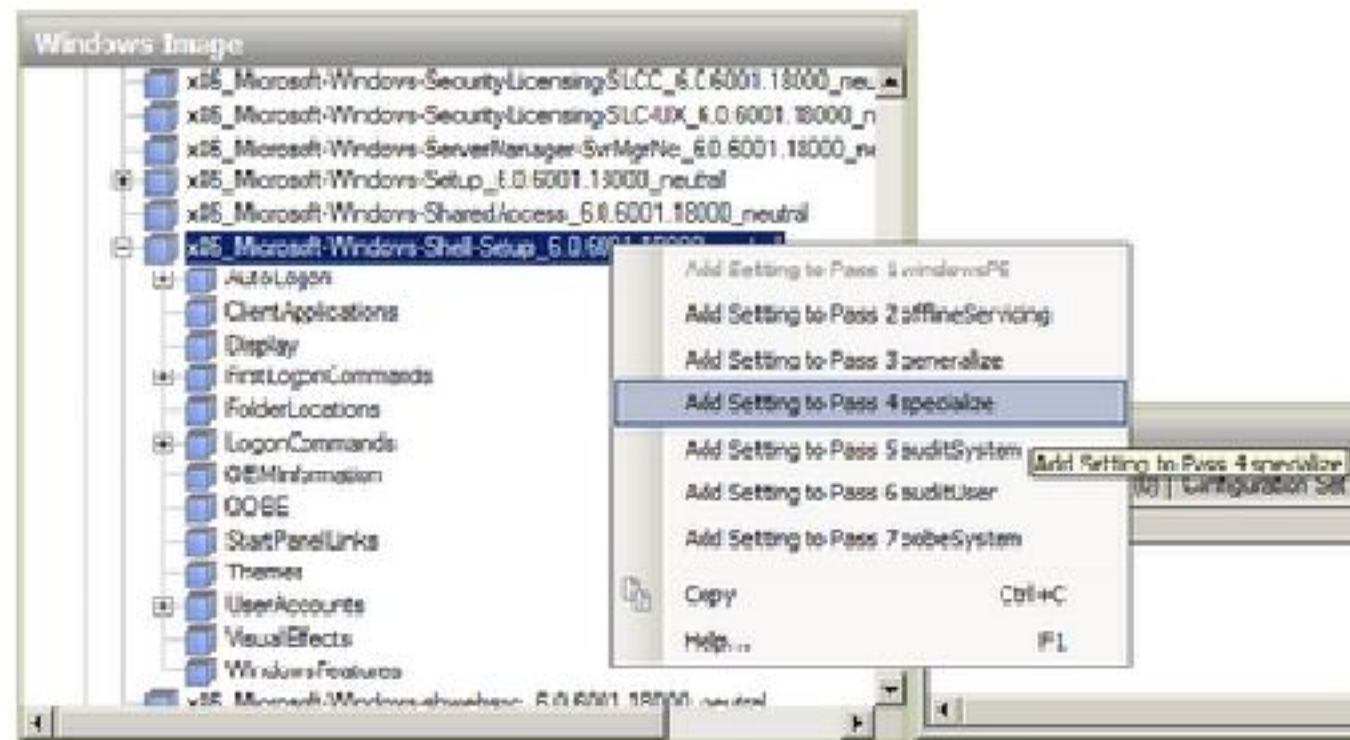
Paso 5 - Agregar las opciones de instalación desatendida para que nuestra imagen esté lista para ser utilizada apenas la necesitemos.

En nuestro caso estamos armando un archivo de instalación desatendida con las opciones necesarias para que el sistema vuelva a reconfigurarse luego de un sysprep. En este ejemplo utilizaremos la entrada **Microsoft-Windows-Shell-Setup**.



Para agregarlas, desde la ventana Windows Image, hay que expandir *Windows Longhorn ENTERPRISE*, luego *Components* y buscamos *x86_Microsoft-Windows-Shell-Setup_6.0.6001.18000_Neutral*.

Con botón derecho seleccionamos *x86_Microsoft-Windows-Shell-Setup_6.0.6001.18000_Neutral* y lo agregamos a la Fase 4 haciendo click en *Add Setting to Pass 4 Specialize* (observar que esta opción puede agregarse a diferentes fases teniendo diferentes campos a llenar según en la fase en la que se agregue - esto permite manejar un solo archivo de instalación desatendida para todo el ciclo de vida de una imagen de Windows 2008)



En el medio de Windows SIM aparecerá en la Fase 4 la opción que acabamos de agregar. Si clickeamos sobre la opción *x86_Microsoft-Windows-Shell-Setup_6.0.6001.18000_Neutral*, sobre la derecha aparecerán los campos a completar.

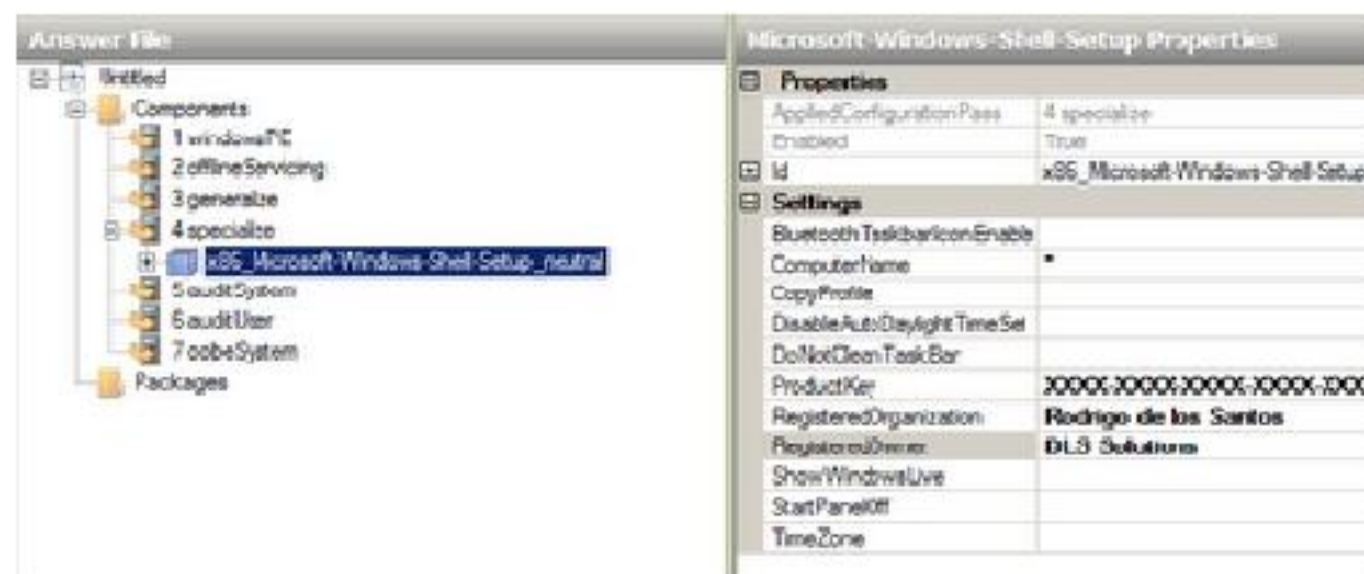
Los campos que conviene completar son:

ComputerName: Nombre de Computadora o * para generación Random

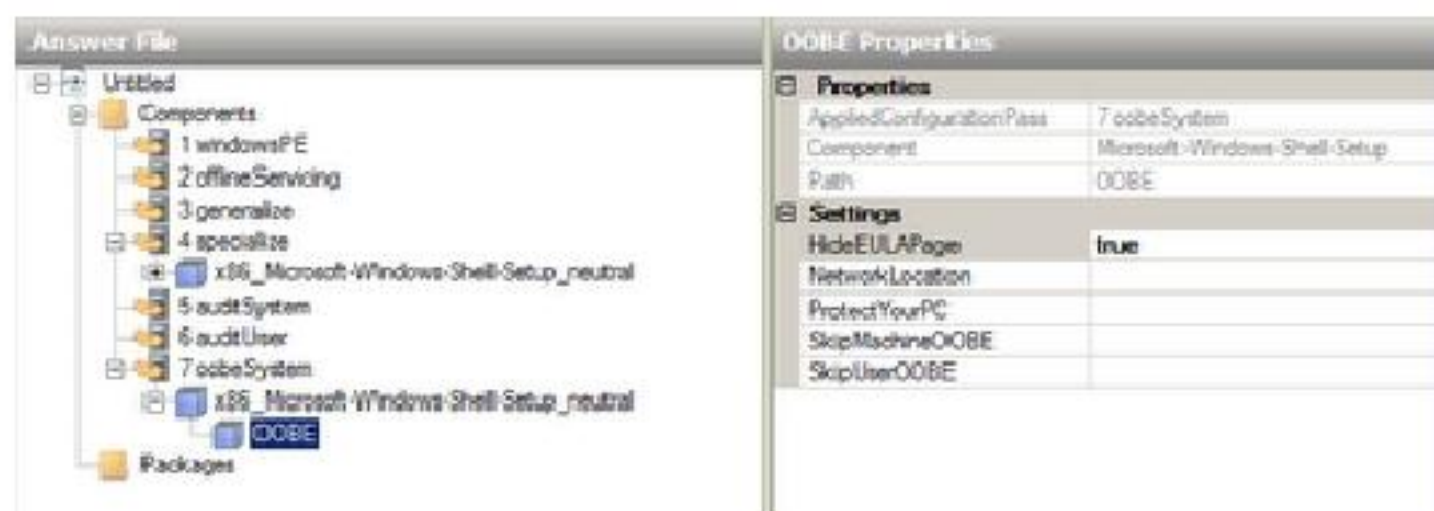
ProductKey: Product Key

RegisteredOwner: Nombre del usuario que registra la licencia de Windows Server 2008

RegisteredOrganization: Nombre del usuario que registra la licencia de Windows Server 2008



Una opción interesante es evitar que nos muestre el Eula. Para ello, debajo de *x86_Microsoft-Windows-Shell-Setup_6.0.6001.18000_Neutral* aparece *OBEE*. Agregamos esa opción a la Fase OobeSystem clickeando con botón derecho sobre OobeSystem y luego *Add Setting to Pass 7 OobeSystem* y ponemos en True la propiedad **HideEulaPages**.

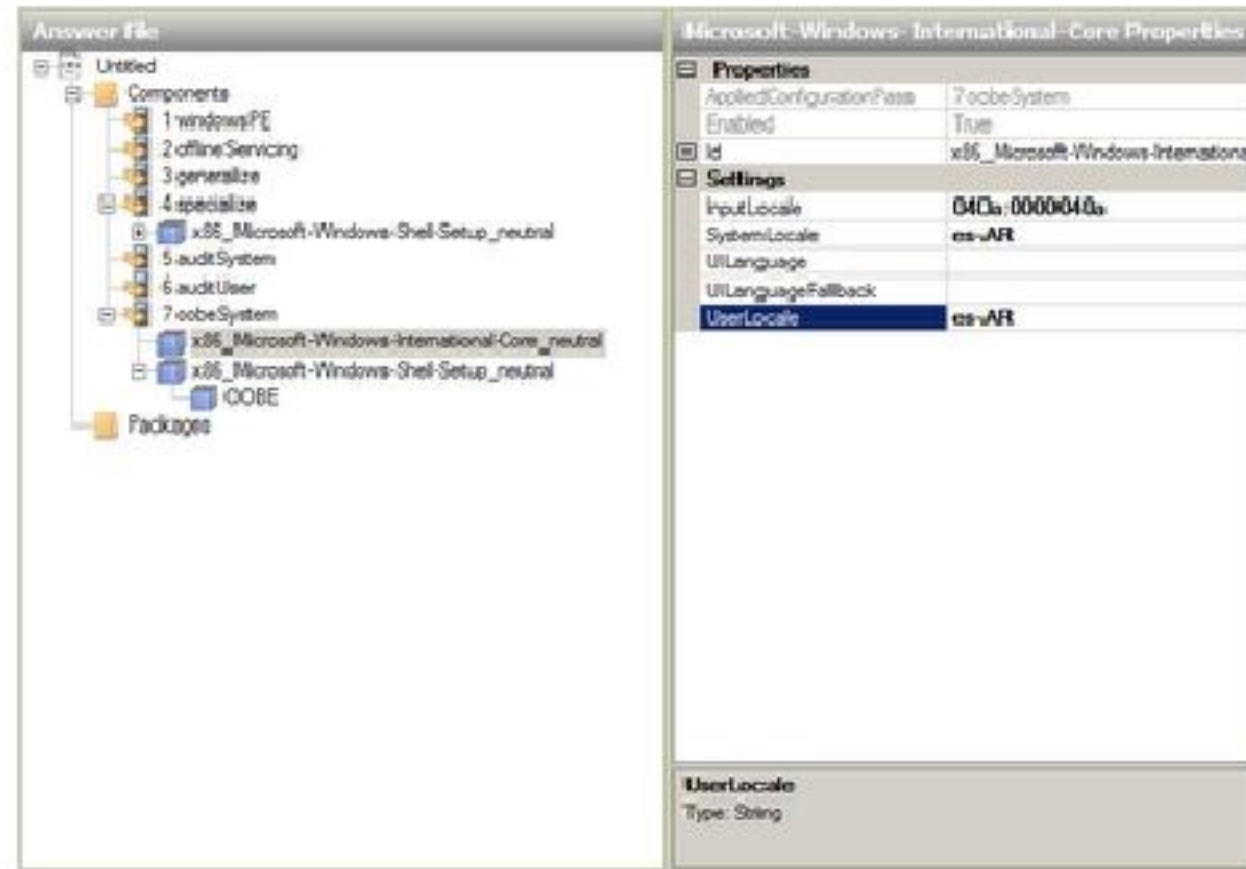


Para que no tengamos que decidir sobre que Input Locale y Lenguaje será el disponible para esa instalación de Windows 2008 se puede agregar *x86_Microsoft-Windows-International-Core_Neutral* en "Pass 7 OobeSystem" y completar los siguientes campos

[InputLocale](#)

[SystemLocale](#)

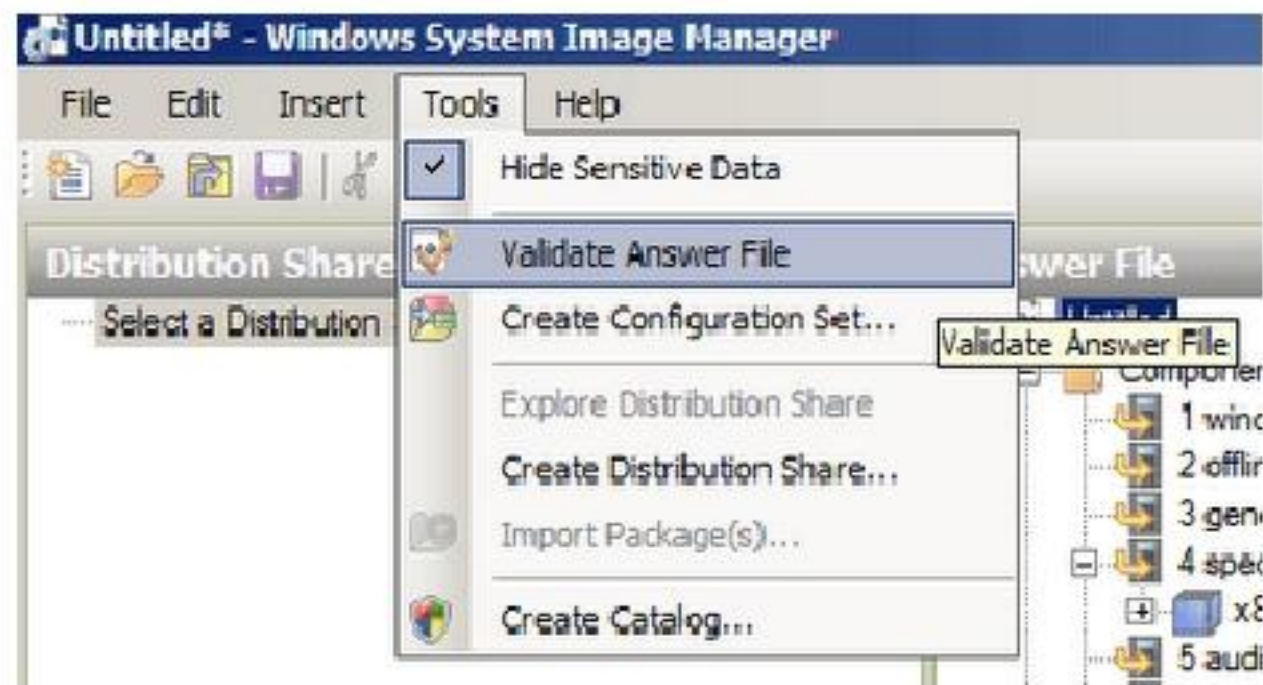
[UserLocale](#)

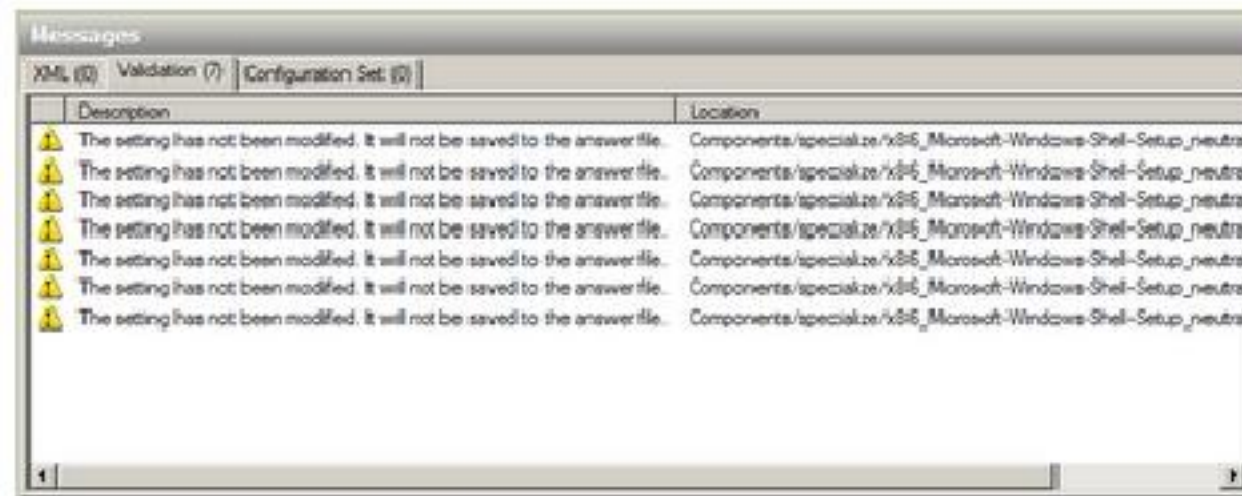


Existen muchísimas opciones más como que el password del usuario Administrator se establezca automáticamente, que la máquina pertenezca a un dominio, etc.

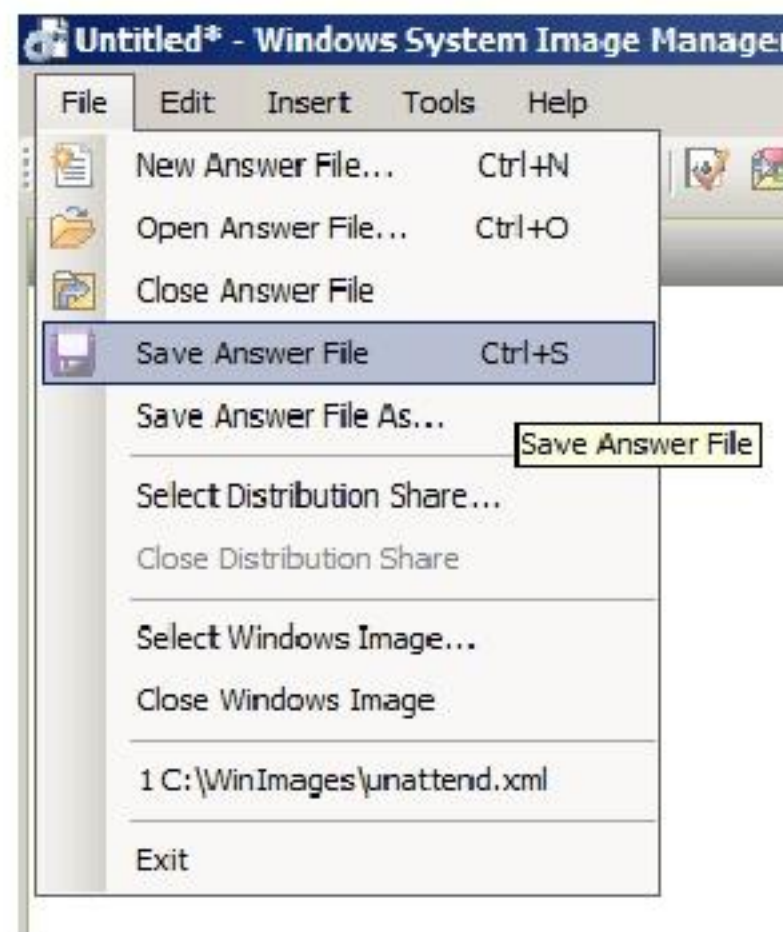
Paso 6 - Validar el Archivo de Instalación Desatendida y Guardarlo.

Para asegurarnos que el archivo se completo correctamente y no nos faltan datos requeridos, desde el menú *Tools* existe la Opción *Validate Answer File*. En el area de mensajes aparecerá la validación del archivo. Ojo porque no validará la KEY si fue ingresada correctamente.





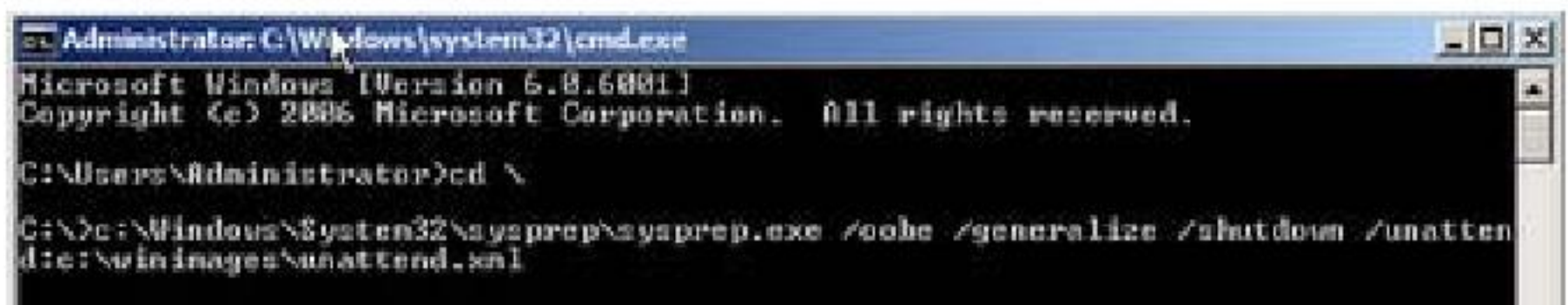
Luego desde el menú *File* se encuentra la opción *Save Answer File* en donde nos pedirá un nombre de archivo con extensión *.xml*



Paso 7 – Listo. Vamos a usar Sysprep

Una vez guardado el archivo con extensión *.xml* solo falta correr sysprep. Para ello se copia el archivo xml en la máquina Origen y se corre el siguiente comando desde la Línea de Comando:

%windir% \system32 \sysprep \sysprep.exe /Oobe /Generalize /shutdown /Unattend:<Ubicación del archivo.xml>



Este comando removerá el SID del sistema operativo y lo marcará para que, cuando encienda, lo haga en modo Oobe ejecutando las instrucciones que hayamos definido en Generalize, Specialize y oobeSystem en el archivo unattend.xml. Además realizará un Shutdown del Sistema Operativo.

Solo resta copiar el VHD a otra ubicación o marcar al archivo como Read Only y utilizarlo como BASE de un disco Diferencial.

Gestión de equipo virtual

A este punto ya se ha conseguido instalar un sistema operativo y necesitará cambiar entre el equipo virtual y el equipo host (aunque quizá ya lo sepa).

Liberar el Mouse

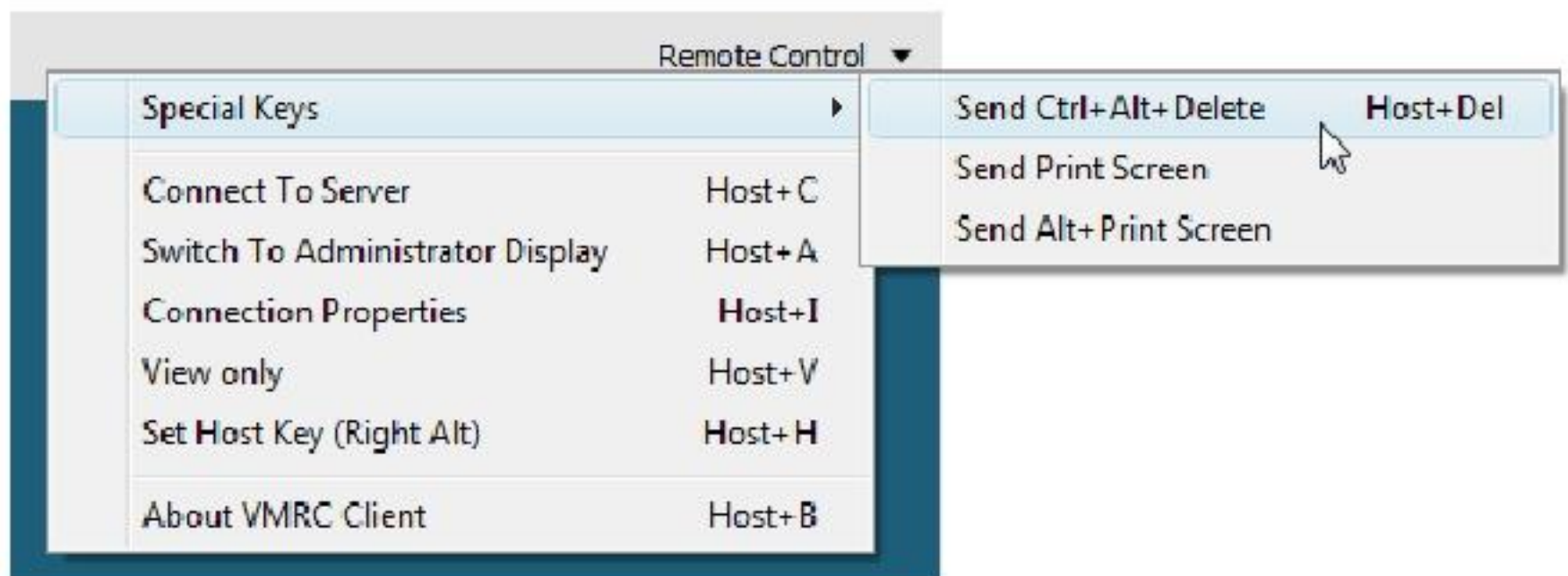
Cuando haya hecho clic dentro de la ventana de la maquina virtual, observará que el mouse es capturado dentro de los límites de la ventana.

Presiones y suelte la tecla Alt Gr y mueva el mouse fuera de la ventana.

Enviar teclas Control + Alt + Supr

Existen dos formas de enviar la combinación Control + Alt + Supr.

1. Utilizar el Menú **Remote Control**.



2. O También puede pulsar AltGr + Suprimir.

Guardar estado y cerrar equipo virtual

1. Use el comando Guardar estado del menú de opciones de la parte inferior de la máquina virtual.



* Advertencia: la seguridad SSL no está habilitada para esta conexión

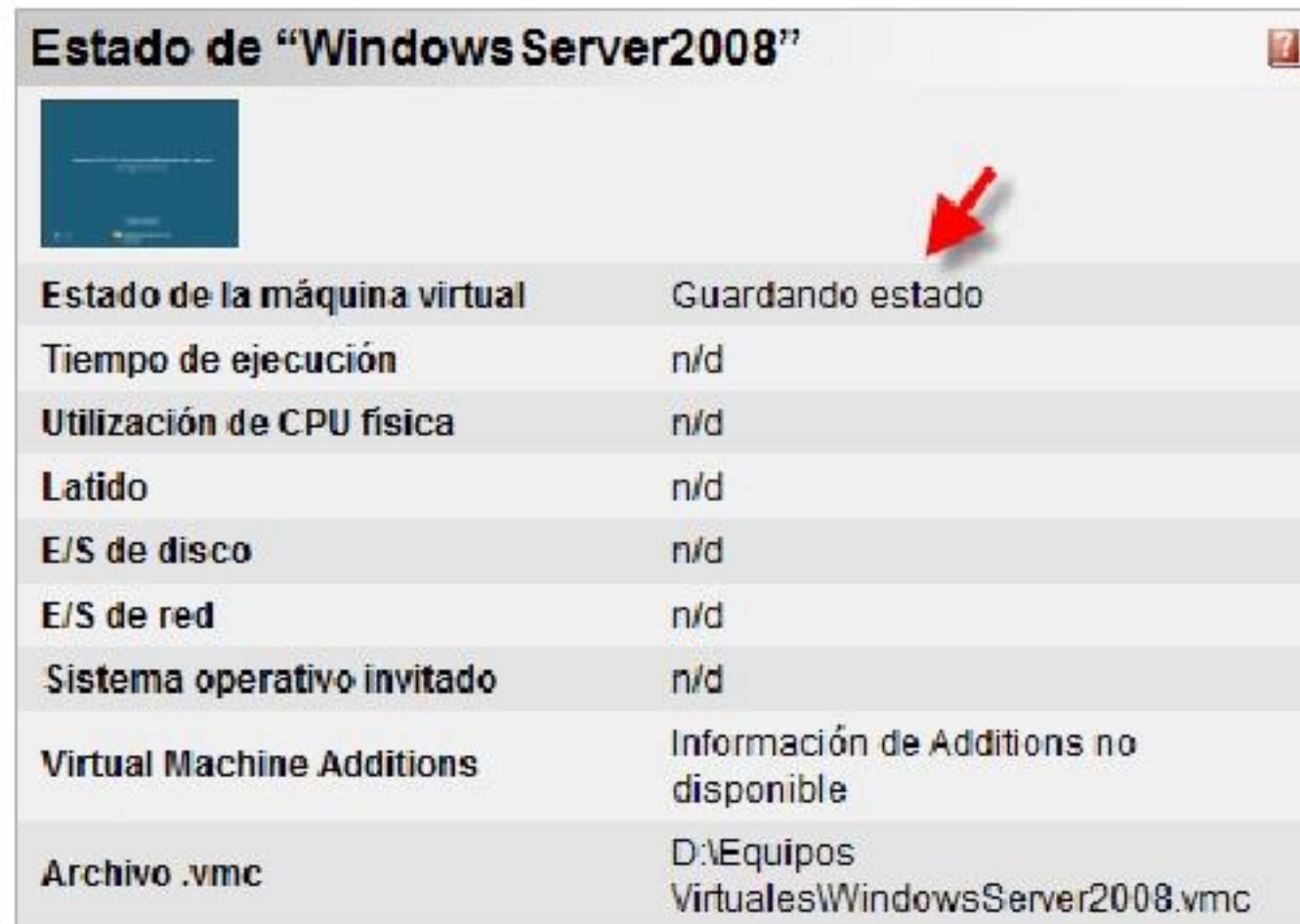


El Control remoto para máquinas virtuales requiere Internet Explorer 8 o superior. Si aparece arriba, compruebe los 'controles ActiveX firmados' adicionales para usar el Control remoto.

Parece que Virtual Machine Control Panel no está instalado cuando haga clic dentro de la ventana del mouse, presione la tecla Alt Gr (de la misma manera predeterminada). Este es un elemento de menú Establecer.



2. Luego visualizará la pantalla de Estado de la máquina virtual con el mensaje **Guardando estado**.



Reanudar equipo virtual

1. Puede hacer clic en la miniatura para restaurar la máquina virtual.



2. O, también puede señalar el nombre del S.O. (WindowsServer2008) y seleccionamos **Restaurar desde el estado guardado**.



Roles del Servidor

Los roles o funciones se agregan o quitan directamente a través de la ventana **Tareas de configuración inicial**, en la sección 3, **Personalizar el servidor**.

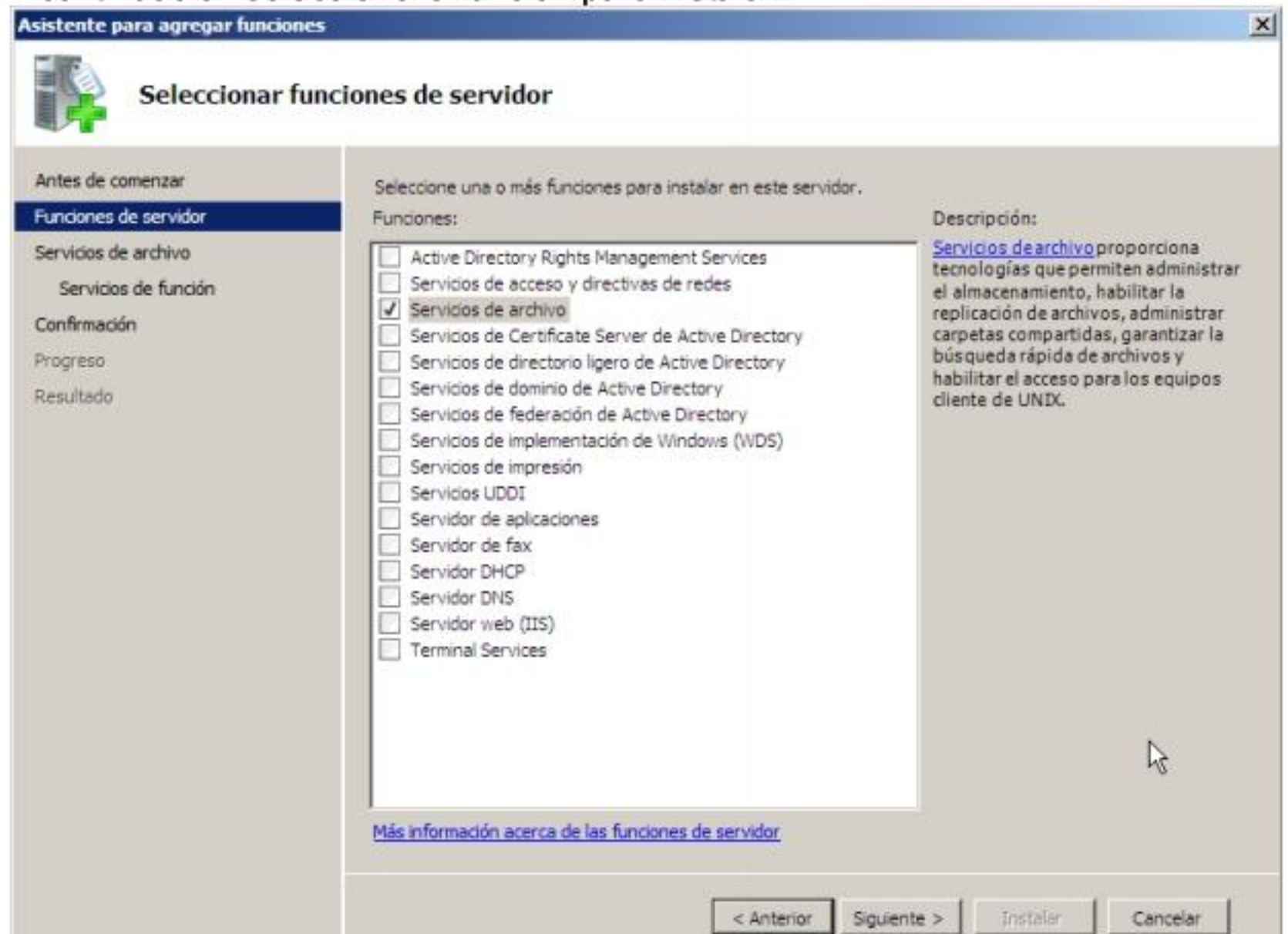
3 Personalizar este servidor Personalizar el servidor

 Agregar funciones	Funciones:	Ninguna
 Agregar características	Características:	Herramientas de administración remota del servidor
 Habilitar Escritorio remoto	Escritorio remoto:	Deshabilitado
 Configurar Firewall de Windows	Firewall:	Activado

Agregar y/o Quitar roles a un Servidor

Agregar función

1. Haga clic en **Agregar funciones**.
2. Se mostrará una ventana de bienvenida
3. Haga clic en **Siguiente**
4. A continuación seleccione la función para instalar.



Asistente para agregar funciones

Seleccionar funciones de servidor

Antes de comenzar

Funciones de servidor

Servicios de archivo

Servicios de función

Confirmación

Progreso

Resultado

Seleccione una o más funciones para instalar en este servidor.

Funciones:

- Active Directory Rights Management Services
- Servicios de acceso y directivas de redes
- Servicios de archivo**
- Servicios de Certificate Server de Active Directory
- Servicios de directorio ligero de Active Directory
- Servicios de dominio de Active Directory
- Servicios de federación de Active Directory
- Servicios de implementación de Windows (WDS)
- Servicios de impresión
- Servicios UDDI
- Servidor de aplicaciones
- Servidor de fax
- Servidor DHCP
- Servidor DNS
- Servidor web (IIS)
- Terminal Services

Descripción:

Servicios de archivo proporciona tecnologías que permiten administrar el almacenamiento, habilitar la replicación de archivos, administrar carpetas compartidas, garantizar la búsqueda rápida de archivos y habilitar el acceso para los equipos cliente de UNIX.

[Más información acerca de las funciones de servidor](#)

< Anterior Siguiente > Instalar Cancelar

5. Haga clic en **Siguiente**, y posiblemente se le pida que configure algunas opciones propias de cada opción seleccionada, continúe con el proceso hasta llegar al botón **Instalar**.

Quitar función

Para quitar una función:

1. Haga clic en Inicio, y seleccione **Administrador del Servidor**.
2. Haga clic en **Funciones**.
3. Haga clic en **Quitar funciones**.



Tareas de configuración Inicial

Existen tareas comunes que de forma continua se verifican o realizan en un Servidor.

Tales como:

1. Establecer la zona horaria
2. Configurar los adaptadores de red
3. Configurar el nombre de equipo y dominio
4. Configurar las actualizaciones automáticas
5. Agregar funciones.



Comandos a través de la Consola

La instalación de línea de comandos del Administrador de servidores acepta parámetros para instalar o quitar una o varias funciones, servicios de función y características separadas por espacios. Si desea instalar o quitar más de una función, servicio de funciones o características en un servidor mediante una sola consola.

Utilizaremos el comando **ServerManagerCmd.exe**.

Sintaxis:

ServerManagerCmd.exe -query [<consulta.xml>] [-logPath <registro.txt>]

ServerManagerCmd.exe -inputPath <respuesta.xml> [-resultPath <resuelto.xml>]

ServerManagerCmd.exe -install <Id. del comando> [setting <nombre de configuración>]*[-allSubFeatures] [-resultPath <resultado.xml> [-restart] | -whatIf] [-logPath <registro.txt>]

ServerManagerCmd.exe -remove <Id. del comando> [-resultPath <resultado.xml> [-restart] | -whatIf] [-logPath <registro.txt>]

ServerManagerCmd.exe [-help | -?]

ServerManagerCmd.exe -version

Ejemplos

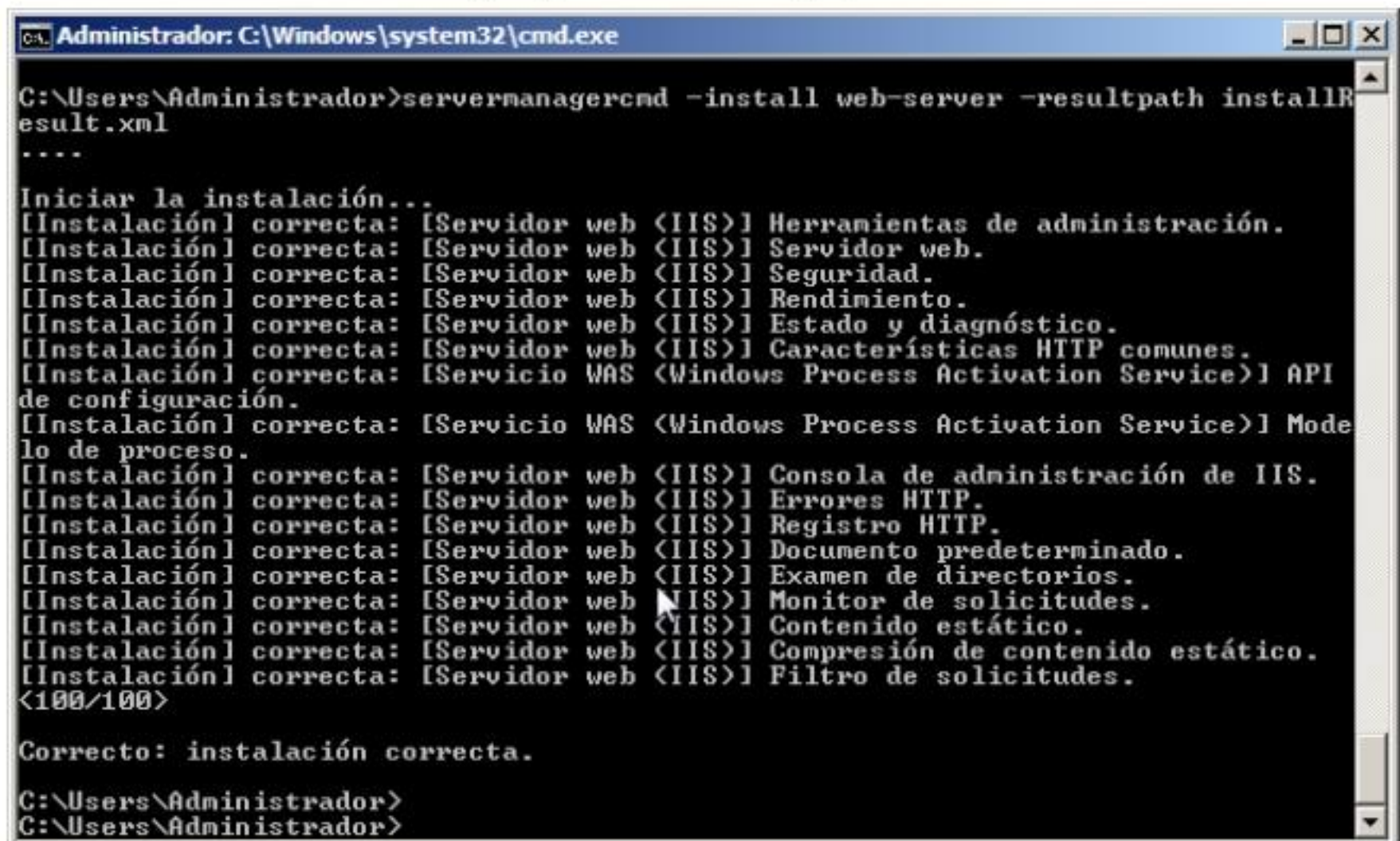
ServerManagerCmd.exe -query

ServerManagerCmd.exe -install Web-Server -resultPath installResult.xml

ServerManagerCmd.exe -inputPath install.xml -whatIf

Resultado de Instalar un servidor Web

Observe el proceso de instalación de cada componente necesario para utilizar Internet Information Services (IIS) y convertir el equipo en un servidor web.





Preguntas de Repaso

1. Investigación:
 - a. Qué diferencia de un disco virtual diferencial de un disco virtual típico.
 - b. Qué comando utilizaría para instalar un servidor WINS usando el comando ServerManagerCmd.
 - c. Al instalar varios sistemas operativos en una máquina se genera un menú de booteo que aparece al encender el equipo ¿De qué manera se puede cambiar las descripciones de nombre para cada sistema operativo instalado en ese menú?
2. Describa el proceso de instalación del complemento Virtual Machine Additions e indique para qué sirve.
3. Elabore un cuadro comparativo entre la tecnología Xeon e Itanium
4. Qué diferencia tiene la arquitectura x86 y x64.
5. Qué caracteriza una arquitectura de 32bits y 64bits.



Implementación de Active Directory en la infraestructura de red

En este capítulo trataremos:

- Identificará las características del Active Directory
- Reconocerá la terminología de Active Directory.
- Identificará la arquitectura del Active Directory
- Comprenderá la planificación del espacio de nombres y dominios.

Introducción:

El Active Directory permite gestionar los diferentes objetos de nuestra arquitectura de red. Es importante e imprescindible su uso para el administrador.



Introducción a los servicios de directorio

El servicio de directorio se encarga de administrar todos los objetos del sistema de red. En versiones anteriores de Windows server se utilizó Active Directory para esta tarea pero en Windows Server 2008 se utiliza Active Directory Domain Services (AD DS).

Por otro lado, Active Directory Lightweight Directory Services reemplaza a "Active Directory Application Mode" o ADAM.

De tal manera que con estas funcionales el Servidor realizará los siguientes roles:

1. AD DS
2. AD LDS y
3. DNS.

Se administran centralmente a través del Server Manager

Al Instalar estos servicios en un Server Core se provee de una menor superficie de ataque debido a los pocos componentes instalados.

AD DS proporciona una base de datos distribuida que almacena y administra información acerca de los recursos de red y datos específicos de las aplicaciones con directorio habilitado. Los administradores pueden usar AD DS para organizar los elementos de una red (por ejemplo, los usuarios, los equipos y otros dispositivos) en una estructura de contención jerárquica. La estructura de contención jerárquica incluye el bosque de Active Directory, los dominios del bosque y las unidades organizativas de cada dominio. El servidor que ejecuta AD DS se llama controlador de dominio.

Terminología de Active Directory

Bosque

El bosque actúa como un límite de seguridad para la organización y define el ámbito de autoridad de los administradores. De forma predeterminada, el bosque contiene un solo dominio llamado dominio raíz del bosque.

Árbol

Debería crear un árbol de dominios sólo si es necesario crear un dominio cuyo espacio de nombres DNS no está relacionado con los demás dominios del bosque. Esto significa que no es necesario que el nombre del dominio raíz del árbol (y todos sus dominios secundarios) contenga el nombre completo del dominio primario.

Por ejemplo, treyresearch.net puede ser un árbol de dominios del bosque contoso.com. Lo más habitual es que se creen árboles de dominios como parte de una adquisición comercial o una fusión de varias organizaciones. Un bosque puede contener uno o más árboles de dominios.

Antes de crear un árbol de dominios, cuando desee un espacio de nombres DNS diferente, considere la posibilidad de crear otro bosque. La opción de varios bosques proporciona autonomía administrativa, aislamiento de las particiones de directorio de configuración y esquema, límites de seguridad independientes y la flexibilidad de usar un diseño de espacio de nombres independiente para cada bosque.

Dominio

Se pueden crear dominios en el bosque para facilitar la partición de los datos de AD DS, lo que permite a las organizaciones replicar datos sólo si es necesario. Esto permite que AD DS se ajuste de forma global en una red con un ancho de banda limitado. Además, un dominio de Active Directory es compatible con otras funciones clave relacionadas con la administración, incluidas la identidad de usuario, la autenticación y las relaciones de confianza en la red.

Unidades organizativas

Las unidades organizativas simplifican la delegación de autoridad para facilitar la administración de un gran número de objetos. Mediante la delegación, los propietarios pueden transferir una autoridad total o limitada sobre los objetos a otros usuarios o grupos. La delegación es importante porque ayuda a distribuir la administración de un gran número de objetos para una serie de usuarios en quienes se confía para realizar tareas de administración.

Sitios

Los sitios de AD DS representan la estructura física, o topología, de la red. AD DS usa la información de topología de red, que se almacena en el directorio como objetos de sitio, subred y vínculo a sitios, para generar la topografía de replicación más eficaz. La topología de replicación en sí consta de un conjunto de objetos de conexión que permiten la replicación de entrada desde un controlador de dominio de origen al controlador de dominio de destino que almacena el objeto de conexión.

Es importante distinguir entre sitios y dominios. Los sitios representan la estructura física de la red, mientras que los dominios representan la estructura lógica de la organización. Los objetos de sitios y sus contenidos se replican en todos los controladores de dominios del bosque, independientemente del dominio o del sitio

SubRed

Un objeto de subred de AD DS agrupa a los equipos adyacentes prácticamente de la misma forma que los códigos postales agrupan las direcciones postales adyacentes. Al asociar un sitio con una o más subredes, se asigna un conjunto de direcciones IP al sitio.

El término "subred" en AD DS no tiene la definición de conexión exacta del conjunto de todas las direcciones que hay detrás de un único enrutador. El único requisito de una subred de AD DS es que el prefijo de la dirección se ajuste al formato IP versión 4 (IPv4) o IP versión 6 (IPv6).

Cuando se agrega la función de servidor de Servicios de dominio de Active Directory para crear el primer controlador de dominio en un bosque, se crea un sitio predeterminado (Default-First-Site-Name) en AD DS. Mientras éste sea el único sitio del directorio, todos los controladores de dominio que se agreguen al bosque se asignarán a este sitio. Sin embargo, si el bosque tiene varios sitios, se deben crear subredes que asignen direcciones IP a Default-First-Site-Name así como a todos los sitios adicionales.

Vínculo entre sitios

Las redes suelen constar de un conjunto de redes de área local (LAN) que se conectan mediante WAN. En AD DS, los objetos de vínculos a sitios representan las conexiones de WAN entre sitios. Mientras que la replicación dentro de un sitio se desencadena automáticamente cuando se produce la actualización de un directorio,



la replicación entre sitios (a través de vínculos WAN más costosos y lentos) está programada para que se produzca cada tres horas. Puede cambiar el programa predeterminado para que se produzca durante los períodos que especifique y al final de los intervalos que indique, de forma que pueda controlar el tráfico de vínculos de WAN

Relación de confianza

Es una relación que permite que los usuarios de un dominio puedan acceder a los recursos de otro dominio que no sea del grupo matriz y viceversa. Partiendo de este punto, un proveedor puede hacer que su directorio activo mantenga una relación con el de sus clientes para manejar accesos a aplicaciones puntuales siempre con esquemas de seguridad definidos.

Administración de esquemas

Es el conjunto de definiciones de los tipos de objeto que puede contener el Directorio Activo y se encuentra almacenado en todos los controladores de dominio del bosque.

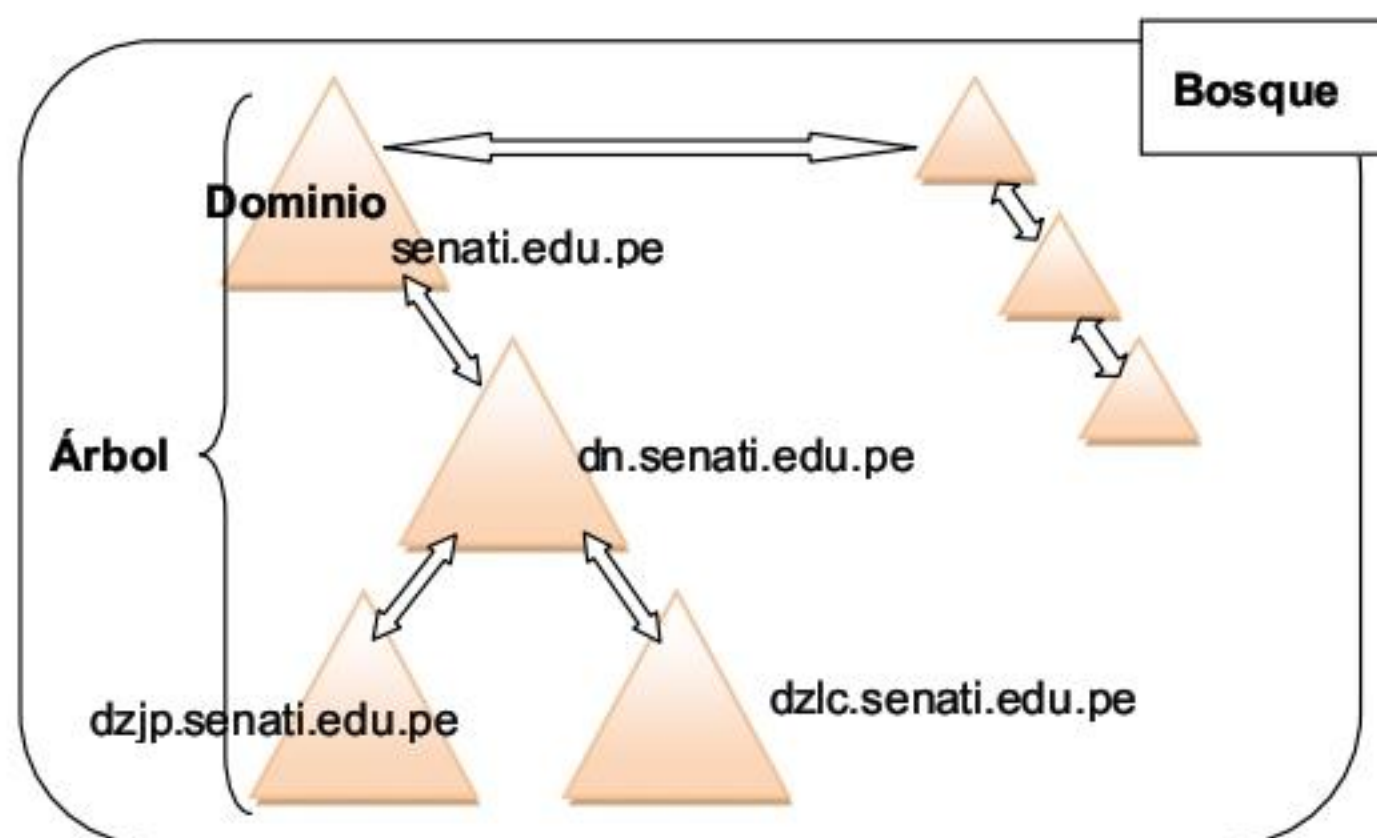
Catálogo Global

Se compone de toda la información de todos los dominios del bosque y se alhoja en una base de datos dispersa en uno o varios servidores. Esto agiliza la búsqueda de objetos a través de los diferentes dominios, proporciona información acerca de los miembros de los grupos universales y autenticar a los usuarios que usan un Nombre de Dominio Principal (UPN).

Planificación de espacio de nombres y dominios

Al crear un espacio de nombres, debe elegir uno de los dos tipos de espacios de nombres: un espacio de nombres independiente o un espacio de nombres basado en el dominio. Además, si elige un espacio de nombres basado en el dominio, debe elegir un modo de espacio de nombres: modo Windows 2000 Server o modo Windows Server 2008.

Al crear un espacio de nombres, debe elegir un espacio de nombres independiente o un espacio de nombre basado en el dominio. Elija un espacio de nombres independiente si se da alguna de las siguientes condiciones en el entorno



Arboles y bosques

El contenedor del Directorio Activo de mayor tamaño se denomina Bosque. Dentro de los Bosques se encuentran los Dominios y dentro de los Dominios están las Unidades Organizativas.

Dependiendo del tamaño de la empresa deberá instalarse varios controladores de dominio, los cuáles se compondrán de un **Dominio Raíz**, con varios **subdominios** formando un árbol invertido. Cada subdominio contará con su propio **Controlador de Dominio** pero estarán unidos a través de **Relaciones de confianza** entre **Dominios** y **Réplica** (total o parcial) de la base de datos del Servicio de directorio. Cada **Controlador de dominio** será un equipo-servidor individual. Un mismo equipo-servidor no puede ser controlador de varios dominios.

Las Relaciones de confianza entre los dominios de un árbol son obvias y automáticas, mientras que las de distintos árboles en un bosque pueden no serlo.

Todos los árboles de un bosque comparten el mismo **catálogo global** (la base de datos donde se almacena el esquema y los datos del directorio) y cuentan con relaciones de confianza que permiten, por ejemplo, que un usuario de un dominio inicie sesión en otro dominio del mismo bosque.

Dominios y unidades organizativas

Se puede definir un dominio, también, como un conjunto de normas que permiten administrar los recursos y clientes en una red local. Al utilizar un solo dominio se simplifican mucho las tareas administrativas.

Las unidades organizativas son contenedores del Directorio Activo en los que pueden colocar: Usuarios, grupos, equipos y otras unidades organizativas. No puede contener objetos de otros dominios.

Diseño de una estructura de dominios

Es importante planificar el crecimiento de la red y los recursos que requerirá cada parte de la organización, eso nos permitirá determinar cuántos controladores de dominio se necesitan.

De tal manera que tendrá que considerar los sitios que creará, los controladores de dominio, unidades organizativas etc.

Los sitios abarcan varios dominios, pero no forman parte del espacio de nombres del dominio, controla la replicación de la información del dominio y ayudan a determinar la proximidad de los recursos.

Cada controlador de dominio usa un Security Account Manager (SAM) para mantener una lista de combinaciones nombre_usuario y contraseña. El controlador de dominio entonces forma una central repositoria de passwords que están enlazadas a nombres de usuario (un password por usuario), lo cual es más eficiente que mantener en cada máquina cliente, centenares de passwords para cada recurso de red disponible.



Instalación de Active Directory

Instalar el Servicio de controlador de dominio

Para instalar el Active Directory primero debe configurar el Servicio de Dominios en el equipo servidor, y para ello siga los siguientes pasos:

1. En la ventana **Administrador del Servidor** haga clic en **Agregar Funciones**.



2. Seleccione el elemento **Servicios de Dominio de Active Directory**.



Tal como indica la descripción: El servicio de dominio de Active Directory almacena información acerca de los objetos de la red y pone esta información a disposición de los usuarios y administradores de red. AD DS usa CONTROLADORES DE DOMINIO para proporcionar a los usuarios de red, acceso a los recursos permitidos en toda la red mediante un único proceso de inicio de sesión.

3. Haga clic en **Siguiente**.
4. Para confirmar que se desea instalar funciones, servicios o características, haga clic en **Siguiente**.
5. Confirme los servicios seleccionados y haga clic en **Instalar**.



6. Se mostrará el progreso de la instalación. Espere un momento.



- Esta primera parte concluirá con una ventana en la que se indica que el Servicio de dominio de Active Directory, ya se instaló correctamente y que ahora puede proceder con instalar un Controlador de Dominio. Clic en Cerrar.

Instalar el primer controlador de dominio

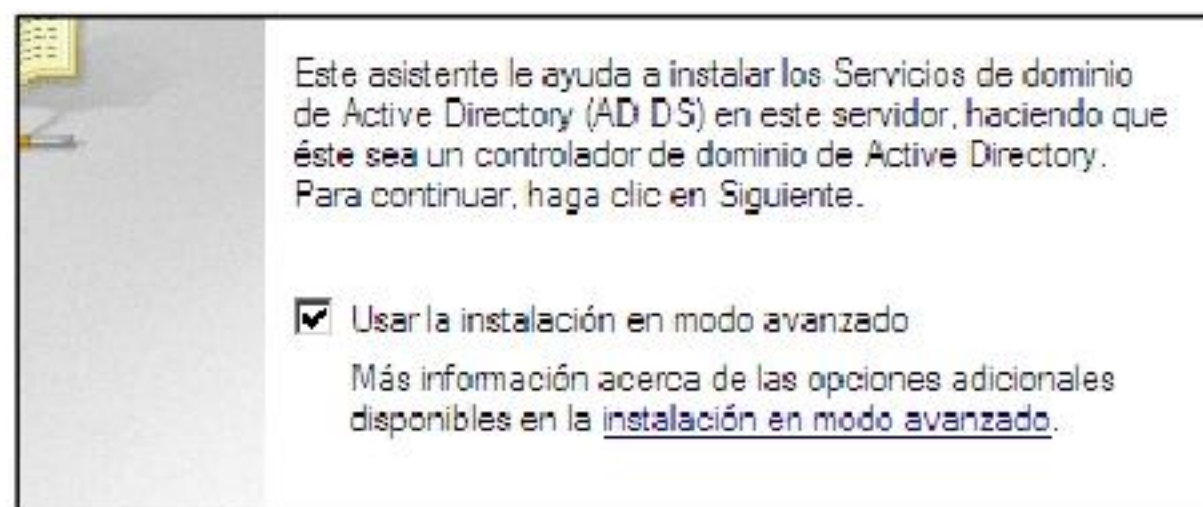
Con esto se ha terminado de preparar el equipo para la función de Servicio de Directorio, pero ahora se necesita convertirla en un Controlador de dominio, para ello haremos una PROMOCIÓN del equipo a CONTROLADOR DE DOMINIO usando el comando DCPROMO.

Pero antes revisemos algunos requisitos previos a la instalación:

- Se debe iniciar con nivel sesión con privilegios de administrador.
- Para instalar el complemento **Esquema del Directorio Activo** (sólo para controladores de dominio), escriba en el símbolo de sistema: **regsvr32 schmmgmt.dll**, con lo que se logra que esté disponible en la consola Microsoft (MMC).
- Tenga claro qué tipo de instalación va a realizar: Un controlador de dominio para un dominio nuevo o un controlador de dominio adicional, se va a establecer un árbol de dominio nuevo o dominio secundario, o si se crea un nuevo bosque o dentro de un bosque ya existente.
- Configure los dispositivos de red y/o modem, conecte los cables y dispositivos de conectividad externos (por ejemplo un switch)
- Debe asignarse una dirección IP estática.
- Defina previamente una partición o disco para instalar la Base de datos y el Registro de Transacciones. Los cuales se deben almacenar en volúmenes diferentes.
- Haga clic en Inicio, escriba DCPROMO y pulse Enter.



- Se iniciará el asistente, active la casilla **Usar la instalación en modo avanzado**. Luego haga clic en siguiente.



- A continuación recibirá un aviso de **Compatibilidad de sistema operativo**. Algunas aplicaciones y servicios que requieran un nivel de seguridad más alto (es decir menos vulnerables) probablemente no funcionen adecuadamente. Haga clic en Siguiente



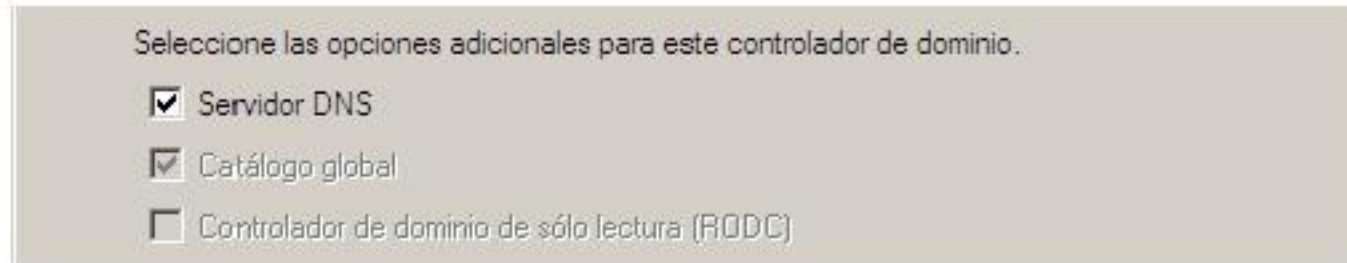
10. A continuación seleccione **Crear un dominio nuevo en un bosque nuevo** y haga clic en **Siguiente**.

11. Ahora defina el nombre DNS para el dominio raíz del bosque, para nuestro caso asignaremos el nombre **senati.edu.pe**. Luego haga clic en **Siguiente**.
12. Asigne el nombre NetBIOS, que permitirá identificar al dominio en equipos que tienen versiones anteriores de Windows, especialmente las versiones que no soportan nombres DNS, como Windows 98 y Windows NT 4.0. En nuestro caso será **SENATI**.

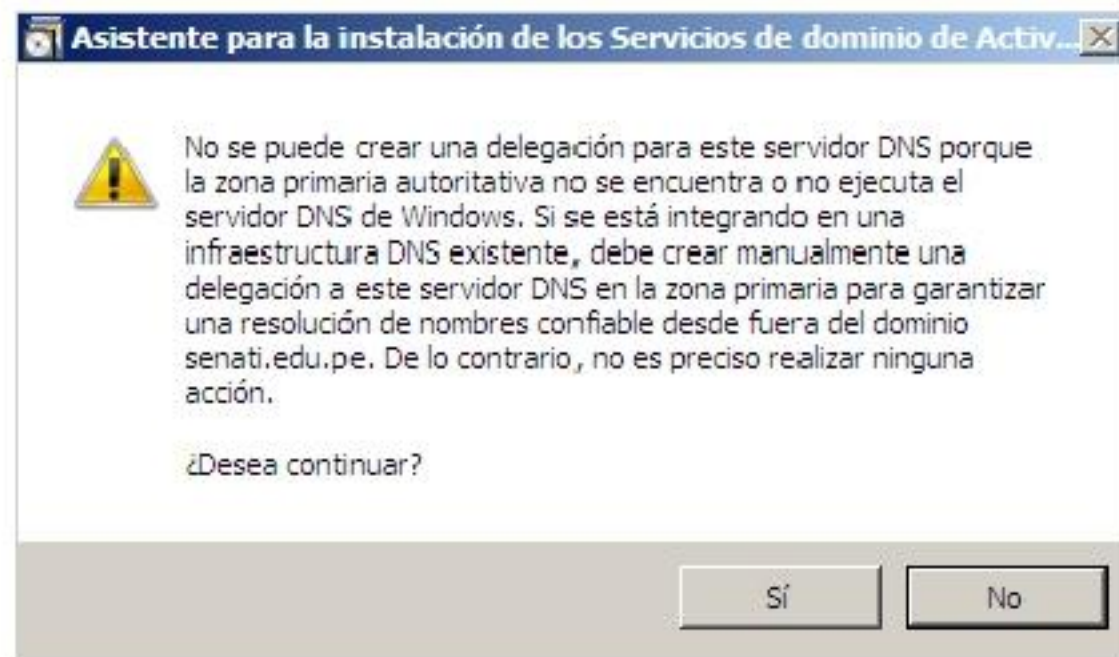
13. Seleccione el **Nivel de funcionamiento del bosque**, el cuál definirá qué características estarán disponibles en todo el bosque. **Windows 2000**.

14. Seleccione el **Nivel de funcionamiento del dominio: Windows 2000 nativo**.

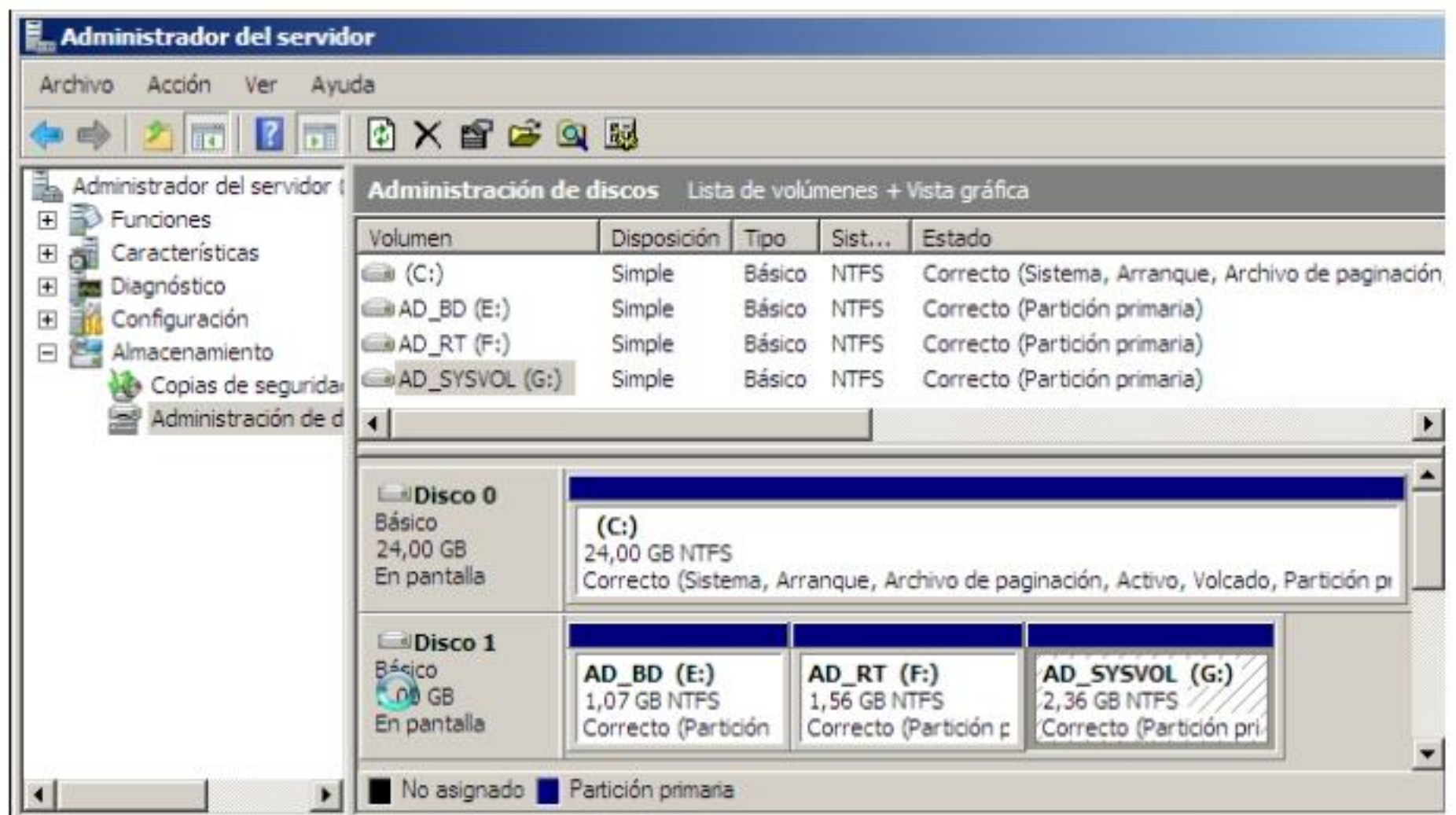
15. Uno de los requisitos para Active Directory es que el controlador de dominio raíz también tenga instalado el servicio DNS, por eso lo instalaremos a continuación.



16. Debido a que aún no se ha instalado DNS recibirá el siguiente mensaje. Haga clic en **Sí**.

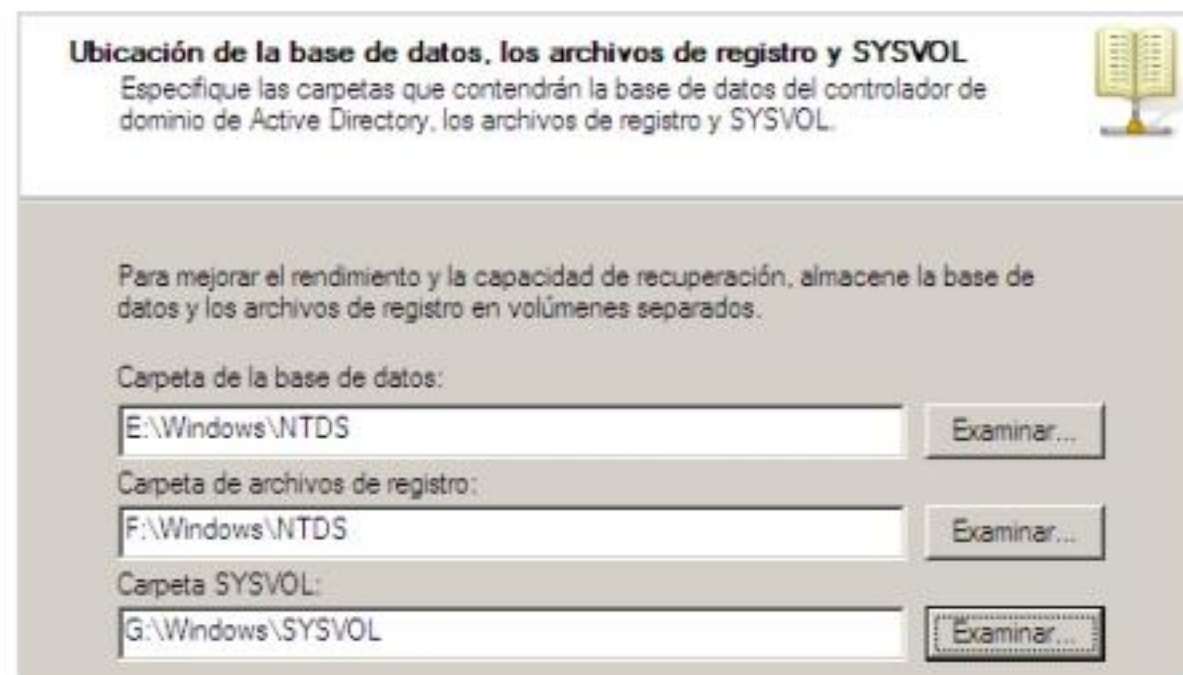


17. El Active Directory guardará su base de datos por defecto en la Unidad C:\Windows\NTDS. Pero adicionalmente tendrá que indicar la ubicación de la carpeta de archivos de registro y la carpeta SYSVOL. La mejor configuración en lo que a rendimiento se refiere, es guardar la base de datos y el archivo de registros en diferentes particiones y en un disco duro diferente al disco de Inicio del sistema. Es por eso que debe crear 3 particiones simples en el Segundo disco duro.

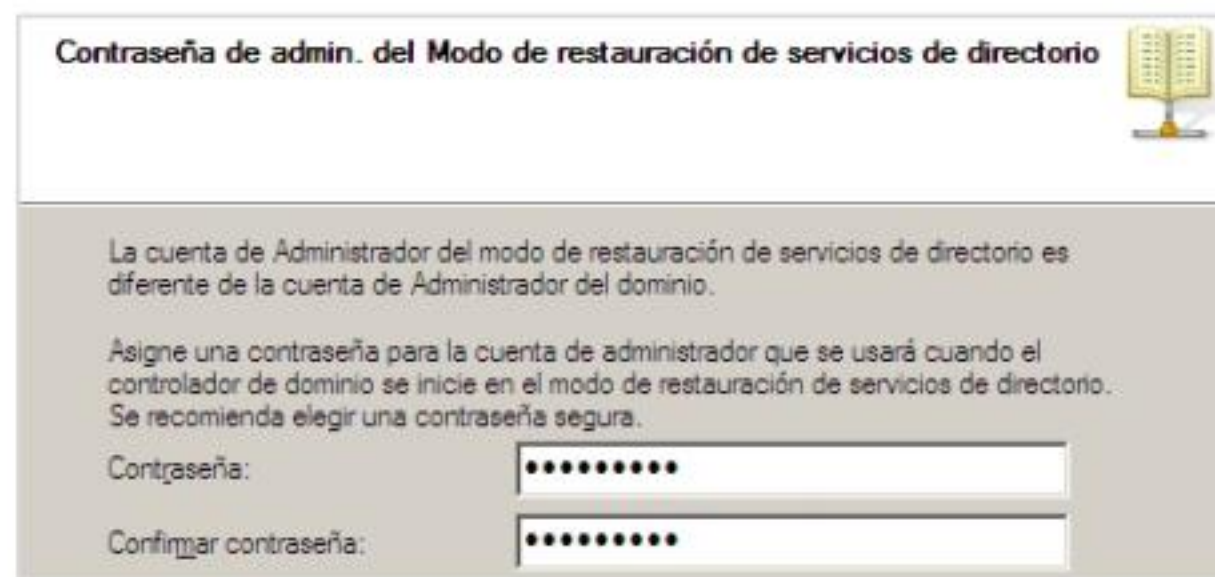




18. Ahora configure las opciones según aparece en la siguiente ventana. Y hacemos clic en Siguiente.



19. Como cualquier otro sistema el Windows Server pudiera experimentar un fallo en el Servicio de Directorio. Para ello se ha creado un modo de ingreso al sistema llamado **modo de restauración del servicio de directorio** el cual permite restaurar el Active Directory a través de un Backup previo



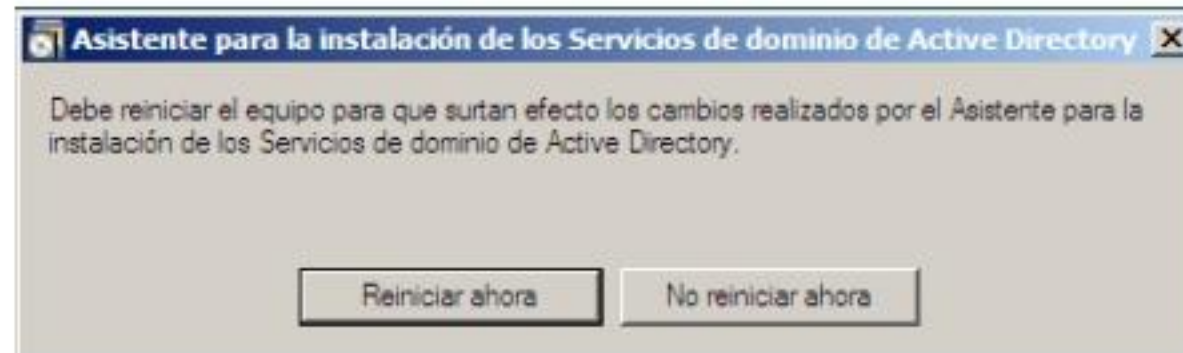
20. Ya estamos por terminar, se presentará una pantalla de Resumen. Aquí puede exportar la configuración en un archivo, para futuras instalaciones. Haga clic en siguiente.

Si hacemos clic en el botón **Exportar configuración**, observará el siguiente cuadro de diálogo. Escriba un nombre para el archivo de configuración, por ejemplo **configAD.txt**. Haga clic en Guardar.



A continuación observará la confirmación de la exportación. Haga clic en aceptar. Luego clic en Siguiente.

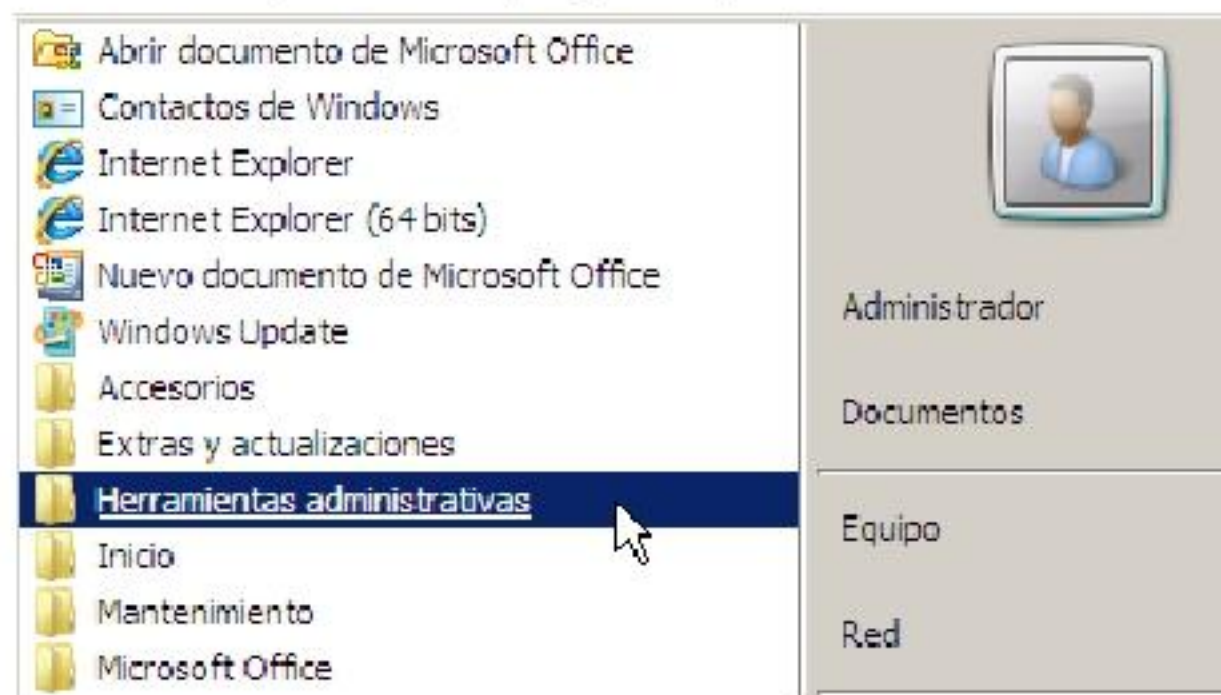
21. Inicialá el proceso de copia e instalación de los archivos para que funcione el servicio DNS y el Active Directory. Espere.
22. Esperamos un momento y luego aparece el cuadro de **Finalización del Asistente**. Haga clic en Finalizar
23. Vamos a reiniciar el equipo para completar el proceso Haga clic en **Reiniciar ahora**.



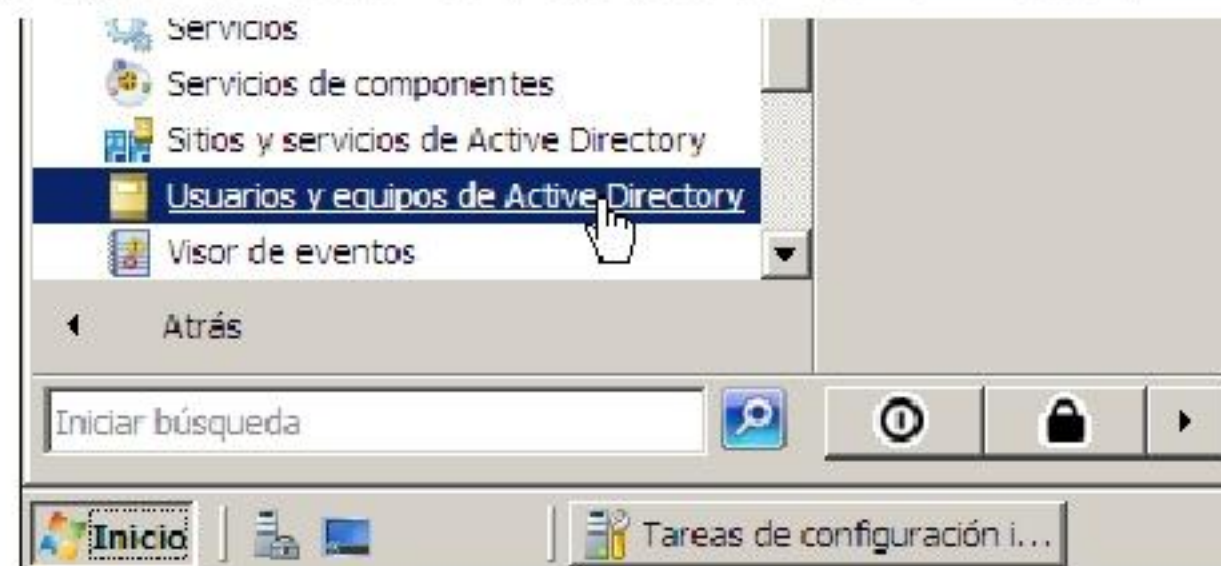
Acceso a las herramientas para gestionar el Active Directory

Ahora que ya se ha completado la instalación de la herramienta de gestión para Active Directory, vamos a ver de qué manera vamos a usarlas.

1. Haga clic en Inicio, Todos los programas, herramientas administrativas.



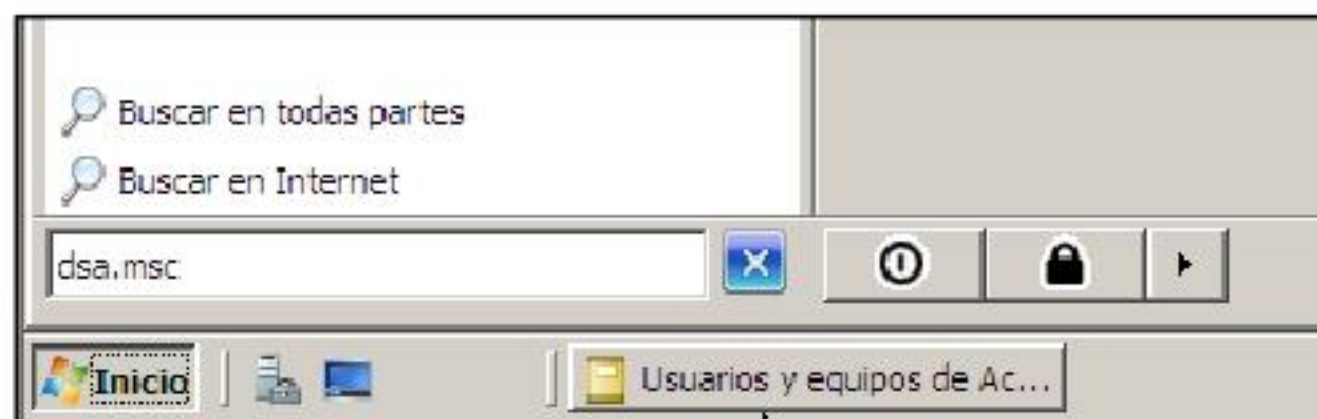
2. Luego haga clic en **Usuarios y equipos de Active Directory**.



3. Cargará la siguiente consola.

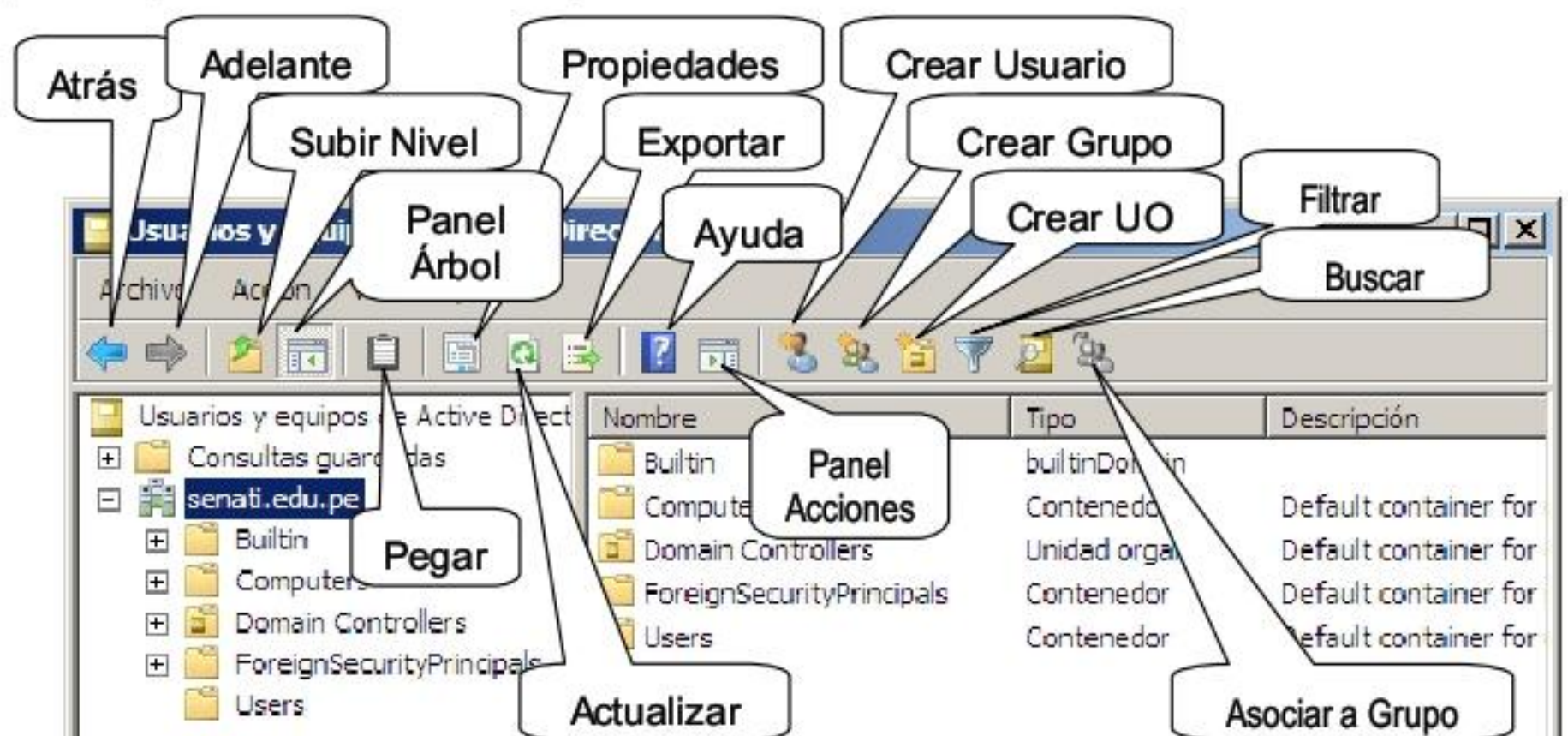


Otra manera de cargar el Active Directory es utilizando un comando a través de Ejecutar. Escriba dsa.msc y pulse Enter.



Reconocimiento del entorno de trabajo de Active Directory

La Interface de la consola **Usuarios y equipos de Active Directory**, se ha desarrollado tomando en cuenta una interface típica de exploración de carpetas, es por eso que encontrará botones que le serán familiares.



Copia de Seguridad del Active Directory

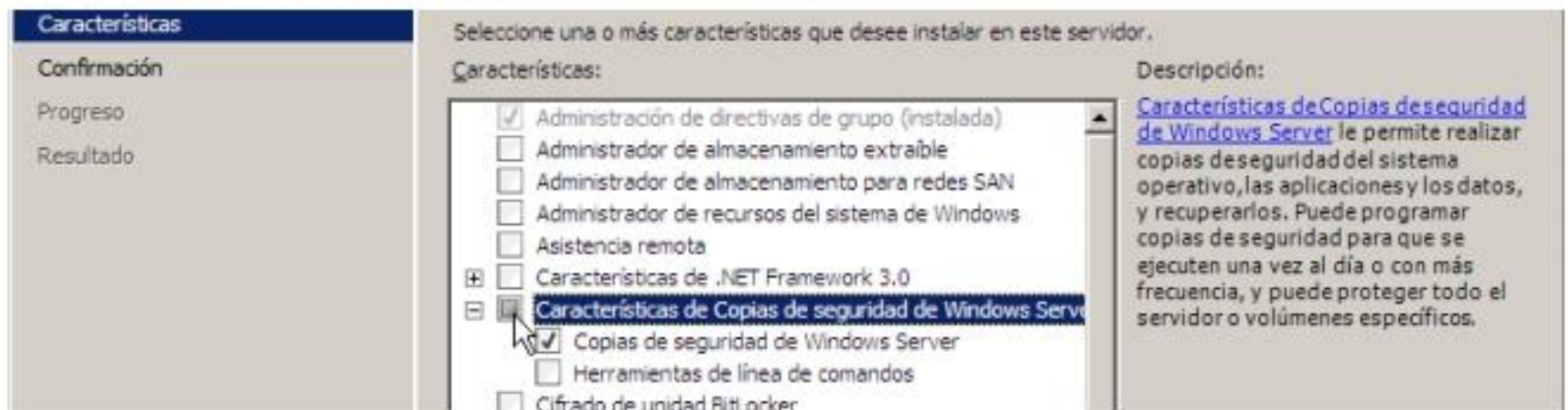
Luego de crear diferentes objetos en el Active Directory, será necesario tener un respaldo en caso de desastres, como una falla de los discos duros, el procesador, placa, etc. Por supuesto, crear el archivo de copia de seguridad es sólo parte de la solución, se debe tener una copia en cinta de backup, y se debe contratar los servicios de custodia de cintas a empresas dedicadas al rubro. En Perú, dos empresas sobresalen en esta última tarea, Hermes y Iron Mountain.

Instalación de la característica de copia de seguridad

1. En la ventana de **Tareas de configuración**, seleccione **Agregar característica**.



2. Observará el siguiente cuadro de diálogo, haga clic en **Características de Copia de seguridad de Windows Server**.



3. Si hace clic en **Herramientas de línea de comandos**, se brindará la posibilidad de instalar el conjunto de herramientas por línea de comandos denominado **PowerShell**, por ahora no es nuestro tema, así es que hacemos clic en **Cancelar**. Luego haga clic en **Siguiente**.





- Para dar inicio al proceso de instalación, haga clic en el botón **Instalar**. Espere a que termine la instalación.
- A continuación observará que la instalación ha terminado con la siguiente confirmación

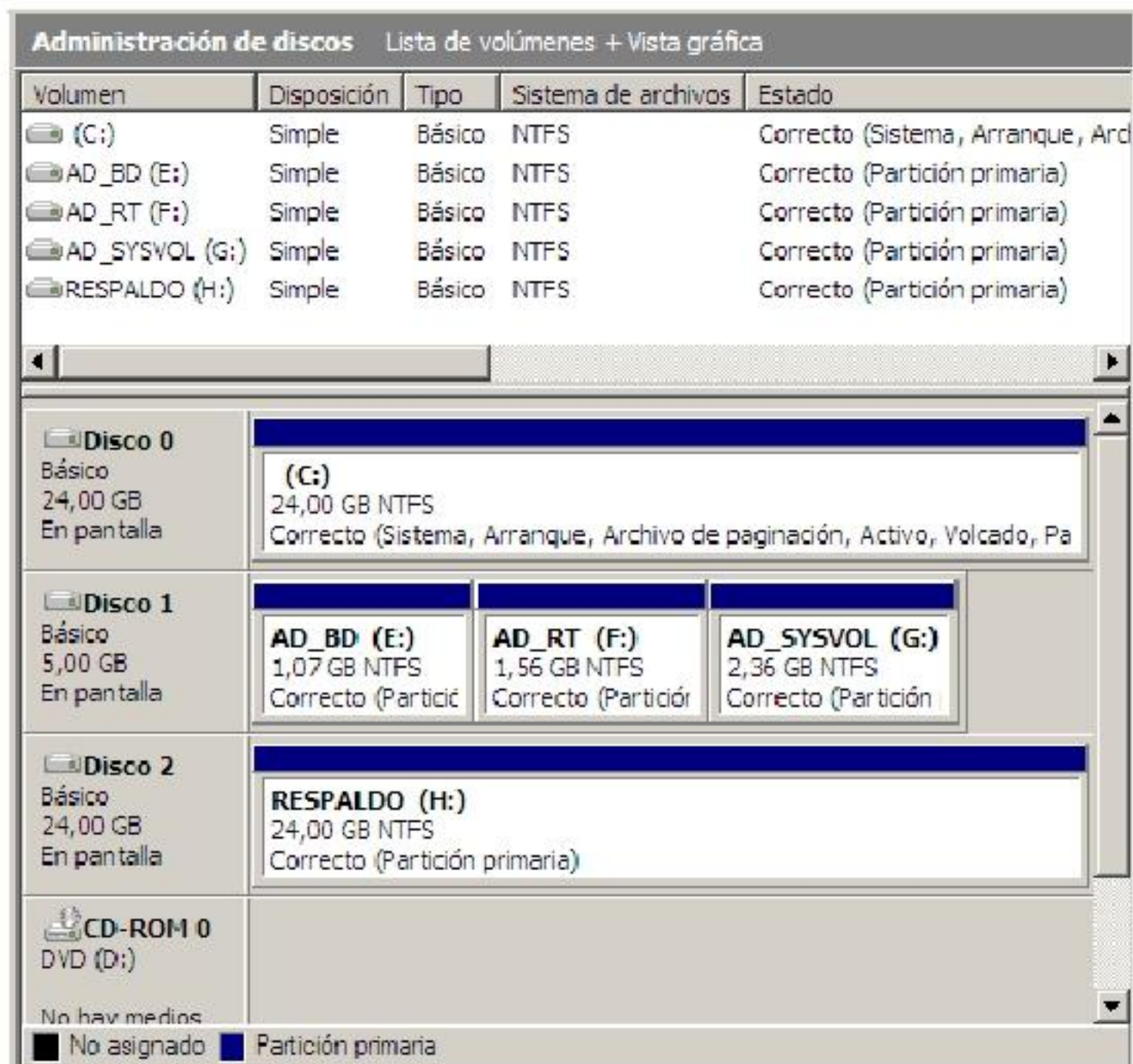


- Haga clic en **Cerrar**.

Realizar copia de seguridad del Estado del Sistema

Puede utilizar el comando **Wbadmin start systemstatebackup** para crear una copia de seguridad del estado del sistema de un equipo. Una copia de seguridad de este tipo sólo se puede guardar en un disco conectado localmente (ya sea interno o externo) y no se puede guardar en un DVD ni en una carpeta de red. No incluye volúmenes completos ni archivos, sólo los archivos del sistema, el active directory y otros elementos necesarios para el funcionamiento del Sistema Operativo y el Active Directory.

- Compruebe que dispone de una partición para diferente u otro disco para almacenar la copia de seguridad. Para nuestro caso disponemos de un disco H de 25GB que será usado para guardar las copias de seguridad.



2. Abra el símbolo de sistema con privilegios de administrador.
3. Escriba **wbadmin start systemstatebackup -backupTarget:H:** y pulse Enter.

Donde: -backupTarget: indica la ubicación que tendrá el backup del estado del sistema, en este caso la unidad H:

4. Se le pedirá que confirme el inicio de la copia del systemstate. Pulse la letra S y luego Enter.

```

C:\Administrador: Símbolo del sistema - wbadmin START SYSTEMSTATEBACKUP -BACKUPTARGET:H:
Microsoft Windows [Versión 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Administrador>wbadmin START SYSTEMSTATEBACKUP -BACKUPTARGET:H:
wbadmin 1.0 - Herramienta de línea de comandos de copia de seguridad
(C) Copyright 2004 Microsoft Corp.

Iniciando copia de seguridad del estado del sistema [20/07/2008 23:07]
Recuperando información del volumen...

Esto haría una copia de seguridad del estado del sistema de los volúmenes Disco
local(C:), AD_BD(E:), AD_RT(F:), AD_SYSVOL(G:) a H:.
¿Desea iniciar la operación de copia de seguridad?
[S] Sí [N] No _
  
```

5. Luego empezará la selección de archivos automáticamente que serán respaldados, además aparecerá un indicador de progreso. Espere, pues este proceso tomará varios minutos.

```

Creando instantánea de los volúmenes solicitados para la copia de seguridad.
Creando instantánea de los volúmenes solicitados para la copia de seguridad.
Creando instantánea de los volúmenes solicitados para la copia de seguridad.
Identificando los archivos del estado del sistema que se incluirán en la copia d
e seguridad (puede tardar unos minutos)...
Se encontraron (337) archivos
Se encontraron (1372) archivos
Se encontraron (2580) archivos
Se encontraron (5031) archivos
Se encontraron (7081) archivos
Se encontraron (9759) archivos
Se encontraron (12606) archivos
Se encontraron (15707) archivos
Se encontraron (27216) archivos
Se encontraron (33760) archivos
Se encontraron (42973) archivos
Se encontraron (56228) archivos
Se encontraron (60278) archivos
Se encontraron (63182) archivos
Se encontraron (63182) archivos
Búsqueda de archivos del estado del sistema completa
Iniciando copia de seguridad de los archivos
Progreso general: 0% (actualmente haciendo copia de seguridad de archivos notifi
cados por 'System Writer')
Progreso general: 0% (actualmente haciendo copia de seguridad de archivos notifi
cados por 'System Writer')
Progreso general: 0% (actualmente haciendo copia de seguridad de archivos notifi
cados por 'System Writer')
Progreso general: 0% (actualmente haciendo copia de seguridad de archivos notifi
cados por 'System Writer')
  
```

```

Copia de seguridad de archivos notificados por 'Registry Writer' completada
Copia de seguridad de archivos notificados por 'NTDS' completada
Progreso general: 100% (actualmente haciendo copia de seguridad de archivos del
estado del sistema adicionales)

Resumen de la copia de seguridad:
-----
Copia de seguridad del estado del sistema completada correctamente [20/07/2008 2
3:44]

Registro de archivos cuya copia de seguridad se completó correctamente
'C:\Windows\Logs\WindowsServerBackup\SystemStateBackup 20-07-2008 23-13-51.log'

C:\Users\Administrador>
  
```




Recuperar el SystemState a partir de una copia de seguridad.

Para recuperar el SystemState utilice el comando **Wbadmin start systemstaterecovery**, desde el símbolo de sistema con privilegios de administrador.

Ejemplo: `wbadmin start systemstaterecovery`.

1. Determine el id de la versión de backup que desee restaurar. Utilice el comando **wbadmin get versions**.

```
Administrador: Símbolo del sistema
C:\Users\Administrador>
C:\Users\Administrador>WBADMIN GET VERSIONS
wbadmin 1.0 - Herramienta de línea de comandos de copia de seguridad
(C) Copyright 2004 Microsoft Corp.

Hora de copia de seguridad: 20/07/2008 23:13
Destino de copia de seguridad: Disco duro etiquetado H:
Identificador de versión: 07/20/2008-21:13
Se puede recuperar: Aplicaciones, Estado del sistema

C:\Users\Administrador>
```

2. Nótese que aparece como Identificado de versión: **07/20/2008-21:13**. Este dato nos servirá para realizar la restauración. Otro detalle a tener presente es que una carpeta puede contener varias copias de seguridad del sistema actual y de otros equipos, y esto debe tenerse en cuenta el momento de restaurar.
3. Reinicie el equipo en **modo de restauración del servicio de directorio**.
4. En el símbolo de sistema con privilegios de administrador escriba:

**wbadmin start systemstaterecovery -version:07/20/2008-21:13
-backupTarget:H: -machine:Server2008.**

Preguntas de Repaso

1. Investigación:
 - a. Que comando utilizaría en Ejecutar para abrir la herramienta **Tareas de configuración**.
 - b. Qué herramientas estarán disponibles si se instala el **PowerShell**.
2. Qué diferencias existen entre las **Funciones** y **Características**.
3. Elabore copias de seguridad del SystemState al menos de 2 equipos y guárdelos en una carpeta compartida. ¿Qué proceso realizaría para recuperar el sistema de una de las máquinas?



Virtualización de servidores

En este capítulo trataremos:

- Aprenderá el uso de la tecnología de virtualización
- Administrará Máquinas virtuales

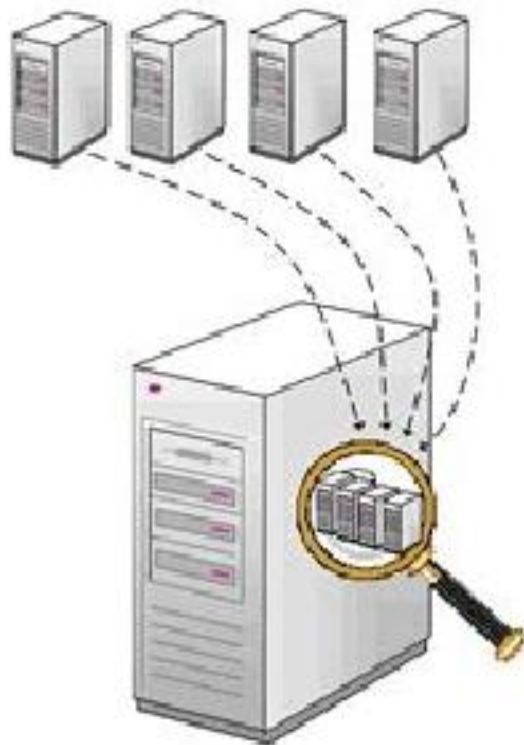
Introducción:

Windows Server Virtualization, permite a los clientes ejecutar múltiples sistemas operativos simultáneamente en un único servidor físico, donde cada uno de los sistemas operativos se ejecuta como un computador autónomo.



Introducción a la Virtualización en Windows Server 2008

Lo primero que vamos a indicar es que Windows Server Virtualization (WSv), es sólo para ediciones de 64bits y no sobre entornos de 32bits.



Requiere procesadores que soporten **Virtualización asistida por hardware** tales como la tecnología AD-V o Intel VT. Esta tecnología es conocida como Hyper-V.

Windows Server Virtualization es una tecnología eficaz de virtualización con sólidas características de administración y seguridad. WSv permite que los negocios aprovechen su familiaridad existente con la administración de servidores Windows y la flexibilidad y beneficios de seguridad de la virtualización sin necesidad de adquirir software de terceros. Microsoft y sus asociados ofrecen el soporte técnico completo para sistemas operativos invitados Windows y Linux compatibles. WSv es una plataforma sumamente flexible, de alto rendimiento, rentable y con buen soporte.

Crear las extensiones AMD-V e Intel VT han sido necesarias para que el hypervisor corra fuera de contexto, es decir, que el código y los datos del hypervisor no se mapean en una dirección/espacio del equipo host.

Por lo tanto, el HYPERVISOR, depende del procesador y sus extensiones.

Por razones de seguridad se requiere que el procesador soporte DEP a nivel de hardware (Data Execution Prevention); para Intel XD (eXecute Disable) y para AMD NX (No eXecute).

Debido a los múltiples equipos que correrán sobre un guest (invitado) se requiere gran cantidad de RAM (2GB a 8GB, dependiendo de las funcionalidades que desee ejecutar, para entornos de prueba, pero en entornos de producción quizá necesite 128GB)



Revisión de Arquitecturas de 32 y 64 bits

En primer lugar, debemos comprender a qué se refieren las expresiones x86, 32bits, x64 y 64bits. A continuación brindaremos información específica para entender la diferencia entre estas arquitecturas

Entendiendo el tema de Arquitecturas

Los registros en un procesador se dividen generalmente en tres grupos: enteros, coma flotante y otros. En todos los procesadores de propósito general, sólo los registros enteros pueden almacenar punteros (una dirección de algún dato en memoria). Los registros que no son de enteros no se pueden utilizar para almacenar punteros para leer o escribir memoria y por tanto no se pueden utilizar para evitar cualquier restricción impuesta por el tamaño de los registros enteros.

Casi todos los procesadores de propósito general (con la notable excepción de muchos ARM e implementaciones MIPS de 32 bits) han integrado hardware de coma flotante, que puede o no utilizar registros de 64 bits para transportar datos con el fin de procesarlos. Por ejemplo, la arquitectura X86 incluye instrucciones de coma flotante del x87 que utiliza 8 registros de 80 bits en una configuración en forma de pila; revisiones posteriores del x86 y la arquitectura x86-64 también incluyen instrucciones SSE que utilizan 8 registros de 128 bits (16 registros en el x86-64). En contraste, el procesador de 64 bits de la familia DEC Alpha define 32 registros de coma flotante de 64 bits además de sus 32 registros de enteros de 64 bits.

Arquitectura x86

x86 es la denominación genérica dada a ciertos microprocesadores de la familia Intel, sus compatibles y a la arquitectura básica de estos procesadores, por la terminación de sus nombres: 8086, 80286, 80386 y 80486. Los sucesores del 80486 pasarán a ser llamados por nombres no numéricos, bajo la denominación Pentium, sin embargo todavía se los llama procesadores de la familia x86.

La comercial popularidad de esta arquitectura hizo que muchos fabricantes, además de Intel, empezaran a fabricar en masa microprocesadores basados en esta arquitectura. Estas compañías son entre otras AMD, Cyrix, NEC Corporation y Transmeta.

La arquitectura es notablemente no limpia, por mantener compatibilidad con la línea de procesadores de 16 bits de Intel, que a su vez también eran compatibles con una familia de procesadores de 8 bits. Existen dos sucesores de 64 bits para esta arquitectura:

- IA64, empleada en los procesadores Itanium de Intel y no compatible con X86, excepto bajo emulación.
- AMD64 o x86-64, de AMD, que es básicamente una extensión de 64 bits de la familia x86.

Además, técnicamente, la arquitectura x86 es denominada IA32 (Intel Architecture 32 bits).

En 1978, Intel comenzó a comercializar el procesador 8086, un ambicioso chip de 16 bits potencialmente capaz de ser el corazón de computadoras de propósito múltiple. El 8086 se comercializó en versiones desde 4,77 y hasta 10MHz.



Al 8086 lo sucedió el 80286 en 1982 (en el cual se basó la IBM PC/AT, 1985). Este chip, de 24/16 bits, implementó el modo protegido de ejecución, sentando las bases para la aparición de los verdaderos sistemas multitarea de escritorio. El 80286 apareció a 6MHz, y a lo largo de los años llegó hasta los 12MHz. Hubo varios sistemas operativos que aprovecharon su modo protegido para ofrecer multitarea real, tales como las primeras versiones de OS/2, o Xenix.

Pero el verdadero boom de la multitarea no llegó hasta el nacimiento del 80386 (1985) - Un avance tan fuerte que hoy en día es común referirse como i386 a toda la línea de procesadores que le siguieron (también es común la referencia IA32, Intel Architecture of 32 bits). El 386 fue el primer procesador de Intel de 32 bits, y - magníficas noticias para los desarrolladores- utilizarlo para aplicaciones de multitarea sería ya mucho más fácil de lo que lo fue con el 80286. El 80386 maneja velocidades de 16 a 33MHz

En 2001, tras una muy larga etapa de desarrollo, fue anunciado el Itanium. Éste es el primer CPU desde 1978 que produce Intel que no es compatible con la arquitectura x86 - esta nueva arquitectura de 64 bits es denominada IA64. Hoy en día, la competencia se pone más difícil aún para Intel, pues AMD -compañía rival de Intel- anunció la arquitectura x86-64, que es una extensión a la i386 (compatible con todo el software ya existente) permitiéndole ejecutar código de 64 bits.

La tendencia actual de los fabricantes es presentar diseños que integren múltiples núcleos dentro de un mismo chip, buscando así conjurar las ventajas de los sistemas multiprocesador. De esta manera, tanto Intel, con Pentium D, como AMD, con Athlon, ya presentan al mercado modelos de dos núcleos, cuatro y más (Intel proyecta lograr microprocesadores de 84 núcleos hacia el año 2010).

Desde 2005 Apple integra a sus computadoras la Arquitectura x86 para uso exclusivo de los procesadores Dual Core, reemplazando la tecnología Power PC, de Motorola. Mac OS X V10.4 Tiger incorpora soporte para la arquitectura x86 (aunque Mac OS X 10.5 Leopard puede ser usado tanto en RISC Power PC Reciente como en Intel x86). La Migración de Power PC RISC A Intel Architecture x86 Se completó con éxito en 2006

Arquitectura x64

Esta arquitectura está diseñada para trabajar con códigos de 64bits.

Los microprocesadores de 64 bits han existido en los superordenadores desde 1960 y en servidores y estaciones de trabajo basadas en RISC desde mediados de los años 1990.

En 2003 empezaron a ser introducidos masivamente en los ordenadores personales (previamente de 32 bits) con las arquitecturas x86-64 y los procesadores PowerPC G5.

Aunque una CPU puede ser internamente de 64 bits, su bus de datos o bus de direcciones externos pueden tener un tamaño diferente, más grande o más pequeño y *el término se utiliza habitualmente para describir también el tamaño de estos buses.*

Por ejemplo, muchas máquinas actuales con procesadores de 32 bits usan buses de 64 bits (p.ej. el Pentium original y las CPUs posteriores) y pueden ocasionalmente ser conocidas como "64 bits" por esta razón. El término también se puede referir al tamaño de las instrucciones dentro del conjunto de instrucciones o a cualquier otro elemento de datos (p.ej. las cantidades de 64 bits de coma flotante de doble precisión son comunes). Sin más calificaciones, sin embargo, la arquitectura de los

ordenadores de 64 bits tiene integrados registros que son de 64 bits, que permite soportar (interna y externamente) datos de 64 bits.

En arquitectura de ordenadores, 64 bits es un adjetivo usado para describir enteros, direcciones de memoria u otras unidades de datos que comprenden hasta 64 bits (8 octetos) de ancho, o para referirse a una arquitectura de CPU y ALU basadas en registros, bus de direcciones o bus de datos de ese ancho.

Relación con la Memoria

Muchas CPUs están actualmente diseñadas para que los contenidos de un único registro puedan almacenar la dirección de memoria de cualquier dato en la memoria virtual. Por tanto, el número total de direcciones en memoria virtual — la suma total de datos que el ordenador puede mantener en su área de trabajo — es determinado por el ancho de estos registros. Empezando en los años 1960 con el IBM S/360, luego (entre muchos otros) el miniordenador VAX de DEC en los años 1970 y luego con el Intel 80386 a mediados de los años 1980, un consenso de facto instauró que 32 bits era un tamaño conveniente de registro. Un registro de 32 bits significa que se puede referenciar 2³² direcciones o 4 gigabytes de RAM. En el momento en que estas arquitecturas fueron concebidas, 4 gigabytes de memoria estaban muy lejos de las cantidades disponibles en instalaciones que se consideraban suficiente "espacio" para direccionamiento. Las direcciones de 4 gigabytes se consideraban un tamaño apropiado con el que trabajar por otra importante razón: 4 mil millones de enteros son suficientes para asignar referencias únicas a la mayoría de cosas físicamente contables en aplicaciones como bases de datos.

No obstante, con el paso del tiempo y las continuas reducciones en el coste de la memoria (examine la Ley de Moore), al comienzo de los años 1990, comenzaron a aparecer instalaciones con cantidades de RAM próximas a los 4 gigabytes, y comenzó a ser deseable el uso de espacios de memoria virtual que superaban el límite de 4 gigabytes para manejar ciertos tipos de problemas. Como respuesta, varias empresas empezaron a lanzar nuevas familias de chips con arquitecturas de 64 bits, inicialmente para superordenadores, estaciones de trabajo de grandes prestaciones y servidores. Las computadoras de 64 bits se han ido moviendo hacia el ordenador personal, con algunos modelos de las líneas Macintosh de Apple Computer cambiando a procesadores PowerPC 970 (llamados "G5" por Apple) en 2003 y a procesadores EM64T de 64 bits en 2006, y con procesadores x86-64 llegando a ser comunes en PCs de gama alta. La aparición de la arquitectura de 64 bits efectivamente incrementa el límite a 2⁶⁴ direcciones, equivalente a 17,179,869,184 gigabytes o 16 exabytes de RAM. Para poner esto en perspectiva, en los días en que 4 MB de memoria principal eran comunes, el límite máximo de memoria de 2³² direcciones era unas 1000 veces mayor que la configuración típica de memoria. En 2007, cuando 1GB de memoria principal es común, el límite de 2⁶⁴ es unos diez mil millones de veces superior, es decir diez millones de veces más de espacio.

Muchos PCs de 64 bits del mercado tienen actualmente un límite artificial en la cantidad de memoria que pueden reconocer, pues las limitaciones físicas hacen muy poco probable que se vaya a necesitar soporte para los 16 exabytes de capacidad total. El Mac Pro de Apple, por ejemplo, puede configurarse físicamente con hasta 32 gigabytes de memoria, y por ello no hay necesidad de soportar más allá de esa cantidad. Un núcleo Linux reciente puede ser compilado con soporte para hasta 64 Gigabytes de memoria. Según Apple la nueva versión de su sistema operativo teóricamente soporta 16 Terabytes de memoria.



32 bits contra 64 bits

El cambio de una arquitectura de 32 bits a una de 64 bits es una alteración fundamental, y muchos sistemas operativos tienen que modificarse ostensiblemente para aprovechar las ventajas de la nueva arquitectura. El resto del software también tiene que ser portado para usar las nuevas capacidades; el software antiguo normalmente es soportado a través del modo de hardware compatible (en el que los nuevos procesadores soportan las versiones antiguas del conjunto de instrucciones antiguo de 32 bits, así como las de la versión de 64 bits), a través de emulación software o por la implementación de un núcleo de procesador de 32 bits dentro del procesador de 64 bits (como con los procesadores Itanium de Intel, que incluyen un núcleo de procesador x86 para ejecutar aplicaciones x86 de 32 bits). Los sistemas operativos para estas arquitecturas de 64 bits generalmente soportan aplicaciones de 32 bits y de 64 bits.

Una excepción significativa de esto es el AS/400, cuyo software se ejecuta en un conjunto de instrucciones virtual, llamado TIMI (Technology Independent Machine Interface) que se traduce a código nativo por software de bajo nivel antes de ser ejecutado. El software de bajo nivel es todo lo que ha de ser reescrito para portar todo el SO y el software a una nueva plataforma, como cuando IBM hizo la transición de su línea desde los antiguos juegos de instrucciones de 32/48 ("IMPI") al PowerPC de 64 bits (IMPI no tenía nada que ver con el PowerPC de 32 bits, así que fue incluso una transición mayor que la de un juego de instrucciones de 32 bits a su equivalente de 64 bits).

Mientras las arquitecturas de 64 bits incontestablemente hacen más sencillo el trabajar con grandes conjuntos de datos en aplicaciones como el vídeo digital, computación científica y grandes bases de datos, ha habido un debate considerable sobre si los modos de compatibilidad con 32 bits serán más rápidos que los sistemas de 32 bits del mismo precio para otras tareas. En las arquitecturas x86-64 (AMD64 y EM64T, IA-32e), la mayoría de los sistemas operativos de 32 bits y aplicaciones pueden ejecutarse sin problemas en el hardware de 64 bits.

Las máquinas virtuales de JAVA de 64 bits de Sun son más lentas en el arranque que las de 32 bits porque Sun sigue asumiendo que todas las máquinas de 64 bits son servidores y sólo han implementado el compilador de "servidor" (C2) para plataformas de 64 bits. El compilador "cliente" (C1) produce código más lento, pero compila mucho más rápido. Así que aunque un programa Java en una JVM de 64 bits puede funcionar mejor en un periodo grande de tiempo (típico de aplicaciones "servidoras" de ejecución larga), su tiempo de arranque será probablemente mucho mayor. Para aplicaciones de vida corta (como el compilador de Java, javac) el incremento en el tiempo de arranque puede dominar el tiempo de ejecución, haciendo la JVM de 64 bits más lenta en conjunto.

Debería notarse que la velocidad no es el único factor a considerar en una comparación de procesadores de 32 bits y 64 bits. Usos como la multitarea, las pruebas de carga y el clustering (para computación de alto rendimiento) pueden ser más idóneos para una arquitectura de 64 bits teniendo en cuenta un desarrollo correcto. Los clusters de 64 bits han sido ampliamente usados en grandes organizaciones como IBM, Vodafone, HP y Microsoft, por esta razón.

Disponibilidad del Software para x86 y x64

Los sistemas de 64 bits algunas veces carecen de software equivalente escrito para arquitecturas de 32 bits. Los problemas más graves son debidos a controladores de dispositivo incompatibles. Aunque gran parte del software puede ejecutarse en modo de compatibilidad con 32 bits (también conocido como un modo emulado, p. ej. la Tecnología Microsoft WoW64), normalmente es imposible ejecutar un driver (o un programa similar) en ese modo ya que habitualmente se ejecuta entre el SO y el hardware, donde no se puede usar la emulación directa. Muchos paquetes de software de código abierto pueden simplemente ser compilados desde las fuentes para trabajar en un entorno de 64 bits en sistemas operativos como Linux. Todo lo que se necesitaría en este caso es un compilador (normalmente GCC) para la máquina de 64 bits.

Tecnología de virtualización

Con todos estos avances ahora es posible simular sistemas completos en un solo equipo físico, permitiéndonos realizar lo siguiente:

1. Agregar en caliente cualquier forma de almacenamiento
2. Adicionar dinámicamente NIC's virtuales y puede aprovechar la seguridad de las VLAN's que corran en planos inferiores.
3. Migrar equipos de Virtual Server a Windows Server Virtualization.
4. Soporte para NAT y cuarentena de red para Máquinas virtuales, seguridad basada en roles, GPO's, contadores de uso, invitados/guest NO-Microsoft, instantáneas de las Máquinas virtuales mediante el uso de volumen Shadow copy Service (VSS), control de recursos usando Windows System Resource Manager (WSRM, clustering, etc)
5. Soporte de Server Core como partición padre, lo que ofrece una menor superficie de ataque y menores recursos consumidos.
6. Gestión por WMI.
7. Interfaz de Scripting
8. Monitorización de estado del servidor.
9. Soporte a Sistemas operativos guest de otros fabricantes.
10. Posibilidad de sacar Snapshots de máquinas virtuales.

Beneficios de la Virtualización

1. Reducción de costos de funcionamiento y mantenimiento de servidores físicos mediante el aumento de la utilización del hardware.
2. Aumentar el desarrollo y prueba de la eficiencia mediante la reducción de la cantidad de tiempo que se tarda en crear hardware y software y se reproducen entornos de prueba.
3. Mejora la disponibilidad del servidor sin necesidad de utilizar el mayor número de computadores físicos.
4. Aumentar o reducir los recursos de los servidores en respuesta a los cambios en la demanda.
5. Aumento de la productividad administrativa y capacidad de respuesta. Hyper-V permite a las organizaciones de Tecnología de Información incrementar su productividad administrativa y desplegar rápidamente nuevos servidores para hacer frente a necesidades empresariales en constante cambio.
6. Soporta la solución de virtualización de servidores: Virtual Server 2005 R2, Hyper-V, y Virtual Machine Manager.



Escenarios de Virtualización

Consolidación de Servidores

La virtualización permite consolidar las cargas de trabajo asignadas a un equipo servidor específico, en un número más reducido, así mismo intensifica su uso.

Esto implica que menos personal maneje estos servidores, menos espacio físico ocupado para los centros de cómputo y una reducción en el consumo de energía, porque

su existencia no implica, de ninguna manera, un mayor consumo de corriente. Con el mismo consumo eléctrico puede tener 10 o 20 Servidores virtuales.



Continuidad del negocio

Esta nueva tecnología proporciona la capacidad para la eficiencia de recuperación de desastres para reducir al mínimo el tiempo de inactividad.

Como los sistemas operativos y las instancias de las aplicaciones se conservan en archivos de datos, la virtualización ayuda a automatizar y racionalizar los procesos de backups, duplicación y movimiento de datos.



Pruebas y desarrollo

Simplifica los procesos de pruebas de laboratorio, de nuevas aplicaciones o sistemas operativos y de hardware, asegurando compatibilidad entre los nuevos elementos y la estructura vigente.

Hyper-V ayuda a minimizar la prueba de hardware, mejora la gestión del ciclo de vida y mejora la cobertura de la prueba.



Delegaciones remotas

La virtualización contribuye a optimizar el uso de todos los recursos disponibles, independizando cada elemento en función de los otros y convirtiéndolos en servicios que se encuentran disponibles en forma inmediata.



Características de Windows Server Virtualization

Windows Hypervisor

Capa muy delgada de software que aprovecha el controlador de Windows Server y la tecnología de virtualización asistida por hardware.

Soporta clientes de 64 bits

Esto permite a las organizaciones virtualizar sus aplicaciones intensivas en memoria y se beneficien del aumento de memoria accesible en un entorno de 64bits

Soporte para múltiples clientes

Hyper-V ofrece ahora la capacidad de asignar múltiples recursos de CPU a una sola máquina virtual y permite la virtualización de aplicaciones multihilo.

Migración de las máquinas virtuales

Puede mover una máquina virtual de una máquina física a otra con un mínimo de tiempo de inactividad.

Nueva arquitectura de virtualización de dispositivos

Se dispone de una nueva arquitectura de E/S virtualizada. Esto proporciona a los clientes un alto rendimiento y bajos gastos generales.

Manipulación VHD Offline

Tenemos capacidad de tener acceso a archivos dentro de un VHD sin tener que implementar una máquina virtual. Esto proporciona a los administradores un acceso granular a los VHD's y la capacidad para realizar algunas tareas de gestión fuera de línea.



Tipos de virtualización

Virtualización de Máquinas (Servidores)

La virtualización de máquina utiliza software para crear una máquina virtual que emula los servicios y capacidades del hardware subyacente. Esto permite ejecutar más de un sistema operativo en una única máquina. En los servidores, este enfoque se denomina Virtualización de Servidores; en PC para el usuario final, se denomina la virtualización de escritorio.

La característica "Hyper-V estará integrada como parte de Microsoft Windows Server 2008 (también accesible de forma independiente y separada como servidor independiente: Microsoft Hyper-V Server. Tanto esta tecnología, como la incorporada actualmente en Microsoft Virtual Server 2005 R2-- conforman la propuesta de Microsoft en Virtualización de Servidores.

Virtualización de Máquinas (Puesto de trabajo)

Microsoft Virtual PC permite la ejecución de diferentes sistemas operativos en la misma máquina, lo que nos da gran flexibilidad a la hora de ejecutar aplicaciones no compatibles con un SO determinado, además de permitirnos disponer de mayor eficacia en el desarrollo y testeo de nuevo software. Existe además un componente adicional denominado Windows Vista Enterprise Centralized Desktop donde un desktop puede ser hosteado por completo en el server para posteriormente ser derivado de forma remota por completo a otro PC.

Virtualización de Aplicaciones

Separa la aplicación del sistema operativo, lo que reduce los conflictos entre aplicaciones, y simplifica las distribuciones y actualizaciones de software.

Microsoft SoftGrid Application Virtualization transforma las aplicaciones en un servicio virtual, gestionado de forma centralizada, y del que se hace un streaming a los puestos de trabajo, servidores o portátiles cuando y donde sea necesario. Esto es una auténtica "pasada". os imagináis el control del que dispones sobre una de las tareas más pesadas de administrar como son el despliegue de software cliente, las actualizaciones , parcheo etc..?

Virtualización de Presentación

Permite que una aplicación en un equipo pueda ser controlada por otro en una ubicación diferente.

Microsoft Windows Server Terminal Services, es ya un clásico que todos conocéis. Una aplicación de puesto de trabajo puede ejecutarse en un servidor compartido y presentar la interfaz de usuario en un sistema remoto como un desktop remoto, un cliente ligero etc.

Virtualización de almacenamiento

Donde los usuarios acceden a aplicaciones y datos sin preocuparse de donde se almacenan

Virtualización de red

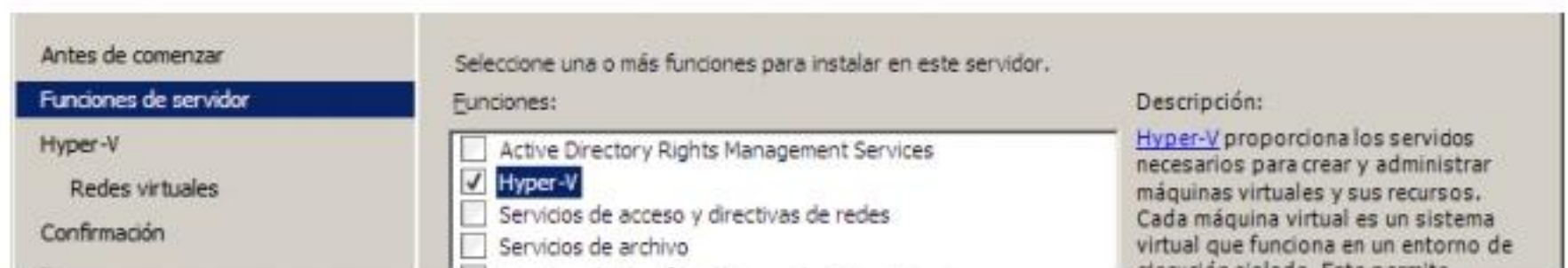
Que permite a los usuarios remotos navegar en la red de una empresa como si estuvieran conectados físicamente.

Instalación de sistemas virtualizados

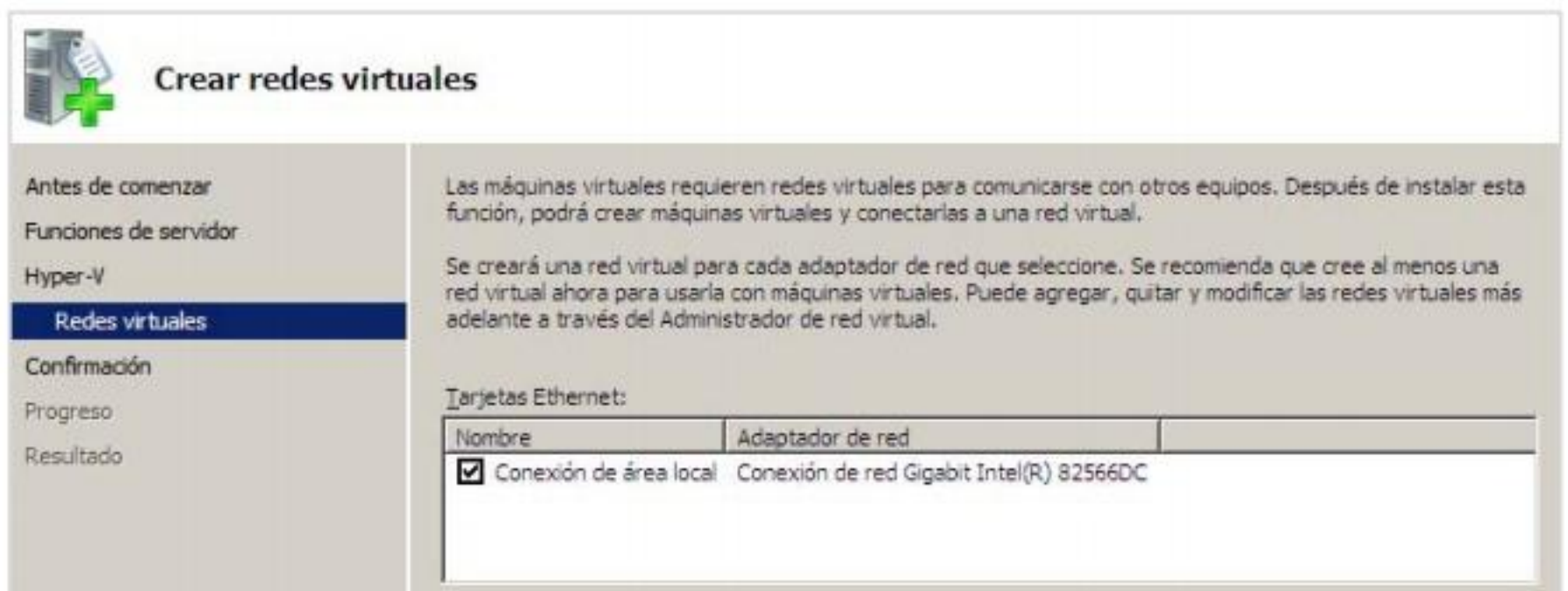
Puede instalar una gran cantidad de sistemas operativos sobre estas plataformas de virtualización, pero vamos a concentrarnos en Windows XP y Linux

Instalación de la función Hyper-V

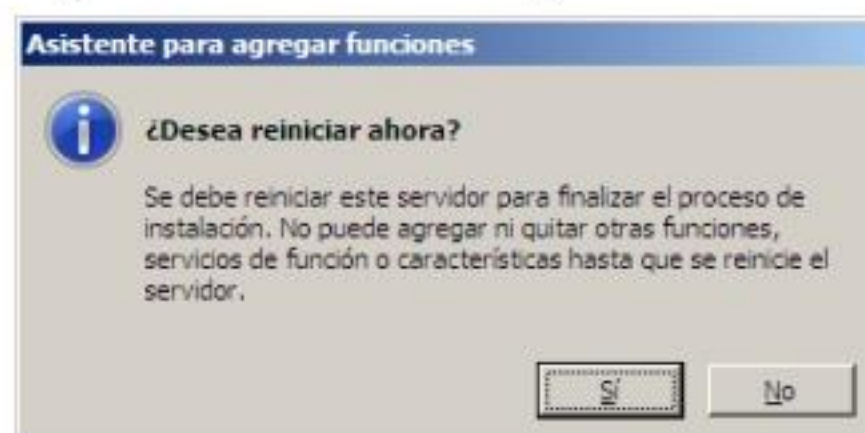
1. Como primer paso, seleccione **Agregar función de Tareas de configuración**.
2. Observará la siguiente ventana, seleccione Hyper-V y haga clic en siguiente



3. Aparece una ventana informativa de la función que está instalando, haga clic en **Siguiente**
4. Active la **Tarjeta de Red** con la cual se establecerá una red virtual y haga clic en siguiente.



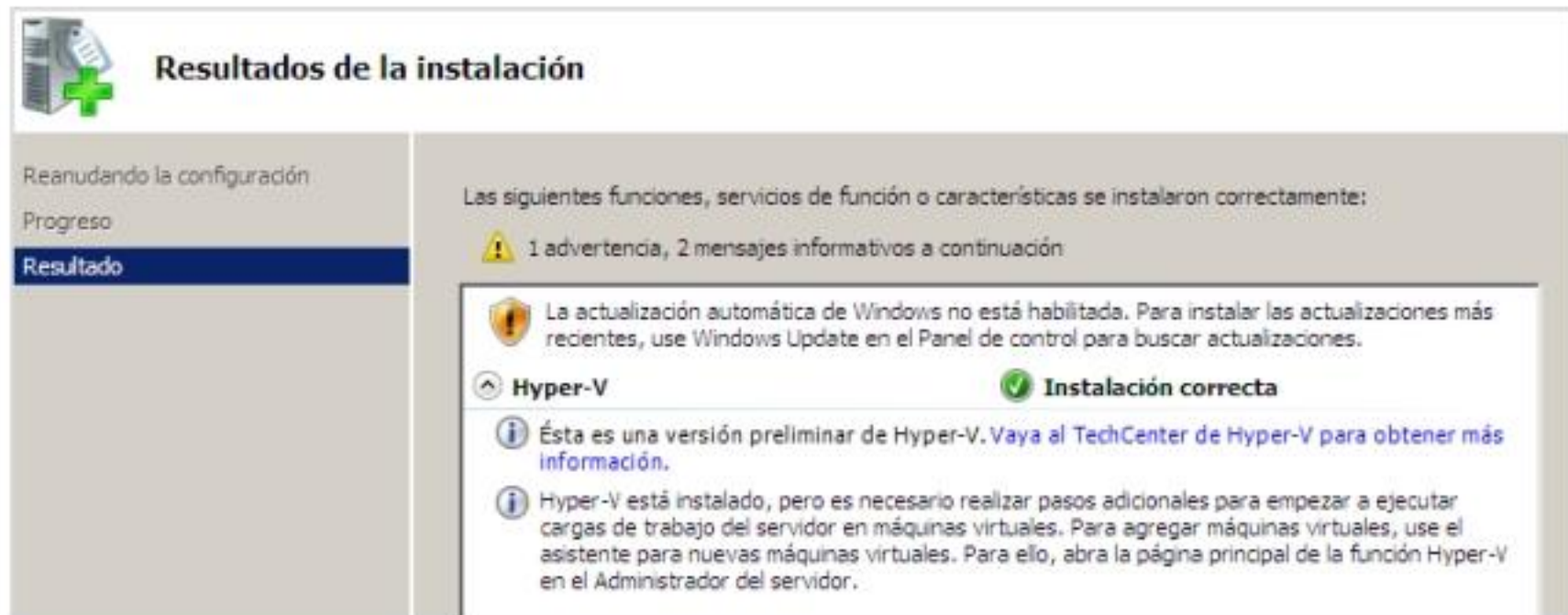
5. Confirme que todas las opciones son correctas y haga clic en siguiente
6. Luego de la instalación de la función se solicitará que reinicie
7. Haga clic en **Cerrar**.
8. Conteste **Sí** al siguiente cuadro de diálogo



9. Espere a que reinicie el sistema

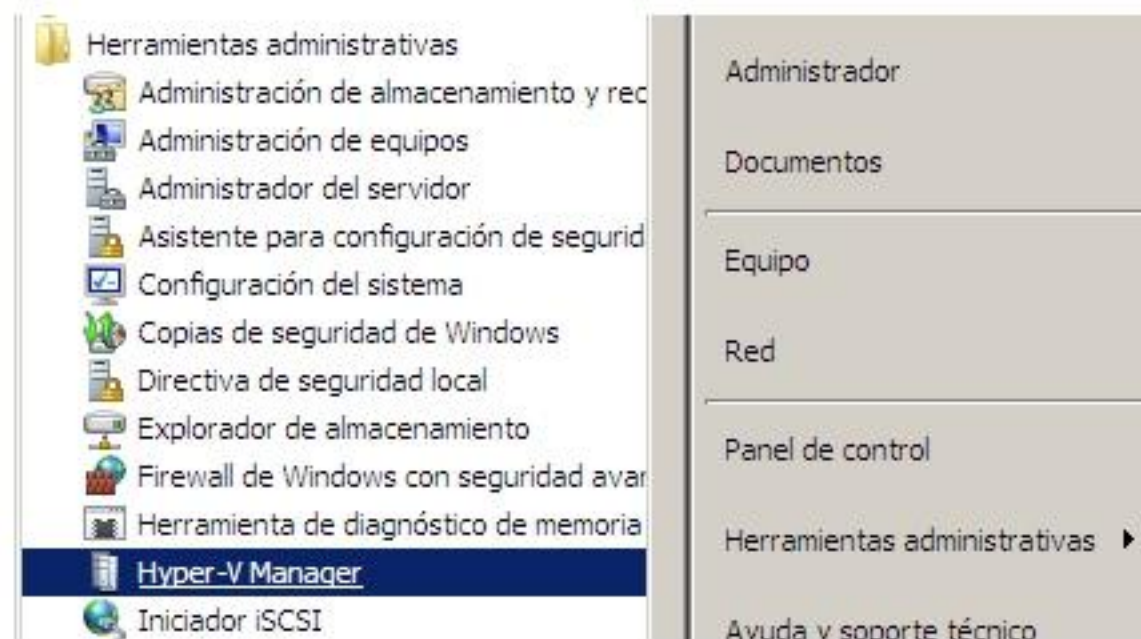


10. Luego del reinicio observará la confirmación de la instalación. Haga clic en Cerrar.

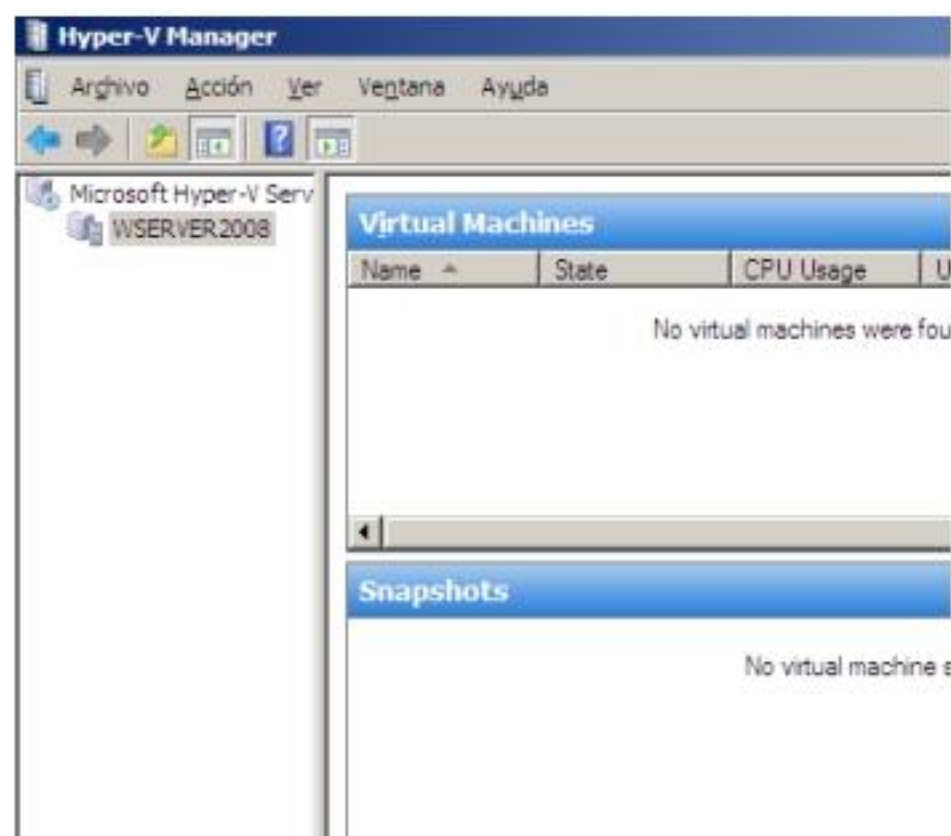


Iniciar el Administrador Hyper-V

1. Haga clic en Inicio, Herramientas administrativas y luego en Hyper-V Manager.



2. Confirme los términos de la licencia de Hyper-V, activando la casilla **I have read and agreed this EULA** y luego haga clic en Accept.
3. Luego observará la siguiente ventana, a través de la cual podrá administrar los equipos virtuales.

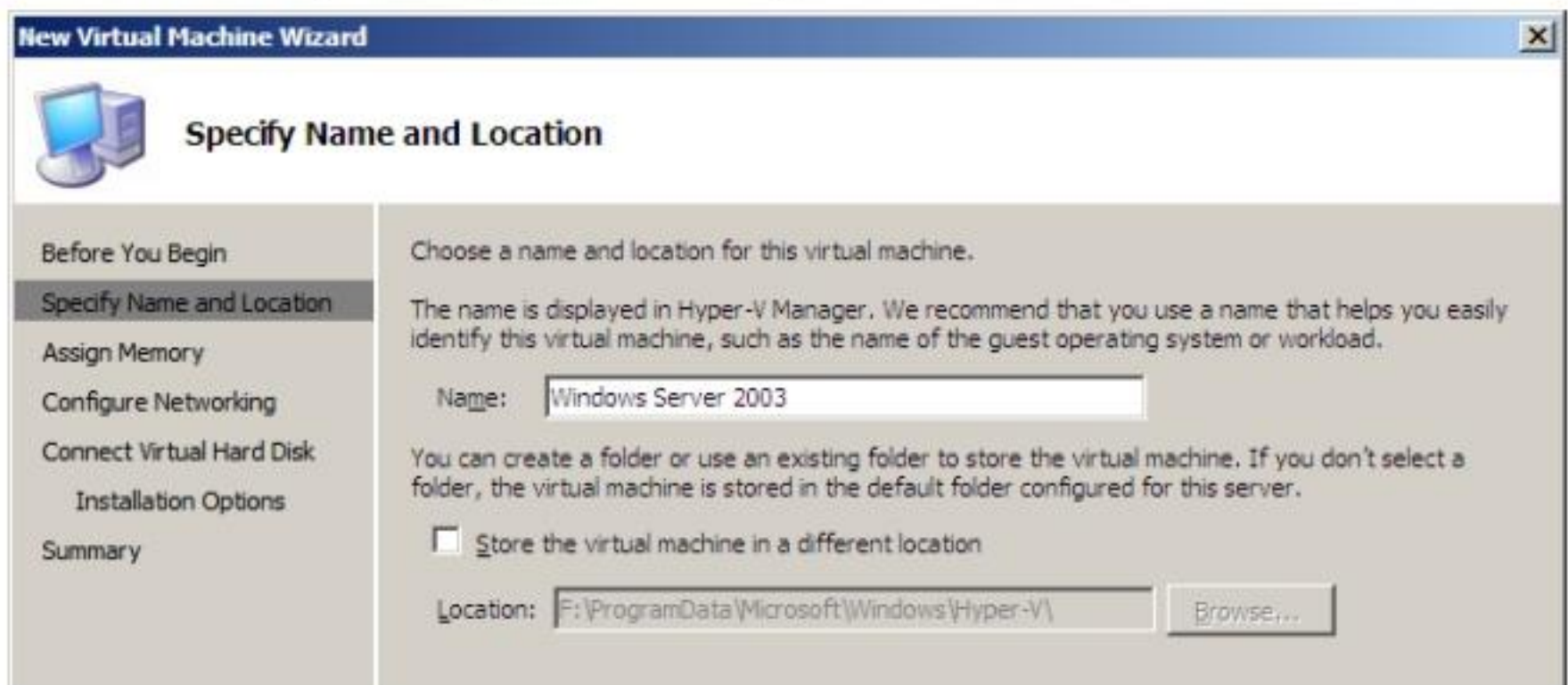


Crear equipo Virtual

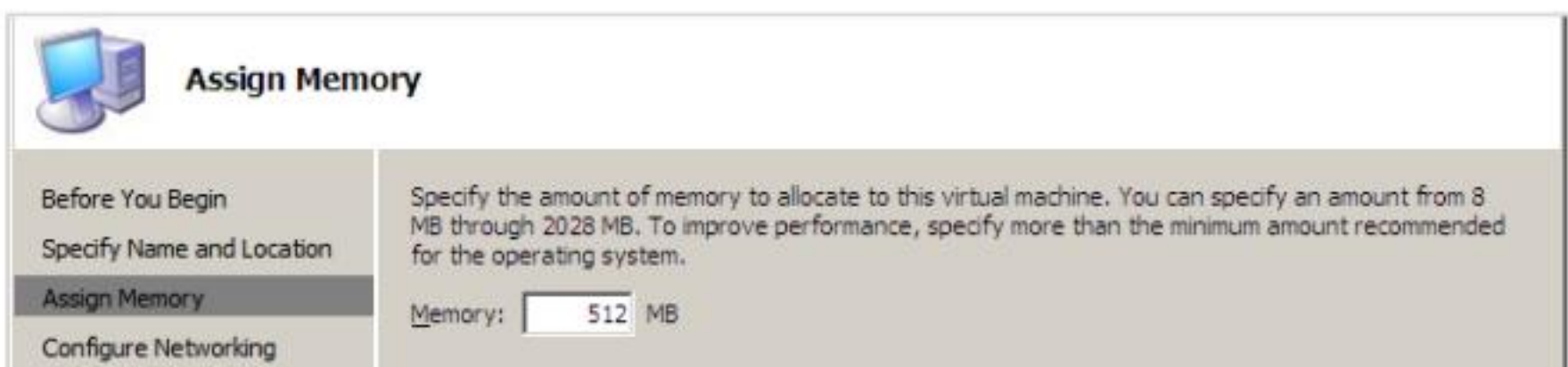
1. Haga clic en **New** del panel Acciones.
2. Seleccione **Virtual Machine**.



3. Se mostrará la pantalla introductoria de la tarea que vamos a realizar, en este caso, crear una máquina virtual.
4. Haga clic en **Next**.
5. Indique el nombre de la máquina virtual. Generalmente será el nombre del sistema operativo que instalará. Haga clic en **Next**.



6. Establezca la cantidad de memoria asignada. En nuestro caso 512MB.



7. Establezca la tarjeta de red con la cual trabajará el equipo virtual.





8. Establezca la configuración para el disco virtual. Para nuestro caso Windows Server 2003 y un tamaño de 20GB para el disco duro virtual.

Connect Virtual Hard Disk

Before You Begin
Specify Name and Location
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

Create a virtual hard disk

Name:

Location:

Size: GB (Maximum: 2040 GB)

Use an existing virtual hard disk

Location:

Attach a virtual hard disk later

9. A continuación establezca las opciones de la instalación que se va a desarrollar, como bootear desde el CD o cargar una imagen ISO.

Installation Options

Before You Begin
Specify Name and Location
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

You can install an operating system now if you have access to the setup media, or you can install it later.

Install an operating system later

Install an operating system from a boot CD/DVD-ROM

Media

Physical CD/DVD drive:

Image file (.iso):

Install an operating system from a boot floppy disk

Media

Virtual floppy disk (.vfd):

Install an operating system from a network-based installation server

10. Para nuestro caso es la imagen ISO de Windows Server 2003.

Before You Begin
Specify Name and Location
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

You can install an operating system now if you have access to the setup media, or you can install it later.

Install an operating system later

Install an operating system from a boot CD/DVD-ROM

Media

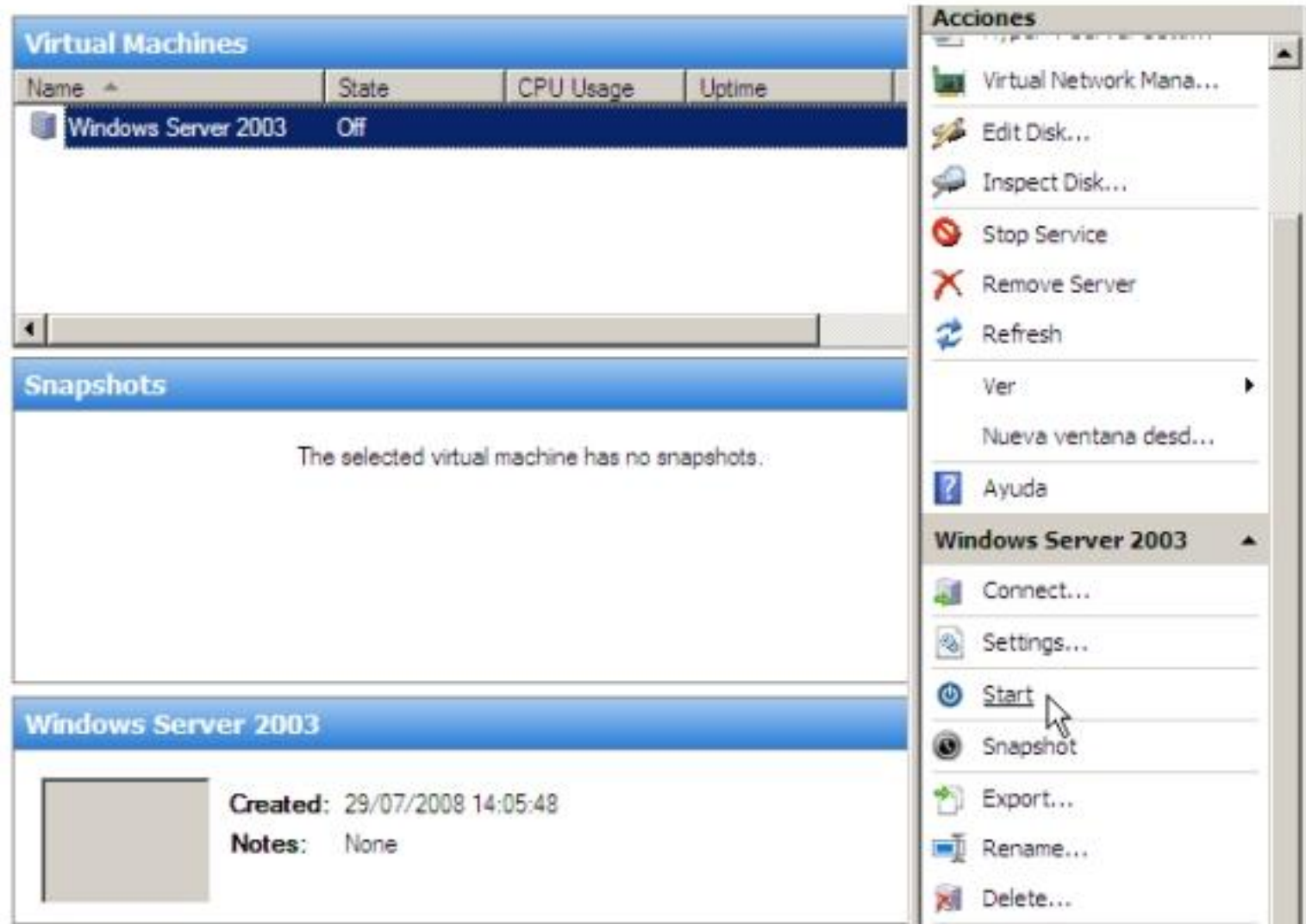
Physical CD/DVD drive:

Image file (.iso):

11. Se presenta una hoja de resumen. Haga clic en **Finish**.

Instalar un Sistema Operativo

1. En la ventana seleccione la máquina virtual y haga clic en **Start** del Panel Acciones.



2. Espere un momento y luego haga clic en **Connect** del Panel Acciones.



3. Observará una ventana con el proceso de instalación en curso. Continúe con la instalación.





Actividades para Instalar Windows XP y Linux

Realice las siguientes actividades:

1. Instalación de un Cliente Windows XP
2. Instalación de un Servidor Linux

Preguntas de Repaso

1. Investigación:
 - a. Qué proceso llevaría a cabo para trasladar una máquina virtual de Virtual Server 2005 a Hyper-V.
 - b. Indique el proceso para crear una red virtual con Hyper-V
2. Qué versiones de Windows Server Soportan Virtualización.
3. Realice una instalación Core de Windows Server 2008 en una nueva máquina virtual
 - a. Configure el adaptador de red
4. Realice una instalación de Linux en una nueva máquina virtual.
 - a. Configure el adaptador de red
5. Verifique la conectividad de los servidores virtuales: Core Windows Server 2008 y Linux a través de los comandos pertinentes.



Gestión de unidades organizativas y usuarios

En este capítulo trataremos:

- Aprenderá el uso de unidades organizativas
- Aprenderá a crear y administrar cuentas de usuario
- Aprenderá a crear perfiles de usuarios

Introducción:

Se puede crear contenedores de los objetos disponibles en el Active Directory, se puede brindar una identidad a cada empleado de la empresa y configurar un entorno de trabajo para cada uno de ellos.



Uso de Unidades Organizativas

Las Unidades organizativas permiten organizar los objetos del Directorio Activo de tal manera que su administración se más sencilla. Es un contenedor lógico, a la que se le puede introducir diferentes objetos, tales como: Equipos, contactos, grupos, impresoras, usuarios, etc.

Es importante diferenciar entre carpetas (parte del Sistema de Directorio Activo) y las Unidades Organizativas (Creadas por intervención del usuario).

Las carpetas **Computers y Users**, se conservan por compatibilidad con Windows NT para recoger todas las cuentas existentes en dominios NT al hacer la transmisión a Window Server 2008.

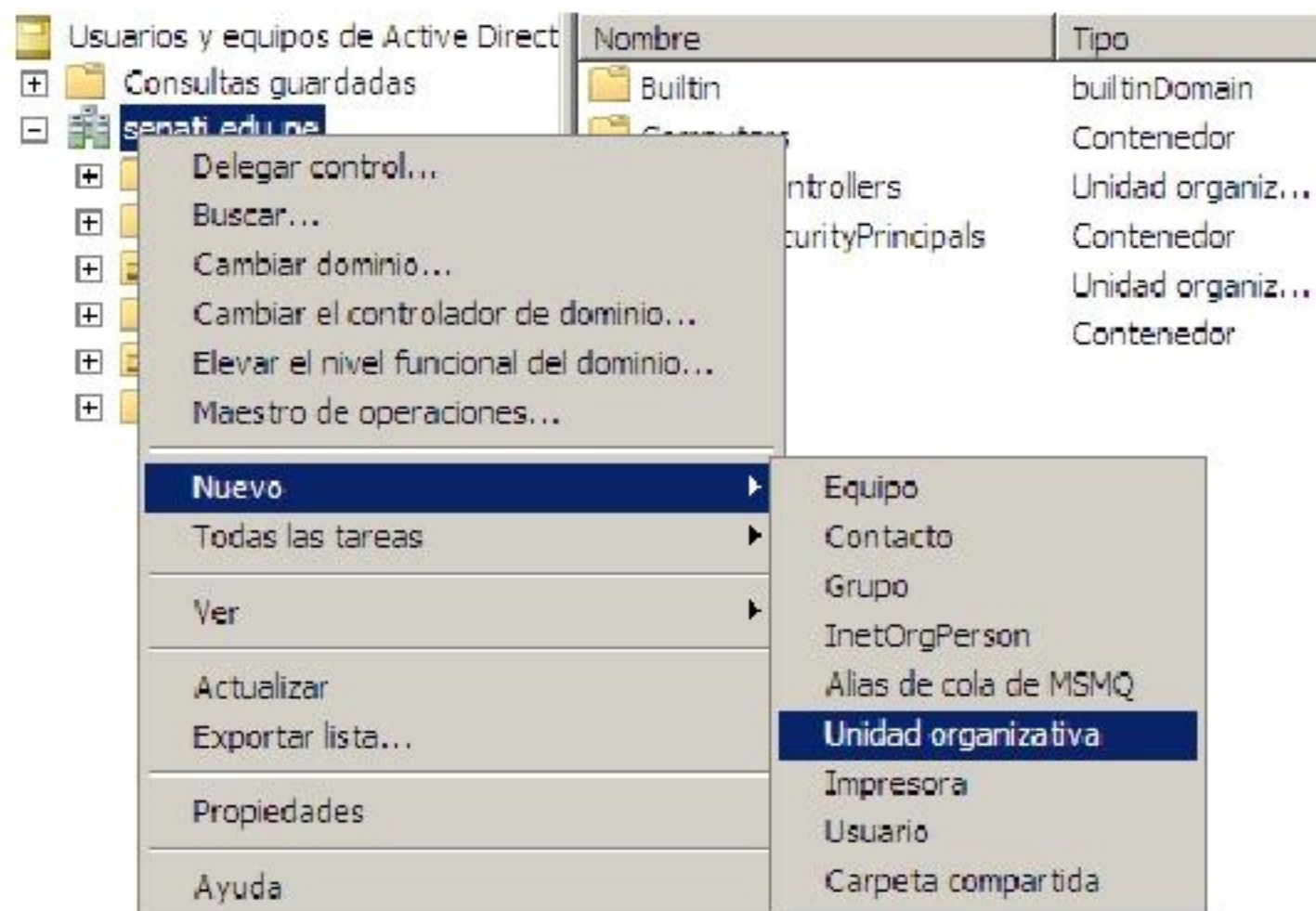
Puede crear unidades organizativas basadas en 3 criterios fundamentales:

1. Ubicación Geográfica (Perú, Canadá, Lima, Cuzco, etc.)
2. Área o Departamento (Contabilidad, Ventas, Gerencia, etc.)
3. Cargo o Función (Empleados, Gerentes, Administradores, Alumnos, etc.)

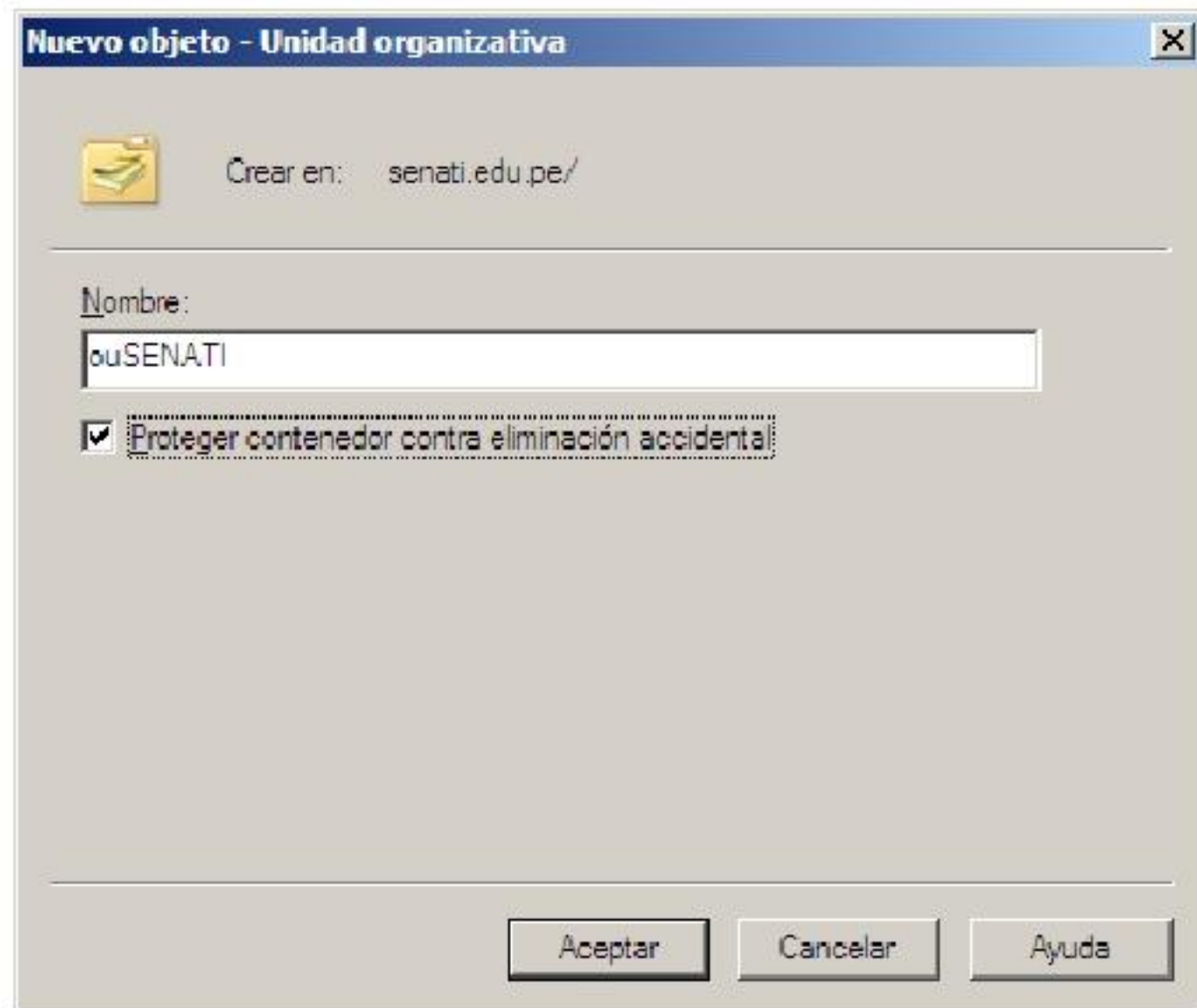
Creación de Unidades organizativas

Se pueden crear unidades organizativas anidadas, ya que no hay límite de niveles de anidación.

1. Abra la ventana de complemento **Usuarios y equipos de Active Directory**.
2. Seleccione el dominio.
3. Haga clic derecho sobre el nombre del dominio, señale Nuevo, y haga clic sobre Unidad organizativa.



4. En el asistente que aparecerá a continuación escriba el nombre de la unidad organizativa, por ejemplo **ouSENATI** (ou es un prefijo de Organizational Unit, y ayuda a identificar el tipo de objeto que se está creando, no es obligatorio su uso)



Por defecto, las unidades organizativas tendrán un atributo de protección llamado **Proteger contenedor contra eliminación accidental**, que evita se pueda borrar el objeto usando el comando Eliminar de los menús o barras de herramientas, y deberá desactivarlo antes de proceder con su eliminación.

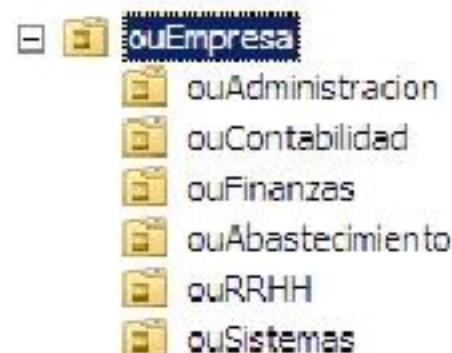
- Haga clic en Aceptar y observará que se ha creado la unidad organizativa en el dominio.



Ahora puede crear más unidades organizativas dentro de **ouSENATI**.

Actividad 1

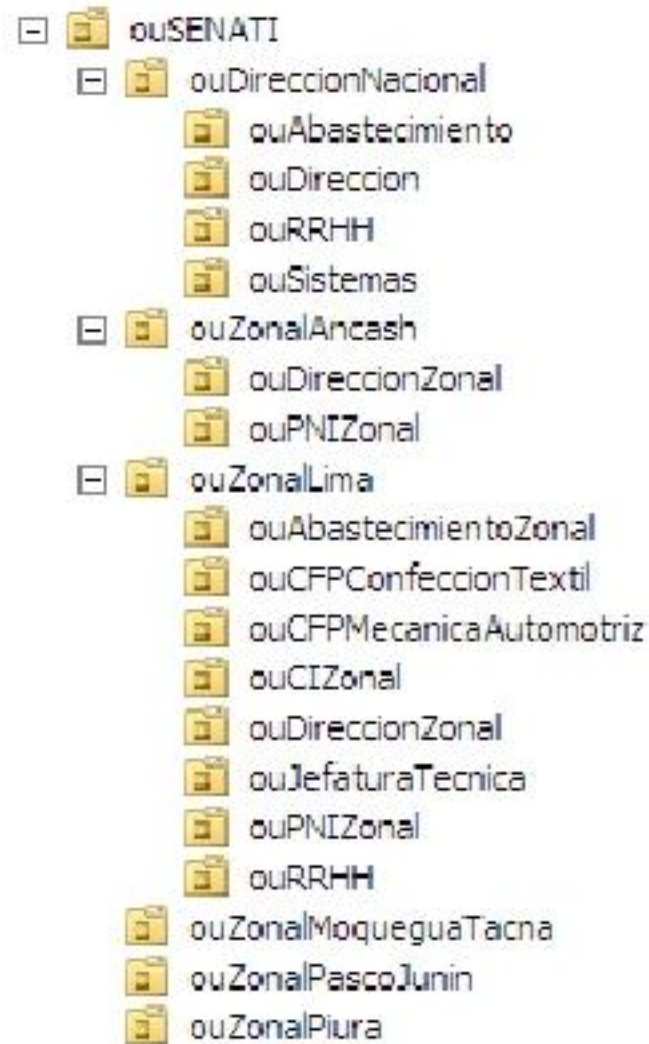
- Crea el siguiente grupo de unidades organizativas.





Actividad 2

1. Crear el siguiente grupo de unidades organizativas



Propiedades de las unidades organizativas

Como todo objeto, las unidades organizativas tienen propiedades particulares, y se pueden visualizar de forma básica y avanzada. Observemos la diferencia

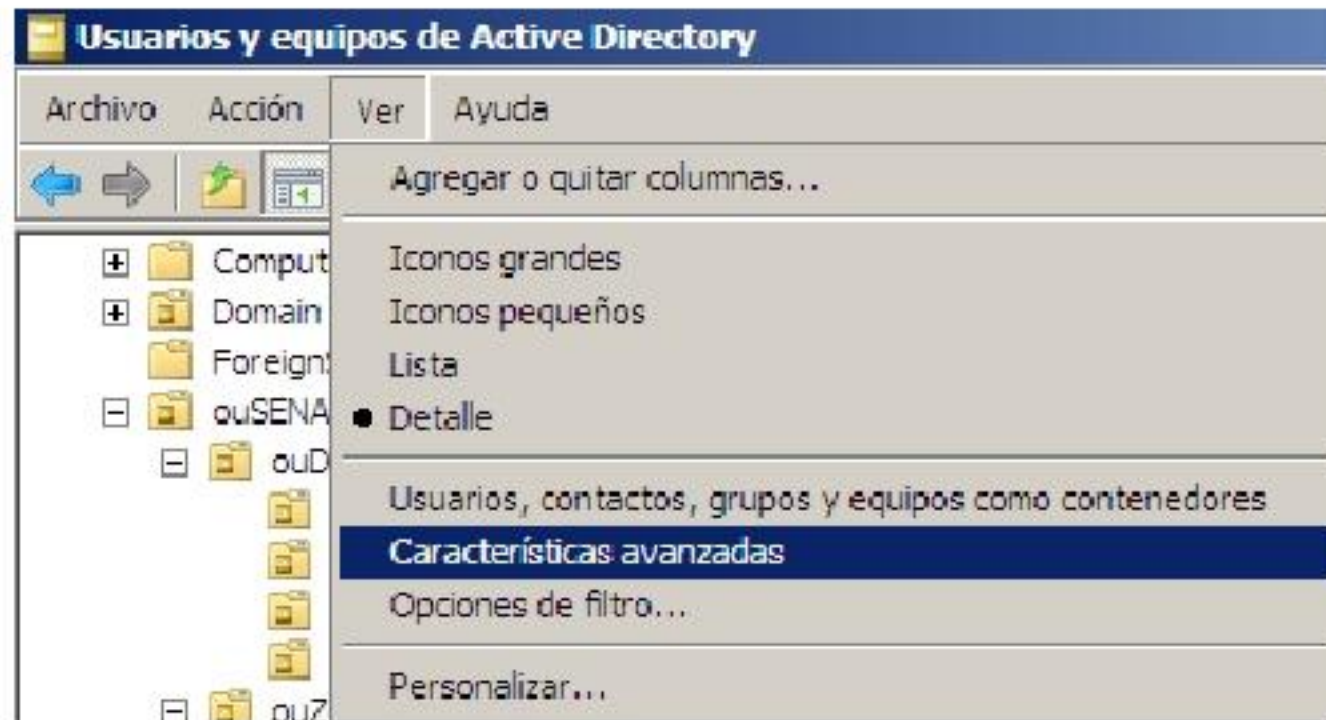
Forma Básica.

1. Clic derecho en la unidad organizativa y haga clic en Propiedades.
2. Observará las siguientes fichas **General**, **Administrador por** y **COM+**.



Forma avanzada

1. Menú Ver, opción Características avanzadas.



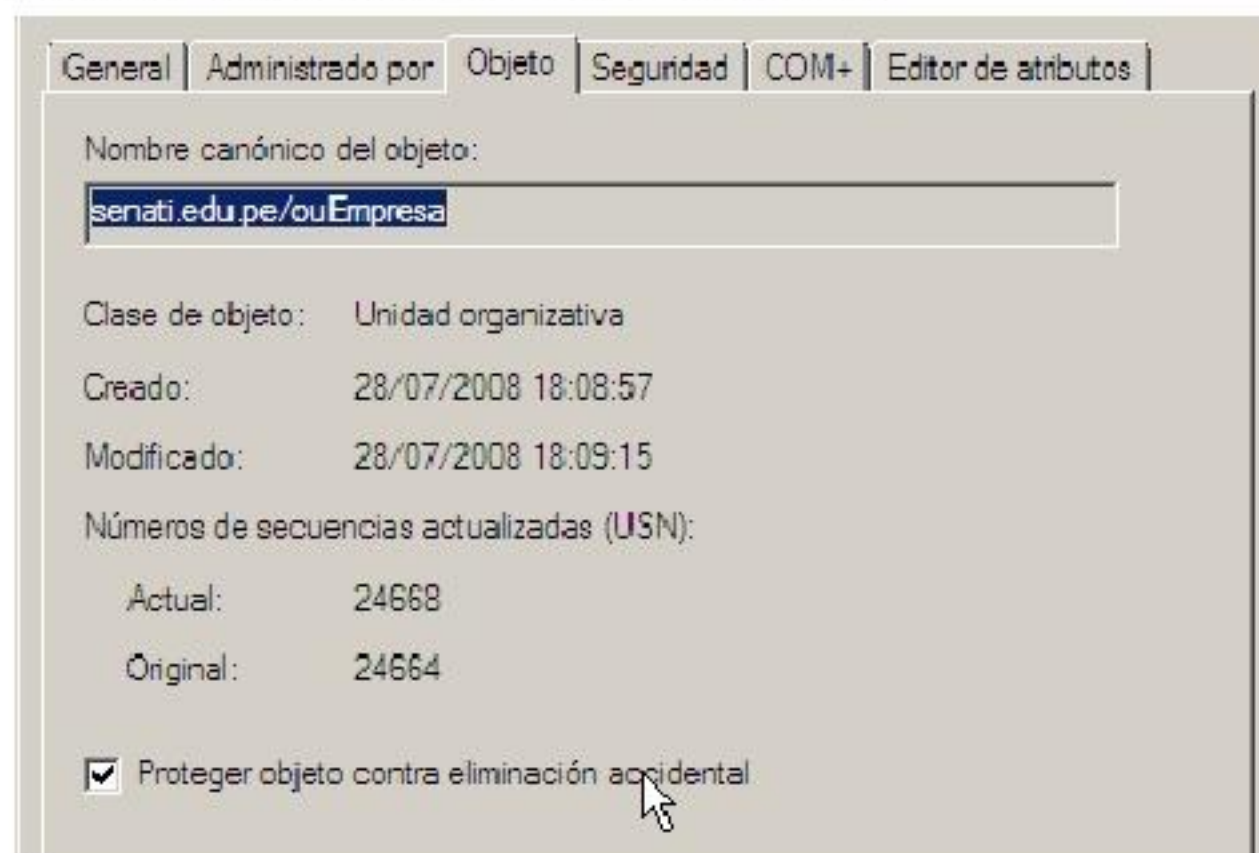
2. Clic derecho en la unidad organizativa y haga clic en Propiedades.
3. Observará las siguientes fichas: **General, Administrador por, Objeto, Seguridad, COM+ y Editor de atributos.**



Traslado de unidades organizativas

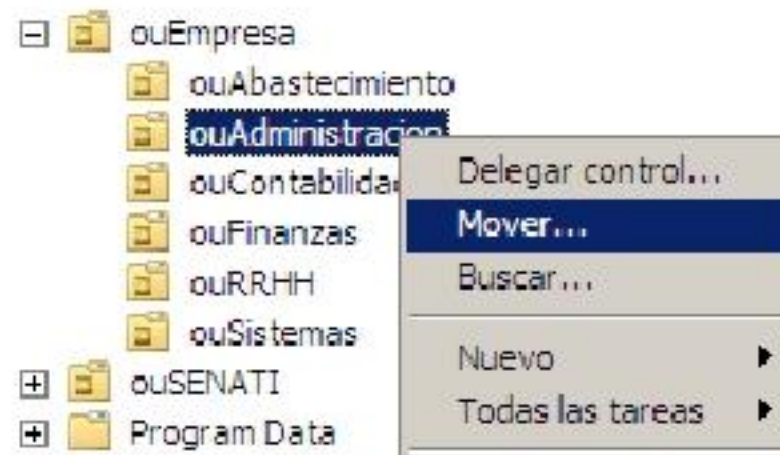
Para trasladar (mover) una unidad organizativa primero debe deshabilitar la opción **Proteger contenedor contra eliminación accidental.**

1. Asegúrese de que el modo de **Características avanzadas**, esté activo.
2. Clic derecho en la unidad organizativa, y seleccione propiedades.
3. Haga clic en la ficha Objeto y desactive la propiedad **Proteger contenedor contra eliminación accidental.** Clic en Aceptar

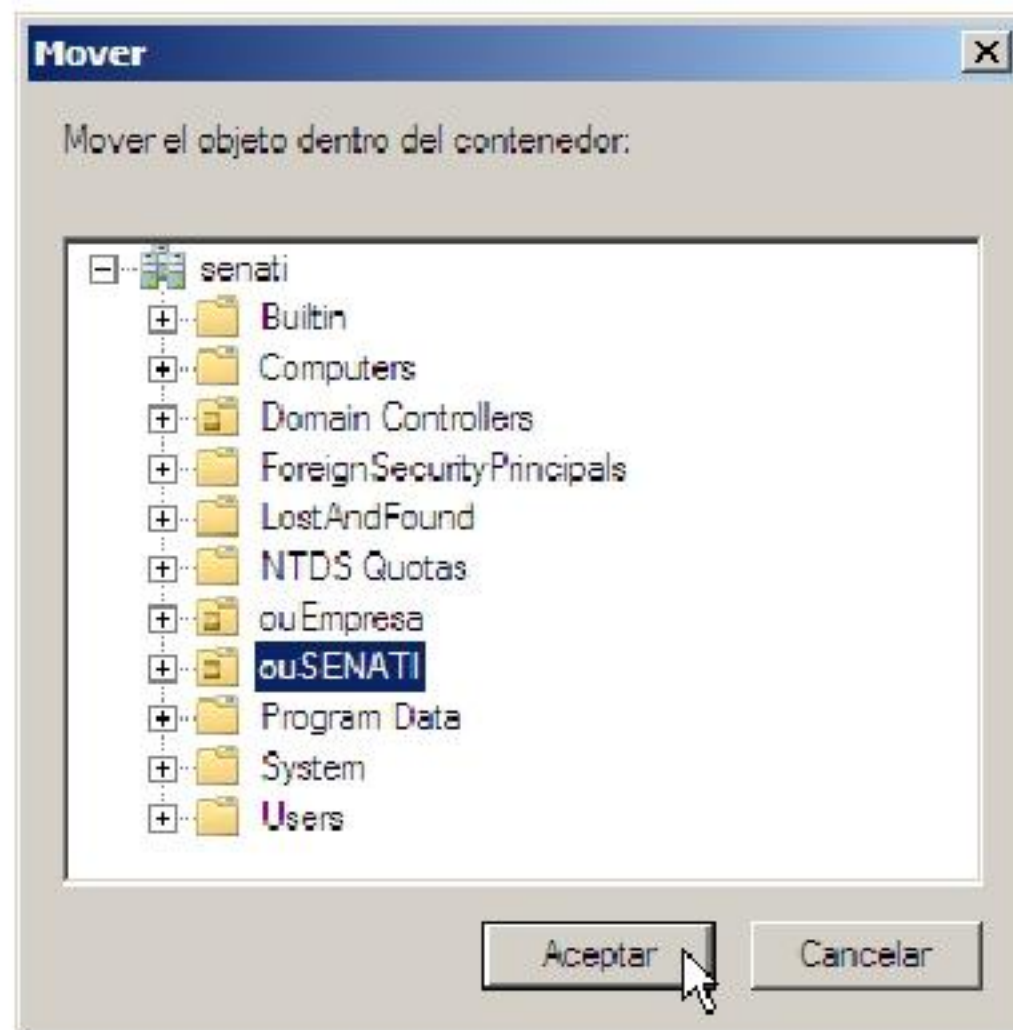




4. Haga clic derecho sobre la unidad organizativa.
5. Haga clic en Mover.

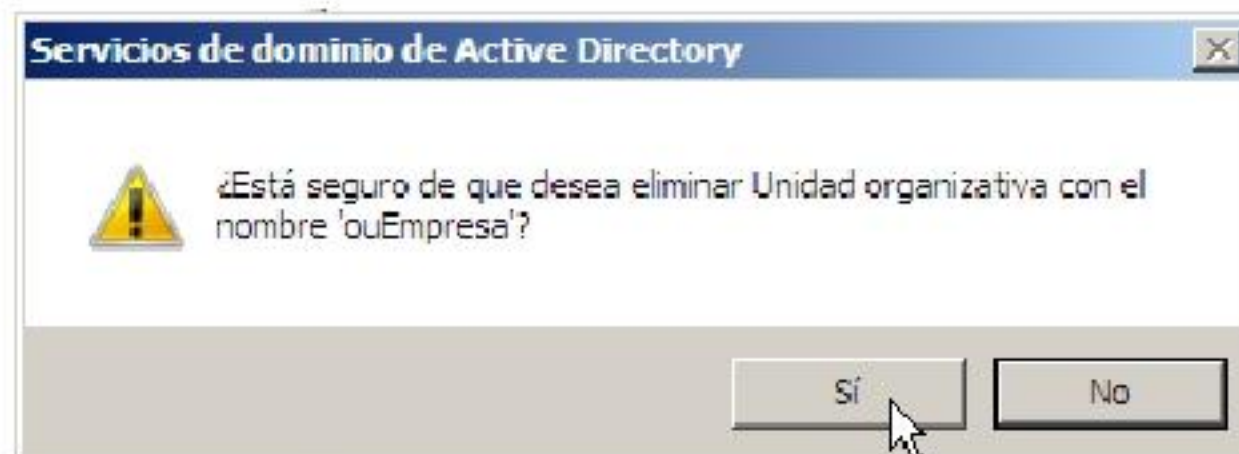


6. Seleccione la ubicación destino y haga clic en aceptar.



Eliminación de Unidades organizativas

1. Asegúrese de tener desactivada la opción **Proteger contenedor contra eliminación accidental**.
2. Luego haga clic derecho sobre la unidad organizativa y haga clic en Sí.



Elementos disponibles dentro de una OU

1. Equipo.- Representa a las computadoras que se conectan al dominio.
2. Contacto.- Es una cuenta de usuario, con una dirección de correo electrónico asociada de manera opcional, pero que no puede utilizarse para iniciar sesión en el dominio.
3. Grupo.- Son objetos mediante los cuales se definen las credenciales que se asignarán a las cuentas, autorizándoles o denegándoles el acceso a los recursos.
4. InetOrgPerson.- Es una clase de objeto que facilita la transición desde servicios de directorio ajenos a Microsoft, siempre que utilicen los protocolos LDAP o X.500
5. Alias de la cola de MSMQ.- Representa un tipo de recurso que puede ser compartido entre las cuentas que forman parte de la Unidad Organizativa.
6. Impresora.- Facilita el proceso de compartir una impresora entre los usuarios que pertenezcan a la Unidad organizativa o dominio.
7. Usuario.- Cada cuenta se define como un hombre, el identificador de usuario y una contraseña.
8. Carpeta compartida.- Carpeta en la que los usuarios pueden encontrar información o almacenarla, según las credenciales con que cuente.

Creación de cuentas de Usuario

Las cuentas de usuario de Active Directory representan entidades físicas, como personas. Las cuentas de usuario también se pueden usar como cuentas de servicio dedicadas para algunas aplicaciones.

A veces, las cuentas de usuario también se denominan entidades de seguridad. Las entidades de seguridad son objetos de directorio a los que se asignan automáticamente identificadores de seguridad (SID), que se pueden usar para obtener acceso a recursos del dominio. Principalmente, una cuenta de usuario:

Autentica la identidad de un usuario.

Una cuenta de usuario permite que un usuario inicie sesión en equipos y dominios con una identidad que el dominio pueda autenticar. Un usuario que inicia sesión en la red debe tener una cuenta de usuario y una contraseña propias y únicas. Para maximizar la seguridad, evite que varios usuarios compartan una misma cuenta.

Autoriza o deniega el acceso a los recursos del dominio.

Después de que un usuario se autentica, se le concede o se le deniega el acceso a los recursos del dominio en función de los permisos explícitos que se le hayan asignado en el recurso.

Denominación de cuentas de usuario

El contenedor de usuarios de Usuarios y equipos de Active Directory muestra tres cuentas de usuario integradas: Administrador, Invitado y Asistente de ayuda. Estas cuentas de usuario integradas se crean automáticamente al crear el dominio.

Puede crear un nombre de usuario basado en ciertas consideraciones:


- El nombre de cuenta puede seguir un patrón en común: La primera letra del nombre seguido del apellido paterno, y si hay duplicación puede agregarse una letra del segundo apellido o quizá el segundo nombre, o en todo caso el año de nacimiento expresado en 2 dígitos.



- Las contraseñas deben ser expresiones que incluyan mayúsculas y minúsculas, números, espacios en blanco y algún carácter especial. Se recomienda que sea de una longitud de más de 12 caracteres.

Tipos de cuentas

Cada cuenta integrada tiene una combinación diferente de derechos y permisos. La cuenta Administrador es la que tiene más derechos y permisos en el dominio, mientras que la cuenta Invitado tiene derechos y permisos limitados. En la tabla siguiente se describen las cuentas de usuario predeterminadas de los controladores de dominio en los que se ejecuta el sistema operativo Windows Server® 2008.

Cuenta predeterminada	Descripción
Administrador	<p>La cuenta Administrador tiene control total del dominio. Puede asignar derechos de usuario y permisos de control de acceso a los usuarios del dominio según sea necesario. Esta cuenta sólo se debe usar para las tareas que requieran credenciales administrativas. Es recomendable que configure esta cuenta con una contraseña segura.</p> <p>La cuenta Administrador es un miembro predeterminado de los siguientes grupos de Active Directory: Administradores, Administradores del dominio, Administradores de organización, Propietarios del creador de directivas de grupo y Administradores de esquema. La cuenta Administrador nunca se puede eliminar ni quitar del grupo Administradores, pero es posible cambiarle el nombre o deshabilitarla. Como es sabido que la cuenta Administrador existe en muchas versiones de Windows, si le cambia el nombre o la deshabilita dificultará el acceso a ella a usuarios malintencionados.</p> <p>La cuenta Administrador es la primera cuenta que se crea cuando se configura un nuevo dominio con el Asistente para la instalación de los Servicios de dominio de Active Directory.</p> <p> Importante</p> <p>Aunque la cuenta Administrador esté deshabilitada, puede seguir usándose para obtener acceso a un controlador de dominio con el modo seguro.</p>
Invitado	<p>Los usuarios que no tienen una cuenta en el dominio pueden usar la cuenta Invitado. Un usuario cuya cuenta se haya deshabilitado (pero no eliminado) también puede usar la cuenta Invitado. La cuenta Invitado no requiere ninguna contraseña.</p> <p>Puede asignar derechos y permisos para la cuenta Invitado de la misma forma que para cualquier cuenta de usuario. De manera predeterminada, la cuenta Invitado es miembro del grupo integrado Invitados y del grupo global Invitados de dominio, lo que permite al usuario iniciar sesión en un dominio. La cuenta Invitado está deshabilitada de forma predeterminada y recomendamos que permanezca así.</p>

Asistente de ayuda (se instala con una sesión de Asistencia remota)	Es la cuenta principal para establecer una sesión de Asistencia remota. Esta cuenta se crea automáticamente al solicitar una sesión de Asistencia remota. Tiene acceso limitado al equipo. La cuenta Asistente de ayuda se administra mediante el servicio Administrador de sesión de Ayuda de escritorio remoto. La cuenta se elimina automáticamente si no hay solicitudes de Asistencia remota pendientes.
----------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Consideraciones sobre las cuentas de usuario y de sistema:

1. **Cuentas creadas por el usuario.**
 - a. Permite a los usuarios registrarse en la Red
 - b. Permite acceder a los recursos y realizar determinadas tareas si se tienen los permisos y derechos apropiados
 - c. Contienen nombre de usuario, contraseña y una descripción
 - d. Se clasifican en dos:
 - i. **Cuentas de usuario del dominio:** Permite registrarse en un dominio y obtener acceso a los recursos de la red. Deben ser creadas en Unidades Organizativas.
 - ii. **Cuentas de usuario Locales:** Permite a los usuarios registrarse y obtener acceso a los recursos sólo en la computadora donde se creó la cuenta de usuario local.
2. **Cuentas del sistema.**
 - a. Invitado
 - i. Usada para usuarios ocasionales
 - ii. Permite acceder a los recursos de la computadora local
 - iii. Está deshabilitada por defecto
 - iv. Se recomienda cambiarle el nombre y descripción
 - b. Administrador
 - i. Usada para administrar el dominio
 - ii. Permite el mantenimiento de usuarios, grupos y cuentas; la administración de políticas de seguridad y de los recursos de la red.
 - iii. Asignar derechos y permisos a las cuentas de usuario
 - iv. La persona encargada de instalar el Directorio Activo en el equipo crea la contraseña de esta cuenta durante la instalación.
 - v. Se recomienda cambiarle el nombre y descripción
 - vi. Crea otra cuenta llamada Administrador con privilegios mínimos que sirva de señuelo a otros atacantes.
 - vii. Asigna una contraseña larga y compleja
 - viii. Cambia la contraseña periódicamente

Actividad 3

1. Cambia el nombre de usuario y descripción del usuario Invitado y Administrador.
2. Crea una cuenta denominada administrador y asígnale privilegios limitados.
3. Deshabilite la cuenta del administrador e inicie sesión en modo seguro. ¿Será posible?
4. Cree una cuenta de usuario de dominio denominada prueba, deshabilítela y trate de iniciar sesión. ¿Será posible?



Opciones de las cuentas de usuario

Las cuentas de usuario tienen diversas propiedades, entre ellas:

1. Nombre la persona que usar la cuenta, así como su apellido.
2. Nombre para mostrar
3. Descripción
4. Oficina
5. Número de teléfono
6. Nombre de inicio de sesión de usuario
7. Horas de inicio de sesión
8. Inicio de sesión en...

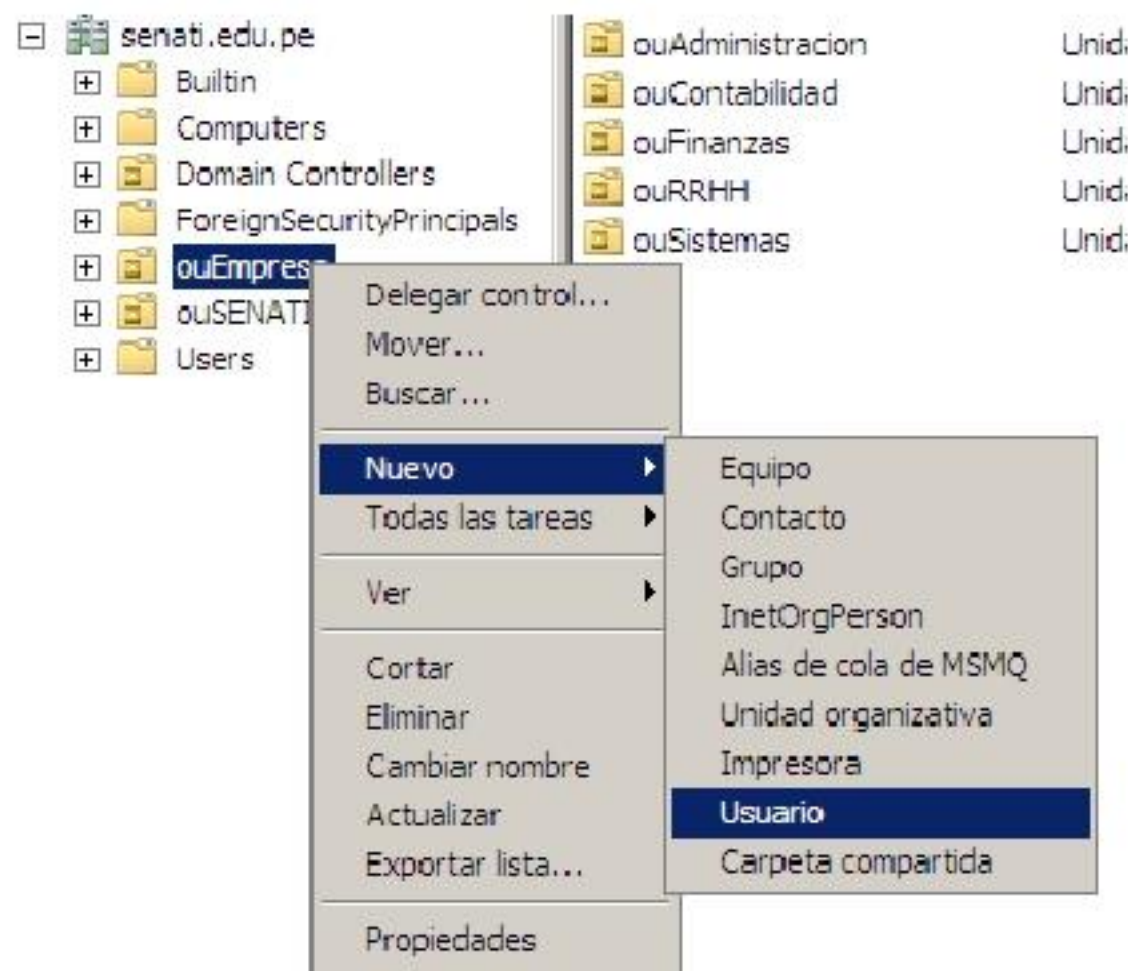
Creación de cuentas de usuario de dominio

Las cuentas de usuario de dominio se crean en el Active Directory y se pueden utilizar para iniciar sesión en cualquier equipo que esté unido al dominio.

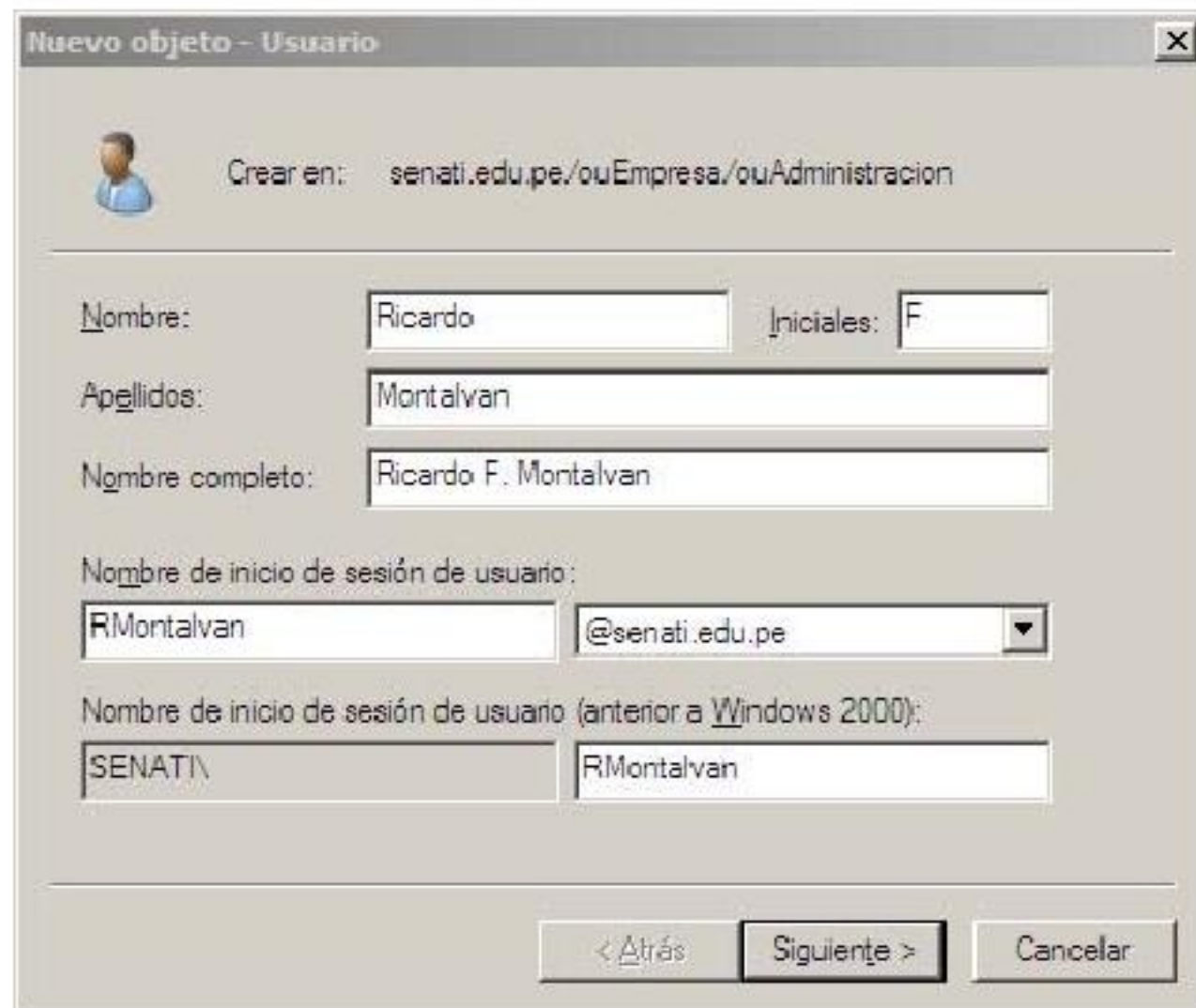
Sin embargo, en caso se encuentre en un dominio diferente o en un Grupo de trabajo, y desee conectarse a un recurso compartido en un dominio diferente se le solicitará que ingrese las credenciales de un usuario existente en el dominio.

Para crear una cuenta siga los siguientes pasos:

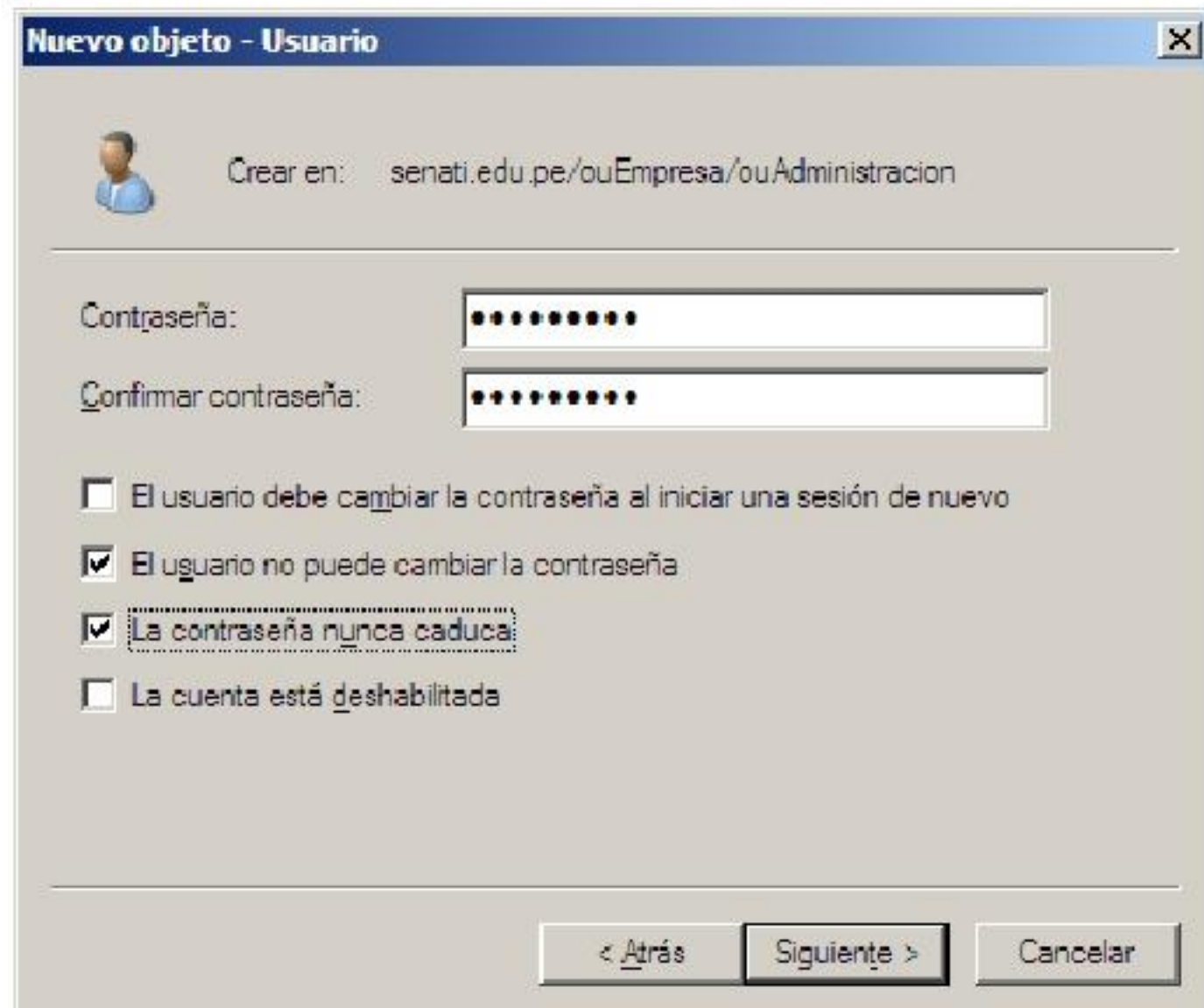
1. Haga clic derecho en la Unidad organizativa donde la creará, seleccione **Nuevo** y haga clic en **Usuario**.



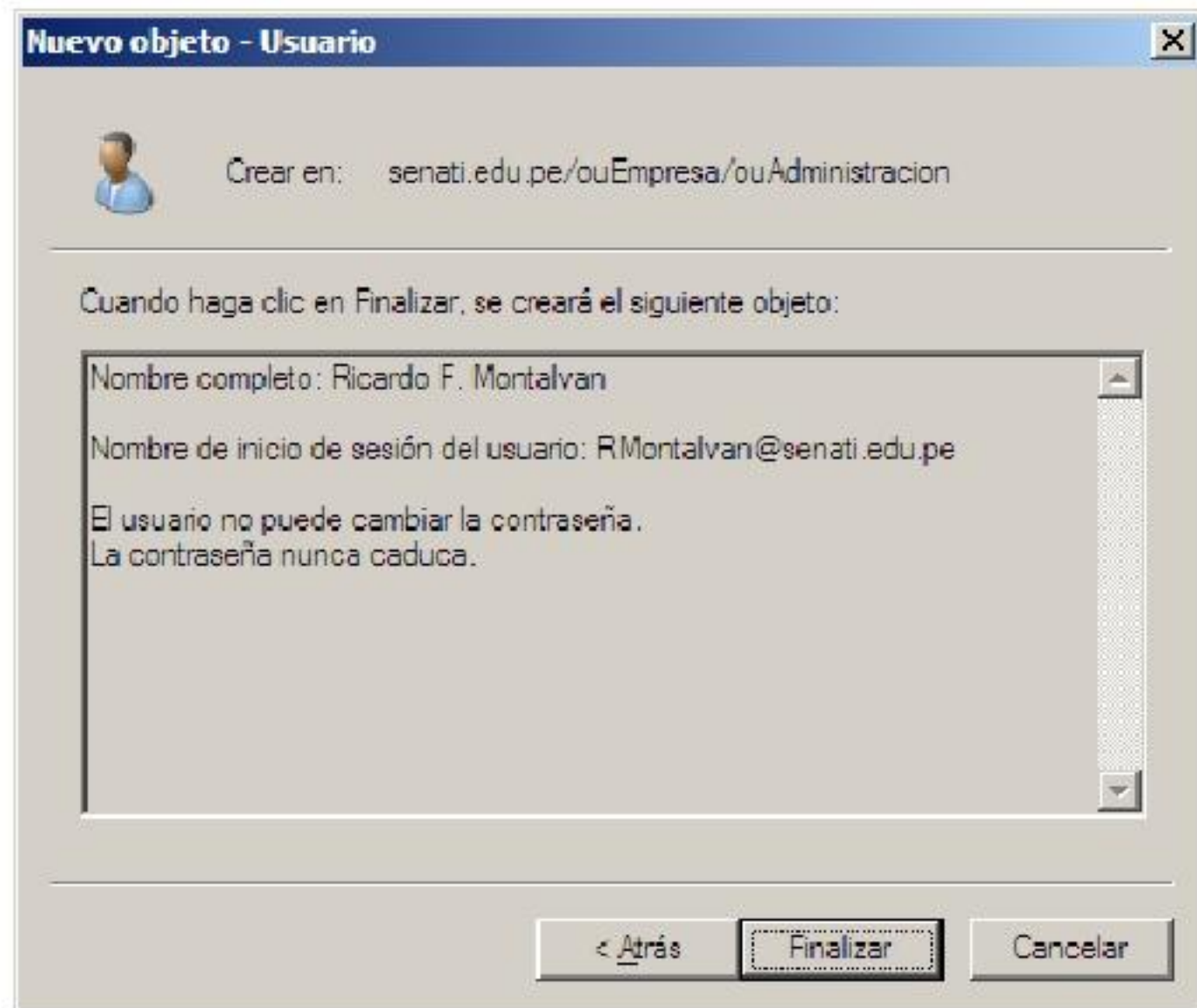
2. Aparecerá el siguiente cuadro de diálogo. Llene los datos del usuario.



3. Escriba la contraseña dos veces y configure algunas opciones. Haga clic en siguiente.



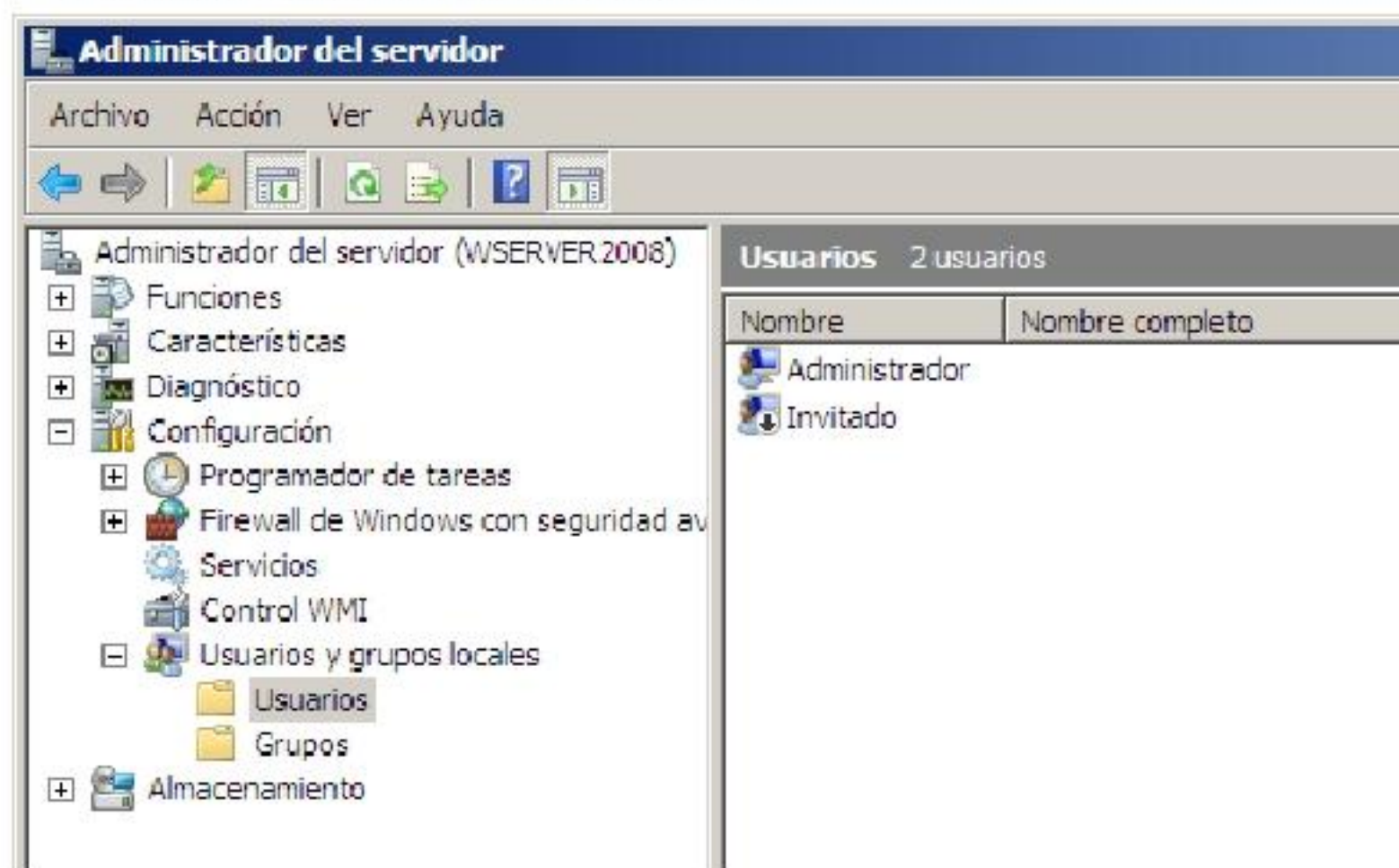
4. Confirme los datos y haga clic en Finalizar.



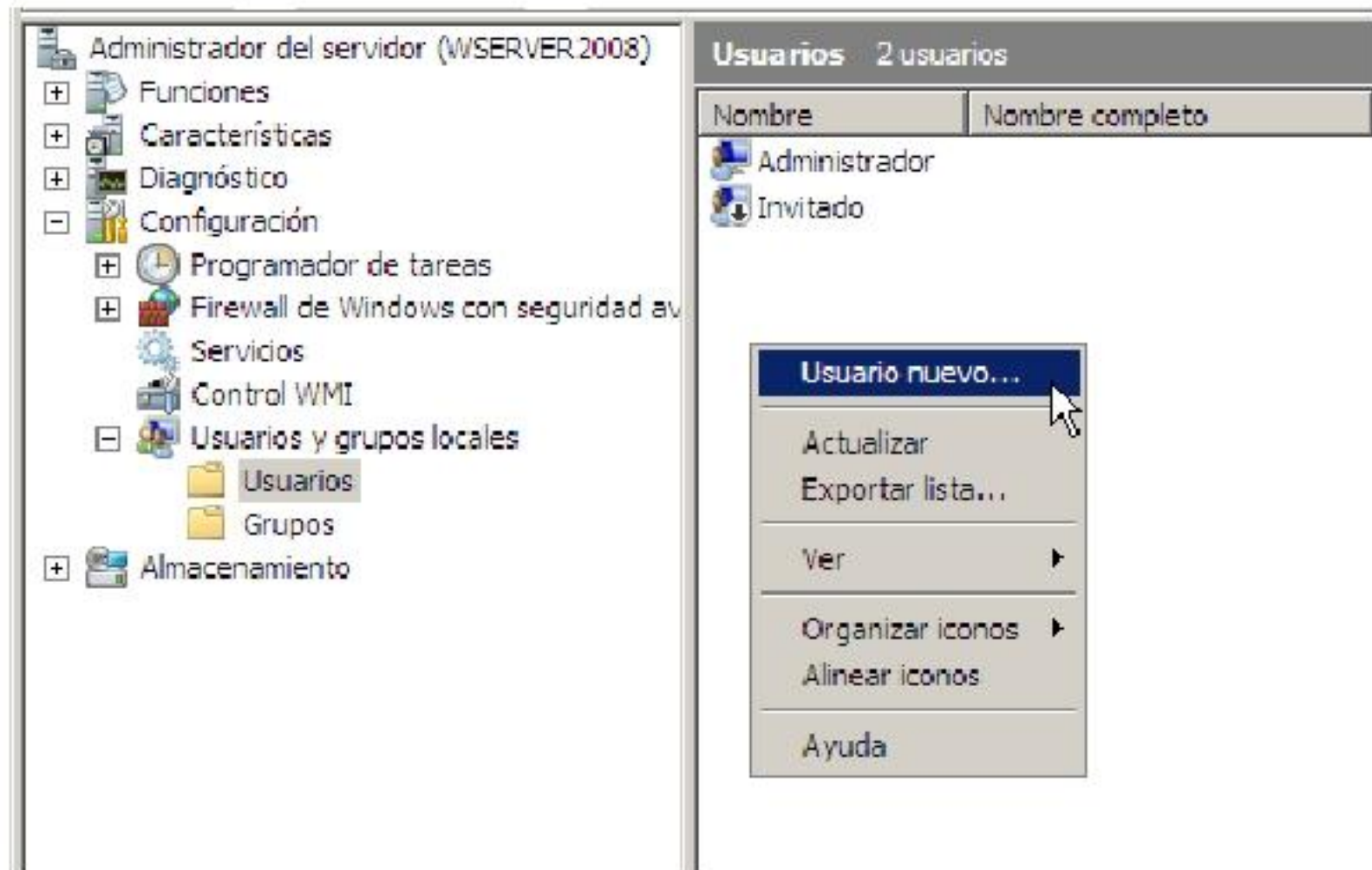
Creacion de cuentas de usuario locales

Las cuentas locales solo se pueden crear en servidores que no tienen instalado Active Directory.

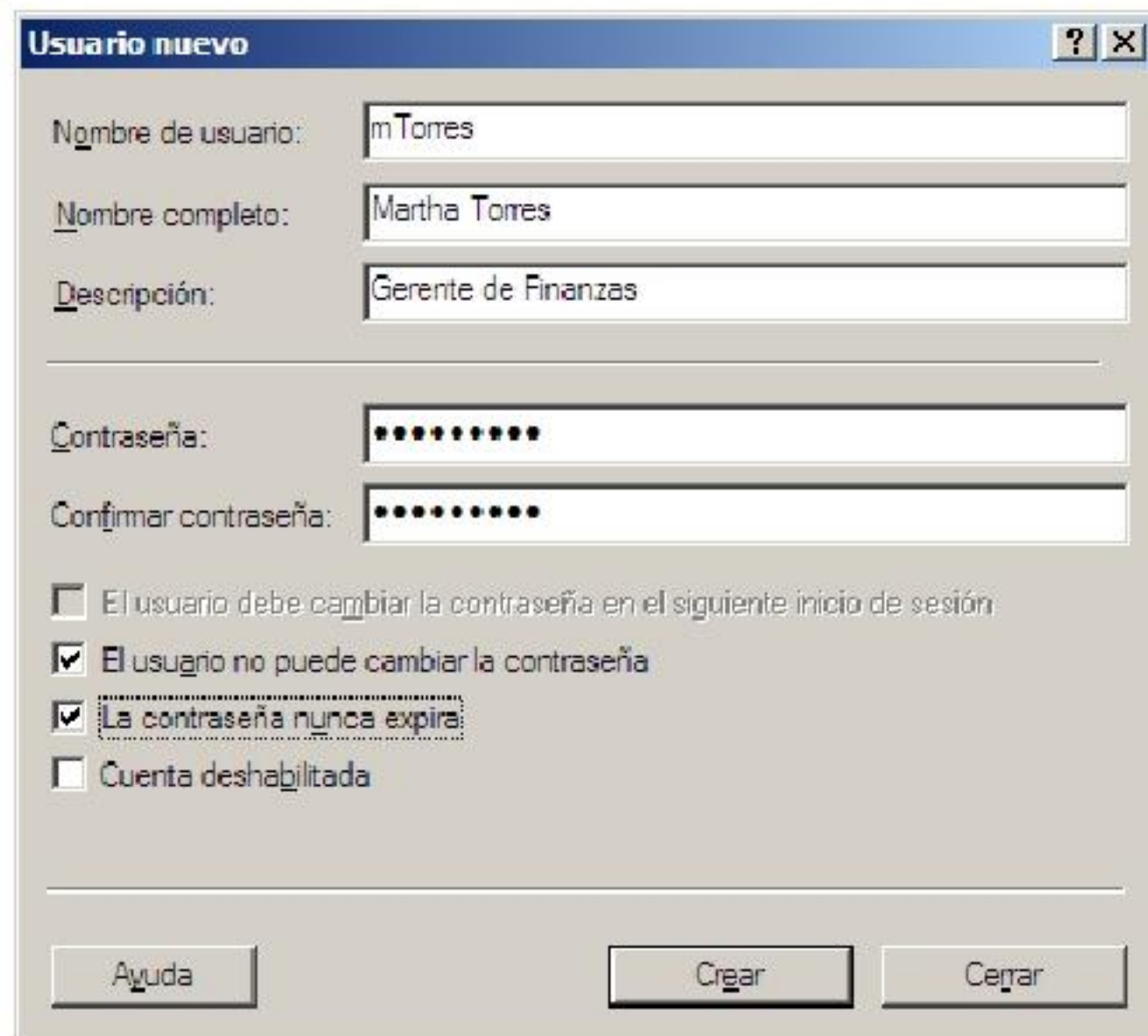
1. Observará una diferencia entre el **Administrador del Servidor**, en la sección **Configuración**. Seleccione **Usuarios**.



- Haga clic derecho sobre la sección Usuarios o en el Panel derecho. Haga clic en **Usuario nuevo....**



- Observará el siguiente cuadro de diálogo. Ingrese la información del usuario. Y haga clic en **Crear**.



The 'Usuario nuevo' dialog box contains the following fields and options:

- Nombre de usuario: mTorres
- Nombre completo: Martha Torres
- Descripción: Gerente de Finanzas
- Contraseña: [Redacted]
- Confirmar contraseña: [Redacted]
- El usuario debe cambiar la contraseña en el siguiente inicio de sesión
- El usuario no puede cambiar la contraseña
- La contraseña nunca expira
- Cuenta deshabilitada

Buttons at the bottom: Ayuda, Crear, Cerrar.



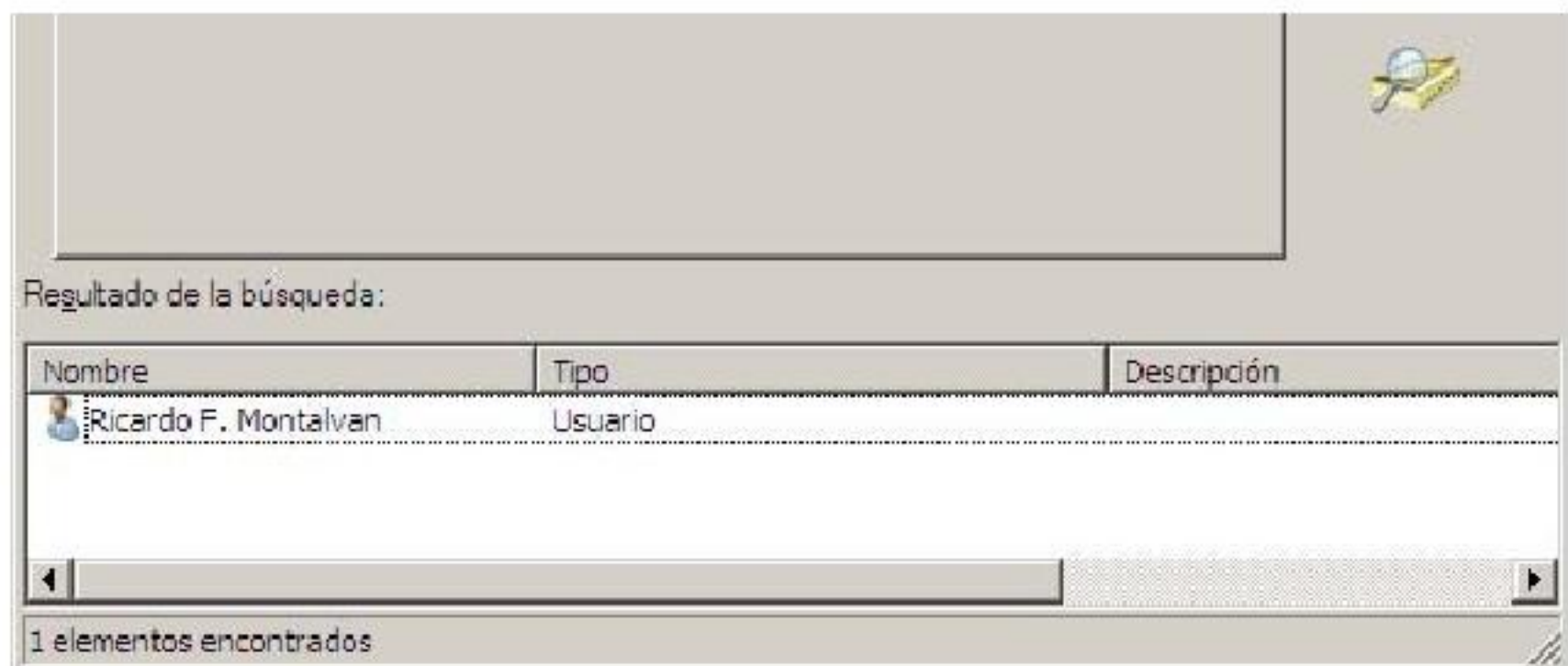
Administración de cuentas de usuario

Busqueda de cuentas de usuario

1. Si desea, puede seleccionar una unidad organizativa para empezar la búsqueda desde dicha unidad.
2. Haga clic en el menú **Acción** y luego en **Buscar**.



3. Escriba alguna palabra que asocie al objeto buscado. Por ejemplo escriba, **Montalvan**. Y luego haga clic en **Buscar**.



4. Observará el resultado en la parte inferior

Deshabilitación de cuentas de usuario

En ocasiones será necesario conservar una cuenta para un uso posterior, pero se requerirá que no esté disponible para uso por ninguna persona. En tal caso puede optar por deshabilitar la cuenta.

1. Haga clic derecho sobre la cuenta de usuario
2. Luego, haga clic en **Deshabilitar cuenta**.

Eliminación de cuentas de usuario

1. Seleccione la cuenta
2. Haga clic derecho sobre ella, y luego haga clic en Eliminar.

Traslado de cuentas de usuario

El proceso es idéntico a trasladar unidades organizativas

1. Seleccione la cuenta
2. Haga clic derecho sobre ella y luego haga clic en Mover
3. Seleccione el destino y haga clic en Aceptar.

Desbloqueo de cuentas de usuario

No debe confundirse la opción deshabilitar con desbloqueo, esta última ocurre luego de un número significativo de errores al momento de iniciar sesión.

1. Clic derecho sobre una cuenta de usuario y luego clic en Propiedades.
2. Ficha Cuenta, clic en **Desbloquear cuenta**.

Propiedades de la cuenta de usuario

En la siguiente tabla se muestran las principales propiedades

Control	Detalles
Nombre de inicio de sesión de usuario	<p>En el cuadro de texto de la izquierda dispone de espacio para escribir el nombre de cuenta de este usuario. Es el nombre con el que el usuario iniciará sesión en un dominio de Active Directory.</p> <p>La lista desplegable de la derecha muestra los sufijos de nombre principal de usuario (UPN) que se pueden usar para crear el nombre de inicio de sesión del usuario. La lista contiene el nombre completo del Sistema de nombres de dominio (DNS) del dominio actual, el nombre DNS completo del dominio raíz del bosque actual y los sufijos UPN alternativos creados con Dominios y confianzas de Active Directory.</p>
Nombre de inicio de sesión de usuario (anterior a Windows 2000)	<p>El cuadro de texto de sólo lectura que está a la izquierda muestra el nombre de dominio que usan los equipos en los que se ejecutan sistemas operativos anteriores a Windows 2000. Este nombre se usará también en la sintaxis anterior a Windows 2000 para el inicio de sesión de usuario, nombreDeDominio\nombreDeUsuario.</p> <p>En el cuadro de texto de la derecha dispone de espacio para escribir el nombre de inicio de sesión de usuario anterior a Windows 2000. Este nombre de usuario está en el formato anterior a Windows 2000, que es nombreDeDominio\nombreDeUsuario.</p>
Horas de inicio de sesión	<p>Haga clic en este botón para cambiar las horas durante las que el objeto seleccionado puede iniciar sesión en el dominio. De manera predeterminada, el inicio de sesión en el dominio se permite las 24 horas del día durante los 7 días a la semana. Tenga presente que este control no afecta a la posibilidad de que el usuario inicie sesión localmente en un equipo con una cuenta de equipo local en lugar de con una cuenta de dominio.</p>



Iniciar sesión en	Haga clic en este botón para especificar las restricciones de inicio de sesión en estaciones de trabajo que permitirán a este usuario iniciar sesión sólo en los equipos del dominio que se hayan especificado. De manera predeterminada, un usuario puede iniciar sesión en cualquier estación de trabajo unida al dominio. Tenga presente que este control no afecta a la posibilidad de que el usuario inicie sesión localmente en un equipo con una cuenta de equipo local en lugar de con una cuenta de dominio.
Desbloquear cuenta	<p>Permite desbloquear cuentas de usuario bloqueadas porque se produjeron demasiados errores al intentar iniciar sesión.</p> <p>Notas</p> <p>Cuando el controlador de dominio actual indica que la cuenta de usuario seleccionada está "no bloqueada", este control sólo está habilitado si el nivel funcional del dominio está establecido en Windows Server 2008. En otras palabras, sólo los controladores de dominio de Windows Server 2008 permiten "desbloquear" cuentas de usuario. Esta característica es especialmente útil cuando las cuentas de usuario se bloquean en controladores de dominio de sólo lectura (RODC) y la información de bloqueo no se replica en los demás controladores de dominio. No obstante, tenga en cuenta que la operación de desbloqueo sólo se puede realizar en un controlador de dominio de escritura.</p> <p>Cuando el controlador de dominio actual indica que la cuenta de usuario seleccionada está "bloqueada", el texto de la casilla es Desbloquear cuenta. La cuenta está actualmente bloqueada en este controlador de dominio de Active Directory.</p>
Opciones de cuenta	<p>Éstas son las opciones de cuenta de usuario de Active Directory:</p> <ul style="list-style-type: none">• El usuario debe cambiar la contraseña en el siguiente inicio de sesión• El usuario no puede cambiar la contraseña• La contraseña nunca expira• Almacenar contraseña utilizando cifrado reversible• Cuenta deshabilitada• La tarjeta inteligente es necesaria para un inicio de sesión interactivo• La cuenta es importante y no se puede delegar• Usar tipos de cifrado DES para esta cuenta• Esta cuenta admite cifrado AES de Kerberos de 128 bits• Esta cuenta admite cifrado AES de Kerberos de 256 bits• No pedir la autenticación Kerberos previa <p>Nota</p> <p>Las opciones de cifrado AES de Kerberos (tanto la de 128 bits como la de 256 bits) sólo están disponibles cuando el nivel funcional del dominio se establece en Windows Server 2008 o Windows Server 2003. El Estándar de cifrado avanzado (AES) es un nuevo algoritmo de cifrado que ha normalizado el National Institute of Standards and Technology (NIST). Se espera que su uso se extienda en los próximos años.</p>

La cuenta expira	<p>Establece la directiva de expiración de cuenta de este usuario. Tiene las opciones siguientes:</p> <p>Use Nunca para indicar que la cuenta seleccionada nunca expirará. Esta opción es la predeterminada para los usuarios nuevos.</p> <p>Seleccione Fin de y, a continuación, seleccione una fecha si desea que la cuenta del usuario expire en una fecha determinada.</p>
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Opciones de cuenta

Cada cuenta de usuario de Active Directory tiene varias opciones que determinan cómo se autentica en la red alguien que inicie sesión con esa cuenta de usuario concreta.

Con las opciones de la tabla siguiente se puede establecer la configuración de las contraseñas y la información específica de la seguridad de las cuentas de usuario.

Opción de cuenta	Descripción
El usuario debe cambiar la contraseña en el siguiente inicio de sesión	Obliga al usuario a cambiar su contraseña la próxima vez que inicie sesión en la red. Habilite esta opción cuando desee estar seguro de que el usuario es la única persona que conoce la contraseña.
El usuario no puede cambiar la contraseña	Impide que un usuario cambie su contraseña. Habilite esta opción si desea mantener el control de una cuenta de usuario, tal como una cuenta Invitado o una cuenta temporal.
La contraseña nunca expira	Impide que una contraseña de usuario expire. Recomendamos que las cuentas de servicio tengan esta opción habilitada y usen contraseñas seguras.
Almacenar contraseñas usando cifrado reversible	Permite al usuario iniciar sesión en una red de Windows desde un equipo Apple. Si el usuario no inicia sesión desde un equipo Apple, no habilite esta opción.
Cuenta deshabilitada	Impide al usuario iniciar sesión con la cuenta seleccionada. Muchos administradores usan cuentas deshabilitadas como plantillas para las cuentas de usuario normales.
La tarjeta inteligente es necesaria para un inicio de sesión interactivo	Requiere que el usuario posea una tarjeta inteligente para iniciar sesión en la red de forma interactiva. El usuario debe tener también un lector de tarjetas inteligentes conectado al equipo y un número de identificación personal (NIP) para la tarjeta inteligente. Cuando se habilita esta opción, la contraseña de la cuenta de usuario se establece automáticamente en un valor aleatorio y complejo, y se habilita la opción de cuenta La contraseña nunca expira.



Se confía en la cuenta para su delegación	<p>Permite que un servicio que se ejecute con esta cuenta realice operaciones en nombre de otras cuentas de usuario en la red. Un servicio que se ejecuta con una cuenta de usuario (también conocida como cuenta de servicio) en la que se confía para la delegación, puede suplantar a un cliente para obtener acceso a los recursos del equipo donde se ejecuta el servicio o a los recursos de otros equipos. En un bosque que se encuentre establecido en el nivel funcional de Windows Server 2008, esta opción está en la ficha Delegación. Está disponible sólo para las cuentas a las que se han asignado nombres principales de servicio (SPN), lo que se consigue a través del comando setspn de Windows Server 2008 (abra una ventana del símbolo del sistema y escriba setspn). Se trata de una característica crítica para la seguridad, por lo que se debe usar con precaución.</p> <p>Esta opción sólo está disponible en los controladores de dominio con Windows Server 2008 y que tengan funcionalidad de dominio Windows 2000 mixta o Windows 2000 nativa. Si en los controladores de dominio se ejecuta Windows Server 2008 y el nivel funcional del dominio se encuentra establecido en el nivel funcional de bosque de Windows Server 2008, use la ficha Delegación del cuadro de diálogo de propiedades del usuario para configurar las opciones de delegación. La ficha Delegación sólo aparece para las cuentas que tengan asignados SPN.</p>
La cuenta es importante y no se puede delegar	Puede usar esta opción si otra cuenta no puede asignar esta cuenta para su delegación (por ejemplo, una cuenta Invitado o temporal).
Usar tipos de cifrado DES para esta cuenta	Ofrece compatibilidad con el Estándar de cifrado de datos (DES). DES admite varios niveles de cifrado, como el estándar MPPE (Cifrado punto a punto de Microsoft) de 40 bits, el estándar MPPE de 56 bits, el estándar MPPE Strong de 128 bits, DES IPsec (Protocolo de seguridad de Internet) de 40 bits, DES IPsec de 56 bits y Triple DES (3DES) IPsec.
No pedir la autenticación Kerberos previa	Ofrece compatibilidad con implementaciones alternativas del protocolo Kerberos. Tenga cuidado cuando habilite esta opción, porque la autenticación Kerberos previa proporciona una mayor seguridad y requiere la sincronización de hora entre el cliente y el servidor.

Perfiles de usuario

Los perfiles de usuario son el conjunto de características que incluyen, el escritorio, carpeta mis documentos, favoritos, y toda la información que le permite iniciar sesión en un equipo. Pueden ser de tres tipos: Locales, Móviles y Obligatorios.

Los perfiles Locales son los más usados, ya que, tanto móviles como obligatorios requieren copiar archivos del perfil desde un recurso compartido hasta el equipo donde se está iniciando sesión.

Todos los perfiles se guardan en la carpeta **C:\Usuarios** y son inicialmente una copia de la carpeta **Default**.

Si el usuario nunca ha iniciado sesión en un determinado equipo, cuando lo haga, se creará una carpeta de perfil en ese equipo, ha esto se le denomina **Perfil Local**.

Puede configurar una carpeta compartida, con los permisos adecuados y luego direccionar la carpeta de perfil a dicha carpeta. Utilice la ficha **Perfil** y escriba una ruta como la siguiente: [\\wserver2008\Perfiles\%username%](#), ha esto se le denomina **Perfil Móvil**.

`%username%` es una variable del sistema que representa el nombre de la cuenta de usuario que está modificando.

Dentro de la carpeta del perfil se crea un archivo NTUSER.DAT, puede cambiar el nombre a NTUSER.MAN, lo que provocará que el perfil no guarde los cambios realizados en el mismo, de tal manera que se pierdan todas las modificaciones que se hayan hecho al perfil.

Recuerde que el uso de perfiles móviles y obligatorios en ambientes corporativos se evita por su alto consumo de ancho de banda al momento de copiar los archivos al equipo y su actualización cuando el usuario cierra sesión.

Directorio Particular

El directorio particular es una carpeta utilizada y accesible únicamente por el usuario, además se puede asignar una unidad de red a dicha carpeta.

Se debe crear una carpeta compartida para almacenar las carpetas de directorio particular.

Luego puede usar una ruta como; [\\wserver2008\DirPersonal\%username%](#)

Y asignarle una letra de unidad, que será accesible cada vez que el usuario inicie sesión, a través de Mi PC.

Preguntas de Repaso

1. Investigación:
 - a.Cuál es la longitud máxima para un nombre de usuario
 - b.Cuál es la longitud mínima de una contraseña
 - c. Cuántas contraseñas son recordadas por defecto como histórico
 - d. Cuántas veces puedo equivocarme en la contraseña antes de que la cuenta se bloquee.
 - e. Porqué crear una cuenta de equipo antes de unir el equipo físico al dominio.
2. Realice las siguientes actividades:



- a. Configure un usuario para que acceda a los recursos del dominio, utilizando tres equipos distintos y únicamente de Lunes a Viernes, de 13:00 a 21:00
- b. Cree 2 usuarios, inicie sesión con ambos desde un cliente Windows XP que esté conectado al dominio, realice cambios en su entorno de trabajo, cierre sesión y explore sus carpetas de perfil con la cuenta administrador local del Cliente Windows XP. También revise la carpeta Usuarios del Controlador de Dominio y note si se crearon también perfiles de usuario allí.
- c. Intente iniciar sesión el servidor usando una de las cuentas creadas anteriormente. ¿Qué mensaje recibo? Investigue qué hacer para que una cuenta estándar pueda iniciar sesión en el controlador de dominio.

Ejercicio Práctico

Considere las siguientes situaciones y datos para Diseñar un sistema de Red capaz de dar el soporte necesario a la misma.

La Empresa Montero S.A. contrata sus servicios como Administrador de Redes y proporciona los siguientes datos:

1. Las siguientes personas harán uso de la red.
 - a. Jorge Tafur (Gerente General)
 - b. Miguel Millano(Sub Gerente)
 - c. Miguel Quispe (Gerente Técnico)
 - d. Margot Donaire (Asistente Administrativo de la Gerencia técnica)
 - e. Frank Molina (Supervisor Area 1 Turno mañana)
 - f. Jorge Muñoz (Supervisor Area 2 Turno mañana)
 - g. Victor Mimbela (Supervisor Area 3 Turno mañana)
 - h. Marcos Torres (Supervisor Area 1 Turno noche)
 - i. Francisco Dominguez (Supervisor Area 2 Turno noche)
 - j. Richard Morris (Supervisor Area 3 Turno noche)
 - k. Manuel Pacora (Contador)
 - l. Susana Frey (Asistente administrativo de Contabilidad)
 - m. Jared Yafac (Gerente de RRHH)
 - n. Viviana Martinoti (Asistente administrativo de RRHH)
 - o. Lizeth Coronado (Gerente de Finanzas)
 - p. Mark Romero (Asistente administrativo de Finanzas)
 - q. Desire More (Gerente de Marketing)
 - r. Raúl Thomas (Asistente administrative de Marketing)
 - s. Mónica Suarez(Promotora de Ventas)
 - t. Vanesa Farfan (Promotora de Ventas)
 - u. Ivan Farías (Promotor de Ventas)
 - v. Martha Molina (Promotor de Ventas)
2. Existen 500 trabajadores más que necesitan acceder en forma esporádica a la red de la empresa por lo que se necesita una cuenta especial para todos ellos.
3. Todos los Gerentes trabajan de Lunes a Viernes de 9:00am a 5:00pm.
4. Los Supervisores trabajan de Lunes a Sábado de 7:45 am a 4:00 pm (Turno mañana) y de 4:00pm a 12am (Turno noche)
5. Los promotores de venta trabajan de 8:00 a 18:00 de Lunes a Sábado



Estrategias de Seguridad a través de Grupos

En este capítulo trataremos:

- Planificará una estrategia de grupos
- Entenderá la importancia de una estrategia de grupos
- Aprenderá a crear grupos de usuarios
- Identificará los grupos predefinidos
- Aprenderá a establecer derechos de usuario

Introducción:

Controlar el acceso a los recursos es una de las tareas más significativas de la administración de la red. Por lo que deberá entender qué técnicas son empleadas para simplificar la concesión de permisos.



Introducción a Grupos

Un grupo es un conjunto de cuentas de usuario y de equipo, contactos y otros grupos que se pueden administrar como una sola unidad. Los usuarios y los equipos que pertenecen a un grupo determinado se denominan miembros del grupo.

Los grupos de los Servicios de dominio de Active Directory (AD DS) son objetos de directorio que residen en un dominio y en objetos contenedores Unidad organizativa (OU). AD DS proporciona un conjunto de grupos predeterminados cuando se instala y también incluye una opción para crearlos.

Los grupos de AD DS se pueden usar para:

- ❖ **Simplificar la administración** al asignar los permisos para un recurso compartido a un grupo en lugar de a usuarios individuales. Cuando se asignan permisos a un grupo, se concede el mismo acceso al recurso a todos los miembros de dicho grupo.
- ❖ **Delegar la administración** al asignar derechos de usuario a un grupo una sola vez mediante la directiva de grupo. Después, a ese grupo le puede agregar miembros que desee que tengan los mismos derechos que el grupo.
- ❖ **Crear listas de distribución** de correo electrónico.

Los grupos se caracterizan por su **ámbito** y su **tipo**. El ámbito de un grupo determina el alcance del grupo dentro de un dominio o bosque. El tipo de grupo determina si se puede usar un grupo para asignar permisos desde un recurso compartido (para grupos de seguridad) o si se puede usar un grupo sólo para las listas de distribución de correo electrónico (para grupos de distribución).

También existen grupos cuyas pertenencias a grupos no se pueden ver ni modificar. Estos grupos se conocen con el nombre de identidades especiales. Representan a distintos usuarios en distintas ocasiones, en función de las circunstancias. Por ejemplo, el grupo Todos es una identidad especial que representa a todos los usuarios actuales de la red, incluidos invitados y usuarios de otros dominios.

Grupos predeterminados

Los grupos predeterminados, como es el caso del grupo Administradores del dominio, son grupos de seguridad que se crean automáticamente cuando se crea un dominio de Active Directory. Estos grupos predefinidos pueden usarse para ayudar a controlar el acceso a los recursos compartidos y para delegar funciones administrativas específicas en todo el dominio.

A muchos grupos predeterminados se les asigna automáticamente un conjunto de derechos de usuario que autorizan a los miembros del grupo a realizar acciones específicas en un dominio, como iniciar sesión en un sistema local o realizar copias de seguridad de archivos y carpetas. Por ejemplo, un miembro del grupo Operadores de copia de seguridad puede realizar operaciones de copia de seguridad para todos los controladores de dominio del dominio.

Cuando se agrega un usuario a un grupo, ese usuario recibe:

- ❖ Todos los derechos de usuario asignados al grupo
- ❖ Todos los permisos asignados al grupo para los recursos compartidos

Los grupos predeterminados se encuentran en el contenedor Builtin y en el contenedor Users. Los grupos predeterminados del contenedor Builtin tienen el ámbito de grupo Integrado local. Su ámbito de grupo y tipo de grupo no se pueden cambiar. El contenedor Users incluye grupos definidos con ámbito Global y grupos

definidos con ámbito Local de dominio. Los grupos ubicados en estos contenedores se pueden mover a otros grupos o unidades organizativas del dominio, pero no se pueden mover a otros dominios.

Ámbito de grupo

Los grupos se caracterizan por un ámbito que identifica su alcance en el bosque o árbol de dominios. Existen tres ámbitos de grupo: local de dominio, global y universal.

Grupos locales de dominio

Los miembros de los grupos locales de dominio pueden incluir otros grupos y cuentas de dominios de Windows Server 2003, Windows 2000, Windows NT y Windows Server 2008. A los miembros de estos grupos sólo se les pueden asignar permisos dentro de un dominio.

Los **grupos con ámbito Local de dominio** ayudan a definir y administrar el acceso a los recursos dentro de un dominio único. Estos grupos pueden tener los siguientes miembros:

- ❖ Grupos con ámbito Global
- ❖ Grupos con ámbito Universal
- ❖ Cuentas
- ❖ Otros grupos con ámbito Local de dominio
- ❖ Una combinación de los anteriores

Por ejemplo, para conceder acceso a una impresora determinada a cinco usuarios, puede agregar las cinco cuentas de usuario a la lista de permisos de la impresora. Sin embargo, si posteriormente desea que esos cinco usuarios tengan acceso a otra impresora, deberá volver a especificar las cinco cuentas en la lista de permisos para la nueva impresora.

Con un poco de previsión, puede simplificar esta tarea administrativa rutinaria al crear un grupo con ámbito Local de dominio y asignarle permisos de acceso a la impresora. Coloque las cinco cuentas de usuario en un grupo con ámbito Global y agregue este grupo al grupo que tiene ámbito Local de dominio. Cuando desee que los cinco usuarios tengan acceso a una nueva impresora, asigne permisos de acceso a la nueva impresora al grupo con ámbito Local de dominio. Todos los miembros del grupo con ámbito Global recibirán automáticamente el acceso a la nueva impresora.

Grupos globales

Los miembros de los grupos globales pueden incluir sólo otros grupos y cuentas del dominio en el que se encuentra definido el grupo. A los miembros de estos grupos se les pueden asignar permisos en cualquier dominio del bosque.

Use los grupos con ámbito Global para administrar objetos de directorio que requieran un mantenimiento diario, como las cuentas de usuario y de equipo. Dado que los grupos con ámbito Global no se replican fuera de su propio dominio, las cuentas de un grupo con ámbito Global se pueden cambiar frecuentemente sin generar tráfico de replicación en el catálogo global.

Aunque las asignaciones de derechos y permisos sólo son válidas en el dominio en el que se asignan, al aplicar grupos con ámbito Global de manera uniforme entre los dominios apropiados, es posible consolidar las referencias a cuentas con fines similares. De esta manera se simplifica y se racionaliza la administración de grupos entre dominios. Por ejemplo, en una red que tenga dos dominios, Europe y UnitedStates, si hay un grupo con ámbito Global denominado GLAccounting en el



dominio UnitedStates, debería haber también un grupo denominado GLAccounting en el dominio Europe (a menos que esa función de contabilidad (Accounting) no exista en el dominio Europe).

Importante

Recomendamos encarecidamente que use grupos globales o universales en lugar de grupos locales de dominio cuando especifique permisos para objetos de directorio de dominio que se repliquen en el catálogo global.

Grupos universales

Los miembros de los grupos universales pueden incluir otros grupos y cuentas de cualquier dominio del bosque o del árbol de dominios. A los miembros de estos grupos se les pueden asignar permisos en cualquier dominio del bosque o del árbol de dominios.

Use los grupos con ámbito Universal para consolidar los grupos que abarquen varios dominios. Para ello, agregue las cuentas a los grupos con ámbito Global y anide estos grupos dentro de los grupos que tienen ámbito Universal. Si usa esta estrategia, los cambios de pertenencias en los grupos que tienen ámbito Global no afectan a los grupos con ámbito Universal.

Por ejemplo, si una red tiene dos dominios, Europe y UnitedStates, y hay un grupo con ámbito Global denominado GLAccounting en cada dominio, cree un grupo con ámbito Universal denominado UAccounting que tenga como miembros los dos grupos GLAccounting, UnitedStates\GLAccounting y Europe\GLAccounting. Después, podrá usar el grupo UAccounting en cualquier lugar de la organización. Los cambios de pertenencia de los grupos GLAccounting individuales no producirá la replicación del grupo UAccounting.

No cambie la pertenencia de un grupo con ámbito Universal frecuentemente. Los cambios de pertenencia de este tipo de grupo hacen que se replique toda la pertenencia del grupo en cada catálogo global del bosque.

Tipos de grupo

Hay dos tipos de grupos en AD DS:

- ❖ Grupos de distribución y
- ❖ Grupos de seguridad.

Los **grupos de distribución** se usan para crear listas de distribución de correo electrónico y los grupos de seguridad se usan para asignar permisos para los recursos compartidos.

Los grupos de distribución sólo se pueden usar con aplicaciones de correo electrónico (como Microsoft Exchange Server 2007) para enviar mensajes a conjuntos de usuarios. Los grupos de distribución no tienen seguridad habilitada, lo que significa que no pueden aparecer en las listas de control de acceso discrecional (DACL). Si necesita un grupo para controlar el acceso a los recursos compartidos, cree un grupo de seguridad.

Si se usan con cuidado, los grupos de seguridad son eficaces para conceder acceso a los recursos de la red. Con los grupos de seguridad se puede:

- ❖ Asignar derechos de usuario a los grupos de seguridad de AD DS

Se asignan **derechos de usuario** a un grupo de seguridad para determinar lo que pueden hacer los miembros de ese grupo en el ámbito de un dominio (o bosque). A algunos grupos de seguridad se les asignan derechos de usuario automáticamente cuando se instala AD DS para ayudar a los administradores a definir la función administrativa de una persona en el dominio. Por ejemplo, si se agrega un usuario al grupo Operadores de copia de seguridad de Active Directory, éste puede realizar operaciones de copia de seguridad y restauración de archivos y directorios en cada controlador de dominio del dominio.

❖ Asignar permisos para recursos a los grupos de seguridad

Los permisos y los derechos de usuario no son lo mismo.

Los **permisos** determinan quién puede obtener acceso a un recurso compartido y el nivel de acceso, como Control total. Los grupos de seguridad se pueden usar para administrar el acceso y los permisos en un recurso compartido. Algunos permisos que se establecen en objetos de dominio se asignan automáticamente para proporcionar varios niveles de acceso a los grupos de seguridad predeterminados, como el grupo Operadores de cuentas o el grupo Administradores del dominio.

Como sucede con los grupos de distribución, los grupos de seguridad también se pueden usar como entidades de correo electrónico. Al enviar un mensaje de correo electrónico al grupo, se envía a todos sus miembros.

Identidades especiales

Además de los grupos de los contenedores Users y Builtin, los servidores en los que se ejecuta Windows Server 2008 o Windows Server 2003 incluyen varias identidades especiales.

Por comodidad se las suele llamar grupos. Estos grupos especiales no tienen pertenencias específicas que se puedan modificar.

Sin embargo, pueden representar a distintos usuarios en distintas ocasiones, en función de las circunstancias. Los grupos siguientes son identidades especiales:

Identidad Especial	Descripción
Inicio de sesión anónimo	Este grupo representa a los usuarios y servicios que obtienen acceso a un equipo y sus recursos a través de la red sin usar un nombre de cuenta, contraseña o nombre de dominio. En los equipos con Windows NT y versiones anteriores, el grupo Inicio de sesión anónimo es un miembro predeterminado del grupo Todos. En los equipos con Windows Server 2008 o Windows Server 2003, el grupo Inicio de sesión anónimo no es miembro del grupo Todos de manera predeterminada.
Todos	Este grupo representa a todos los usuarios actuales de la red, incluidos invitados y usuarios de otros dominios. Cuando un usuario inicia sesión en la red, se agrega automáticamente al grupo Todos.
Red	Este grupo representa a los usuarios que obtienen acceso en ese momento a un recurso dado a través de la red, frente a los usuarios que obtienen acceso a un recurso mediante un inicio de sesión local en el equipo en el que reside el recurso.



	Cuando un usuario obtiene acceso a un recurso dado a través de la red, se agrega automáticamente al grupo Red.
Interactivo	Este grupo representa a todos los usuarios que disponen de una sesión iniciada en un equipo determinado y que están obteniendo acceso a un recurso ubicado en ese equipo, frente a los usuarios que obtienen acceso al recurso a través de la red. Cuando un usuario obtiene acceso a un recurso dado en el equipo en el que ha iniciado sesión, se agrega automáticamente al grupo Interactivo.

Aunque a las identidades especiales se les puede conceder derechos y permisos para los recursos, sus pertenencias no se pueden ver ni modificar. Las identidades especiales no tienen ámbitos de grupo. Los usuarios son asignados automáticamente a ellas cuando inician sesión u obtienen acceso a un recurso concreto.

Información sobre creación de grupos

En AD DS, los grupos se crean en los dominios. Para crear grupos se utiliza Usuarios y equipos de Active Directory. Con los permisos necesarios, se pueden crear grupos en el dominio raíz del bosque, en cualquier otro dominio del bosque o en una unidad organizativa.

Además de por el dominio en el que se crea, un grupo también se caracteriza por su ámbito. El ámbito de un grupo determina lo siguiente:

- ❖ El dominio desde el que se pueden agregar miembros
- ❖ El dominio en el que son válidos los derechos y permisos asignados al grupo

Elija el dominio o la unidad organizativa donde va a crear un grupo en función de las tareas de administración que requiera el grupo. Por ejemplo, si un directorio tiene varias unidades organizativas y cada una tiene un administrador diferente, puede crear grupos con ámbito Global dentro de esas unidades organizativas para que los administradores administren la pertenencia a grupos de los usuarios de las unidades organizativas que les correspondan. Si se necesitan grupos para controlar el acceso fuera de la unidad organizativa, puede anidar los grupos de la unidad organizativa dentro de grupos con ámbito Universal (u otros grupos con ámbito Global) que puede utilizar en otros lugares del bosque.

Nota

Es posible mover grupos dentro de un dominio, pero sólo los grupos con ámbito Global se pueden mover entre dominios diferentes. Los derechos y permisos que se asignan a un grupo con ámbito Universal se pierden cuando el grupo se mueve a otro dominio y deben realizarse nuevas asignaciones.

Niveles de Funcionamiento

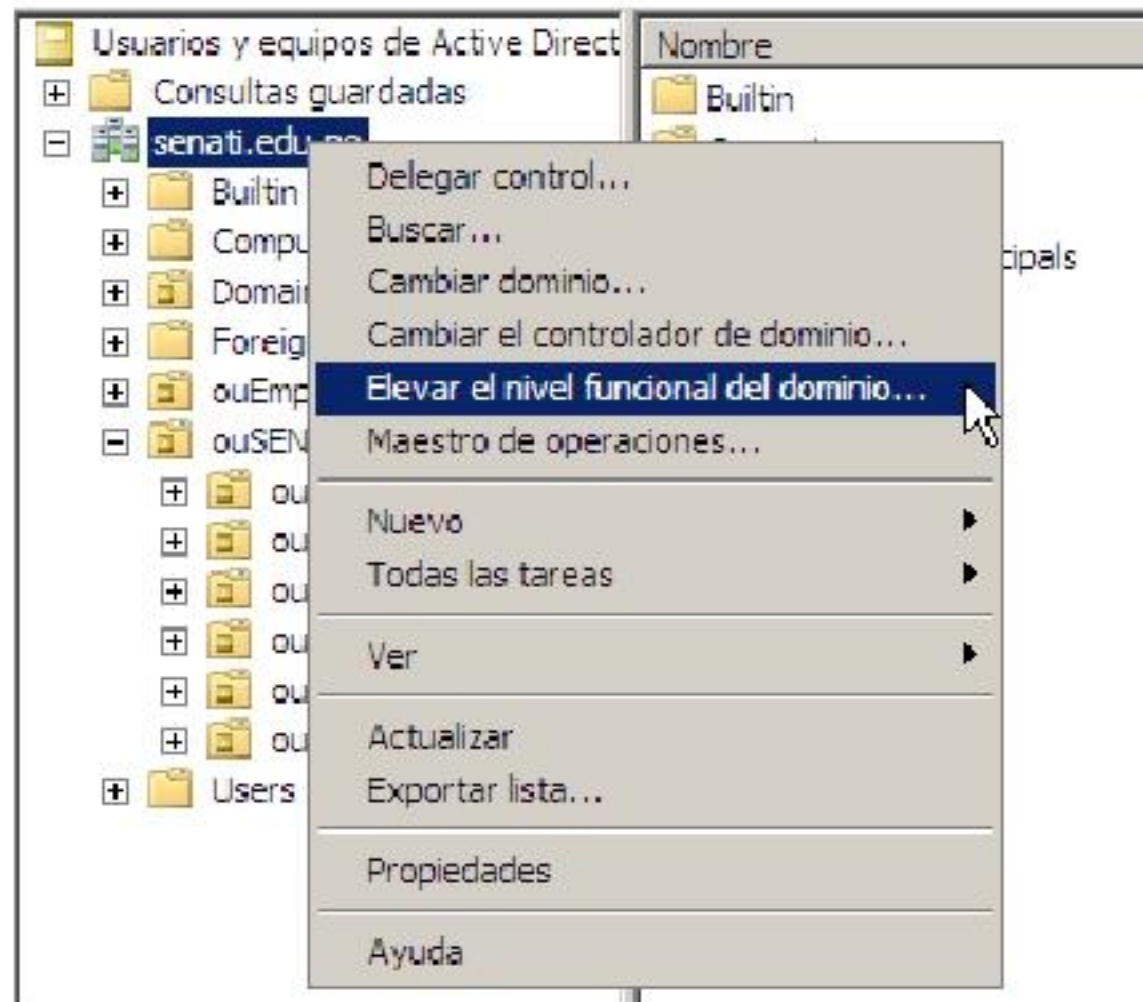
El nivel funcional determina cómo se comportarán los grupos dentro del bosque y a la vez determina qué clase de características estarán disponibles, como por ejemplo la capacidad de unir bosques.

Si el nivel funcional del dominio se encuentra definido como nativo de Windows 2000 o superior, el dominio contiene una jerarquía de unidades organizativas y la administración se delega a los administradores de cada unidad organizativa, puede que sea más eficaz anidar los grupos con ámbito Global. Por ejemplo, si OU1

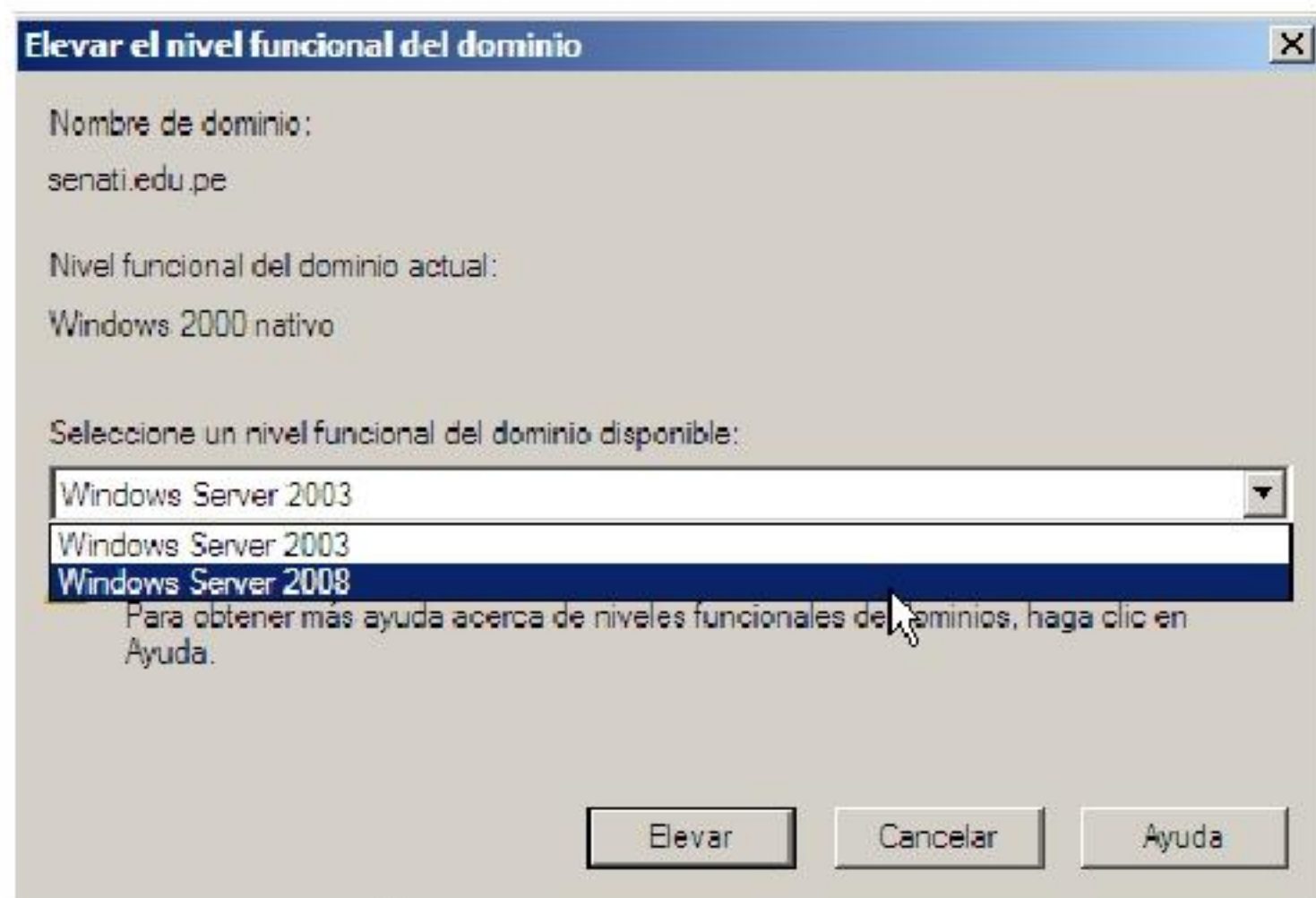
contiene a OU2 y OU3, un grupo con ámbito Global en OU1 puede tener como miembros a los grupos con ámbito Global en OU2 y OU3. En OU1, el administrador puede agregar o quitar miembros de grupo de OU1 y los administradores de OU2 y OU3 pueden agregar o quitar miembros de grupo para las cuentas de sus propias OU sin tener derechos administrativos para el grupo con ámbito Global en OU1.

Cambiar el nivel funcional del dominio

- ❖ En la herramienta Usuarios y equipos de Active Directory, haga clic derecho en el dominio, y seleccione **Elevar el nivel funcional del dominio**.



- ❖ Observará el siguiente cuadro de diálogo, con el cual podrá observar el nivel funcional actual, y además, cambiar a un nivel superior.





Planificación de estrategias de grupo

En Active Directory, se crearán un gran número de grupos de distribución y seguridad. Las siguientes convenciones de nomenclatura pueden ayudar a administrar estos grupos. Las organizaciones establecen sus propias convenciones de nomenclatura para los grupos de distribución y de seguridad.

Un nombre de grupo debería identificar su ámbito, tipo, la finalidad de su creación y los permisos que puede tener.

Determinación de los nombres de grupo

Grupos de Seguridad

Tenga en cuenta los siguientes puntos al definir una convención de nomenclatura para los grupos de seguridad:

Ámbito de los grupos de seguridad

Aunque el tipo y ámbito de grupo se muestra como tipo de grupo en Usuarios y equipos de Active Directory, las organizaciones suelen incorporar el ámbito en la convención de nomenclatura del nombre de grupo.

Por ejemplo, para identificar el ámbito de los grupos de seguridad, Northwind Traders añade una letra al principio del nombre de grupo:

- ❖ G IT Admins

G para grupos globales

- ❖ U All IT Admins

U para grupos universales

- ❖ DL IT Admins Full Control

DL para grupos locales de dominio

Poseción del grupo de seguridad

El nombre de un grupo de seguridad de dominio, ya sea universal, global o local de dominio, debe identificar de forma clara al propietario del grupo e incluir el nombre del departamento o equipo al que pertenece.

A continuación, se muestra un ejemplo de convención de nomenclatura que podría utilizar Northwind Traders para identificar al propietario del grupo:

- ❖ G Marketing Managers
- ❖ DL IT Admins Full Control

Nombre de dominio

El nombre de dominio o su abreviatura se coloca al principio del nombre de grupo a petición del cliente. Por ejemplo:

- ❖ G NWTraders Marketing
- ❖ DL S.N.MSFT IT Admins Read

Finalidad del grupo de seguridad

Por último, se puede incluir en el nombre la finalidad empresarial del grupo y los permisos máximos que debería tener el grupo en la red. Esta convención de nomenclatura se suele aplicar a los grupos locales o grupos locales de dominio.

A continuación, se muestra un ejemplo de convención de nomenclatura que podría utilizar Northwind Traders para identificar la finalidad del grupo de seguridad: Northwind Traders utiliza un descriptor para identificar los permisos máximos que debería tener el grupo en la red. Por ejemplo:

- ❖ DL IT London OU Admins
- ❖ DL IT Admins Full Control

Grupos de distribución

Como los grupos de seguridad se utilizan sobre todo para la administración de la red, sólo el personal encargado de esta tarea debe utilizar la convención de nomenclatura. Los usuarios finales utilizan grupos de distribución; por lo tanto, debe interesarles la convención de nomenclatura que sigue.

Al definir una convención de nomenclatura para los grupos de distribución, tenga en cuenta los siguientes puntos:

Nombres de correo electrónico

- ❖ **Longitud.** Utilice un alias corto. Para respetar las normas actuales de datos descendentes, la longitud mínima de este campo es de tres caracteres y la longitud máxima, de ocho.
- ❖ **Palabras ofensivas.** No cree grupos de distribución con palabras que puedan considerarse ofensivas. Si no está seguro, no utilice la palabra.
- ❖ **Permitidos.** Puede utilizar cualquier carácter ASCII. Los únicos caracteres especiales permitidos son el guión (-) y el carácter de subrayado (_).
- ❖ **Designaciones especiales.** No utilice las siguientes combinaciones de caracteres para los grupos de distribución:
 - ◆ Un carácter de subrayado (_) al principio del nombre de grupo del alias.
 - ◆ Un nombre o una combinación de nombre y apellidos que pueda confundirse fácilmente con un nombre de cuenta de usuario.

Nombres para mostrar

- ❖ **Alias de usuario.** Con el fin de estandarizar los nombres, no incluya un alias como parte del nombre para mostrar (por ejemplo, Informes directos de Sfeli). Incluya el nombre completo (por ejemplo, Informes directos de Susana Félix).
- ❖ **Palabras ofensivas.** No cree grupos de distribución con palabras que puedan considerarse ofensivas.
- ❖ **Discusiones sociales.** No debería permitirse la utilización de grupos de distribución para discusiones sociales, porque el área de carpetas públicas es un medio más eficaz para transmitir y almacenar un gran número de comunicaciones relacionadas con discusiones sociales. Ya que un mensaje puede ser visto por varios usuarios, se minimiza el tráfico de red y el almacenamiento de datos si se utilizan las carpetas públicas en lugar de los grupos de distribución.
- ❖ **Longitud.** La longitud máxima de este campo es de 40 caracteres. Se aceptan abreviaturas, siempre que su significado no sea confuso.
- ❖ **Estilo.** No ponga en mayúsculas toda la descripción, pero sí la primera letra del nombre para mostrar. Utilice ortografía y puntuación correctas.
- ❖ **Parte superior de la libreta de direcciones.** No utilice la palabra Un/a, números, caracteres especiales (sobre todo, comillas) o un espacio en blanco al inicio de la descripción. Esto hace que aparezca en la parte superior de la libreta de direcciones. La libreta de direcciones debería comenzar por nombres de usuario individuales que empiecen por A.



- ❖ **Caracteres especiales.** Las barras diagonales (/) se aceptan en los nombres para mostrar, pero no al inicio de los nombres de servidor. No utilice más de un apóstrofe (') y ninguno de los siguientes caracteres especiales: " * @ # \$ % | [] ; < > =

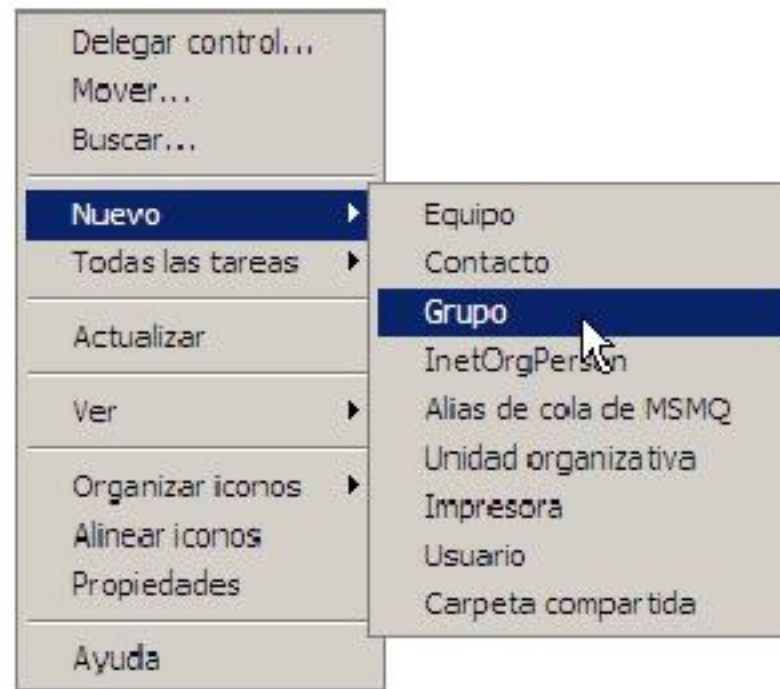
Posesión

Un único grupo de distribución puede tener un máximo de cinco copropietarios.

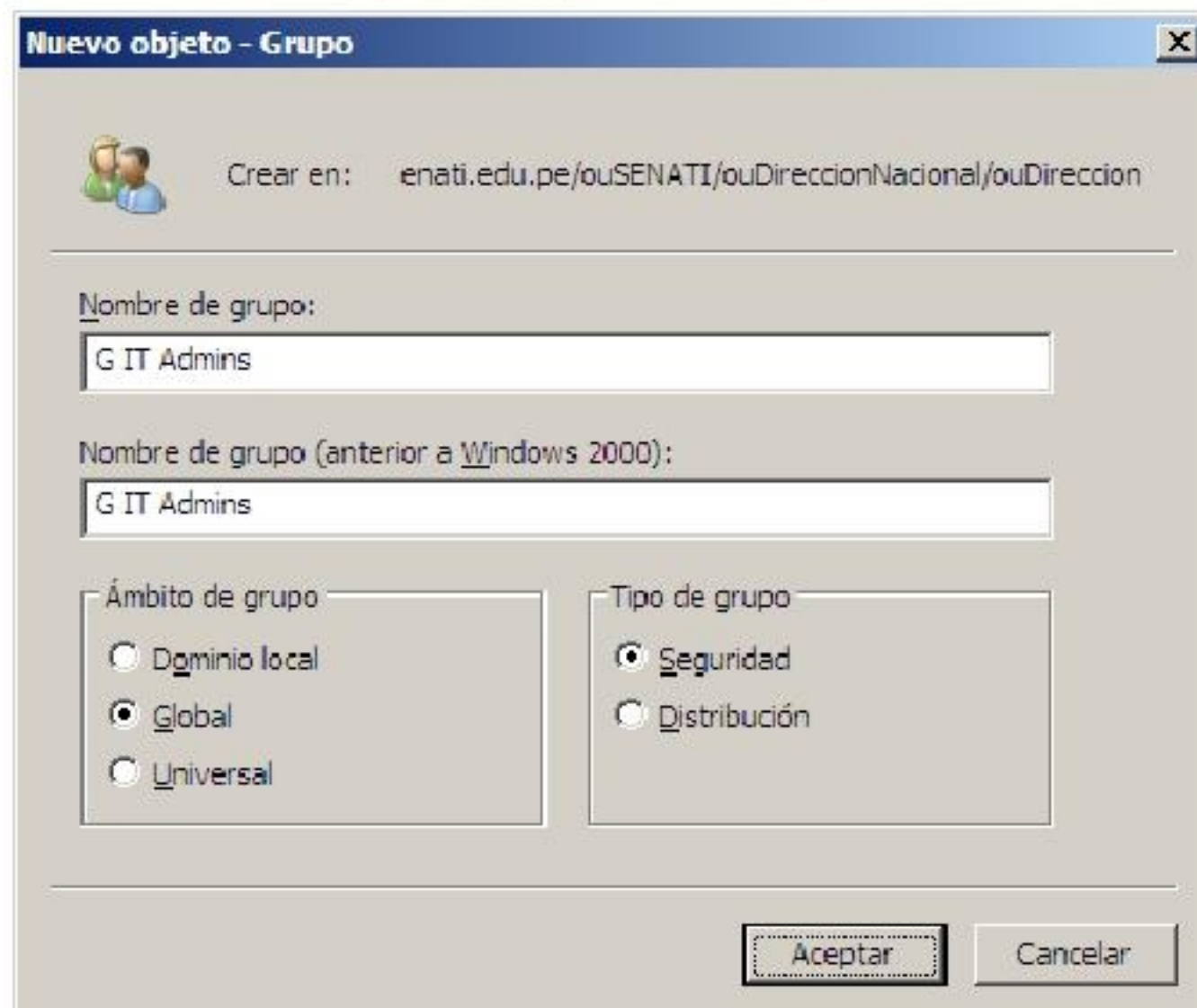
Implementación de Grupos

Creacion de grupos

1. Haga clic derecho en una unidad organizativa o en una zona libre del área de trabajo.
2. Luego señale **Nuevo** y haga clic en **Grupo**.



3. Escriba el nombre del grupo y haga clic en **Aceptar**.

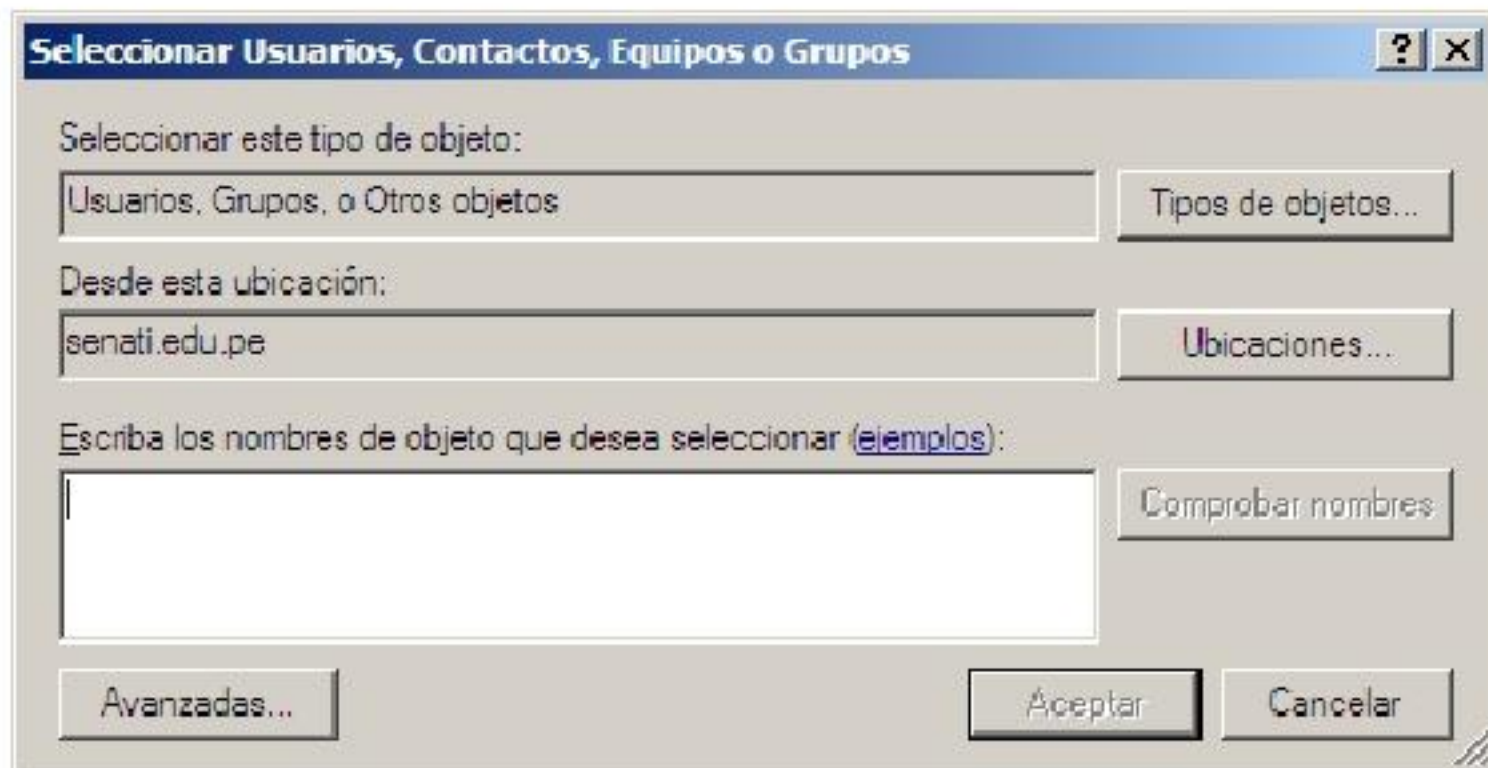


Puede realizar otros tipos de acción sobre un grupo, tales como:

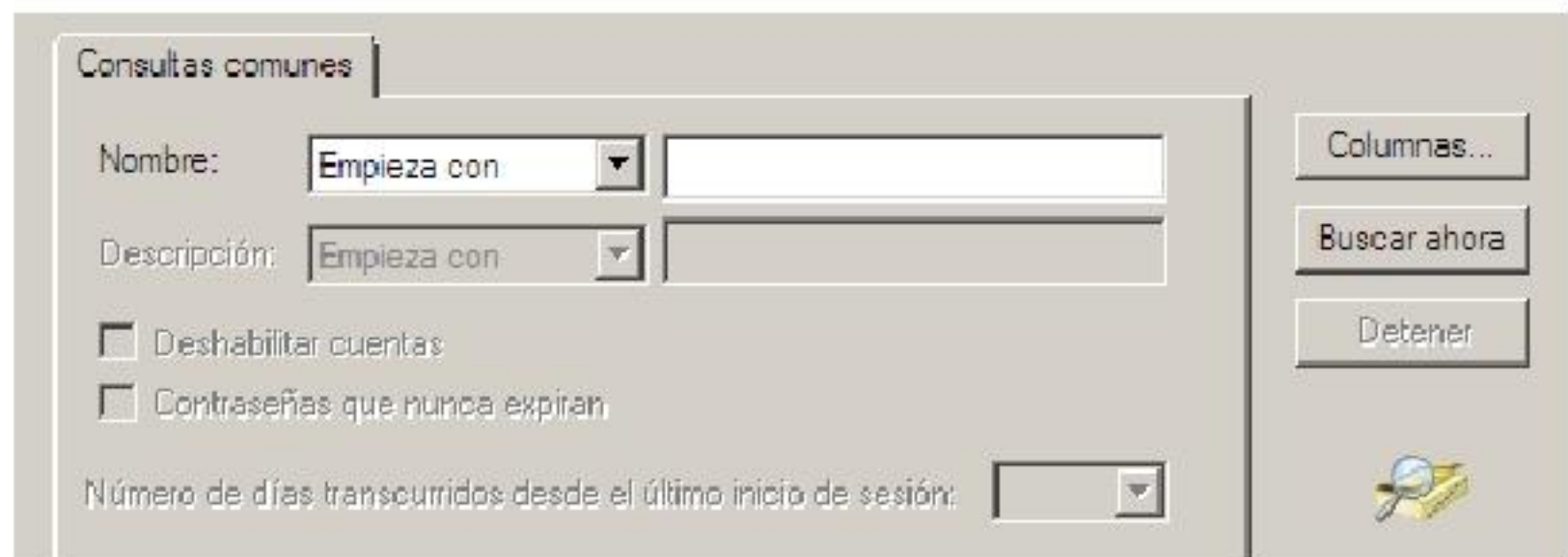
1. Eliminación de grupos.
2. Adición de usuarios a un grupo. (Describiremos este proceso)
 - a. Haga clic derecho en el grupo.
 - b. Haga clic en **Agregar a un grupo**.
 - c. Seleccione la ficha **Miembros**.



- d. Se mostrará el siguiente cuadro de diálogo, haga clic en el botón **Avanzadas....**

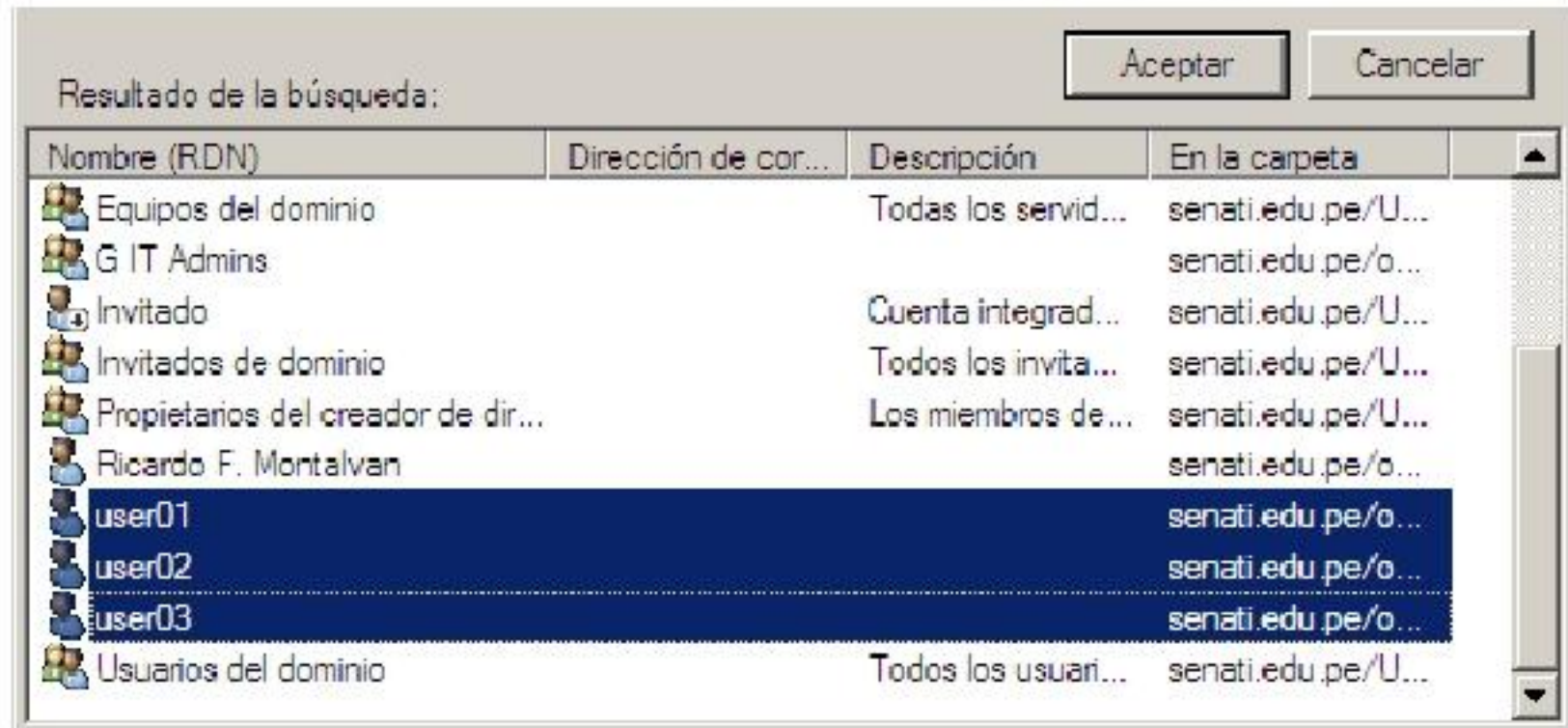


- e. En el cuadro de diálogo siguiente, si desea puede escribir el nombre de usuario que busca o en todo caso haga clic en el botón **Buscar ahora**.

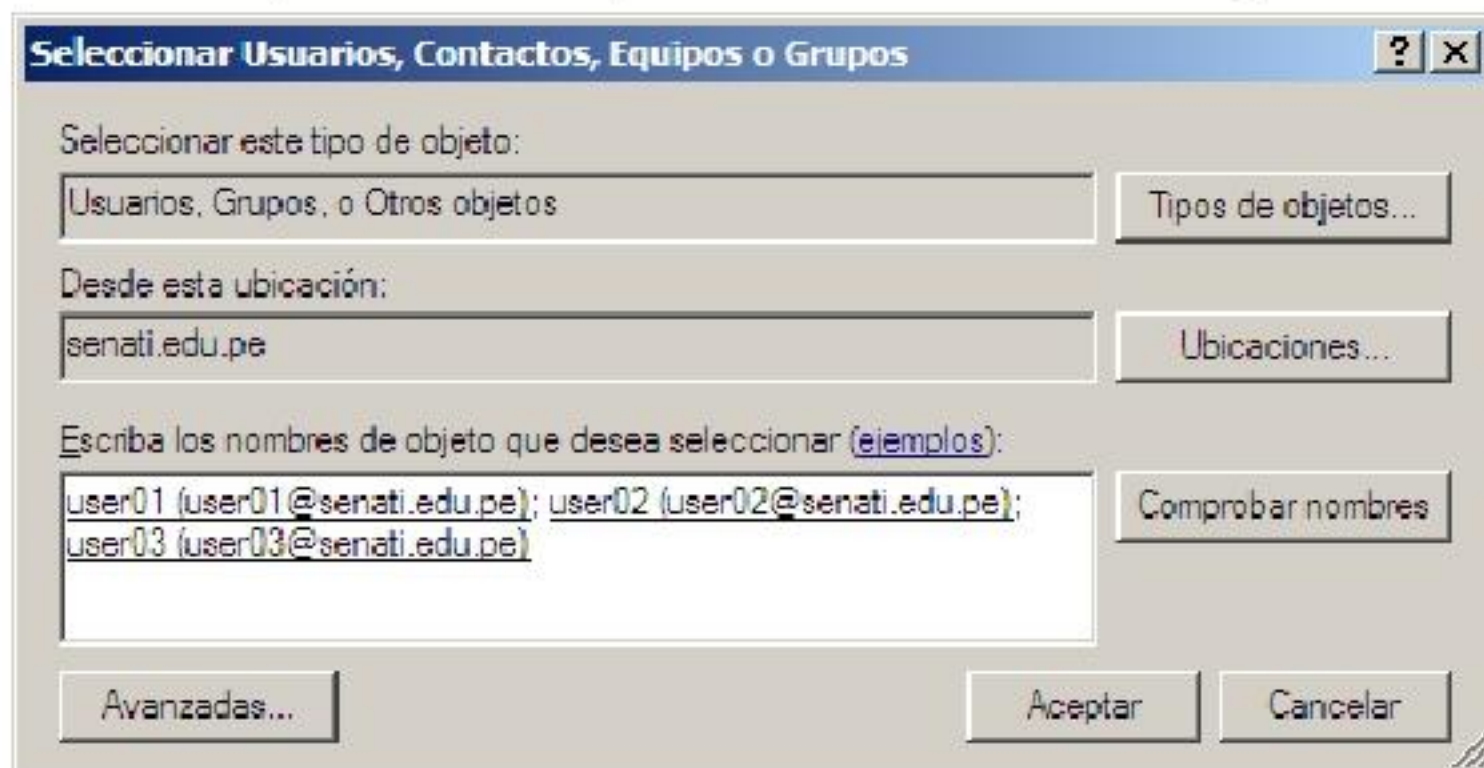




f. Seleccione los usuarios que necesita agregar y haga clic en Aceptar.



g. Aparecerán los usuarios seleccionados y comprobados. En esta ventana también puede escribir el nombre de usuario y utilizar el botón Comprobar nombres para verificar su existencia. Haga clic en Aceptar.



h. La lista se agregará a las propiedades del grupo. Haga clic en Aceptar.



Actividad 1

Crear grupos mediante Usuarios y equipos de Active Directory

1. Cree los siguientes grupos globales en la unidad organizativa Locations/NombreEquipo/Grupos:
 - a. G NombreEquipo Accounting Managers
 - b. G NombreEquipo Accounting Personnel
2. Cree los siguientes grupos locales de dominio en la unidad organizativa Locations/NombreEquipo/Grupos:
 - a. DL NombreEquipo Accounting Managers Full Control
 - b. DL NombreEquipo Accounting Managers Read
 - c. DL NombreEquipo Accounting Personnel Full Control
 - d. DL NombreEquipo Accounting Personnel Read

Ejercicio Grupal Práctico (fórmense grupos de 3 personas para analizar la solución)

Tomando en cuenta el ejercicio práctico desarrollado en el capítulo anterior, considere la siguiente configuración existente y a partir de ellos cree los Grupos pertinentes, respetando los patrones y normas estudiados en el presente capítulo.

1. Los siguientes usuarios ya deben existir en su empresa (Sucursal Principal).
 - a. Jorge Tafur (Gerente General)
 - b. Miguel Millano (Sub Gerente)
 - c. Miguel Quispe (Gerente Técnico)
 - d. Margot Donaire (Asistente Administrativo de la Gerencia técnica)
 - e. Frank Molina (Supervisor Area 1 Turno mañana)
 - f. Jorge Muñoz (Supervisor Area 2 Turno mañana)
 - g. Victor Mimbela (Supervisor Area 3 Turno mañana)
 - h. Marcos Torres (Supervisor Area 1 Turno noche)
 - i. Francisco Dominguez (Supervisor Area 2 Turno noche)
 - j. Richard Morris (Supervisor Area 3 Turno noche)
 - k. Manuel Pacora (Contador)
 - l. Susana Frey (Asistente administrativo de Contabilidad)
 - m. Jared Yafac (Gerente de RRHH)
 - n. Viviana Martinoti (Asistente administrativo de RRHH)
 - o. Lizeth Coronado (Gerente de Finanzas)
 - p. Mark Romero (Asistente administrativo de Finanzas)
 - q. Desire More (Gerente de Marketing)
 - r. Raúl Thomas (Asistente administrativo de Marketing)
 - s. Mónica Suarez (Promotora de Ventas)
 - t. Vanesa Farfan (Promotora de Ventas)
 - u. Ivan Farías (Promotor de Ventas)
 - v. Martha Molina (Promotor de Ventas)
 - w. Una cuenta especial para todos los obreros.
2. Se necesitará futuramente configurar diferentes permisos y derechos en carpetas compartidas, impresoras, directivas y otros, por lo que se debe crear grupos tomando en cuenta (Se deja a criterio de los integrantes del grupo)
 - a. Crecimiento de la empresa a diferentes sucursales a nivel nacional, con la consecuente adición de servidores y controladores de dominio.
 - b. Carpetas compartidas que de acuerdo al grupo que representa, por ejemplo Gerentes necesitarán acceso a los diferentes carpetas de sus áreas con nivel de control total, mientras que otros recursos pueden requerir sólo lectura. De la misma manera, los supervisores quizá necesiten acceso de sólo lectura a todos los recursos de su área.



Preguntas de Repaso

1. Investigación:
 - a. Qué proceso se realiza para cambiar el ámbito de un grupo.
2. ¿Cuál es la diferencia entre los grupos: Dominio Local, Global y Universal?
3. ¿Puede un grupo Universal contener a grupos de Dominio Local? ¿Por qué?
4. ¿Puede un grupo Universal contener a grupos Globales? ¿Por qué?
5. ¿Puede un grupo Universal contener a grupos Universales? ¿Por qué?
6. ¿Puede un grupo Global contener a grupos de Dominio Local? ¿Por qué?
7. ¿Puede un grupo Global contener a grupos Globales? ¿Por qué?
8. ¿Puede un usuario pertenecer a varios grupos?



Gestión de recursos compartidos

En este capítulo trataremos:

- Aprenderá a compartir una carpeta
- Aprenderá a establecer permisos a una carpeta compartida
- Identificará los recursos compartidos administrativos

Introducción:

Sin duda una de las tareas más utilizadas en la administración de red es el compartir recursos. Cómo se comparten los recursos en una red, de tal manera que solo las personas pertinentes tengan acceso. De eso tratará el siguiente capítulo.



Aspectos fundamentales del uso compartido de archivos

Puede compartir archivos y carpetas de diferentes maneras. La manera más habitual de compartir archivos en Windows es compartirlos directamente desde el equipo. Windows proporciona dos métodos para compartir archivos de esta manera: puede compartir archivos desde cualquier carpeta del equipo o desde la carpeta pública. El método que use depende de si desea almacenar las carpetas compartidas, con quién desea compartirlas y cuánto control desea tener sobre los archivos. Cualquier método le permite compartir archivos o carpetas con alguien que use el equipo u otro equipo en la misma red. Si busca maneras adicionales de compartir archivos, en este artículo también se indican otros métodos que puede utilizar.

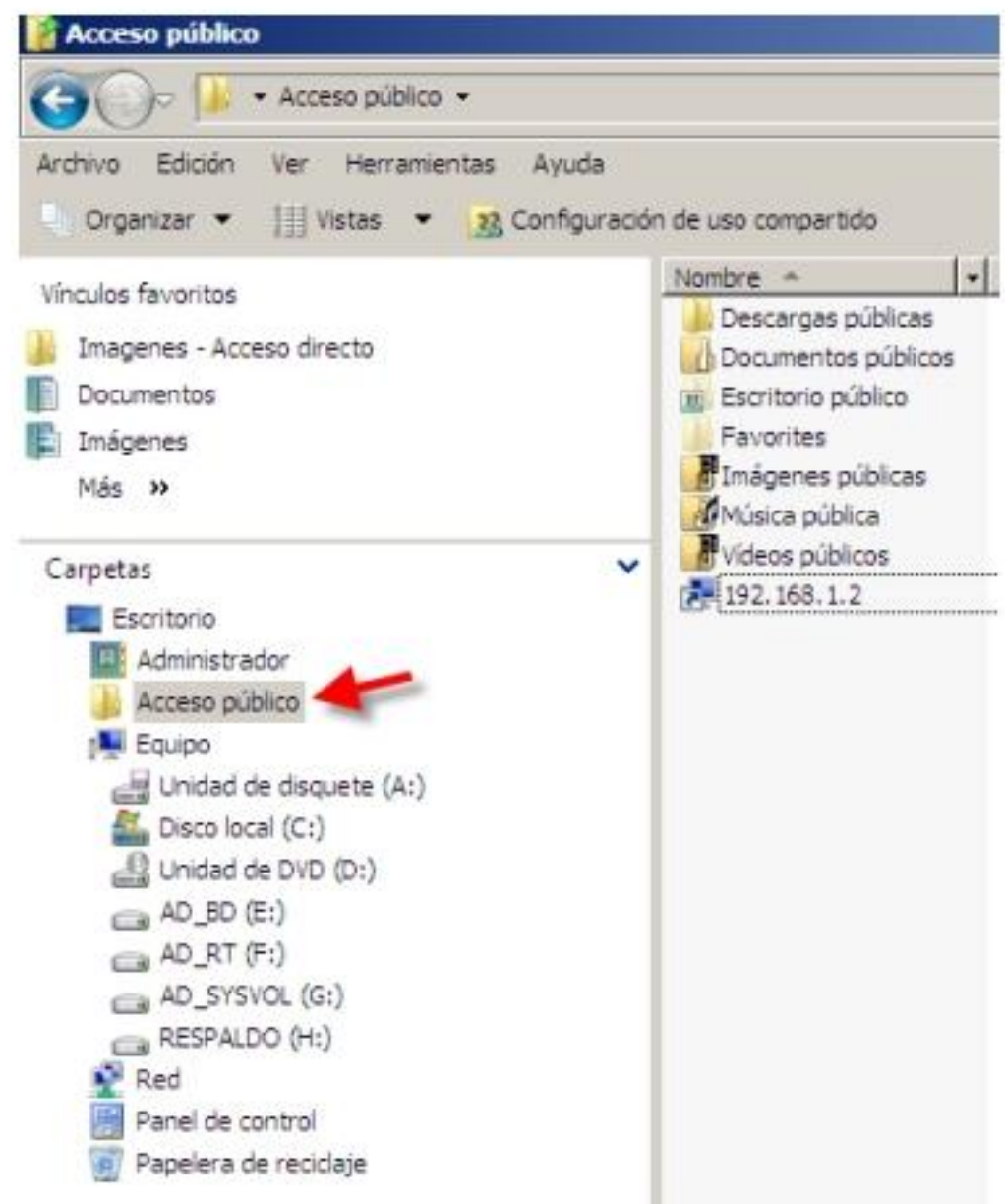
Compartir archivos desde cualquier carpeta del equipo

Con este método de compartir archivos, puede decidir quién podrá realizar cambios a los archivos que comparte y qué tipo de cambios (de haber alguno) pueden realizar en los mismos. Puede hacerlo estableciendo permisos de uso compartido. Los permisos de uso compartido se pueden conceder a un individuo o a un grupo de usuarios de la misma red. Por ejemplo, puede permitir a algunas personas ver únicamente los archivos compartidos y a otras verlos y cambiarlos. Las personas con las que comparte podrán ver únicamente dichas carpetas que ha compartido con ellas.

También puede utilizar este método de compartir como una manera de obtener acceso a los archivos compartidos cuando utilice otro equipo, puesto que cualquier archivo que comparte con otras personas también está visible para usted desde otro equipo.

Compartir archivos desde la carpeta pública del equipo

Con este método de compartir, copia o mueve archivos a la carpeta pública y los comparte desde dicha ubicación. Si activa el uso compartido de archivos para la carpeta pública, cualquiera con una cuenta de usuario y una contraseña en el equipo, así como todos en la red, podrán ver todos los archivos de la carpeta pública y sus subcarpetas. No puede limitar a las personas a que sólo vean algunos archivos de la carpeta pública. Sin embargo, puede establecer permisos que limiten a las personas el acceso a la carpeta pública o que les limiten el cambio de archivos o la creación de nuevos.



Qué método de compartición se va a utilizar

Hay varios factores que se deben tener en cuenta a la hora de decidir si desea compartir archivos desde cualquier carpeta o desde la carpeta pública.

Utilice cualquier carpeta para compartir si:

- Prefiere compartir carpetas directamente desde la ubicación en la que están almacenadas (normalmente en las carpetas Documentos, Imágenes o Música) y desea evitar almacenarlas en la carpeta pública.
- Desea poder establecer permisos de uso compartido para individuos en lugar de todos los usuarios de la red, dando a algunas personas un acceso mayor o menor (o ningún acceso en absoluto).
- Comparte muchas imágenes digitales, música u otros archivos grandes que serían incómodos de copiar en una carpeta compartida independiente. Puede que no desee que estos archivos ocupen espacio en dos ubicaciones diferentes del equipo.
- A menudo crea archivos nuevos o actualiza archivos que desea compartir y no desea molestarlos copiándolos en la carpeta pública.

Utilice la carpeta pública para compartir si:

- Prefiere la simplicidad de compartir los archivos y las carpetas desde una ubicación única del equipo.
- Desea poder ver rápidamente todo lo que ha compartido con los demás, con sólo mirar en la carpeta pública.
- Desea que todo lo que está compartiendo se mantenga independiente de sus propias carpetas Documentos, Música e Imágenes.
- Desea establecer permisos de uso compartido para todos los usuarios de la red y no tiene que establecer permisos de uso compartido para individuos.

Otras maneras de compartir archivos

Hay varias maneras diferentes de compartir archivos que no requiere que comparta archivos desde carpetas específicas. También puede compartir archivos empleando:

- Una red de equipo a equipo (ad hoc). Si desea compartir archivos entre dos equipos que no estén ya en la misma red pero que se encuentran en la misma habitación, puede crear una red de equipo a equipo, también conocida como red ad hoc. Una red ad hoc es una conexión temporal entre equipos y dispositivos utilizados para un fin específico, como compartir documentos durante una reunión. Para obtener más información, consulte Configurar una red de equipo a equipo (ad hoc).
- Medios extraíbles. Puede copiar archivos a cualquier clase de medios extraíbles, incluyendo disco duros portátiles, CDs, DVDs y tarjetas de memoria flash. A continuación, puede insertar o conectar dicho medio a otro equipo y copiar los archivos a dicho equipo o dar los medios extraíbles a las personas con las que desea compartir los archivos y dejar que copien los propios archivos. Para obtener más información, consulte Copiar archivos a otro equipo.



- Correo electrónico. Si sólo tiene uno o dos archivos para compartir y no son muy grandes, puede que piense que es sencillo compartirlos adjuntándolos a un mensaje de correo electrónico. Para obtener información acerca de cómo enviar datos adjuntos con Windows Mail, consulte Enviar un dato adjunto en un mensaje de Windows Mail.
- Área de encuentro de Windows. Esta característica de Windows le permite configurar una sesión en la que puede compartir documentos, programas o su escritorio con otros participantes de sesión. Para obtener más información, consulte Área de encuentro de Windows: preguntas más frecuentes
- Programa de uso compartido de archivos compatible con Windows. Hay muchos programas disponibles diseñados para ayudar a las personas a compartir archivos.
- La web. Hay muchos sitios web dedicados a compartir fotografías y otros tipos de archivos.
- Mensajes instantáneos. La mayoría de los programas de mensajería instantánea le permiten compartir archivos con personas mientras está conversando en línea con ellas.

Establecer permisos para Carpetas compartidas

Los permisos de recurso compartido se aplican a los usuarios que se conectan a una carpeta compartida a través de la red. Estos permisos no afectan a los usuarios que inician sesión localmente o mediante Escritorio remoto.

Para establecer permisos para los usuarios que se conectan localmente o mediante Escritorio remoto, utilice las opciones de la ficha Seguridad en lugar de la ficha Permisos de los recursos compartidos. Se establecerán permisos en el nivel del sistema de archivos NTFS. Si se establecen tanto permisos de recurso compartido como permisos de sistema de archivos para una carpeta compartida, se aplicarán los permisos más restrictivos al conectarse a la carpeta compartida.

Por ejemplo, para conceder a los usuarios de un dominio acceso de lectura a una carpeta compartida, en la ficha Permisos de los recursos compartidos, establezca permisos a Control total para el grupo Todos. En la ficha Seguridad, especifique un acceso más restrictivo estableciendo permisos de acceso de lectura para el grupo Usuarios del dominio. El resultado es que un usuario que es miembro del grupo Usuarios del dominio cuenta con acceso de sólo lectura a la carpeta compartida, tanto si el usuario se conecta a través de un recurso compartido de red, como si lo hace a través de Escritorio remoto o si inicia sesión localmente.

Puede establecer permisos de nivel de sistema de archivos en la línea de comandos utilizando la herramienta de sistema operativo Cacs.exe. Esta herramienta sólo se ejecuta en un volumen NTFS.

Establecer permisos en carpetas compartidas

- Mediante la interfaz de Windows
- Mediante una línea de comandos

Para establecer permisos en una carpeta compartida mediante la interfaz de Windows

1. Abra Administración de equipos. Haga clic en Inicio y Panel de control y haga doble clic en Herramientas administrativas, y, a continuación, haga clic en Administración de equipos.
2. Si aparece el cuadro de diálogo Control de cuenta de usuario, confirme que la acción que muestra es la que desea y, a continuación, haga clic en Continuar.
3. En el árbol de la consola, haga clic en Herramientas del sistema, haga clic en Carpetas compartidas y, a continuación, haga clic en Recursos compartidos.
4. En el panel de detalles, haga clic con el botón secundario en la carpeta compartida y, a continuación, haga clic en Propiedades.
5. En la ficha Permisos de los recursos compartidos, establezca los permisos que desee:
 - a. Para asignar permisos a un usuario o grupo a una carpeta compartida, haga clic en Agregar. En el cuadro de diálogo Seleccionar usuarios, equipos o grupos, busque o escriba el nombre del usuario o grupo y, a continuación, haga clic en Aceptar.
 - b. Para revocar el acceso a una carpeta compartida, haga clic en Quitar.
 - c. Para establecer permisos individuales para el usuario o grupo, en Permisos de grupos o usuarios, seleccione Permitir o Denegar.
6. Para establecer permisos de archivos y carpetas que se apliquen a los usuarios que inicien sesión localmente o mediante Terminal Services, haga clic en la ficha Seguridad y establezca los permisos adecuados.

Para especificar permisos de archivos para un usuario mediante una línea de comandos

1. Para abrir la ventana elevada del símbolo del sistema, haga clic en Inicio, seleccione Todos los programas, Accesorios, haga clic con el botón secundario en Símbolo del sistema y, a continuación, haga clic en Ejecutar como administrador.
2. Si aparece el cuadro de diálogo Control de cuenta de usuario, confirme que la acción que muestra es la que desea y, a continuación, haga clic en Continuar.
3. Para especificar permisos individuales para un usuario o grupo, escriba:

```
cacls /G <usuario:permiso>
```

Por ejemplo, para especificar permisos de escritura para un usuario con el nombre de usuario Pablo en un archivo denominado 002.jpg, escriba:

```
cacls 002.jpg /G Pablo:w
```

4. Para revocar el acceso a la carpeta compartida, escriba:

```
cacls /R <usuario>
```

Por ejemplo, para revocar el acceso a la carpeta compartida para un usuario con el nombre de usuario Pablo, escriba:

```
Cacls/R Pablo
```




Valor	Descripción
cacls	Muestra o modifica las listas de control de acceso (ACL) de los archivos.
/R	Revoca los derechos de acceso del usuario especificado
/G	Concede derechos de acceso al usuario especificado
<user>	Usuario o grupo cuyos derechos de acceso están estableciéndose.
<permission>	Permiso que se concede al usuario. Puede ser uno de los siguientes: N (Ninguno) W (Escribir) C (Cambiar) F (Control total)

Administración de permisos para carpetas compartidas

Los permisos en un recurso compartido, como una carpeta o volumen, vienen determinados por los permisos NTFS locales de dicho recurso, así como por el protocolo usado para obtener acceso al recurso compartido:

- Protocolo SMB (bloque de mensajes del servidor)

El control de acceso basado en SMB (para sistemas de archivos basados en Windows) se implementa mediante la concesión de permisos a usuarios individuales y grupos.

- Protocolo NFS (Network File System)

El control de acceso basado en NFS (para sistemas de archivos basados en UNIX) se implementa mediante la concesión de permisos a equipos cliente y grupos específicos, mediante el uso de nombres de red.

Los permisos de acceso final a un recurso compartido se determinan teniendo en cuenta los permisos NTFS y los permisos de protocolo compartido, y aplicando después los permisos más restrictivos.

Puede configurar permisos para un recurso compartido durante la creación de una nueva carpeta o volumen compartido con el Asistente para aprovisionar carpetas compartidas o seleccionando un recurso compartido existente y haciendo clic en Propiedades en el panel Acciones.

Permisos NTFS

Puede configurar los permisos NTFS locales para una carpeta o volumen compartido mediante Administración de almacenamiento y recursos compartidos, de las formas que se indican a continuación:

- Nuevos recursos compartidos. En el Asistente para aprovisionar carpetas compartidas, antes de seleccionar un protocolo de uso compartido de red, puede modificar los permisos NTFS para la carpeta o volumen que va a compartir. Estos permisos NTFS se aplicarán tanto de forma local como al obtener acceso al recurso a través de la red. Para modificar los permisos NTFS, en la página Permisos NTFS, seleccione Sí, cambiar los permisos NTFS y, a continuación, haga clic en Editar permisos.
- Recursos compartidos existentes. Puede modificar los permisos NTFS de una de las carpetas o volúmenes compartidos de los que aparecen en la ficha Recursos compartidos. Para modificar los permisos NTFS, seleccione la carpeta o volumen; en el panel Acciones, haga clic en Propiedades y, en la ficha Permisos, haga clic en Permisos NTFS.

Permisos SMB

El control de acceso basado en SMB de un recurso compartido se determina a través de dos conjuntos de permisos: Permisos NTFS y permisos de recurso compartido. Normalmente, los permisos de recurso compartido sólo se usan para el control de acceso en equipos que no usan el sistema de archivos NTFS.

Los permisos NTFS y los permisos de recurso compartido son independientes en el sentido de que ninguno afecta al otro, y el más restrictivo de los dos será el que se aplique al recurso compartido.

Si usa Administración de almacenamiento y recursos compartidos, puede especificar permisos compartidos para los recursos compartidos basados en SMB de las siguientes formas:

- ❖ Nuevos recursos compartidos. En el Asistente aprovisionar carpetas compartidas, si selecciona SMB como protocolo de uso compartido, puede especificar los siguientes permisos de acceso basados en SMB en la página Permisos SMB:
 - ◆ Todos los usuarios y grupos sólo tienen acceso de lectura. El permiso resultante será el permiso Lectura para el grupo Todos.
 - ◆ Los administradores tienen Control total; todos los otros usuarios y grupos sólo tienen acceso de Lectura. El grupo Administradores tendrá el permiso Control total, mientras que al grupo Todos se le concederá el permiso Lectura.
 - ◆ Los administradores tienen Control total; todos los demás usuarios y grupos sólo tienen acceso de lectura y de escritura. El grupo Administradores tendrá el permiso Control total, mientras que al grupo Todos se le concederá tanto el permiso Lectura como el permiso Escritura.
 - ◆ Los usuarios y grupos tienen permisos de los recursos compartidos personalizados. Para usar esta opción, debe especificar todos los grupos y usuarios que vayan a tener acceso compartido, así como los permisos específicos de recursos compartidos (Control total, Cambiar, Lectura) que se concederán o denegarán a cada uno de ellos.



- ❖ Recursos compartidos existentes. Puede modificar los permisos de recurso compartido de una de las carpetas o volúmenes compartidos de los que aparecen en Protocolo: SMB en la ficha Recursos compartidos. Para modificar los permisos de recurso compartido, seleccione la carpeta o volumen; en el panel Acciones, haga clic en Propiedades y, en la ficha Permisos, haga clic en Permisos de los recursos compartidos.

Permisos NFS

El control de acceso basado en NFS de un recurso compartido se determina basándose en los grupos y nombres de red. Para poder usar permisos NFS, primero debe instalar la función Servicios para Network File System (NFS) mediante Administrador del servidor. Después de instalar Servicios para NFS, use NFSAdmin.exe para crear grupos de clientes y para agregar equipos cliente a dichos grupos antes de configurar los permisos de recursos compartidos NFS.

Si usa Administración de almacenamiento y recursos compartidos, podrá especificar permisos compartidos para los recursos compartidos basados en NFS de las siguientes formas:

- ❖ Nuevos recursos compartidos. En el Asistente para aprovisionar carpetas compartidas, si selecciona NFS como protocolo de uso compartido, la página Permisos NFS estará disponible en el asistente. Debe especificar si el acceso lo controlará un equipo cliente (host) específico o un grupo de clientes. Para configurar permisos NFS en un recurso compartido, puede hacer lo siguiente:
 - ◆ Agregar, editar o quitar permisos para grupos de clientes y hosts. El valor predeterminado es acceso de sólo lectura para el grupo TODOS LOS EQUIPOS. Puede agregar cualquier grupo de clientes o host previamente creado (mediante NFSAdmin.exe) y conceder los permisos adecuados a cada uno de ellos (sin acceso, sólo lectura, lectura-escritura).

Además, puede seleccionar la opción Permitir acceso a la raíz para cada grupo de cliente y host; no obstante, no se recomienda ya que supone un riesgo para la seguridad.

- ◆ Especifique si debe permitirse el acceso anónimo al recurso compartido. Esta opción no está habilitada de forma predeterminada por motivos de seguridad. Aunque el acceso anónimo puede resultar de utilidad para solucionar problemas o en entornos de prueba, no es recomendable para uso general.

Para permitir el acceso anónimo, el Asistente para aprovisionar carpetas compartidas modifica los permisos NTFS en la carpeta o volumen con objeto de conceder acceso al grupo de seguridad Todos.

Al habilitar el acceso anónimo, también se habilita la directiva de seguridad Permitir la aplicación de los permisos Todos a los usuarios anónimos, que agrega el principio Inicio de sesión anónimo al grupo de seguridad Todos. De esta forma, los usuarios anónimos pueden desplazarse a través de carpetas a las que, de otro modo, no tendrían acceso al navegar por la ruta de acceso de un objeto de la carpeta

compartida; pero el usuario no puede ver el contenido de las carpetas en las que no tiene permiso de acceso.

- ❖ Recursos compartidos existentes. Puede modificar los permisos NFS de una de las carpetas o volúmenes compartidos de los que aparecen en Protocolo: NFS, en la ficha Recursos compartidos. Para modificar los permisos de recurso compartido, haga clic en la carpeta o volumen; en el panel Acciones, haga clic en Propiedades y, en la ficha Permisos, haga clic en Permisos NFS. Para configurar permisos, puede agregar, editar o quitar permisos para cada grupo de clientes o host individual para el que desee configurar el acceso.

Consideraciones adicionales

- ❖ Conceder a un usuario el permiso NTFS Control total en un recurso compartido permite a ese usuario tomar posesión de la carpeta o volumen, a menos que esté restringido de alguna forma. Tenga especial cuidado al conceder Control total.
- ❖ Si desea administrar el acceso a una carpeta o volumen exclusivamente mediante permisos NTFS, defina los permisos de recurso compartido Control total para Todos. Esto simplifica la administración de los permisos de recursos compartidos, pero los permisos NTFS son más complejos que los permisos de recursos compartidos.
- ❖ Los permisos NTFS influyen sobre el acceso local y remoto. Se aplican con independencia del protocolo. Por el contrario, los permisos de recurso compartido sólo se aplican a recursos de red compartidos. Los permisos de recurso compartido no restringen el acceso de ningún usuario local o usuario de Terminal Server. Por tanto, los permisos de recurso compartido no ofrecen privacidad entre los usuarios de un equipo usado por varios usuarios.
- ❖ De forma predeterminada, el grupo Todos no incluye el grupo Anónimo, por lo que los permisos que se aplican al grupo Todos no afectan al grupo Anónimo.
- ❖ No es posible modificar los permisos de acceso de carpetas o volúmenes que se comparten con fines administrativos, como C\$ y ADMIN\$.
- ❖ Para abrir Administración de almacenamiento y recursos compartidos, haga clic en Inicio, seleccione Herramientas administrativas y, a continuación, haga clic en Administración de almacenamiento y recursos compartidos.

Administración de un recurso compartido existente

Puede usar **Administración de almacenamiento y recursos compartidos** para administrar todas las carpetas y volúmenes compartidos disponibles en el servidor. La ficha Recursos compartidos ofrece una lista de todos los recursos compartidos que pueden administrarse.

También puede ver qué usuarios están obteniendo acceso en estos momentos a una carpeta o archivo del servidor y desconectar a un usuario si es preciso.



Acceso al Administrador

1. Abra el Administrador del Servidor.
2. Encontrará la opción en la siguiente ruta:



3. Visualizará las siguiente fichas: **Recursos compartidos** y **Volúmenes**.

Administración de almacenamiento y recursos compartidos

Recursos compartidos | Volúmenes

10 entradas

Nombre ...	Protocolo	Ruta local	Cuota	Filtrad...
Protocolo: SMB (10 elementos)				
ADMIN\$	SMB	C:\Windows		
C\$	SMB	C:\		
E\$	SMB	E:\		
Empresa	SMB	F:\Empresa		
F\$	SMB	F:\		
G\$	SMB	G:\		
H\$	SMB	H:\		
IPC\$	SMB			
NETLOGON	SMB	G:\Windows\SYSTEM32\sysvol\senati.edu.pe\...		
SYSVOL	SMB	G:\Windows\SYSTEM32\sysvol		

Administración de almacenamiento y recursos compartidos

Recursos compartidos | Volúmenes

6 entradas

Volumen	Capaci...	Espacio li...	% libre	Tipo	Sistem...	Instant...	Indiz...
Tipo: Simple (6 elementos)							
(D:)	0,00 KB	0,00 KB	0%	Simple	Descon...		
(C:)	24,0 GB	12,0 GB	49%	Simple	NTFS		
AD_B...	1,07 GB	1,03 GB	95%	Simple	NTFS		
AD_R...	1,56 GB	1,50 GB	95%	Simple	NTFS		
AD_SY...	2,36 GB	1,82 GB	77%	Simple	NTFS		
RESPA...	24,0 GB	14,2 GB	59%	Simple	NTFS		

Visualización y modificación de las propiedades de una carpeta compartida

Puede usar Administración de almacenamiento y recursos compartidos para ver y modificar las propiedades de una carpeta o volumen compartido, incluidos los permisos NTFS locales y los permisos de acceso de red de dicho recurso compartido.

El mínimo requerido para completar este procedimiento es la pertenencia al grupo Administradores o un grupo equivalente.

Para ver o modificar las propiedades de una carpeta o volumen compartido

1. En la ficha Recursos compartidos, haga clic en la carpeta o volumen compartido de SMB (bloques de mensaje del servidor) o NFS (Network File System) cuyas propiedades desee ver o modificar.
2. En el panel Acciones, haga clic en Propiedades.
3. Modifique la configuración según corresponda y, a continuación, haga clic en Aceptar.

Consideraciones adicionales

- ❖ Para obtener información acerca de los permisos de acceso para los recursos compartidos, consulte Administración de permisos para carpetas compartidas.
- ❖ No es posible modificar los permisos de acceso de carpetas o volúmenes compartidos con fines administrativos, como C\$ y ADMIN\$.
- ❖ Para abrir Administración de almacenamiento y recursos compartidos, haga clic en Inicio, seleccione Herramientas administrativas y, a continuación, haga clic en Administración de almacenamiento y recursos compartidos.

Dejar de compartir un recurso

Puede dejar de compartir una carpeta o un volumen de los que se muestran en la ficha Recursos compartidos de Administración de almacenamiento y recursos compartidos. Si los protocolos SMB (bloque de mensajes del servidor) y NFS (Network File System) comparten el acceso a una carpeta o a un volumen, deberá dejar de compartir dicha carpeta o volumen de forma individual para cada protocolo.

Si deja de compartir una carpeta o volumen en uso, los datos podrían dañarse. Antes de dejar de compartir un recurso, compruebe que no se esté utilizando y que no haya usuarios conectados al mismo. El mínimo requerido para completar estos procedimientos es la pertenencia al grupo Administradores o un grupo equivalente.

Para dejar de compartir una carpeta o un volumen

1. En la ficha Recursos compartidos, haga clic en la carpeta o volumen compartido de SMB o NFS que desee dejar de compartir.
2. En el panel Acciones, haga clic en Detener uso compartido.
3. Cuando se le pida que confirme la acción, revise la advertencia y, si todavía desea continuar, haga clic en Sí.



Consideraciones adicionales

Para abrir Administración de almacenamiento y recursos compartidos, haga clic en Inicio, seleccione Herramientas administrativas y, a continuación, haga clic en Administración de almacenamiento y recursos compartidos.

Crear un acceso directo a una unidad de red (asignar)

Cuando se crea un acceso directo a una carpeta o a un equipo compartido de una red (llamado también asignación de una unidad de red), se puede obtener acceso a él desde Equipo o desde el Explorador de Windows sin tener que buscarlo o escribir su dirección de red.

1. Haga clic para abrir Equipo.
2. Haga clic el menú Herramientas y, a continuación, en Conectar a unidad de red.
3. En la lista Unidad, haga clic en una letra de unidad. Puede seleccionar cualquier letra disponible.
4. En el cuadro Carpeta, escriba la ruta de acceso a la carpeta o equipo, o haga clic en Examinar para buscarlos. Para conectarse cada vez que inicie una sesión en el equipo, seleccione la casilla Conectar de nuevo al iniciar sesión.
5. Haga clic en Finalizar. Ahora el equipo está conectado, o asignado, a la unidad de red.

Accesos directos a ubicaciones de Internet como sitios web o sitios FTP.

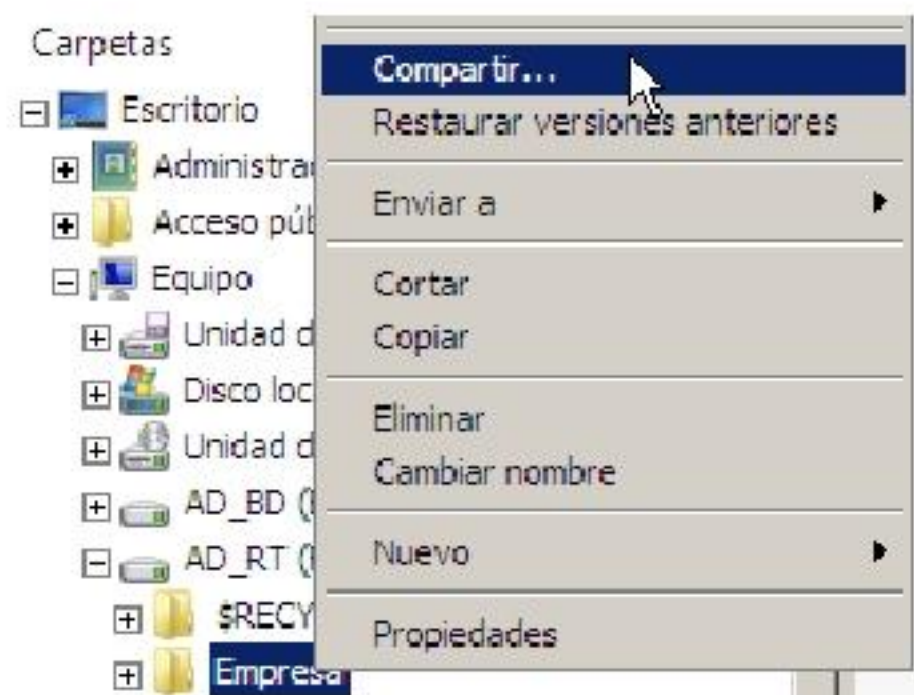
Puede hacerlo del siguiente modo:

1. Haga clic para abrir Equipo.
2. Haga clic con el botón secundario en cualquier área de la carpeta y, a continuación, haga clic en Agregar una ubicación de red.
3. Siga los pasos del asistente para agregar un acceso directo a una ubicación de la red, un sitio web o un sitio FTP.

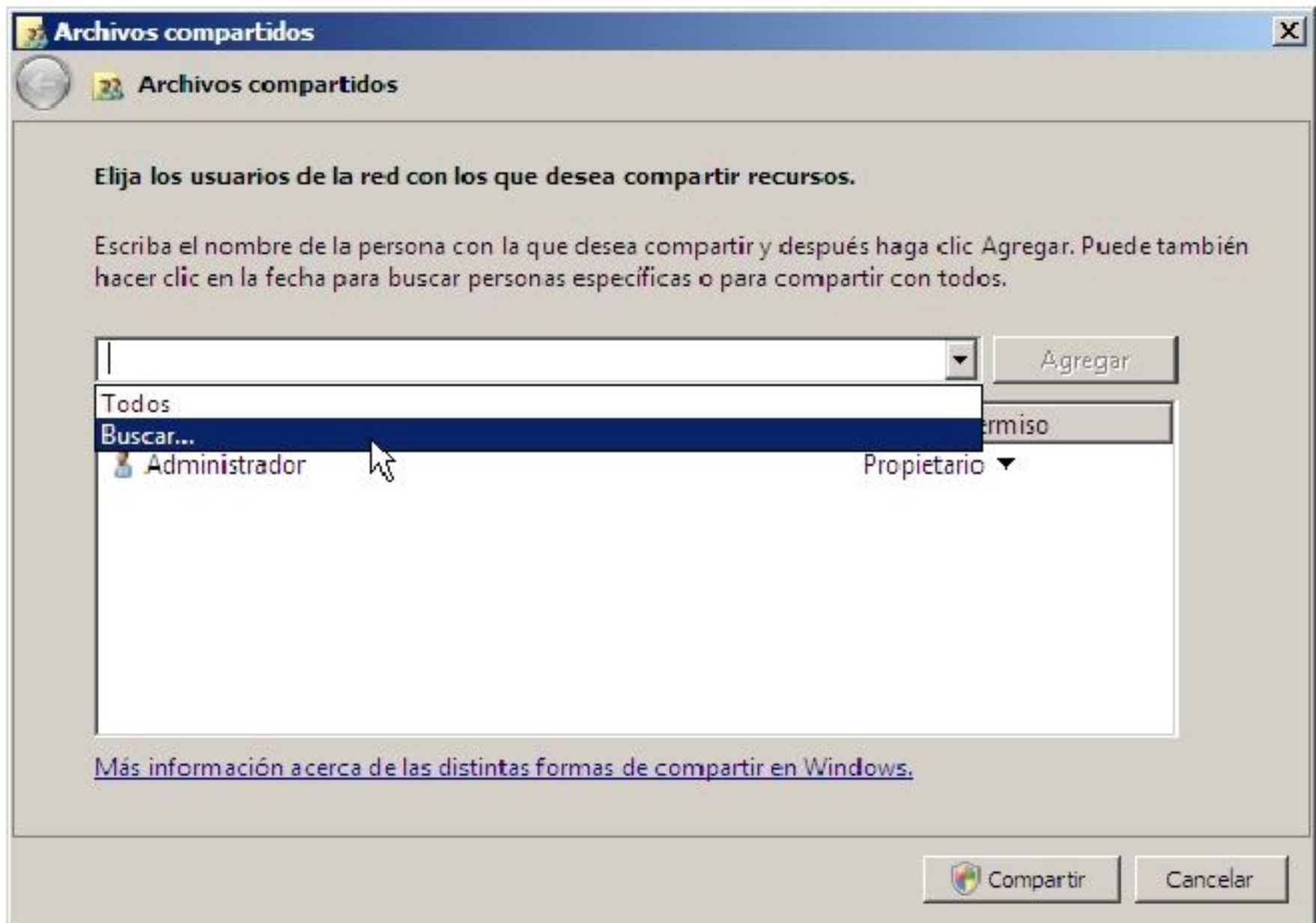
Ubicaciones de red sustituye a Sitios de red en esta versión de Windows.

Compartir carpetas

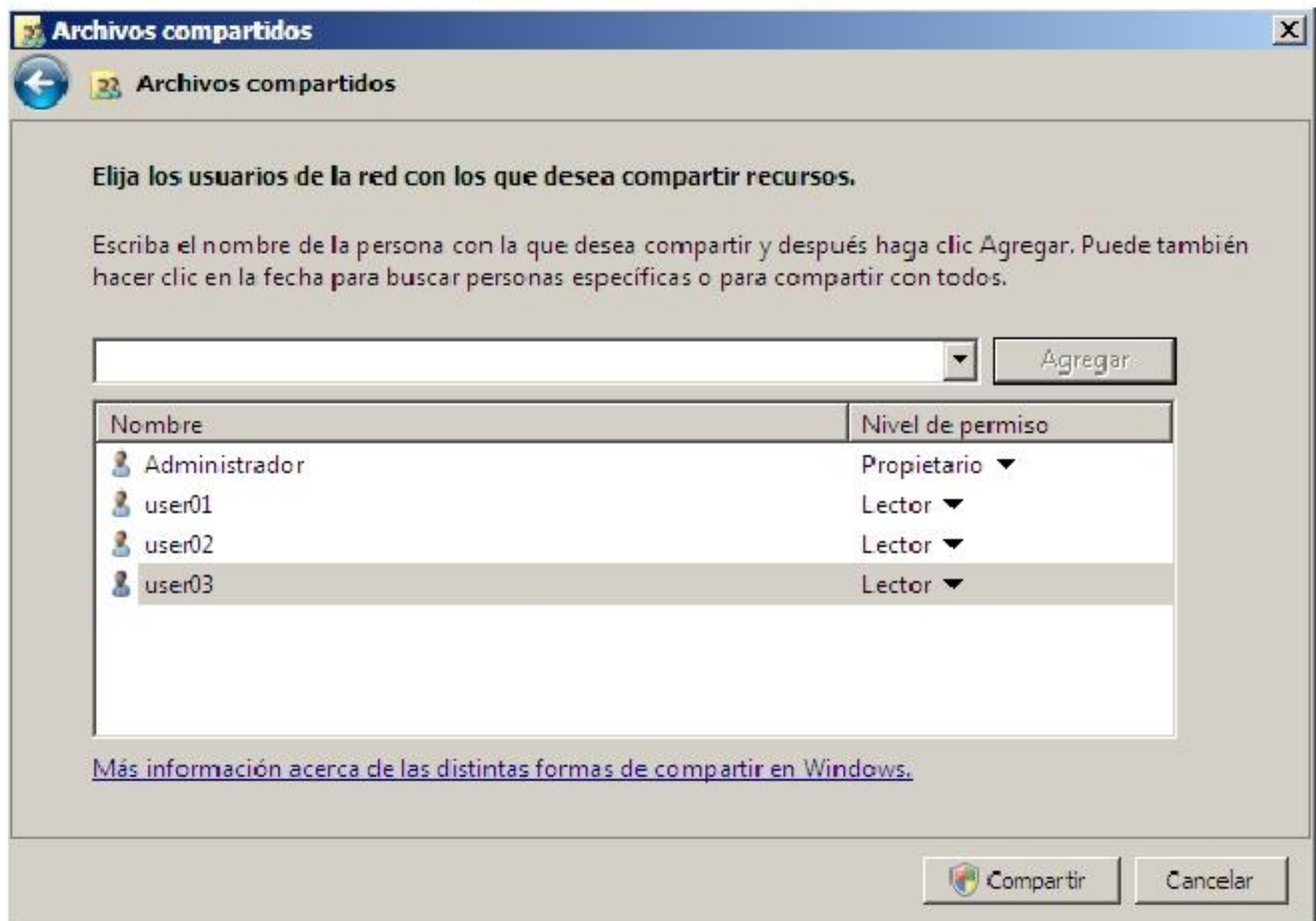
1. Haga clic derecho sobre la carpeta
2. Seleccione Compartir.



3. Observará el siguiente cuadro de diálogo, expanda la lista y seleccione **Buscar** para encontrar usuarios.

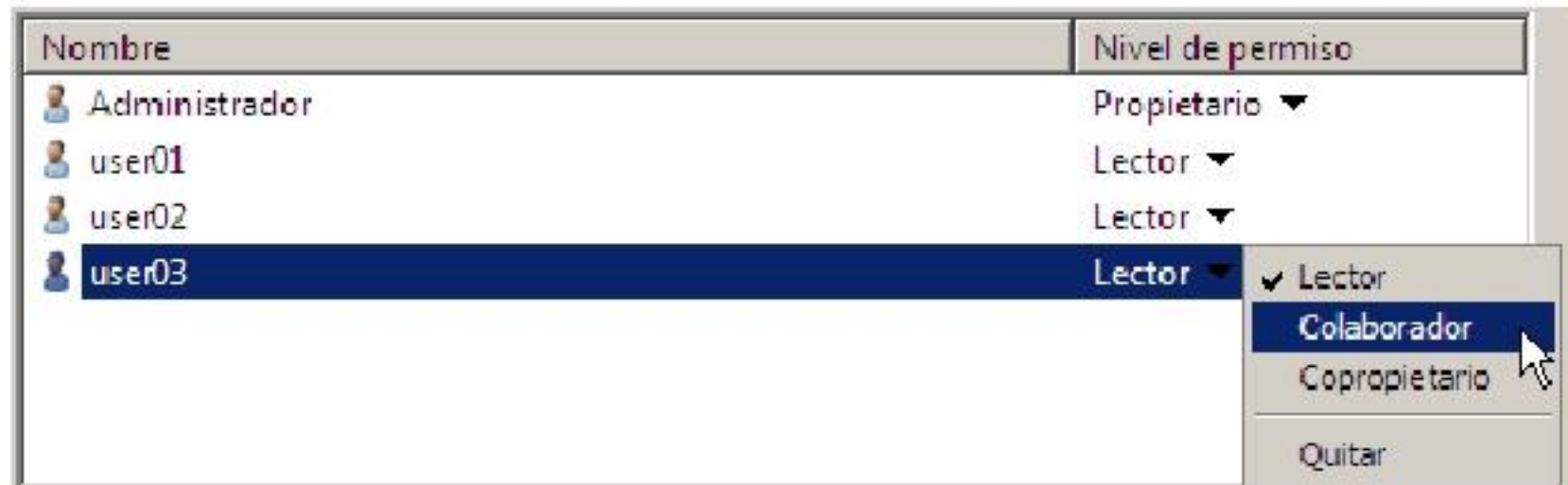


4. Seleccione los usuarios y se mostrarán de la siguiente manera.

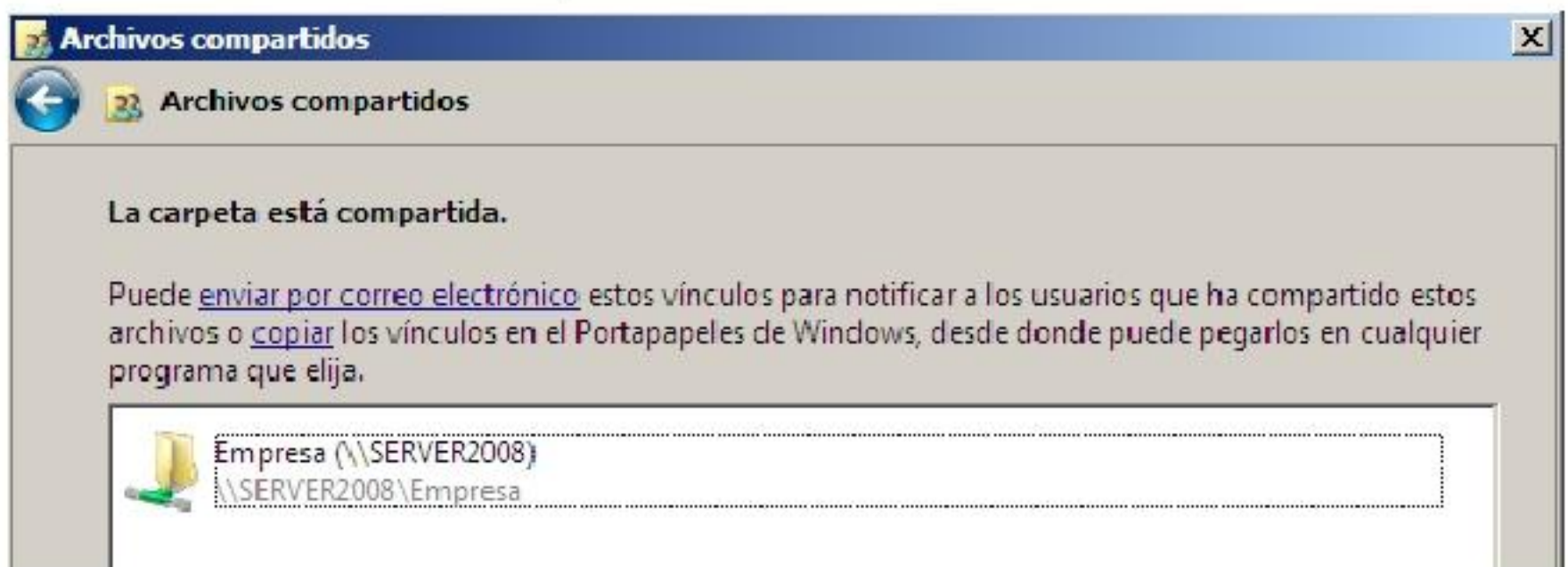




5. Puede cambiar el nivel de permiso entre Lector, Colaborador y Copropietario.



6. Finalmente confirme el proceso haciendo clic en Listo.



7. Se mostrará una carpeta con el siguiente icono.



Preguntas de Repaso

1. Cree un árbol de carpetas y comparta las mismas con diferentes niveles de acceso. Desde equipos cliente inicie sesión con los usuarios creados y que tienen permiso sobre las carpetas, anote las acciones que puede realizar sobre ellos.
2. Para qué sirve la utilidad NFSAdmin.exe
3. Cómo se deshabilita el acceso anónimo a los recursos
4. Cree unidades de red para todas las carpetas que ha compartido
5. Elabore un cuadro comparativo de los permisos NTFS, SMB, NFS



Trabajando con permisos NTFS

En este capítulo trataremos:

- Identificará la herencia de permisos NTFS
- Aprenderá a establecer permisos NTFS
- Aprenderá a determinar los permisos efectivos combinados
- Aprenderá a establecer cuotas de disco

Introducción:

La seguridad se establece a través de los permisos en particiones NTFS. Todos los sistemas operativos para redes tienen una manera de controlar el acceso a través del sistema de archivo y un conjunto de protocolos específicos para esa tarea. El tema es bastante amplio, por eso centraremos la atención en los puntos más críticos y lo demás se desarrollará con trabajos de investigación y trabajos grupales.



Sistema de archivos NTFS

Sistema de archivos para formatear los discos duros de los equipos para que puedan almacenar información. NTFS ofrece varias mejoras en comparación con los sistemas de archivos de tabla de asignación de archivos (FAT) anteriores, como permisos de archivo y carpeta, cifrado y compresión de archivos.

Comparación de los sistemas de archivos NTFS y FAT

Un sistema de archivos es la estructura subyacente que un equipo usa para organizar los datos de un disco duro. Si está instalando un disco duro nuevo, tiene que realizar las particiones y formatearlo empleando un sistema de archivos para poder comenzar a almacenar datos o programas. En Windows, las tres opciones del sistema de archivos que tiene para elegir son NTFS, FAT32 y la anterior y poco usada FAT (también conocida como FAT16).

NTFS

NTFS es el sistema de archivos preferido para esta versión de Windows. Tiene muchos beneficios respecto al sistema de archivos FAT32, entre los que se incluye:

- La capacidad de recuperarse a partir de algunos errores relacionados con el disco automáticamente, lo que FAT32 no puede hacer.
- Compatibilidad mejorada para discos duros más grandes.
- Mejor seguridad porque puede utilizar permisos y cifrado para restringir el acceso a archivos específicos para usuarios aprobados.

FAT32

FAT32, y el menos usado FAT, se usan en versiones anteriores de sistemas operativos de Windows, incluyendo Windows 95, Windows 98 y Windows Millennium Edition. FAT32 no tiene la seguridad que NTFS proporciona, por lo que si tiene una partición FAT32 o volumen en el equipo, cualquier usuario que tenga acceso al equipo puede leer el archivo incluido. FAT32 también tiene limitaciones de tamaño. No puede crear una partición FAT32 mayor que 32GB en esta versión de Windows y no puede almacenar un archivo mayor que 4GB en una partición FAT32.

La razón principal de utilizar FAT32 es que tiene un equipo que a veces ejecutará Windows 95, Windows 98 o Windows Millennium Edition y en otras ocasiones ejecutará esta versión de Windows, conocida como configuración de arranque múltiple. Si éste es el caso, tendrá que instalar el sistema operativo anterior en una partición FAT32 o FAT y asegurarse de que es una partición primaria (una que puede alojar un sistema operativo). Las particiones adicionales a las que tendrá acceso cuando use estas versiones anteriores de Windows también estarán formateadas con FAT32. Estas versiones anteriores de Windows pueden tener acceso a volúmenes o particiones NTFS en una red pero no en el equipo.

Convertir un disco duro o partición al formato NTFS

El sistema de archivos NTFS proporciona un mejor rendimiento y seguridad para los datos de discos duros y particiones o volúmenes que el sistema de archivos FAT usado en alguna versión anterior de Windows. Si tiene una partición que utiliza el sistema de archivos FAT16 o FAT32 anterior, puede convertirlo a NTFS empleando el comando convert. La conversión a NTFS no afecta a los datos de la partición:

- ❖ Después de convertir una partición a NTFS, no puede volver a su conversión anterior. Si desea utilizar el sistema de archivos FAT en la partición de nuevo, tendrá que volver a formatear la partición y esto borrará todos los datos que se encuentren en la misma.
- ❖ Algunas versiones anteriores de Windows no pueden leer datos en particiones NTFS locales. Si tiene que utilizar una versión anterior de Windows para obtener acceso a una partición del equipo, no la convierta.
- ❖ Aunque la posibilidad de que los datos se pierdan o se dañen durante una conversión es mínima, debería realizar una copia de seguridad de todos los datos de la partición antes de comenzar.
- ❖ Cierre los programas abiertos que se ejecutan en la partición o unidad lógica que se van a convertir.
- ❖ Haga clic en el botón Inicio, haga clic en Todos los programas, haga clic en Accesorios, haga clic con el botón secundario en Símbolo del sistema y, a continuación, haga clic en Ejecutar como administrador. Si se le solicita una contraseña de administrador o una confirmación, escriba la contraseña o proporcione la confirmación.
- ❖ En la ventana Símbolo del sistema, escriba `convert letra_unidad: /fs:ntfs`, donde `letra_unidad` es la letra de la unidad que desea convertir y, a continuación, presione ENTRAR. Por ejemplo, `convert E: /fs:ntfs` convertiría la unidad E al formato NTFS.
- ❖ Escriba el nombre del volumen que desea convertir y, a continuación, presione ENTRAR. Para ver los volúmenes disponibles, haga clic en el botón Inicio y, a continuación, en Equipo. Los volúmenes aparecen enumerados en Unidades de disco duro.

Si la partición que está convirtiendo contiene archivos de sistema, que sería el caso si está convirtiendo todo el disco duro, tendrá que reiniciar el equipo para que la conversión tenga efecto. Si recibe un error, trate de eliminar los archivos innecesarios, o realice una copia de seguridad de los archivos en otra ubicación, para liberar espacio en disco.

¿Qué son los permisos?

Los permisos son reglas asociadas a los objetos de un equipo o red, como archivos y carpetas.

Los permisos determinan si se puede obtener acceso a un objeto y lo que se puede hacer con él. Por ejemplo, puede obtener acceso a un documento de una carpeta compartida de la red, pero sólo puede leerlo, no modificarlo.

Los administradores del sistema y los usuarios con cuentas de administrador pueden asignar permisos a usuarios individuales o a grupos.

En la siguiente tabla se muestran los niveles de permisos normalmente disponibles para archivos y carpetas.

Nivel de permiso	Descripción
Control total	Los usuarios pueden ver el contenido de un archivo o carpeta, cambiar los archivos y carpetas existentes, crear nuevos archivos y carpetas, y ejecutar programas en la carpeta.
Modificar	Los usuarios pueden cambiar los archivos y carpetas existentes, pero no pueden crear nuevos archivos y carpetas.



Leer y ejecutar	Los usuarios pueden ver el contenido de los archivos y carpetas existentes, y pueden ejecutar programas en la carpeta.
Leer	Los usuarios pueden ver el contenido de una carpeta y abrir archivos y carpetas.
Escribir	Los usuarios pueden crear nuevos archivos y carpetas, y realizar cambios en los archivos y carpetas existentes.

Lo que se debe saber antes de aplicar permisos a un archivo o carpeta

A través de las siguientes preguntas aclararemos algunos puntos.

¿Tengo que aplicar permisos para evitar que otras personas obtengan acceso a mis archivos?

No. Su cuenta de usuario evita que cualquiera que tenga una cuenta estándar en el equipo pueda ver sus archivos. Sin embargo, no impide que alguien que usa una cuenta de administrador en el equipo vea sus archivos. Si existen otras cuentas de administrador en el equipo, en lugar de usar permisos, puede proteger sus archivos cifrándolos con el sistema de cifrado de archivos (EFS). Si crea una cuenta de usuario para otro usuario en el equipo, asegúrese de crear en este caso una cuenta estándar, en lugar de una cuenta de administrador.

¿Tengo que aplicar permisos para compartir mis archivos con otros usuarios en mi equipo?

No. La mejor manera de compartir archivos es compartirlos desde una carpeta individual o mover los archivos a la carpeta pública. Según con quién desee compartir el archivo o carpeta, es posible que pueda aplicar permisos a algunos de sus archivos. En la siguiente tabla se muestran los niveles de permisos normalmente disponibles para archivos y carpetas.

Nivel de permiso	Descripción
Control total	Los usuarios pueden ver el contenido de un archivo o carpeta, cambiar los archivos y carpetas existentes, crear nuevos archivos y carpetas, y ejecutar programas en la carpeta.
Modificar	Los usuarios pueden cambiar los archivos y carpetas existentes, pero no pueden crear nuevos archivos y carpetas.
Leer y ejecutar	Los usuarios pueden ver el contenido de los archivos y carpetas existentes, y pueden ejecutar programas en la carpeta.
Leer	Los usuarios pueden ver el contenido de una carpeta y abrir archivos y carpetas.
Escribir	Los usuarios pueden crear nuevos archivos y carpetas, y realizar cambios en los archivos y carpetas existentes.

Para aplicar permisos a un archivo o carpeta

1. Haga clic con el botón secundario en el archivo o carpeta y, a continuación, haga clic en Propiedades.
2. Haga clic en la ficha Seguridad y, después, en Editar.
3. Efectúe uno de los siguientes pasos:

- a. Para establecer permisos para un usuario que no aparezca en la lista Nombres de grupos o usuarios, haga clic en Agregar, escriba el nombre del usuario o grupo, haga clic en Aceptar, seleccione los permisos y, a continuación, haga clic en Aceptar.
- b. Para cambiar o quitar permisos de un grupo o usuario existentes, haga clic en el nombre del grupo o usuario, seleccione los permisos y, a continuación, haga clic en Aceptar.

¿Existe algún riesgo al aplicar permisos a un archivo o carpeta?

Sí. Windows automáticamente aplica permisos a los archivos o carpetas de acuerdo con la configuración de su cuenta de usuario y, de ser aplicable, el grupo de seguridad en el que se encuentra su cuenta de usuario. Si aplica permisos manualmente a un archivo o carpeta, éstos pueden entrar en conflicto con los permisos existentes y producir resultados no deseados. No se recomienda aplicar permisos a archivos o carpetas.

¿Qué es el cifrado?

El cifrado es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo. Por ejemplo, si realiza una compra a través de Internet, la información de la transacción (como su dirección, número de teléfono y número de tarjeta de crédito) suele cifrarse a fin de mantenerla a salvo. Use el cifrado cuando desee un alto nivel de protección de la información.

¿Qué es el sistema de cifrado de archivos (EFS)?

El sistema de cifrado de archivos (EFS) es una característica de Windows que permite almacenar información en el disco duro en formato cifrado. El cifrado es la protección de mayor nivel que proporciona Windows para ayudarle a mantener la información a salvo.

Éstas son algunas características destacadas de EFS:

- ❖ El cifrado es sencillo. Se realiza activando una casilla en las propiedades del archivo o de la carpeta.
- ❖ El usuario controla quién puede leer los archivos.
- ❖ Los archivos se cifran cuando los cierra, pero cuando los abre quedan automáticamente listos para su uso.
- ❖ Si cambia de idea con respecto al cifrado de un archivo, desactive la casilla en las propiedades del archivo.
- ❖ EFS no es totalmente compatible con Windows Vista Starter, Windows Vista Home Basic ni Windows Vista Home Premium. En estas ediciones de Windows, si dispone de la clave de cifrado o el certificado, puede hacer lo siguiente:
 - ◆ Descifrar los archivos, ejecutando Cipher.exe en la ventana del símbolo del sistema (usuarios avanzados)



- ◆ Modificar un archivo cifrado
- ◆ Copiar un archivo cifrado como descifrado en el disco duro del equipo
- ◆ Importar certificados y claves EFS
- ◆ Crear copias de seguridad de certificados y claves EFS, ejecutando Cipher.exe en la ventana del símbolo del sistema (usuarios avanzados)

Medidas para evitar la pérdida de claves de cifrado

Para poder seguir estos pasos debe haber iniciado la sesión como Administrador.

Si cifra datos en el equipo, necesita algún método para recuperar esos datos en caso de que surja algún problema con la clave de cifrado. Si la clave de cifrado se pierde o queda dañada y no tiene ningún medio de recuperar los datos, éstos se perderán. Lo mismo ocurrirá si usa una tarjeta inteligente para cifrar los datos. Para asegurarse de que siempre puede tener acceso a sus datos cifrados, debe hacer una copia de seguridad de las claves de cifrado. Si hay más de una persona que usa su equipo, o si utiliza una tarjeta inteligente para cifrar archivos, debe crear un certificado de recuperación de archivos.

Copia de seguridad de las claves de cifrado

Una clave de cifrado siempre se asocia (o se vincula) a un certificado de cifrado. Para realizar una copia de seguridad de la clave de cifrado, deberá hacer una copia de seguridad del certificado que usa para el cifrado. Es recomendable que haga la copia de seguridad del certificado en un disquete o en otro medio extraíble (como una unidad flash USB).

1. Inicie una sesión en la cuenta que usó al cifrar los archivos anteriormente.
2. Haga clic para abrir el Administrador de certificados. Si se le solicita una contraseña de administrador o una confirmación, escriba la contraseña o proporcione la confirmación.
3. Haga clic en la flecha situada junto a la carpeta Personal para expandirla.
4. Haga clic en el certificado en el que se enumera Sistema de cifrado de archivos o Permite que se cifren los datos en el disco, en Propósitos planteados. Es posible que deba desplazarse a la derecha para verlo. Debe hacer una copia de seguridad de todos los certificados EFS que haya.
5. Haga clic en el menú Acción, seleccione Todas las tareas y, a continuación, haga clic en Exportar.
6. En el Asistente para exportación de certificados, haga clic en Exportar la clave privada y, a continuación, en Siguiente.
7. Haga clic en Intercambio de información personal y, a continuación, en Siguiente.
8. Escriba la contraseña que desea usar, confirmela y, a continuación, haga clic en Siguiente. En el proceso de exportación, se crea un archivo para almacenar el certificado.
9. Escriba el nombre y la ubicación del archivo (incluya la ruta de acceso completa), o bien haga clic en Examinar, desplácese hasta la ubicación y después escriba el nombre del archivo.
10. Haga clic en Finalizar.

Permisos de recurso compartido y NTFS en un servidor de archivos

En un servidor de archivos, el acceso a una carpeta puede estar determinado por dos conjuntos de entradas de permisos: los permisos de recurso compartido definidos en una carpeta y los permisos NTFS definidos en la carpeta (que también se puede definir en los archivos). Los permisos de recurso compartido suelen utilizarse para administrar equipos con sistemas de archivos FAT32 u otros equipos que no utilizan el sistema de archivos NTFS.

Los permisos de recurso compartido y los permisos NTFS son independientes en el sentido de que ninguno modifica al otro. Los permisos de acceso final en una carpeta compartida se determinan teniendo en cuenta las entradas de permiso de recurso compartido y de permiso NTFS. Se aplicarán siempre los permisos más restrictivos.

En la siguiente tabla se proponen permisos equivalentes que un administrador preocupado por la seguridad puede conceder al grupo Usuarios para determinados tipos de carpetas compartidas. Hay métodos alternativos. Por ejemplo, puede que algunos administradores con experiencia prefieran definir siempre los permisos de recurso compartido en Control total para el grupo Todos y usar los permisos NTFS para restringir el acceso.

Tipo de carpeta	Permisos de recurso compartido	Permisos NTFS
Carpeta pública. Una carpeta a la que todos pueden tener acceso.	Conceder el permiso Cambiar al grupo Usuarios.	Conceder el permiso Modificar al grupo Usuarios.
Carpeta privada. Una carpeta en la que los usuarios pueden dejar informes confidenciales o asignaciones de tareas que sólo puede leer el administrador o el instructor del grupo.	Conceder el permiso Cambiar al grupo Usuarios. Conceder el permiso Control total al administrador del grupo.	Conceder el permiso Escribir al grupo de usuarios que se aplica a Sólo esta carpeta. (Esta opción está disponible en la página Avanzadas). Si cada usuario necesita tener determinados permisos para los archivos que deja, puede crear una entrada de permiso para el identificador de seguridad conocido (SID) Creator Owner y aplicarla a Sólo subcarpetas y archivos. Por ejemplo, puede conceder los permisos Leer y Escribir al SID de Creator Owner en la carpeta privada y aplicarlos a todas las subcarpetas y archivos. De este modo, el usuario que ha dejado o creado el archivo (Creator Owner) tiene la capacidad para leer y escribir en el archivo. Después, Creator Owner



		<p>puede tener acceso al archivo mediante el comando Ejecutar con \\nombreDeServidor\carpetaPrivada\nombreDeArchivo.</p> <p>Conceder el permiso Control total al administrador del grupo.</p>
<p>Carpeta de aplicaciones. Una carpeta que contiene aplicaciones que se pueden ejecutar a través de la red.</p>	<p>Conceder el permiso Leer al grupo Usuarios.</p>	<p>Conceder los permisos Leer, Leer y ejecutar y Mostrar el contenido de la carpeta al grupo Usuarios.</p>
<p>Carpetas particulares. Las carpetas individuales de cada usuario. Sólo el usuario tiene acceso a la carpeta.</p>	<p>Conceder el permiso Control total a cada usuario en su carpeta respectiva.</p>	<p>Conceder el permiso Control total a cada usuario en su carpeta respectiva.</p>

Consideraciones adicionales

- Conceder a un usuario el permiso NTFS Control total en una carpeta permite a ese usuario tomar posesión de la carpeta a menos que esté restringido de alguna forma. Tenga especial cuidado al conceder Control total.
- Si desea administrar el acceso a carpetas exclusivamente mediante permisos NTFS, defina los permisos de recurso compartido Control total para Todos. Así no tendrá que preocuparse de los permisos de recurso compartido, aunque los permisos NTFS son más complejos que los permisos de recurso compartido.
- Los permisos NTFS influyen sobre el acceso tanto local como remoto. Se aplican con independencia del protocolo. Por el contrario, los permisos de recurso compartido sólo se aplican a recursos compartidos de red. No restringen el acceso a ningún usuario local ni a ningún usuario de Terminal Server del equipo en el que tenga establecidos permisos de recurso compartido.
Por lo tanto, no ofrecen privacidad entre usuarios de un equipo que utilizan varios usuarios, ni en un servidor de Terminal Server al que tienen acceso varios usuarios.
- De forma predeterminada, el grupo Todos no incluye el grupo Anónimo, por lo que los permisos que se aplican al grupo Todos no afectan al grupo Anónimo.

Permisos de archivos y carpetas

En la siguiente tabla se muestran las limitaciones de acceso para cada conjunto de permisos NTFS especiales.

Permisos especiales	Control total	Modificar	Leer y ejecutar	Mostrar el contenido de la carpeta (sólo en carpetas)	Lectura	Escritura
Recorrer carpeta / Ejecutar archivo	X	X	X	X		
Listar carpeta / Leer datos	X	X	X	X	X	
Atributos de lectura	X	X	X	X	X	
Atributos extendidos de lectura	X	X	X	X	X	
Crear archivos / Escribir datos	X	X				X
Crear carpetas / Anexar datos	X	X				X
Atributos de escritura	X	X				X
Atributos extendidos de escritura	X	X				X
Eliminar subcarpetas y archivos	X					
Eliminar	X	X				
Permisos de lectura	X	X	X	X	X	X
Cambiar permisos	X					
Tomar posesión	X					
Sincronizar	X	X	X	X	X	X



Importante

- Los grupos o usuarios a los que se otorgó el permiso Control total en una carpeta pueden eliminar cualquier archivo de esa carpeta independientemente de los permisos que protejan a ese archivo.
- Aunque los permisos Mostrar el contenido de la carpeta y Leer y ejecutar parecen tener los mismos permisos especiales, se heredan de forma diferente. El permiso Mostrar contenido de carpeta lo heredan las carpetas y no lo heredan los archivos, y debería aparecer sólo cuando se ven los permisos de carpeta. El permiso Leer y ejecutar lo heredan los archivos y las carpetas, y siempre está presente cuando se ven los permisos de archivo o carpeta.
- En esta versión de Windows y Windows Server 2003, de forma predeterminada, el grupo Todos no incluye el grupo Anónimo, por lo que los permisos que se aplican al grupo Todos no afectan al grupo Anónimo.

Cómo afecta la herencia a los permisos de archivos y carpetas

Después de configurar los permisos en una carpeta principal, los archivos y subcarpetas nuevos creados en ella heredan dichos permisos. Si no desea que hereden los permisos, active Sólo esta carpeta en el cuadro Aplicar en cuando configure los permisos especiales para la carpeta principal. Se puede tener acceso a los permisos especiales a través de la ficha Permisos. Si desea evitar que sólo algunos archivos o subcarpetas hereden los permisos, haga clic con el botón secundario en el archivo o la subcarpeta, haga clic en Propiedades, haga clic en la ficha Seguridad, haga clic en Avanzadas y, a continuación, desactive la casilla Incluir todos los permisos heredables del objeto primario de este objeto.

Si las casillas Permitir o Denegar asociadas a cada permiso aparecen sombreadas, el archivo o carpeta ha heredado permisos de la carpeta primaria. Hay tres modos de realizar cambios en los permisos heredados:

- Seleccione el permiso contrario (Permitir o Denegar) para invalidar el permiso heredado.
- Desactive la casilla Incluir todos los permisos heredables del objeto primario de este objeto.. A continuación puede realizar los cambios en los permisos o quitar usuarios o grupos de la lista de permisos. Sin embargo, el archivo o la carpeta no heredará los permisos de la carpeta principal.
- Realice los cambios en la carpeta primaria y el archivo o la carpeta heredará estos permisos.

En la mayoría de los casos, Denegar invalida Permitir, a menos que una carpeta herede configuraciones en conflicto de diferentes objetos primarios. En ese caso, tendrá preferencia la configuración heredada del objeto primario más cercano al objeto en el subárbol.

Los objetos secundarios sólo heredan los permisos heredables. Cuando se configuran permisos en el objeto primario, se puede decidir si las carpetas o subcarpetas pueden heredarlos con el cuadro Aplicar en de la ficha Permisos del cuadro de diálogo Configuración de seguridad avanzada para <objeto>.

Definir, ver, cambiar o quitar permisos especiales

Cada objeto tiene permisos asociados que pueden restringir el acceso. Puede modificar estos permisos especiales para definir el acceso a un objeto determinado.

Debe ser el propietario del objeto o haber obtenido permiso del propietario para completar este procedimiento. Revise los detalles en la sección "Consideraciones adicionales" de este tema.

Para definir, ver, cambiar o quitar permisos especiales

1. Haga clic con el botón secundario en el objeto en el que desea definir permisos avanzados o especiales, haga clic en Propiedades y, después, haga clic en la ficha Seguridad.
2. Haga clic en Opciones avanzadas y, a continuación, haga clic en Editar.
3. En la ficha Permisos, realice una de las acciones siguientes:
 - Establecer permisos especiales para un grupo o un usuario adicional. Haga clic en Agregar. En Escriba el nombre de objeto a seleccionar (ejemplos), escriba el nombre del usuario o grupo y, después, haga clic en Aceptar.
 - Ver o cambiar permisos especiales para un grupo o un usuario existente. Haga clic en el nombre del grupo o el usuario y, a continuación, haga clic en Editar.
 - Quitar un grupo o usuario existente y sus permisos especiales. Haga clic en el nombre del grupo o el usuario y, a continuación, haga clic en Quitar. Si el botón Quitar no está disponible, desactive la casilla Incluir todos los permisos heredables del objeto primario de este objeto y, a continuación, haga clic en Quitar.
4. En el cuadro Permisos, active o desactive la casilla Permitir o Denegar correspondiente.
5. En el cuadro Aplicar en, haga clic en las carpetas o subcarpetas a las que desea aplicar estos permisos.
6. Para configurar la seguridad de modo que las subcarpetas y archivos no hereden estos permisos, desactive la casilla Aplicar estos permisos a objetos y/o contenedores sólo dentro de este contenedor.
7. Haga clic en Aceptar y, a continuación, en Configuración de seguridad avanzada para <nombreDeObjeto>, haga clic en Aceptar.

Precaución

Si activa la casilla Incluir todos los permisos heredables del objeto primario de este objeto, todas las entradas de permisos de las subcarpetas y archivos se restaurarán a las heredadas del objeto primario. Los permisos implícitos se quitarán y, si el objeto estaba "protegido" contra una herencia automática, la protección también se quitará. Una vez que hace clic en Aplicar o en Aceptar, no puede deshacer esta operación aunque desactive la casilla.



Debe tomar en cuenta que:

- Los grupos o usuarios a los que se ha otorgado Control total en una carpeta pueden eliminar archivos o subcarpetas de esa carpeta independientemente de los permisos que protegen a los archivos y subcarpetas.
- Este procedimiento puede requerir que eleve los permisos mediante Control de cuenta de usuario.
- Para abrir el Explorador de Windows, haga clic en Inicio, seleccione Todos los programas, Accesorios y, a continuación, haga clic en Explorador de Windows.
- El grupo Todos ya no incluye el permiso Inicio de sesión anónimo.
- Si desactiva la casilla Incluir todos los permisos heredables del objeto primario de este objeto, este archivo o carpeta no heredará entradas de permisos del objeto primario.
- Puede definir los permisos NTFS sólo en las unidades con formato para utilizar NTFS.
- Si las casillas en Permisos están sombreadas, los permisos se han heredado de la carpeta principal.

Determinar dónde aplicar permisos

Cuando se establecen permisos avanzados en archivos y carpetas, se puede utilizar el cuadro de diálogo Entrada de permiso para <nombre de objeto> para establecer los objetos descendientes que heredarán permisos.

Para buscar este cuadro de diálogo, haga clic en el botón Opciones avanzadas de la interfaz de usuario de control de acceso. En la ficha Permisos, haga clic en Modificar dos veces.

En el cuadro de diálogo Entrada de permiso para <nombre de objeto>, el cuadro Aplicar en de la ficha Objeto enumera las ubicaciones donde se pueden aplicar permisos. El modo en que se aplican estos permisos depende de si la casilla Aplicar estos permisos a objetos y/o contenedores sólo dentro de este contenedor está activada.

Importante

En el caso de objetos de Active Directory, no sólo los objetos especificados en el cuadro Aplicar en heredan las entradas de control de acceso sino que TODOS los objetos secundarios reciben una copia de esa ACE. Los objetos secundarios no especificados en el cuadro Aplicar en no utilizarán la ACE cuya copia reciben. Sin embargo, si hay suficientes objetos que van a obtener copias de esta ACE, entonces esa mayor cantidad de datos puede ocasionar serios problemas de rendimiento en la red.

De forma predeterminada, esta casilla está desactivada.

Cuando la casilla Aplicar estos permisos a objetos y/o contenedores sólo dentro de este contenedor está desactivada

Aplicar en	Aplica permisos a la carpeta actual	Aplica permisos a las subcarpetas de la carpeta actual	Aplica permisos a los archivos de la carpeta actual	Aplica permisos a todas las subcarpetas subsiguientes	Aplica permisos a los archivos de todas las subcarpetas subsiguientes
Sólo esta carpeta	x				
La carpeta, subcarpetas y archivos	x	x	x	x	x
Esta carpeta y sus subcarpetas	x	x		x	
Esta carpeta y sus archivos	x		x		x
Sólo subcarpetas y archivos		x	x	x	x
Sólo subcarpetas		x		x	
Sólo archivos			x		x

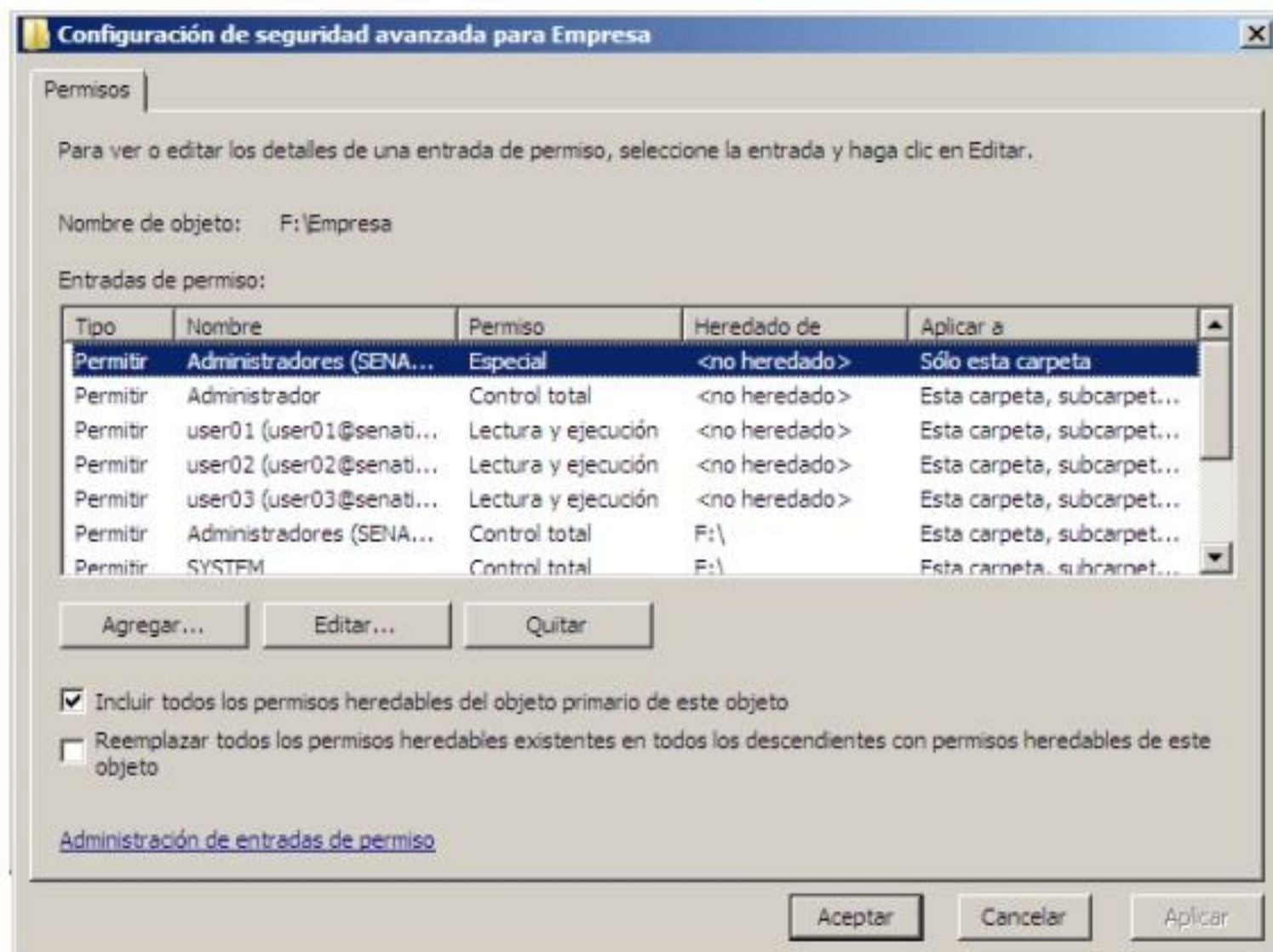
Cuando la casilla Aplicar estos permisos a objetos y/o contenedores sólo dentro de este contenedor está activada

Aplicar en	Aplica permisos a la carpeta actual	Aplica permisos a las subcarpetas de la carpeta actual	Aplica permisos a los archivos de la carpeta actual	Aplica permisos a todas las subcarpetas subsiguientes	Aplica permisos a los archivos de todas las subcarpetas subsiguientes
Sólo esta carpeta	x				
La carpeta, subcarpetas y archivos	x	x	x		
Esta carpeta y sus subcarpetas	x	x			



Esta carpeta y sus archivos	X		X		
Sólo subcarpetas y archivos		X	X		
Sólo subcarpetas		X			
Sólo archivos			X		

Configuración de seguridad avanzada en Permisos



Puede agregar grupos, usuarios o recursos adicionales para contar con permisos NTFS explícitos y tener acceso a este objeto, o puede editar o quitar los permisos NTFS concedidos a un recurso, grupo o usuario del objeto.

Los permisos heredados son los que se propagan a un objeto desde un objeto primario. Los permisos heredados facilitan la tarea de administrar permisos y aseguran su coherencia entre todos los objetos de un contenedor determinado.

Elemento	Descripción
Nombre de objeto	Da nombre al objeto seleccionado actualmente.
Entradas de permisos	Muestra cada entrada de permiso para este objeto: <ul style="list-style-type: none"> • Tipo: permite o deniega a este grupo o usuario el permiso para este objeto • Nombre: recurso, usuario o grupo

	<ul style="list-style-type: none"> • Permiso: restricciones aplicadas actualmente a este objeto para este recurso, usuario o grupo • Heredado de: identifica el objeto primario • Aplicar a: identifica los objetos descendientes a los que también se aplican los permisos
Incluir todos los permisos heredables del objeto primario de este objeto	<p>Si se selecciona, cada objeto secundario tendrá permisos heredados de su objeto primario.</p> <p>Si se anula la selección, los permisos aplicados al objeto primario no se aplicarán a su objeto u objetos secundarios.</p>
Reemplazar todos los permisos heredables existentes en todos los descendientes con permisos heredables de este objeto.	<p>Si se selecciona, los permisos de este objeto primario reemplazarán los de los objetos descendientes.</p> <p>Si se anula la selección, los permisos de cada objeto (tanto de los primarios como de sus descendientes) pueden ser únicos.</p>

Cuotas de disco

Administración de cuotas

En el nodo Administración de cuotas del complemento Microsoft® Management Console (MMC) del Administrador de recursos del servidor de archivos, puede realizar las siguientes tareas:

- Crear cuotas para limitar el espacio asignado a un volumen o carpeta y generar notificaciones cuando se esté a punto de alcanzar o superar el límite de dichas cuotas.
- Generar cuotas automáticas aplicables a todas las carpetas existentes en un volumen o una carpeta y a todas las subcarpetas que se creen en lo sucesivo.
- Definir plantillas de cuota que puedan aplicarse fácilmente a nuevos volúmenes o carpetas y que puedan utilizarse en toda una organización.

Por ejemplo, puede:

- Establecer un límite de 200 megabytes (MB) en las carpetas personales de los usuarios, con una notificación para usted y para el usuario cuando se superen los 180 MB de almacenamiento.
- Establecer una cuota de advertencia de 500 MB en la carpeta compartida de un grupo. Cuando se alcance este límite de almacenamiento, todos los usuarios del grupo recibirán por correo electrónico una notificación en la que se les informará de que la cuota



de almacenamiento se ha ampliado temporalmente a 520 MB para que puedan eliminar los archivos que no necesiten y poder cumplir la cuota predefinida de 500 MB.

- Recibir una notificación cuando una carpeta temporal llegue a tener un uso de 2 gigabytes (GB) sin limitar la cuota de esa carpeta si es necesaria para ejecutar un servicio en el servidor.

Crear una cuota

Las cuotas pueden crearse a partir de una plantilla o con propiedades personalizadas. El procedimiento siguiente describe cómo crear una cuota basada en una plantilla (recomendado). Si necesita crear una cuota con propiedades personalizadas, puede guardar estas propiedades como una plantilla para volver a usarla en el futuro.

Cuando cree una cuota, elija una ruta de acceso, que es un volumen o una carpeta a los que se aplica el límite de almacenamiento. En una ruta de acceso de cuota determinada, puede usar una plantilla para crear uno de los siguientes tipos de cuota.

Una sola cuota que limite el espacio de un volumen o una carpeta en su totalidad.

Una cuota automática, que asigna la plantilla de cuota a una carpeta o un volumen. Las cuotas basadas en esta plantilla se generan automáticamente y se aplican a todas las subcarpetas.

Si las cuotas se crean exclusivamente a partir de plantillas, es posible administrarlas centralmente actualizando las plantillas en lugar de las cuotas individuales. A continuación, puede aplicar los cambios a todas las cuotas basadas en la plantilla modificada. Esta característica simplifica la implementación de los cambios de las directivas de almacenamiento ya que proporciona un punto central donde se pueden llevar a cabo todas las actualizaciones.

Para crear una cuota basada en una plantilla

En Administración de cuotas haga clic en el nodo Plantillas de cuota.

- En el panel de resultados, seleccione la plantilla sobre la que basará la nueva cuota.
- Haga clic con el botón secundario en la plantilla y haga clic en Crear cuota a partir de una plantilla (o seleccione Crear cuota a partir de una plantilla en el panel Acciones). Se abrirá el cuadro de diálogo Crear cuota con las propiedades resumidas de la plantilla de cuota mostrada.
- En Ruta de acceso de cuota, escriba el nombre de la carpeta a la que se aplicará la cuota o búsquela.
- Haga clic en la opción Crear cuota en la ruta de acceso. Observe que las propiedades de la cuota se aplicarán a toda la carpeta.

Para crear una cuota automática, haga clic en la opción Aplicar plantilla autom. y crear cuotas en subcarpetas nuevas y existentes..

En Derivar propiedades desde esta plantilla de cuota, se preselecciona la plantilla usada en el paso 2 para crear la nueva cuota (o puede seleccionar otra plantilla en la lista). Tenga en cuenta que las propiedades de la plantilla se mostrarán en el Resumen de las propiedades de cuota.

Ejercicio Práctico
Escenario:

Este ejercicio se desarrollará en grupo de 3 personas y requerirá de la investigación e implementación de nuevos temas.

La Universidad CertifyHigh necesita configurar un Servidor Windows para las tareas de administración de cuentas y asignación de permisos a carpetas para que accedan adecuadamente a su información. Para ello la universidad provee los siguientes datos:

Información General:
Dirección General:

- a. Steve Emerson – Rector
- b. Susan Brown – Secretaria Ejecutiva

Personal por Facultad:

Facultad	Director	Docentes	Asistentes
Sistemas	Eyvar Tuner	Miguel Cortez Sandro Villaran Hans Montero Marcus Kart	Roxana Bravo
Geología	Michael Ux	Sharon Urbina Marco Tenorio Katy Summer	Sonia Canessa
Contabilidad	Edmar Ércoli	Harun Ledmar Dei Conti	Ruth Francia
Administración	Abdel Samad	Martha Cotrina Sofia Cassani Miriya Terrones Celina Celman	Melany Coronado
Ciencias Sociales	Leonardo Yeltsin	Steven Cópola Marc Mendo Yanira Corona Vincent Ka	Lady Smith
Educación	Taher Le Sage	Tiffany Morales Rosmery Sanchez Jack Ortega	Sandra Sifuentes

Cuentas para alumnos:

1. Se crearán cuentas para cada alumno, según estos se inscriban. Para ello se debe contar con una cuenta plantilla correctamente configurada para realizar copias de la misma posteriormente.

Beneficios que se otorgarán a todos los usuarios:

2. Acceso desde las 8:00 a.m. hasta las 22:00 p.m. de lunes a viernes y los sábados de 8:00 a 14:00.
3. Gozarán de 100 MB de espacio en disco (Cuotas), a excepción de los directores que gozarán de 500 MB.
4. Estructura de árbol de carpetas por Facultad para una mejor organización. Es decir debe crear un árbol de carpetas donde se contenga a todas las facultades. Sólo la carpeta raíz debe estar compartida.
5. Cada usuario recibirá una carpeta personal, en la que podrá guardar sus trabajos, a la cual sólo ingresaran ellos.



Otras indicaciones:

6. Los Directores sólo podrán ingresar a la información contenida en su respectiva Facultad, a fin de realizar cualquier tipo de control o auditoria.
7. Los Docentes necesitan un perfil que se desplace con ellos a través de la red.
8. Un Servidor adicional deberá contar con al menos 2 carpetas compartidas, con las cuales se creará un DFS en el Servidor para proveer acceso a dichas carpetas a través del Server.

Preguntas de Repaso

1. Si a nivel de compartir se indica que el Grupo Todos, tiene nivel de Copropietario y a nivel de la Ficha Seguridad se establece Control Total. ¿Tendrá acceso un usuario estándar?
2. Cuando un usuario tienen acceso a un recurso compartido, con qué permiso se enfrenta ¿Compartir o NTFS?
3. En la siguiente estructura de carpetas: ¿Qué sucede si a un usuario (Juan Pérez por ejemplo), que accede remotamente desde Windows XP se le ha asignado permisos de CONTROL TOTAL sobre su carpeta personal, ESCRIBIR sobre la carpeta Segundo Grado, LEER y ESCRIBIR sobre la carpeta Primaria y LISTAR EL CONTENIDO DE LA CARPETA sobre la carpeta Archivos de Usuarios?, ¿Es posible que dicho usuario acceda a su carpeta personal?, ¿A qué carpetas tiene acceso el usuario?





Servicios de impresión

En este capítulo trataremos:

- Identificará los términos utilizados en la Impresión
- Aprenderá a instalar impresoras
- Aprenderá a configurar una impresora
- Aprenderá a configurar una impresora de Internet

Introducción:

Tarea común para los usuarios, es la impresión, pese al avance todavía es necesario imprimir algunos documentos sobre todo porque se necesitan firmas manuscritas. Como administrador será su responsabilidad facilitar el acceso a la impresora.



Terminología empleada en los Servicios de Impresión

1. **Impresora.** Es la interfaz de software entre el sistema operativo y el dispositivo de impresión.
2. **Dispositivo de impresión.** Es el dispositivo de hardware que produce los documentos impresos físicamente. Windows Server 2008 soporta los siguientes dispositivos:
 - a. **Dispositivos de impresión Locales.** Son aquellos que están conectados a un puerto físico en el servidor de impresión. Se conecta a la computadora mediante una interfaz local como puerto paralelo, serie, USB o SCSI
 - b. **Dispositivo de impresión de Red.** Son aquellos que están conectados al servidor a través de la red. Requieren sus propias tarjetas de interfaz de red y tienen sus propias direcciones de red.
3. **Servidor de impresión.** Es la computadora en la que residen las impresoras asociadas con dispositivos de impresión locales y de red. Procesa los requerimientos de impresión de los clientes.
4. **Controlador de Impresora.** Son uno o más archivos que contienen información requerida para convertir los comandos de impresión en un lenguaje específico de la impresora para hacer posible la impresión.

Instalación de Impresoras en el Servidor

Para imprimir, deberá conectar una impresora directamente al equipo (denominada impresora local), o crear una conexión con una red o impresora compartida.

Para agregar una impresora de red, inalámbrica o Bluetooth

Antes de empezar, asegúrese de conocer el nombre de la impresora que desea agregar. Para buscar el nombre de la impresora, compruebe si el nombre está expuesto en la propia impresora, póngase en contacto con el propietario de la impresora o póngase en contacto con el administrador de red.

1. Haga clic para abrir Impresoras.
2. Haga clic en Agregar una impresora.
3. En el Asistente para agregar impresoras, seleccione Agregar una impresora de red, inalámbrica o Bluetooth.
4. En la lista de impresoras disponibles, seleccione la que desee usar y haga clic en Siguiente. Como el equipo está conectado a una red, sólo las impresoras mostradas en Active Directory del dominio aparecerán en la lista.
5. Si se le solicita, instale el controlador de impresora en el equipo. Si se le solicita una contraseña de administrador o una confirmación, escriba la contraseña o proporcione la confirmación.
6. Complete los pasos adicionales del asistente y, a continuación, haga clic en Finalizar.

Sugerencias

- ❖ Las impresoras disponibles pueden incluir todas las impresoras de una red, como las impresoras Bluetooth e inalámbricas o las impresoras que estén conectadas a otro equipo y estén compartidas en la red. Asegúrese de que tiene permiso para usar estas impresoras antes de agregarlas al equipo.

- ❖ Es conveniente imprimir una página de prueba para comprobar si la impresora funciona correctamente.

Para agregar una impresora local

A través de las indicaciones del fabricante, conecte la impresora al equipo. Windows instalará automáticamente la impresora. Si Windows no puede instalarla, o bien si ha quitado la impresora y desea volver a agregarla, siga estos pasos:

1. Haga clic para abrir Impresoras.
 2. Haga clic en Agregar una impresora.
 3. En el Asistente para agregar impresoras, seleccione Agregar una impresora local.
 4. En la página Elegir un puerto de impresora, asegúrese de que estén seleccionados el puerto de impresora recomendado y el botón de opción Usar un puerto existente y, a continuación, haga clic en Siguiente.
 5. En la página Instalar el controlador de impresora, seleccione el fabricante de la impresora y el nombre de la misma y, a continuación, haga clic en Siguiente.
- ❖ Si la impresora no está en la lista y tiene el disco de instalación de la impresión, haga clic en Utilizar disco y, a continuación, busque la ubicación en el disco en el que están almacenados los controladores de impresora. Para obtener ayuda a la hora de buscar el software de controlador en el disco de instalación, consulte la información del fabricante que se suministra con la impresora.
 - ❖ Si la impresora no está en la lista, y no tiene el disco de instalación de la impresora, haga clic en Windows Update y, a continuación espere mientras Windows comprueba los paquetes de software de controlador disponibles. Cuando aparezca una nueva lista de fabricantes e impresoras, seleccione los elementos adecuados de cada lista para la impresora.
6. Complete los pasos adicionales del asistente y, a continuación, haga clic en Finalizar.
- ❖ Es conveniente imprimir una página de prueba para comprobar si la impresora funciona correctamente.

Quitar una impresora

No puede quitar una impresora si tiene elementos en la cola de impresión. Si hay elementos que esperan imprimirse mientras intenta quitar una impresora, Windows esperará a que la impresión haya finalizado y entonces quitará la impresora. Si tiene permiso para administrar documentos en la impresora, también puede cancelar todos los trabajos de impresión y, a continuación, intentar quitar de nuevo la impresora.

1. Haga clic para abrir Impresoras.
2. Haga clic con el botón secundario del mouse en la impresora que desee quitar y, después, haga clic en Eliminar.

Si no puede eliminar la impresora, vuelva a hacer clic con el botón secundario del mouse en la impresora, haga clic en Ejecutar como administrador y, a continuación,



haga clic en Eliminar. Si se le solicita una contraseña de administrador o una confirmación, escriba la contraseña o proporcione la confirmación.

Sugerencia

Para agregar un acceso directo a Impresoras en el menú Inicio, haga clic con el botón secundario del mouse en el botón Inicio, haga clic en Propiedades y, después, en la ficha Menú Inicio, haga clic en Personalizar. Active la casilla Impresoras y, a continuación, haga clic en Aceptar.

Configuración de Seguridad de Impresoras

Los permisos de la impresora determinan qué propiedades de la impresora puede administrar, por ejemplo cambiar el nombre o compartir una impresora, permitir o eliminar el acceso a la impresora y determinar quién puede administrar documentos o propiedades para la impresora. Normalmente, los permisos de la impresora los administra la persona que la instaló o, si la impresora está conectada a una red comercial o empresarial, un administrador del sistema.

Los permisos se pueden asignar a cada persona que use la impresora o a un grupo de usuarios que tengan el mismo tipo de cuenta de usuario. Por ejemplo, los miembros del grupo de administradores del equipo tienen permiso para administrar las impresoras de forma predeterminada.

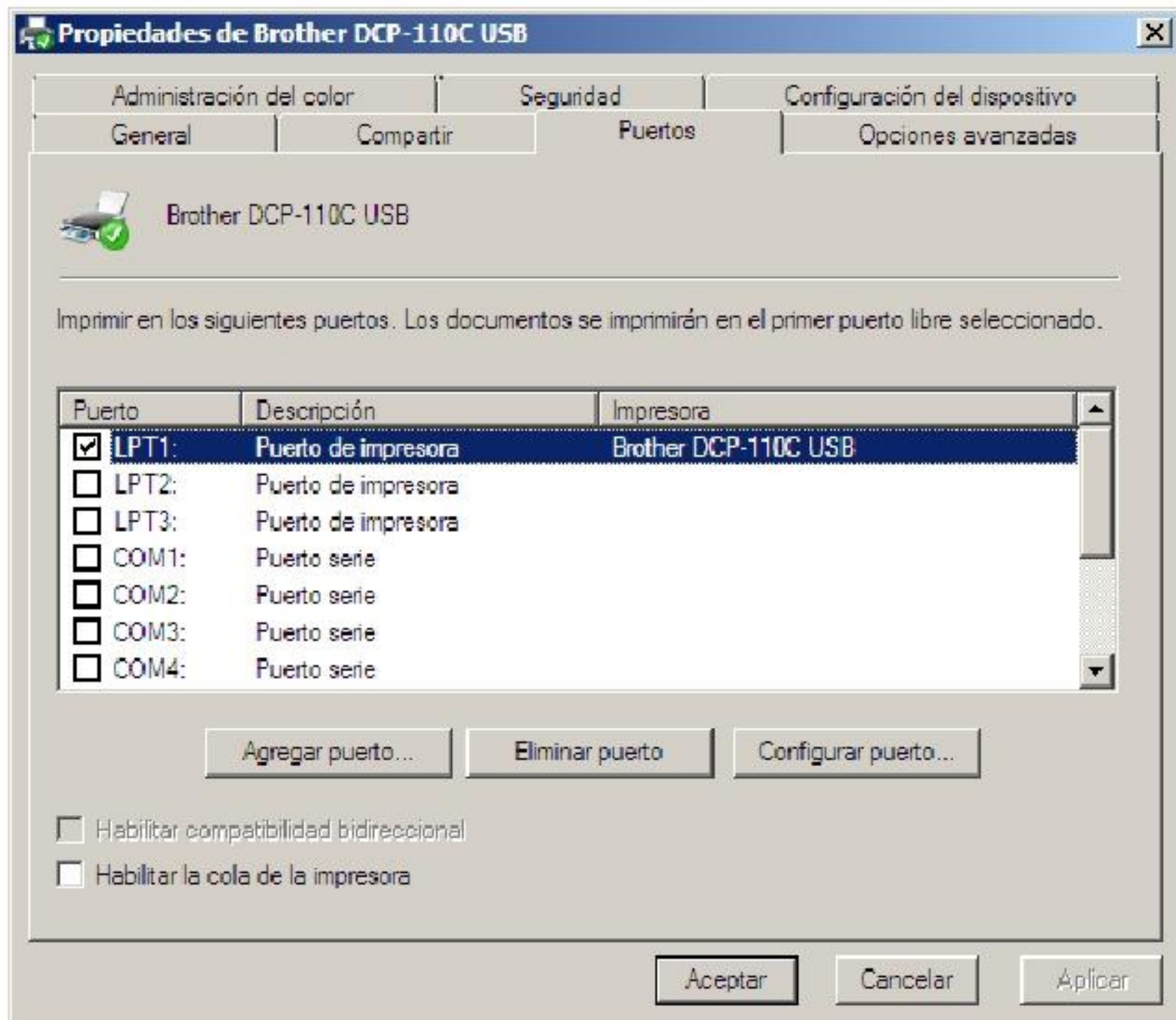
Windows ofrece cuatro tipos de permisos de impresora:

- **Imprimir.** De forma predeterminada, cada usuario puede imprimir y cancelar, pausar o reiniciar documentos o archivos que envíen a una impresora.
- **Administrar documentos.** Si tiene este permiso, puede administrar todos los trabajos de impresión de una impresora que estén esperando en la cola de impresión, incluidos los documentos o archivos impresos por otros usuarios.
- **Administrar impresoras.** Este permiso permite cambiar el nombre, eliminar, compartir y elegir preferencias para la impresora. También permite seleccionar permisos para otros usuarios y administrar todos los trabajos de la impresora. Los miembros del grupo de administradores de un equipo tienen permiso para administrar las impresoras de forma predeterminada.
- **Permisos especiales.** Estos permisos, normalmente sólo utilizados por los administradores del sistema, se pueden usar para cambiar el propietario de la impresora, en caso necesario. Al CREATOR OWNER de la impresora se le conceden todos los permisos de impresora y es, de forma predeterminada, la persona que instaló la impresora.

Opciones de los servidores de impresión

Configuración de puertos

Puede instalar varios dispositivos de impresión iguales en diferentes puertos de la PC y luego activar la **cola de impresión** y activar los puertos por donde enviará la información a imprimir.



Impresoras y active Directory

Publicación de impresoras

1. Verifique que se hayan instalado los Servicios de Impresión en el equipo que tiene el Active Directory para poder publicar impresoras.
2. Debe haber compartido la impresora.
3. Active la casilla **Mostrar lista en el directorio** de la Ficha Compartir en propiedades de la impresora.
4. Clic derecho en una unidad organizativa, seleccione nuevo, luego impresora
5. Escriba el nombre la ruta UNC de la impresora y listo

Distribución de controladores a través de la red

1. En las propiedades de la impresora, seleccione la ficha Compartir
2. Clic en el botón **Controladores adicionales**.
3. Seleccione el tipo de sistema donde se instalarán los drivers.



Ejercicio

Elabore la siguiente organización y realiza las configuraciones de impresión que se indican.

1. Las siguientes personas harán uso de la red en la empresa T-Soro
 - i. Jorge Tafur (Gerente General)
 - ii. Miguel Millano (Sub Gerente)
 - iii. Frank Molina (Encargado de compras)
 - iv. Jorge Muñoz (Asistente del área de compras)
 - v. Victor Mimbela (vendedor)
 - vi. Manuel Pacora (vendedor)
 - vii. Susana Frey (vendedor)
2. Se han comprado 3 Impresoras HP modelo HP Color LaserJet 4550 PCL y se desea que los usuarios vendedores impriman de forma automatizada en cualquiera de las 3 impresoras (En la carpeta de impresoras sólo se debe observar una sola Impresora el cual permitirá imprimir en los puertos LPT1, LPT2 y LPT3)
3. Se ha comprado una impresora Fujitsu DL 3600 y se desea configurar prioridades sobre dicha impresora. De tal manera que los documentos de la Gerencia tengan mayor prioridad, y que luego sigan los documentos del área de ventas y luego la de compras. Además configure cada Impresora para que acceda únicamente el grupo de usuarios que corresponda

Preguntas de Repaso

1. Indique el proceso que realizaría para instalar una impresora de Red desde un Cliente Windows XP
2. Qué proceso realizaría para instalar una impresora por internet.
3. Qué es la cola de impresión y en qué carpeta se almacena.
- 4.Cuál es el propósito de publicar una carpeta
5. Instala una impresora publicada en el AD desde un cliente Windows XP



Fundamentos sobre directivas de grupo

En este capítulo trataremos:

- Identificará los componentes de las directivas de grupo
- Aprenderá a administrar directivas de grupo
- Aprenderá a utilizar el editor de directivas de grupo

Introducción:

Las directivas de grupo permiten al administrador de red, gestionar el entorno sobre los usuarios y las computadoras de una red, definiendo de esta forma el entorno de trabajo una sola vez. A través del presente capítulo se ha reunido información disponible en diversos medios para brindar una idea general del trabajo básico con directivas de grupo.



Introducción a Administración de directivas de grupo

La Administración de directivas de grupo incluye la Consola de administración de directivas de grupo (GPMC), la Microsoft Management Console que permite administrar el costo de las directivas de grupo de forma eficaz para su compañía.

La Consola de administración de directivas de grupo simplifica la administración de la directiva de grupo basada en dominio al proporcionar una sola experiencia de administración, edición y generación de informes de los aspectos centrales de la directiva de grupo. Puede considerar GPMC como un recurso de una sola parada para administrar sus necesidades de directiva de grupo.

La Consola de administración de directivas de grupo incluye:

- Una interfaz de usuario que aumenta la facilidad de uso de la directiva de grupo.
- Copia de seguridad y restauración de los objetos de directiva de grupo (GPO).
- Importación y exportación, así como copia y pegado de GPO y filtros Instrumental de administración de Windows (WMI).
- Administración simplificada de la seguridad relacionada con la directiva de grupo.
- Generación de informes HTML para la configuración de GPO y datos del Conjunto resultante de directivas (RSOP).
- Posibilidad de incluir comentarios basados en texto en los objetos de directiva de grupo y configuración de la directiva basada en el Registro.
- Vistas filtradas de la configuración de la directiva basada en el Registro en función de palabras clave dentro del título, el texto de explicación o los comentarios de la configuración de la directiva.
- Objetos de directiva de grupo de inicio: colecciones portátiles de la configuración de directiva basada en el Registro, que proporcionan puntos de inicio para los GPO.
- Preferencias: veintiuna extensiones de directiva de grupo adicionales que le permiten administrar asignaciones de unidades, valores del Registro, usuarios y grupos locales, servicios, archivos, carpetas y más sin necesidad de aprender ningún lenguaje de scripting.

Modificar objetos de varias directivas de grupo local

Varias directivas de grupo local es una colección de objetos de directiva de grupo local (LGPO), diseñada para mejorar la administración de los equipos que no forman parte de un dominio. Esta colección se compone de los siguientes LGPO:

- Directiva de equipo local. Este LGPO aplica la configuración de directiva al equipo y a los usuarios que inician una sesión en el equipo. Es el mismo LGPO que se incluyó en versiones anteriores de Microsoft Windows.
- Directiva de grupo local de administradores. Este LGPO aplica la configuración de directiva de usuario a los miembros del grupo Administradores.
- Directiva de grupo local de no administradores. Este LGPO aplica la configuración de directiva de usuario a los usuarios que no pertenecen al grupo Administradores.

- Directiva de grupo local de usuarios. Este LGPO aplica la configuración de directiva de usuario a un usuario local específico.

Para modificar objetos de varias directivas de grupo local

1. Abra Microsoft Management Console.
2. Haga clic en Archivo y, a continuación, en Agregar o quitar complemento.
3. Haga clic en el Editor de directivas de grupo local en la lista Complementos disponibles y haga clic en Agregar.
4. Haga clic en el botón Examinar del cuadro de diálogo Seleccionar un objeto de directiva de grupo.
5. Haga clic en la ficha Usuarios del cuadro de diálogo Buscar un objeto directiva de grupo.
6. Haga clic en el usuario o grupo en el que desee crear o modificar una directiva de grupo local. Haga clic en Aceptar, en Finalizar y, a continuación, en Aceptar.
7. Busque y establezca una o varias configuraciones de directiva.

Consideraciones adicionales

1. En los controladores de dominio los objetos de varias directivas de grupo local (MLGPO) no están disponibles.
2. La directiva de grupo local se procesa en el siguiente orden, en el que el LGPO final tiene prioridad sobre el resto:
 1. Directiva de grupo local (también denominada directiva de equipo local).
 2. Directiva de grupo local de administradores o no administradores.
 3. Directiva de grupo local de usuarios.

Apertura del Editor de directivas de grupo local

Puede abrir el Editor de directivas de grupo local mediante la línea de comandos o mediante Microsoft Management Console (MMC).

Para abrir el Editor de directivas de grupo local desde la línea de comandos

- ❖ Haga clic en Inicio, Todos los programas, Accesorios y Ejecutar. Escriba gpedit.msc en el cuadro y haga clic en Aceptar o presione ENTRAR.





Para abrir el Editor de directivas de grupo local como complemento de MMC

Nota

Si desea guardar una consola del Editor de directivas de grupo local y elegir el objeto de directiva de grupo que se abre en ella desde la línea de comandos, active la casilla Permitir que cambie el enfoque del complemento de directivas de grupo cuando se inicie desde la línea de comandos en el cuadro de diálogo Seleccionar un objeto de directiva de grupo.

1. Abra MMC. Haga clic en Inicio; a continuación, en el cuadro Iniciar búsqueda, escriba mmc y presione ENTRAR.
2. En el menú Archivo, haga clic en Agregar o quitar complemento.
3. En el cuadro de diálogo Agregar o quitar complementos, haga clic en Editor de directivas de grupo local y, después, en Agregar.
4. En el cuadro de diálogo Seleccionar un objeto de directiva de grupo, haga clic en Examinar.
5. Haga clic en Este equipo para modificar el objeto de directiva de grupo local, o en Usuarios para modificar los objetos de directiva de grupo local de administrador, no administrador o por usuario.
6. Haga clic en Finalizar, en Cerrar y, a continuación, en Aceptar. El Editor de directivas de grupo local abre el objeto de directiva de grupo (GPO) para modificarlo.

Consola de administración de directivas de grupo

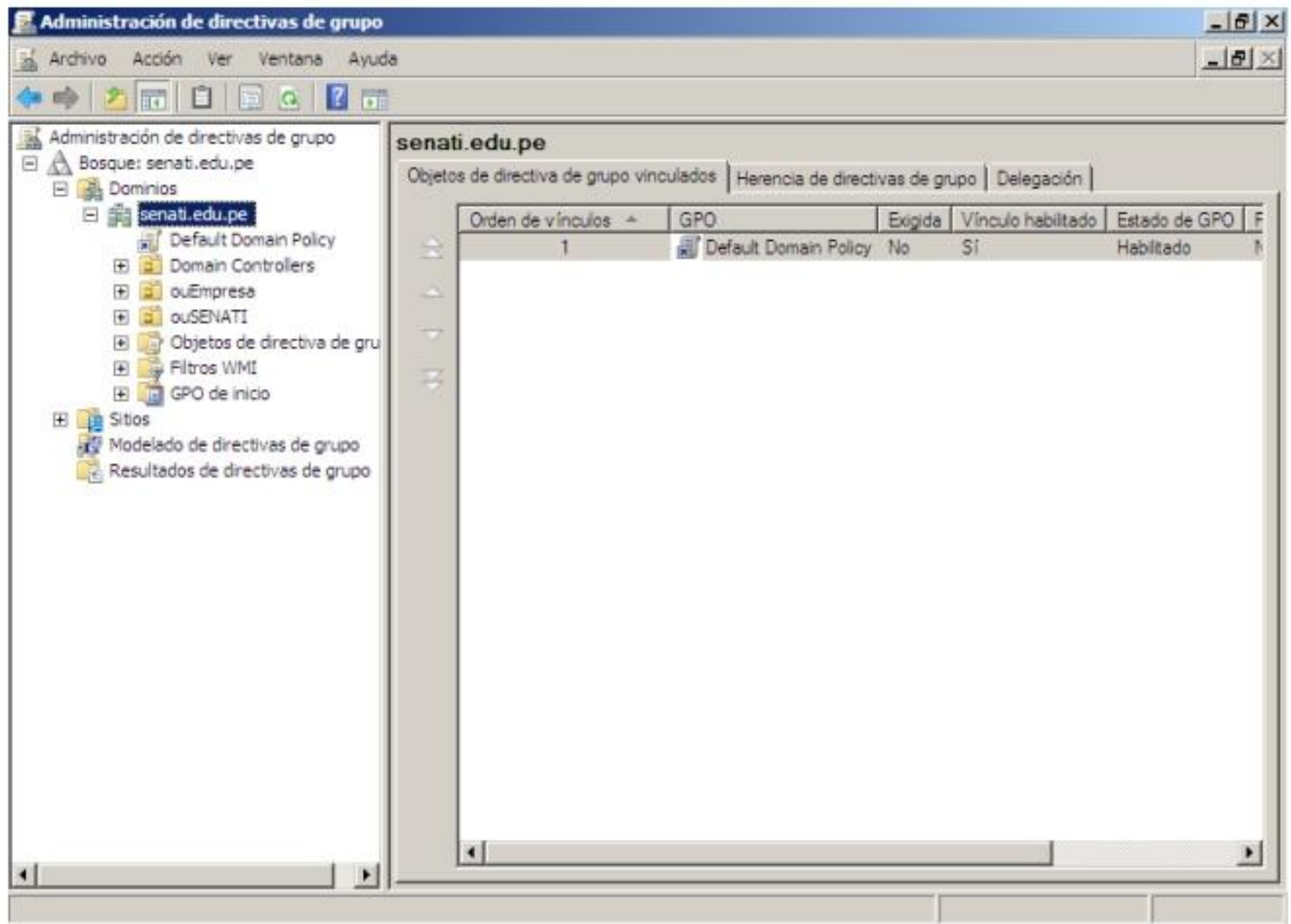
Consola de administración de directivas de grupo (GPMC) es un complemento de scripts de Microsoft Management Console (MMC), que proporciona una única herramienta administrativa para administrar la directiva de grupo en toda la organización. GPMC es la herramienta estándar para administrar la directiva de grupo.

Abrir GPMC

Puede iniciar la Consola de administración de directivas de grupo (GPMC) con uno de estos dos métodos.

Para iniciar GPMC

- ❖ Realice una de estas acciones:
 - Presione la tecla del logotipo de Windows + R para abrir el cuadro de diálogo EJECUTAR. Escriba gpmc.msc en el cuadro de texto y, después, haga clic en Aceptar o presione ENTRAR.
 - Haga clic en Inicio, Todos los programas, Accesorios y, después, en Ejecutar. Escriba gpmc.msc en el cuadro de texto y, después, haga clic en Aceptar o presione ENTRAR.



Personalizar la interfaz de usuario de GPMC

Puede personalizar la interfaz de usuario de la Consola de administración de directivas de grupo (GPMC) mediante los procedimientos que se describen en este tema.

Para configurar las opciones de la interfaz de usuario

1. En el menú Ver de GPMC, haga clic en Opciones.
2. Seleccione una o todas las fichas que se muestran a continuación, de una en una, para personalizar aspectos específicos de la interfaz de usuario de GPMC:

En la ficha Columnas:

1. Seleccione una tabla de la lista desplegable Ubicación de la tabla.
2. En Columnas mostradas en este orden, agregue una marca de verificación junto a cada columna que debe mostrarse.
3. Seleccione una columna y utilice los botones Subir y Bajar para establecer el orden de las columnas.
4. Repita los pasos 2 a 3 para cada tabla de la lista desplegable Ubicación de la tabla que desee cambiar y, a continuación, haga clic en Aceptar.
5. La opción Guardar orden y tamaño de columnas personalizados está activada de forma predeterminada y convierte en permanentes las selecciones de orden y tamaño de las columnas. Desactive esta casilla si no desea mantener las selecciones.



En la ficha Generación de informes, elija una de las opciones siguientes:

- Para especificar que GPMC debe utilizar los archivos .adm locales, seleccione Predeterminado. Si un archivo .adm no se encuentra localmente, GPMC buscará en la carpeta de objetos de directiva de grupo (GPO) de la carpeta sysvol.
- Para especificar una ubicación personalizada que tenga prioridad sobre las ubicaciones predeterminadas, seleccione Personalizada e introduzca la ubicación en la que se almacenan los archivos .adm.

Este procedimiento se aplica sólo a los archivos .adm, no a los nuevos archivos ADMX, que se introdujeron en Windows Vista®. La ubicación de archivos ADMX no se puede configurar. GPMC leerá automáticamente los archivos ADMX del almacén local o el almacén central basado en el dominio.

En la ficha General, seleccione una de las opciones siguientes:

- Para mostrar solamente bosques o dominios que tengan confianza bidireccional con el dominio del usuario, seleccione Habilitar detección de confianza. Esta configuración está activada de forma predeterminada.
- Para mostrar nombres de controlador de nombres de dominio entre paréntesis después de cada dominio en GPMC, seleccione Mostrar controladores de dominio después de los nombres de dominio.
- Para mostrar un cuadro de diálogo de confirmación que distinga entre GPO y vínculos de GPO cada vez que se selecciona un GPO o vínculo de GPO en GPMC, seleccione Mostrar diálogo de confirmación para distinguir entre los GPO y los vínculos de GPO. Esta configuración está activada de forma predeterminada.

La Consola de administración de directivas de grupo (GPMC) usa archivos con una extensión .adm, .admx y .adml para mostrar los nombres descriptivos de las configuraciones de directivas cuando genera informes HTML para GPO, Modelado de directivas de grupo y Resultados de directivas de grupo. Estas opciones permiten controlar la ubicación en la que GPMC lee sólo archivos .adm.

Si agrega o modifica un archivo .adm o ADMX en una ubicación existente, deberá reiniciar GPMC para que GPMC muestre el cambio realizado en el archivo .adm o .admx al mostrar los informes HTML.

GPMC nunca copia los archivos .adm o ADMX en la carpeta sysvol.

Crear un objeto de directiva de grupo

Para crear un objeto de directiva de grupo

1. En el árbol de Consola de administración de directivas de grupo (GPMC), haga clic con el botón secundario en Objetos de directiva de grupo en el bosque y el dominio en el que desee crear un objeto de directiva de grupo (GPO).
2. Haga clic en Nuevo.
3. En el cuadro de diálogo Nuevo GPO, especifique un nombre para el nuevo GPO y, a continuación, haga clic en Aceptar.

Cuando se crea un GPO, dicho GPO no tiene ningún efecto hasta que se vincula a un sitio, dominio o unidad organizativa.

De manera predeterminada, sólo los administradores de dominio, los administradores de organización y los miembros del grupo de propietarios del creador de directivas de grupo pueden crear objetos de directiva de grupo.

Editar un objeto de directiva de grupo

Para editar un objeto de directiva de grupo

1. En el árbol de Consola de administración de directivas de grupo (GPMC), haga doble clic en Objetos de directiva de grupo en el bosque y el dominio que contienen el objeto de directiva de grupo (GPO) que desea editar.
2. Haga clic con el botón secundario en el GPO y, a continuación, haga clic en Modificar.
3. En el árbol de consola, modifique la configuración como corresponda.

El GPO de la directiva de dominio predeterminado y el GPO de la directiva de controladores de dominio predeterminados son vitales para el buen funcionamiento de un dominio. Se recomienda no modificar el GPO de la directiva de controladores de dominio predeterminados ni el GPO de la directiva de dominio predeterminado, excepto en los casos siguientes:

Se requiere que la directiva de cuenta se configure en el GPO de dominio predeterminado.

Si instala aplicaciones en controladores de dominio que requieren la modificación de las configuraciones de derechos de usuario o de auditoría, las modificaciones deben llevarse a cabo en el GPO de directiva de controladores de dominio predeterminados.

De manera predeterminada, sólo los administradores del dominio, los administradores de organización y los miembros del grupo de propietarios del creador de directivas de grupo pueden editar GPO.

Para modificar la configuración de la directiva IPsec en un GPO, debe ser miembro del grupo de administradores de dominio.

Para editar un GPO, también puede hacer clic con el botón secundario en el nombre del GPO en cualquier contenedor al que esté vinculado y, después, hacer clic en Modificar.

Buscar un objeto de directiva de grupo

Para buscar un objeto de directiva de grupo

1. En el árbol de consola de Consola de administración de directivas de grupo (GPMC), haga doble clic en el bosque que contiene el dominio donde desea buscar un objeto de directiva de grupo (GPO). Haga doble clic en Dominios, haga clic con el botón secundario en el dominio y, después, en Buscar.



2. En el cuadro de diálogo Buscar objetos de directiva de grupo, en el cuadro Buscar los GPO en este dominio, seleccione un dominio o Todos los dominios mostrados en este bosque.
3. En el cuadro Elemento que se busca, seleccione el tipo de objeto en el que desea basar la búsqueda.

Si selecciona Grupo de seguridad, aparece el cuadro de diálogo Seleccionar usuarios, equipos o grupos. Especifique el tipo de objeto apropiado, la ubicación del objeto y el nombre de objeto y, a continuación, haga clic en Aceptar.

Puede elegir Vínculos de GPO en el menú desplegable Elemento que se busca para buscar GPO desvinculados y GPO vinculados entre dominios.

4. En el cuadro Condición, seleccione la condición que desea utilizar en la búsqueda.
5. En el cuadro Valor, seleccione o especifique el valor que desea utilizar para filtrar la búsqueda y, a continuación, haga clic en Agregar.
6. Repita los pasos 4 y 5 hasta finalizar la definición de todos los criterios de búsqueda y, a continuación, haga clic en Buscar.
7. Cuando se devuelvan los resultados de la búsqueda, realice una de las acciones siguientes:
 - Para guardar los resultados de la búsqueda, haga clic en Guardar resultados y, a continuación, en el cuadro de diálogo Guardar resultados de búsqueda de GPO, especifique el nombre de archivo para los resultados guardados y haga clic en Guardar.
 - Para ir al GPO encontrado en la búsqueda, haga doble clic en el GPO en la lista de resultados de la búsqueda.
 - Para borrar los resultados de la búsqueda, haga clic en Borrar.

También puede abrir el cuadro de diálogo de búsqueda si hace clic con el botón secundario en un bosque y, a continuación, hace clic en Buscar. En este caso, la búsqueda de GPO en este cuadro de dominio se establece de forma predeterminada en Todos los dominios mostrados en este bosque.

Si se habilita una configuración de directiva y a continuación se quitan todas las configuraciones de directiva de esa extensión, puede que los resultados de las búsquedas sean falsos positivos para determinados tipos de configuración. Esto sucede porque la extensión del GPO aparece como activa.

Agregar un dominio

Después de realizar este procedimiento, puede ver y administrar un dominio de Active Directory existente con la Consola de administración de directivas de grupo (GPMC).

Para agregar un dominio en GPMC

1. En el árbol de consola de GPMC, haga doble clic en el bosque al que desea agregar un dominio, haga clic con el botón secundario en Dominios y, a continuación, haga clic en Mostrar dominios.

2. En el cuadro de diálogo Mostrar dominios, active la casilla que aparece junto a cada dominio que desee agregar a GPMC y, a continuación, haga clic en Aceptar.

Al agregar un dominio a GPMC no se crea un nuevo dominio en Active Directory.

Los dominios siempre aparecen como interlocutores de otro, independientemente de su relación real.

Puede utilizar la función Agregar bosque para agregar dominios de confianza externos.

Especificar un controlador de dominio

Para especificar un controlador de dominio

1. En el árbol de consola de Consola de administración de directivas de grupo (GPMC), realice una de las siguientes acciones:
 - Si desea especificar el controlador de dominio para un dominio, haga doble clic en el bosque que contiene el dominio de interés, haga doble clic en Dominios, haga clic con el botón secundario en el dominio de interés y, a continuación, haga clic en Cambiar el controlador de dominio.
 - Si desea especificar el controlador de dominio para un sitio, haga doble clic en el bosque que contiene los sitios de interés, haga clic con el botón secundario en Sitios y, a continuación, haga clic en Cambiar el controlador de dominio. En la lista desplegable Buscar en este dominio del cuadro de diálogo Cambiar el controlador de dominio, seleccione el dominio en que reside el controlador de dominio.
2. Seleccione la opción de controlador de dominio del cuadro de diálogo Cambiar el controlador de dominio y haga clic en Aceptar.

Todas las operaciones realizadas en un dominio de los objetos de directiva de grupo, grupos de seguridad y unidades organizativas utilizan el controlador de dominio que especificó para el dominio.

Todas las operaciones realizadas en los vínculos a sitios utilizan el controlador de dominio que especificó para los sitios.

Agregar un bosque

Para agregar un bosque

Puede especificar el nombre NetBIOS o el nombre DNS de cualquier dominio del bosque. Si especifica un nombre NetBIOS, debe confirmar que éste se corresponde con el nombre DNS del dominio.

1. En el árbol de consola de Consola de administración de directivas de grupo (GPMC), haga clic con el botón secundario en Administración de directivas de grupo y, a continuación, haga clic en Agregar bosque.
2. En el cuadro de diálogo Agregar bosque, escriba el nombre DNS o NetBIOS de cualquier dominio del bosque y, a continuación, haga clic en Aceptar.



Al agregar un bosque a GPMC no se crea un nuevo bosque en Active Directory.

Los objetos de directiva de grupo no se pueden vincular fuera de un bosque.

La consola GPMC admite la administración de varios bosques desde la consola, cuando existe confianza entre el bosque de destino y el bosque del objeto de usuario.

Puede utilizar la función Agregar bosque para agregar dominios de confianza externos, aunque no haya establecido la confianza de bosque con todo el bosque. Sin embargo, debe existir confianza entre el dominio que desea agregar y el dominio de su objeto de usuario.

Agregar un sitio

Para agregar un sitio

1. En el árbol de consola de Consola de administración de directivas de grupo (GPMC), haga doble clic en el bosque al que desea agregar un sitio, haga clic con el botón secundario en Sitios y, a continuación, haga clic en Mostrar sitios.
2. En el cuadro de diálogo Mostrar sitios, active la casilla que aparece junto a cada sitio que desee mostrar en el árbol de consola y, a continuación, haga clic en Aceptar.

Los sitios no aparecen en el árbol de consola a no ser que se agreguen de forma explícita.

Ver, imprimir y guardar un informe de configuración de Directiva de grupo

Para ver, imprimir y guardar un informe de configuración de Directiva de grupo

1. En el árbol de consola de Consola de administración de directivas de grupo (GPMC), haga doble clic en el bosque que contiene el dominio o unidad organizativa que contiene el objeto de directiva de grupo (GPO) con el que desea trabajar y, después, seleccione el GPO.
2. Haga clic en la ficha Configuración para ver los informes de GPMC.
3. Si desea imprimir o guardar el informe, haga clic con el botón secundario en el informe de configuración del panel de resultados y realice una de las acciones siguientes:
 - Seleccione Imprimir para imprimir el informe.
 - Seleccione Guardar informe para guardar el informe.

Para personalizar la información que aparece en el informe, haga clic en Mostrar u Ocultar para ver exclusivamente los datos que desea ver o imprimir.

Para ver la descripción de una opción en Plantillas administrativas, haga clic en el nombre de opción en el informe.

Desde GPMC no es posible utilizar el teclado para desplazarse por un informe HTML. Para desplazarse por un informe HTML, guarde el informe en un archivo y posteriormente utilice Microsoft Internet Explorer para verlo.

Copiar un objeto de directiva de grupo

Puede copiar un objeto de directiva de grupo (GPO) con el método de arrastrar y colocar o con el método de hacer clic con el botón secundario. Ambos métodos se describen en este tema.

Para copiar un objeto de directiva de grupo (método de arrastrar y colocar)

1. En el árbol de consola de Consola de administración de directivas de grupo (GPMC), haga clic en el objeto de directiva de grupo (GPO) que desee copiar.
2. Realice una de las acciones siguientes:
 - Para crear una copia del GPO en el mismo dominio que el GPO de origen, arrastre y coloque el GPO que desea copiar en Objetos de directiva de grupo, seleccione una opción de permisos en Especificar permisos para el nuevo GPO y, después, haga clic en Aceptar.
 - Para crear una copia del GPO en un dominio diferente, haga doble clic en el dominio de destino y, después, arrastre y coloque el GPO que desea copiar en Objetos de directiva de grupo. Responda a todas las preguntas en el asistente de copia entre dominios que aparece y, a continuación, haga clic en Finalizar.

Para copiar un objeto de directiva de grupo (método de hacer clic con el botón secundario)

1. En el árbol de consola de GPMC, haga clic con el botón secundario en el GPO que desea copiar y, después, haga clic en Copiar.
2. Realice una de las acciones siguientes:
 - Para crear una copia del GPO en el mismo dominio del GPO de origen, haga clic con el botón secundario en Objetos de directivas de grupo, haga clic en Pegar, especifique los permisos para el nuevo GPO en el cuadro Copiar GPO y, a continuación, haga clic en Aceptar.
 - Para crear una copia del GPO en un dominio diferente, haga doble clic en el dominio de destino, haga clic con el botón secundario en Objetos de directivas de grupo y, a continuación, haga clic en Pegar. Responda a todas las preguntas en el asistente de copia entre dominios que aparece y, a continuación, haga clic en Finalizar.

Debe disponer de privilegios para crear GPO en el dominio de destino para completar este procedimiento.

Para realizar operaciones de copia en otro dominio, es posible que necesite especificar una tabla de migración

Importar la configuración de un objeto de directiva de grupo

Para importar la configuración de un objeto de directiva de grupo

1. En el árbol de consola de Consola de administración de directivas de grupo (GPMC), expanda el nodo Objetos de directiva de grupo del bosque y el



dominio que contienen el objeto de directiva de grupo (GPO) cuya configuración desea importar.

2. Haga clic con el botón secundario y haga clic en Importar configuración.
3. Siga las instrucciones del Asistente para importar configuración.

Para llevar a cabo este procedimiento, debe tener permisos de edición en el objeto GPO en el que desea importar la configuración.

Para realizar operaciones de importación en otro dominio o bosque, es posible que necesite especificar una tabla de migración.

Trabajar con tablas de migración

Las tablas de migración se utilizan cuando se copia o importa un objeto de directiva de grupo (GPO) de un dominio o bosque a otro. El principal problema al migrar objetos de directiva de grupo (GPO) entre dominios o bosques es que parte de la información del GPO es específica del dominio o bosque donde está definido el GPO. Al transferir el GPO a un nuevo dominio o bosque, puede que no siempre sea deseable o posible utilizar la misma configuración. Puede utilizar una tabla de migración para hacer referencia a usuarios, grupos, equipos y rutas UNC del GPO de origen con nuevos valores del GPO de destino.

Para crear tablas de migración, puede utilizar el Editor de tablas de migración.

- Rellenar automáticamente una tabla de migración desde un objeto de directiva de grupo
- Crear una tabla de migración

Vincular un objeto de directiva de grupo

Para vincular un GPO

1. En el árbol de consola de la Consola de administración de directivas de grupo (GPMC), localice el sitio, dominio o unidad organizativa al que desea vincular un objeto de directiva de grupo (GPO).
2. Realice una de las acciones siguientes:
 - Para vincular un GPO existente, haga clic con el botón secundario en el dominio o la unidad organizativa dentro del dominio y, a continuación, haga clic en Vincular un GPO existente. En el cuadro de diálogo Seleccionar GPO, haga clic en el GPO que desea vincular y, a continuación, en Aceptar.
 - Para vincular un nuevo GPO, haga clic con el botón secundario en un dominio o una unidad organizativa y, después, haga clic en Crear un GPO en este dominio y vincularlo aquí. En el cuadro Nombre, escriba un nombre para el nuevo GPO y, a continuación, haga clic en Aceptar.

Para vincular un GPO existente a un sitio, dominio o unidad organizativa, debe disponer del permiso Vincular objetos de directivas de grupo sobre ese sitio, dominio o unidad organizativa. De forma predeterminada, sólo los administradores de dominio y los administradores de organización tienen este privilegio para dominios y unidades organizativas. Los administradores de dominio y los administradores de organización del dominio raíz del bosque disponen de este privilegio para los sitios.

Para crear y vincular un GPO, debe disponer de permisos Vincular objetos de directivas de grupo sobre el dominio o unidad organizativa que desee, así como de permiso para crear objetos de directivas de grupo en ese dominio. De forma predeterminada, solamente los administradores de dominio, los administradores de organización y los propietarios del creador de directivas de grupo disponen de permiso para crear GPO.

La opción Crear un GPO en este dominio y vincularlo aquí no está disponible para los sitios. El administrador puede crear un GPO en cualquier dominio del bosque y, después, utilizar la opción Vincular un GPO existente para vincularlo al sitio.

Filtrar con grupos de seguridad

Para filtrar con grupos de seguridad

1. En el árbol de consola de Consola de administración de directivas de grupo (GPMC), expanda Objetos de directiva de grupo y haga clic en el objeto de directiva de grupo (GPO) al que desee aplicar el filtrado de seguridad.
2. En el panel de resultados, en la ficha **Ámbito**, haga clic en **Agregar**.
3. Escriba el nombre de objeto que desea seleccionar, escriba el nombre del usuario, grupo o equipo que desee agregar al filtro de seguridad. Haga clic en **Aceptar**.

Para garantizar que sólo los miembros del grupo o los grupos que agregó en el paso 3 pueden recibir la configuración de este GPO, deberá quitar Usuarios autenticados si este grupo aparece en la ficha **Ámbito**. Haga clic en la ficha **Ámbito**, seleccione este grupo y, después, haga clic en **Quitar**.

Debe disponer de permisos **Editar configuración**, **eliminar**, **modificar seguridad** sobre el GPO para realizar esos procedimientos.

La configuración de un GPO sólo se aplica a los usuarios y equipos que pertenecen al dominio o unidades organizativas a las que está vinculado el GPO, y que se especifican o pertenecen a un grupo especificado en **Filtrado de seguridad**.

Exigir un vínculo de objeto de directiva de grupo

Para exigir un vínculo de objeto de directiva de grupo

1. En el árbol de consola de Consola de administración de directivas de grupo (GPMC), haga doble clic en el bosque que contiene el dominio, sitio o unidad organizativa que contiene el vínculo que desea exigir y, después, realice una de las acciones siguientes:
 - Para aplicar un vínculo de GPO en el nivel de dominio, haga doble clic en **Dominios** y, a continuación, haga doble clic en el dominio que contiene el vínculo de GPO.
 - Para aplicar un vínculo de GPO en el nivel de unidad organizativa, haga doble clic en **Dominios** y, a continuación, haga doble clic en la unidad organizativa que contiene el vínculo de GPO.
 - Para aplicar un vínculo de GPO en el nivel de sitio, haga doble clic en **Sitios** y, a continuación, haga doble clic en el sitio que contiene el vínculo de GPO.



2. Haga clic con el botón secundario en el vínculo de GPO y, a continuación, haga clic en Exigido para habilitar o deshabilitar la obligatoriedad del vínculo. Una marca de verificación junto a Exigido indica que se exige el vínculo.

Debe disponer de permisos Vincular objetos de directiva de grupo del dominio, sitio o unidad organizativa que contiene el vínculo de GPO para realizar este procedimiento.

Para determinar si se exige un vínculo de GPO, también puede hacer clic en el vínculo de GPO y ver la información de la sección Vínculos de la ficha Ámbito.

Deshabilitar la configuración de usuario o del equipo en un objeto de directiva de grupo

Para deshabilitar la configuración de usuario o equipo en un objeto de directiva de grupo

1. En el árbol de Consola de administración de directivas de grupo (GPMC), haga doble clic en el bosque que contiene el dominio o unidad organizativa que contiene el objeto de directiva de grupo (GPO).
2. Haga doble clic en el dominio o la unidad organizativa.
3. Haga clic con el botón secundario en el GPO que contiene la configuración de usuario o equipo que desea deshabilitar, seleccione Estado de GPO y, a continuación, realice el siguiente procedimiento:
 - Haga clic en Configuración de usuario deshabilitada para deshabilitar la configuración de usuario para el GPO.
 - Haga clic en Configuración de equipo deshabilitada para deshabilitar la configuración de equipo para el GPO.
4. Una marca de verificación al lado de Configuración de usuario deshabilitada o Configuración de equipo deshabilitada indica que la configuración del usuario o del equipo está deshabilitada.

Debe tener permisos de Edición en el GPO para realizar este procedimiento.

El Estado de GPO también se puede modificar en la ficha Detalles del GPO.

Deshabilitar un vínculo de objeto de directiva de grupo

Para deshabilitar un vínculo de objeto de directiva de grupo

1. En el árbol de consola de Consola de administración de directivas de grupo (GPMC), haga doble clic para expandir el bosque que contiene el dominio, sitio o unidad organizativa que contiene el vínculo que desea deshabilitar y, después, realice una de las acciones siguientes:
 - Haga clic con el botón secundario en el vínculo de GPO. Una marca de verificación junto a Vínculo habilitado indica que el vínculo está actualmente habilitado.
 - Haga clic en Vínculo habilitado para deshabilitar el vínculo. No se mostrará ninguna marca de verificación cuando el vínculo se deshabilite.

Para completar este procedimiento, debe disponer del permiso Vincular objetos de directiva de grupo en el dominio, sitio o unidad organizativa.

Para determinar si un vínculo de GPO está habilitado, también puede hacer clic en el vínculo de GPO de la información de la sección Vínculos de la ficha Ámbito.

Bloquear herencia

Puede bloquear la herencia de un dominio o unidad organizativa. Al bloquear la herencia se evita que el nivel secundario herede de forma automática los objetos de directiva de grupo (GPO) que están vinculados a unidades organizativas, dominios o sitios superiores.

Para bloquear la herencia

1. En el árbol de consola de Consola de administración de directivas de grupo (GPMC), haga doble clic en el bosque que contenga el dominio o unidad organizativa en el que desee bloquear la herencia de vínculos de GPO y, a continuación, realice una de las acciones siguientes:
 - Para bloquear la herencia de los vínculos de GPO de todo el dominio, haga doble clic en Dominios y, después, haga clic con el botón secundario en el dominio.
 - Para bloquear la herencia de una unidad organizativa, haga doble clic en Dominios, haga doble clic en el dominio que contenga la unidad organizativa y, después, haga clic con el botón secundario en la unidad organizativa.
2. Haga clic en Bloquear herencia.

Para completar este procedimiento, debe disponer del permiso Vincular objetos de directiva de grupo para el dominio o la unidad organizativa.

Si un dominio o una unidad organizativa se configura para bloquear la herencia, aparecerá con un signo de exclamación azul en el árbol de consola.

Los vínculos de GPO que se aplican no se pueden bloquear desde el contenedor primario.

Determinar el conjunto resultante de directivas

Para determinar el conjunto resultante de directivas

1. En el árbol de consola de Consola de administración de directivas de grupo (GPMC), haga doble clic en el bosque en el que desea crear una consulta de resultados de directiva de grupo, haga clic con el botón secundario en Resultados de directiva de grupo y, a continuación, haga clic en Asistente para Resultados de directivas de grupo.
2. En el Asistente para Resultados de directivas de grupo, haga clic en Siguiente y escriba la información correspondiente.
3. Después de terminar el asistente, haga clic en Finalizar.
4. Si desea imprimir o guardar el informe, haga clic con el botón secundario en el informe de configuración del panel de resultados y realice una de las acciones siguientes:



- Seleccione Imprimir para imprimir el informe.
- Seleccione Guardar informe para guardar el informe.

Para obtener acceso a los datos de Resultados de directivas de grupo para un usuario o un equipo, debe tener el permiso Leer para los datos de Resultados de directivas de grupo en el dominio o unidad organizativa que contiene el usuario o el equipo, o bien debe ser miembro de un grupo local de administradores en el equipo de destino.

Para personalizar la información que aparece en el informe, haga clic en Mostrar u Ocultar para ver exclusivamente los datos que desea ver o imprimir.

Desde GPMC no es posible utilizar el teclado para desplazarse por un informe HTML. Para desplazarse por un informe HTML, guarde el informe en un archivo y posteriormente utilice Internet Explorer para verlo.

Si abre una consola guardada anteriormente y desea guardar un informe de Modelado de directivas de grupo o de Resultados de directivas de grupo en XML, vuelva a ejecutar el informe utilizando la opción Volver a ejecutar consulta.

Para ver un informe guardado en un explorador web, debe utilizar Microsoft Internet Explorer® 6 o posterior.

Resultados de directiva de grupo sólo es compatible con equipos que ejecuten Microsoft Windows XP y posteriores.

Simular un conjunto resultante de directivas mediante Modelado de directivas de grupo

Para simular un conjunto resultante de directivas mediante Modelado de directivas de grupo

1. Abra la Consola de administración de directivas de grupo (GPMC). En el árbol de consola, haga doble clic en el bosque en el que desea crear una consulta de Modelado de directivas de grupo, haga clic con el botón secundario en Modelado de directivas de grupo y posteriormente haga clic en el Asistente para Modelado de directivas de grupo.
2. En el Asistente para Modelado de directivas de grupo, haga clic en Siguiente y, después, escriba la información adecuada.
3. Al finalizar, haga clic en Finalizar.
4. Si desea imprimir o guardar el informe, haga clic con el botón secundario en el informe de configuración del panel de resultados y realice una de las acciones siguientes:
 - Seleccione Imprimir para imprimir el informe.
 - Seleccione Guardar informe para guardar el informe.

Para crear una consulta de Modelado de directivas de grupo, debe tener el permiso para realizar análisis de Modelado de directivas de grupo en el dominio o la unidad organizativa que contiene los objetos en los cuales desea ejecutar la consulta.

Modelado de directivas de grupo únicamente está disponible si al menos un controlador de dominio del bosque ejecuta Microsoft Windows Server 2003.

Para personalizar la información que aparece en el informe, haga clic en Mostrar u Ocultar para ver exclusivamente los datos que desea ver o imprimir.

Desde GPMC no es posible utilizar el teclado para desplazarse por un informe HTML. Para desplazarse por un informe HTML, guarde el informe en un archivo y posteriormente utilice Microsoft Internet Explorer para verlo.

Si abre una consola guardada anteriormente y desea guardar un informe de Modelado de directivas de grupo o de Resultados de directivas de grupo en XML, vuelva a ejecutar el informe utilizando la opción Volver a ejecutar consulta.

Para ver un informe guardado en un explorador web, debe utilizar Microsoft Internet Explorer 6 o posterior.

Delegar permisos para vincular objetos de directiva de grupo

Para delegar permisos para vincular objetos de directiva de grupo

1. En el árbol de consola de Consola de administración de directivas de grupo (GPMC), realice una de las siguientes acciones:
 - Para delegar el permiso para vincular objetos de directiva de grupo (GPO) al dominio o a una unidad organizativa, haga clic en el dominio o la unidad organizativa.
 - Para delegar permisos para vincular los GPO a un sitio, haga clic en el sitio.
2. En el panel de resultados, haga clic en la ficha Delegación.
3. En el cuadro de lista desplegable Permiso, seleccione Vincular objetos de directiva de grupo. Haga clic en Agregar.
4. En el cuadro de diálogo Seleccionar usuarios, equipos o grupos, haga clic en Tipos de objetos, seleccione los tipos de objetos en los que desea delegar permisos para el dominio, sitio o unidad organizativa y, después, haga clic en Aceptar.
5. Haga clic en Ubicaciones, seleccione Todo el directorio, o bien el dominio o la unidad organizativa que contiene el objeto en el que desea delegar los permisos y, a continuación, haga clic en Aceptar.
6. En el cuadro Escriba el nombre de objeto a seleccionar, especifique el nombre del objeto en el que desea delegar los permisos mediante una de las siguientes acciones:
 - Si conoce el nombre, escríbalo y haga clic en Aceptar.
 - Para buscar el nombre, haga clic en Opciones avanzadas, escriba los criterios de búsqueda, haga clic en Buscar ahora, escriba el nombre en el cuadro de lista, haga clic en Aceptar y vuelva a hacer clic en Aceptar.
7. En el cuadro de diálogo Agregar grupo o usuario, en la lista desplegable Permisos, seleccione el nivel en el que desea que se apliquen los permisos para este grupo o usuario y, a continuación, haga clic en Aceptar.

Para delegar permisos para vincular los GPO a un sitio, dominio o unidad organizativa, debe tener habilitada la opción Modificar permisos en ellos. De manera



predeterminada, sólo los Administradores de dominio y los Administradores de empresa cuentan con este permiso.

Los usuarios y grupos con permiso para vincular los GPO a sitios, dominios o unidades organizativas específicos pueden vincular GPO, cambiar el orden de los vínculos y configurar el bloqueo de herencia en dichos sitios, dominios o unidades organizativas.

No puede quitar grupos y usuarios que heredan permisos de un contenedor principal.

Preguntas de Repaso

1. Crea directivas para:
 - a. Cambiar el fondo de todos los escritorios de los clientes
 - b. Eliminar el acceso al panel de control de los clientes.
 - c. Redireccionar la carpeta mis documentos a una carpeta de red.
2. Desarrolle la siguiente actividad: Crear y configurar objetos de directiva de grupo (GPO)
 - a. Haga clic en Inicio, seleccione Herramientas administrativas, haga clic con el botón secundario del mouse en Administración de directivas de grupo y, a continuación, haga clic en Ejecutar como.
 - b. En el cuadro de diálogo Ejecutar como, haga clic en El siguiente usuario, escriba un nombre de usuario de SuDominio\Administrador con la contraseña P@ssw0rd y, a continuación, haga clic en Aceptar.
 - c. Expanda Forest (Bosque), expanda Domains (Dominios), expanda su dominio, expanda Group Policy Objects (Objetos de directiva de grupo), haga clic con el botón secundario en Group Policy Objects (Objetos de directiva de grupo) y, a continuación, haga clic en Nuevo.
 - d. Escriba EjercicioGPO como el nombre de su GPO y, a continuación, haga clic en OK (Aceptar).
 - e. Haga clic con el botón secundario en su nombre de dominio, haga clic en Link an Existing GPO (Vincular un GPO existente), haga clic en EjercicioGPO y, a continuación, en OK (Aceptar).
 - f. Haga clic con el botón secundario en EjercicioGPO y, a continuación, en Edit (Editar).
 - g. En Editor de objetos de directiva de grupo, en Configuración de usuario, expanda Plantillas administrativas y, a continuación, haga clic en Menú Inicio y barra de tareas.
 - h. En el panel de detalles, haga doble clic en Quitar el menú Ejecutar del menú Inicio, haga clic en Habilitada y, a continuación, haga clic en Aceptar.
 - i. En el panel de detalles, haga doble clic en Quitar el comando Apagar e impedir el acceso al mismo, haga clic en Habilitada y, a continuación, haga clic en Aceptar.
 - j. Cierre el Editor de objetos de directiva de grupo.
 - k. En Administración de directivas de grupo, expanda y haga clic con el botón secundario en WMI Filters (Filtros WMI) y, a continuación, haga clic en New (Nuevo).
 - l. Escriba EjercicioFiltro como el nombre del filtro WMI, haga clic en Add (Agregar), escriba una consulta adecuada para recuperar la información requerida, haga clic en OK (Aceptar) y, a continuación, haga clic en Save



Mantenimiento la operatibilidad del servidor

En este capítulo trataremos:

- Identificar las características que deben observarse continuamente en el servidor
- Aprenderá a utilizar de forma básica las herramientas de mantenimiento del Servidor

Introducción:

El Monitor de confiabilidad y rendimiento de Windows es un complemento de Microsoft Management Console (MMC) que proporciona herramientas para analizar el rendimiento del sistema.



Introducción al Monitor de confiabilidad y rendimiento de Windows

El Monitor de confiabilidad y rendimiento de Windows es un complemento de Microsoft Management Console (MMC) que proporciona herramientas para analizar el rendimiento del sistema. Desde una sola consola puede supervisar el rendimiento de las aplicaciones y del hardware en tiempo real, personalizar qué datos desea recopilar en los registros, definir umbrales para alertas y acciones automáticas, generar informes y ver datos de rendimientos pasados en una gran variedad de formas.

El Monitor de confiabilidad y rendimiento combina la funcionalidad de herramientas independientes anteriores, incluidos Registros y alertas de rendimiento (PLA), Server Performance Advisor (SPA) y Monitor de sistema. Proporciona una interfaz gráfica para la personalización de conjuntos de recopiladores de datos y sesiones de seguimiento de eventos.

El Monitor de confiabilidad y rendimiento de Windows está formado por tres herramientas de supervisión: Vista de recursos, Monitor de rendimiento y Monitor de confiabilidad. La recopilación y el registro de los datos se realiza mediante conjuntos de recopiladores de datos.

Para iniciar el Monitor de confiabilidad y rendimiento de Windows

Haga clic en Inicio, haga clic en el cuadro Iniciar búsqueda, escriba perfmon y presione ENTRAR.

Vista de recursos

La página principal del Monitor de confiabilidad y rendimiento de Windows es la pantalla Vista de recursos. Al ejecutar el Monitor de confiabilidad y rendimiento de Windows como miembro del grupo local Administradores, puede supervisar el uso y el rendimiento de la CPU, el disco, la red y los recursos de memoria en tiempo real. Para obtener más detalles, incluida información sobre qué procesos utilizan determinados recursos, expanda los cuatro recursos.

Monitor de sistema

El Monitor de rendimiento muestra los contadores de rendimiento de Windows integrados, bien en tiempo real o como una manera de revisar los datos históricos. Puede agregar contadores de rendimiento al Monitor de rendimiento arrastrando y soltando, o creando conjuntos de recopiladores de datos personalizados. Incluye varias vistas de gráficos que le permiten revisar visualmente los datos de registro del rendimiento. Es posible crear vistas personalizadas en el Monitor de rendimiento que se pueden exportar como conjuntos de recopiladores de datos y ser utilizados con características de rendimiento y registro.

Monitor de confiabilidad

El Monitor de confiabilidad ofrece una introducción de la estabilidad del sistema y análisis de tendencias con información detallada sobre eventos individuales que pueden afectar a la estabilidad general del sistema, por ejemplo, instalaciones de software, actualizaciones del sistema operativo y errores de hardware. Comienza recopilando los datos en el momento en el que se instala el sistema.

Acceso a las características del Monitor de confiabilidad y rendimiento

Los miembros del grupo local Administradores, o de un grupo equivalente, pueden usar todas las características del Monitor de confiabilidad y rendimiento de Windows. En la siguiente lista se resumen las características a las que pueden obtener acceso los miembros de otros grupos:

Miembros del grupo Usuarios

- Pueden abrir archivos de registro para verlos en el Monitor de rendimiento y pueden cambiar las propiedades de pantalla del Monitor de rendimiento durante la visualización de datos históricos.
- Pueden usar el Monitor de confiabilidad.
- No pueden crear ni modificar conjuntos de recopiladores de datos, no pueden usar la Vista de recursos ni pueden ver datos de rendimiento en tiempo real en el Monitor de rendimiento.
- No se puede configurar un conjunto de recopiladores de datos para que se ejecute como un miembro del grupo Usuarios.

Miembros del grupo Usuarios del monitor de sistema

- Puede usar todas las características que están disponibles para el grupo Usuarios.
- Pueden ver datos de rendimiento en tiempo real en el Monitor de rendimiento y pueden cambiar las propiedades de pantalla del Monitor de rendimiento durante la visualización de datos en tiempo real.
- No pueden crear ni modificar conjuntos de recopiladores de datos ni pueden usar la Vista de recursos.
- No se puede configurar un conjunto de recopiladores de datos para que se ejecute como un miembro del grupo Usuarios del monitor de sistema.

Miembros del grupo Usuarios del registro de rendimiento

- Puede usar todas las características que están disponibles para el grupo Usuarios del monitor de sistema.
- Pueden crear y modificar conjuntos de recopiladores de datos después de que se asigne al grupo el derecho de usuario Iniciar sesión como proceso por lotes, tal y como se describe en Habilitar el registro para miembros del grupo Usuarios del registro de rendimiento.
- Si es miembro del grupo Usuarios del registro de rendimiento, deberá configurar los conjuntos de recopiladores de datos que cree para que se ejecuten bajo sus propias credenciales.
- No pueden usar el proveedor de seguimiento del kernel de Windows en conjuntos de recopiladores de datos ni pueden usar la Vista de recursos.



Usar el Monitor de confiabilidad para solucionar problemas

El Monitor de confiabilidad le muestra inmediatamente el historial de la estabilidad del sistema y le permite ver diariamente detalles de los eventos que tienen algún tipo de impacto sobre la confiabilidad. Este tema le ayuda a entender los resultados y a realizar los pasos necesarios para mejorar la confiabilidad en función de lo que aprenda.

Gráfico de estabilidad del sistema

El Monitor de confiabilidad mantiene hasta un año del historial de los eventos que afectan a la estabilidad y confiabilidad del sistema. El Gráfico de estabilidad del sistema muestra un gráfico desplazable organizado por fechas.

La mitad superior del Gráfico de estabilidad del sistema muestra un gráfico del índice de estabilidad. En la mitad inferior del gráfico, cinco filas realizan un seguimiento de los eventos de confiabilidad que contribuyen a la medición de la estabilidad del sistema o que proporcionan información relacionada con la instalación y desinstalación del software. Cuando se detectan uno o más eventos de confiabilidad de cada tipo, aparece un icono en la columna correspondiente a esa fecha.

- En el caso de instalaciones y desinstalaciones de software, un icono de información indica que se produjo un evento correcto de ese tipo, o un icono de advertencia indica que se produjo un error de ese tipo.
- En el caso de los demás tipos de evento de confiabilidad, un icono de error indica que se produjo un error de ese tipo.

Si hay disponibles más de 30 días de datos, puede usar la barra de desplazamiento situada en la parte inferior del Gráfico de estabilidad del sistema para buscar las fechas que quedan fuera del rango visible.

Visualización de datos históricos

El Monitor de confiabilidad muestra los datos de la fecha más reciente de manera predeterminada.

Para ver los datos de una fecha concreta, haga clic en la columna correspondiente a esa fecha en el Gráfico de estabilidad del sistema o haga clic en el menú desplegable de fechas para seleccionar una fecha diferente.

Para ver todos los datos históricos disponibles, haga clic en el menú desplegable de fechas y haga clic en Seleccionar todo.

Si hay disponibles más de 30 días de datos, también puede usar la barra de desplazamiento situada en la parte inferior del Gráfico de estabilidad del sistema para examinar las fechas que quedan fuera del rango visible.

Informe de estabilidad del sistema

El Informe de estabilidad del sistema le ayuda a identificar los cambios que contribuyen al índice de estabilidad inferior identificando eventos de confiabilidad. Haga clic en el signo más de la barra de título de cada categoría de eventos de confiabilidad para ver los eventos.

Si ha hecho clic en la columna de una fecha en el Gráfico de estabilidad del sistema, el Informe de estabilidad del sistema mostrará los eventos que se han producido

desde esa fecha. Para ver todos los eventos o elegir una fecha que queda fuera del rango visible en el Gráfico de estabilidad del sistema, haga clic en el menú desplegable de fechas situado en la esquina superior derecha de la ventana y utilice el calendario, o seleccione Todas las fechas.

Eventos de confiabilidad

Los eventos de confiabilidad que se registran en el Informe de estabilidad del sistema son los siguientes:

Cambios del reloj del sistema

En esta categoría se realiza un seguimiento de los cambios significativos que han tenido lugar en la hora del sistema.

Esta categoría no aparece en el Informe de estabilidad del sistema a menos que se seleccione un día en el que se produjo un cambio del reloj significativo. En este caso aparecerá un icono de información en el Gráfico de estabilidad del sistema para cualquier día en el que se haya producido un cambio significativo del reloj.

Tipo de datos	Descripción
Hora anterior	Especifica la fecha y la hora anteriores al cambio del reloj.
Hora nueva	Especifica la fecha y la hora seleccionadas durante el cambio del reloj.
Fecha	Especifica la fecha (en función de la hora nueva) en la que se produjo el cambio del reloj.

Instalaciones y desinstalaciones de software

En esta categoría se realiza el seguimiento de las instalaciones y desinstalaciones de software, incluidos los componentes de los sistemas operativos, las actualizaciones de Windows, los controladores y las aplicaciones.

Tipo de datos	Descripción
Software	Especifica el sistema operativo, el nombre de la aplicación, el nombre de la actualización de Windows o el nombre del controlador.
Versión	Especifica la versión del sistema operativo, de la aplicación o del controlador (este campo no está disponible en el caso de las actualizaciones de Windows).
Actividad	Indica si el evento es una instalación o desinstalación.
Estado de actividad	Indica si la acción se realizó correctamente o si se produjo un error.
Fecha	Especifica la fecha de la acción.

Errores de aplicación

En esta categoría se realiza un seguimiento de los errores de aplicación, incluida la finalización de una aplicación que no responde o de una aplicación que ha dejado de funcionar.



Tipo de datos	Descripción
Aplicación	Especifica el nombre del programa ejecutable de la aplicación que dejó de funcionar o de responder.
Versión	Especifica el número de versión de la aplicación.
Tipo de error	Indica si la aplicación dejó de funcionar o de responder.
Fecha	Especifica la fecha en la que se produjo el error de la aplicación.

Errores de hardware

En esta categoría se realiza un seguimiento de los errores de disco y memoria.

Tipo de datos	Descripción
Tipo de componente	Indica el componente donde se produjo el error.
Dispositivo	Identifica el dispositivo que tiene errores.
Tipo de error	Indica el tipo de error que se ha producido.
Fecha	Especifica la fecha en la que se produjo el error de hardware.

Errores de Windows

En esta categoría se realiza un seguimiento de los errores de arranque y del sistema operativo.

Tipo de datos	Descripción
Tipo de error	Indica si el evento es un error de arranque o un bloqueo del sistema operativo.
Versión	Identifica las versiones del sistema operativo y del service pack
Detalles del error	Proporciona detalles del tipo de error, que puede ser: <ul style="list-style-type: none"> • Error del sistema operativo: indica el código de detención. • Error de arranque: indica el código de motivo.
Fecha	Especifica la fecha en la que se produjo el error de Windows.

Errores varios

En esta categoría se realiza un seguimiento de los errores que tienen un impacto en la estabilidad y que no se pueden incluir en ninguna de las categorías anteriores, incluidos cierres no esperados del sistema operativo.

Tipo de datos	Descripción
Tipo de error	Indica que el sistema se cerró de manera incorrecta.
Versión	Identifica las versiones del sistema operativo y del service pack
Detalles del error	Indica que el equipo no se cerró de manera correcta.
Fecha	Especifica la fecha en la que se produjeron los errores varios.

Uso de los resultados del Monitor de confiabilidad

Si el Monitor de confiabilidad informa de eventos de error de confiabilidad frecuentes, utilice los datos que proporcione para decidir qué pasos puede realizar para mejorar la estabilidad del sistema operativo.

Errores de software

Si el Monitor de confiabilidad informa de errores de aplicación coherentes, errores de Windows o errores de instalación o desinstalación de software, es posible que necesite actualizar la aplicación o los componentes del sistema operativo que generan errores. Utilice el panel de control de Windows Update y el panel de control de Informes de problemas y soluciones para buscar las actualizaciones de las aplicaciones que pueden resolver los problemas.

Si la aplicación que genera el error no es un producto de Microsoft y no existe ninguna solución en el panel de control de Informes de problemas y soluciones, pruebe a buscar actualizaciones de software en el sitio web del fabricante de la aplicación.

Errores de hardware

Si el Monitor de confiabilidad informa de errores de hardware coherentes, es posible que el equipo tenga problemas técnicos graves que no pueda resolver ninguna actualización de software. Póngase en contacto con el fabricante del dispositivo de hardware para obtener otros pasos e información que ayuden a solucionar el problema.

Perspectiva general

Además de identificar los problemas con aplicaciones y componentes de hardware individuales, el gráfico de Monitor de confiabilidad le permite ver inmediatamente si los cambios significativos en la estabilidad comenzaron al mismo tiempo.

Puesto que puede ver toda la actividad de una sola fecha en un informe, puede tomar decisiones fundamentadas sobre cómo solucionar el problema. Por ejemplo, si se informa de errores de aplicación frecuentes que comenzaron a producirse la misma fecha en que aparecieron errores de memoria en la sección Hardware, como primer paso, puede reemplazar la memoria defectuosa. Si se detienen los errores de la aplicación, ello puede significar que se trataba de problemas al obtener acceso a la memoria. Si los errores de la aplicación continúan, el siguiente paso sería reparar las instalaciones.

Para iniciar el Monitor de confiabilidad:

1. Haga clic en Inicio, haga clic en el cuadro Iniciar búsqueda
2. Escriba perfmon y presione ENTRAR
3. Expanda Confiabilidad y rendimiento
4. Expanda Herramientas de supervisión
5. Haga clic en Monitor de confiabilidad.

Para iniciar los paneles de control de Windows Update e Informes de problemas y soluciones, haga clic en Inicio, Panel de control, Sistema y mantenimiento y en Windows Update o Informes de problemas y soluciones. En la Vista clásica del panel de control, los paneles de control se organizan de manera alfabética



Nuevas características del Monitor de confiabilidad y rendimiento de Windows

Conjuntos de recopiladores de datos

Una nueva característica importante del Monitor de confiabilidad y rendimiento de Windows es el Conjunto de recopiladores de datos, que agrupa los recopiladores de datos en elementos reutilizables que se pueden utilizar con diferentes escenarios de supervisión del rendimiento. Una vez que se almacena un grupo de recopiladores de datos como un conjunto de recopiladores de datos, operaciones tales como la programación se pueden aplicar a todo el conjunto mediante un solo cambio de las propiedades.

El Monitor de confiabilidad y rendimiento de Windows también incluye plantillas de conjunto de recopiladores de datos que ayudan a los administradores de sistemas a comenzar a recopilar inmediatamente los datos de rendimiento específicos de una función de servidor o un escenario de supervisión.

Asistentes y plantillas para crear registros

Ahora puede agregar contadores a archivos de registro y programar el inicio, la detención y la duración de los mismos a través de una interfaz de asistente. Además, puede guardar esta configuración como plantilla para recopilar el mismo registro en equipos subsiguientes sin repetir la selección del recopilador de datos ni programar los procesos. Se han incorporado al Monitor de confiabilidad y rendimiento de Windows las características Registros y alertas de rendimiento para que se puedan usar con cualquier conjunto de recopiladores de datos.

Vista de recursos

La página principal del Monitor de confiabilidad y rendimiento de Windows es la nueva pantalla de Vista de recursos, que proporciona una presentación gráfica en tiempo real del uso de la CPU, el disco, la red y la memoria. La expansión de cada uno de estos elementos supervisados permite a los administradores de sistemas identificar qué procesos están utilizando los distintos recursos. En versiones anteriores de Windows, estos datos específicos de los procesos en tiempo real únicamente estaban disponibles de un modo limitado en el Administrador de tareas.

Monitor de confiabilidad

El Monitor de confiabilidad calcula un índice de estabilidad del sistema que refleja si problemas no esperados redujeron la confiabilidad del sistema. Un gráfico del índice de estabilidad en el tiempo identifica rápidamente las fechas en las que comenzaron a producirse los problemas. El informe de estabilidad del sistema que se acompaña proporciona detalles para ayudarle a resolver la causa raíz de la disminución de la estabilidad. La visualización de los cambios realizados en el sistema (instalación o desinstalación de aplicaciones, actualizaciones del sistema operativo, o adición o modificación de controladores) en paralelo con los errores (de aplicación, sistema operativo o hardware) le permite desarrollar una estrategia para resolver los problemas.

Configuración de propiedades unificada para toda la recopilación de datos, incluida la programación

Si está creando un conjunto de recopiladores de datos para un solo uso o para registrar la actividad constantemente, la interfaz usada para la creación, programación y modificación es la misma. Si un conjunto de recopiladores de datos resulta ser útil para supervisar el rendimiento en el futuro, no es necesario que se vuelva a crear. Puede reconfigurarlo o copiarlo como una plantilla.

Informes de diagnóstico fácil de usar

Los usuarios de Server Performance Advisor de Windows Server 2003 ahora pueden encontrar los mismos tipos de informes de diagnóstico en el Monitor de confiabilidad y rendimiento de Windows Vista. El tiempo necesario para generar los informes se ha mejorado y los informes pueden crearse a partir de datos recopilados con cualquier conjunto de recopiladores de datos. Esto permite a los administradores de sistemas repetir informes y evaluar cómo los cambios han afectado al rendimiento o a las recomendaciones sobre los informes.

Supervisar la actividad del sistema con Vista de recursos

La página principal del Monitor de confiabilidad y rendimiento de Windows es la pantalla Vista de recursos. En Vista de recursos, puede supervisar el uso de la CPU, el disco, la red y la memoria en tiempo real.

- Iniciar Vista de recursos
- Identificar el uso de los recursos en Vista de recursos

Iniciar Vista de recursos

El mínimo requerido para completar este procedimiento es la pertenencia al grupo local Administradores o un grupo equivalente.

1. Haga clic en Inicio, haga clic en el cuadro Iniciar búsqueda
2. Escriba perfmon y presione ENTRAR. El Monitor de confiabilidad y rendimiento de Windows se iniciará con la pantalla de Vista de recursos.

También puede iniciar la Vista de recursos en su propia ventana; para ello escriba perfmon /res en el cuadro Iniciar búsqueda o en el símbolo del sistema y presione ENTRAR.

Si Vista de recursos no muestra datos en tiempo real cuando se inicia el Monitor de confiabilidad y rendimiento de Windows, haga clic en el botón Inicio verde situado en la barra de herramientas.

Si aparece el siguiente mensaje, seleccione Tomar control de la sesión.

Otra sesión de seguimiento ya está usando el proveedor de seguimiento del kernel de Windows. Si toma el control de éste, el propietario actual puede dejar de funcionar correctamente.

Si se deniega el acceso, significa que está ejecutando el Monitor de confiabilidad y rendimiento de Windows con credenciales insuficientes. Inicie sesión o ejecute el programa como miembro del grupo Administradores.



Identificar el uso de los recursos en Vista de recursos

Cuatro gráficos de desplazamiento en el panel Introducción a los recursos muestran el uso en tiempo real de la CPU, el disco, la red y la memoria del equipo local. Cuatro secciones expandibles incluidas debajo de los gráficos contienen detalles del nivel de proceso de cada recurso. Haga clic en las etiquetas de los recursos para obtener más información, o haga clic en un gráfico para expandir los detalles correspondientes.

Navegación por vista de recursos

Ordenar columnas por valor	Haga clic en la etiqueta del encabezado de columna para ordenar en orden ascendente. Haga clic en la etiqueta del encabezado de columna una segunda vez para ordenar en orden descendente.
Resaltar una instancia de aplicación	Haga clic en cualquier lugar de la fila de instancia de aplicación para seguir manteniendo el resaltado cuando cambie en la pantalla la posición de la instancia de aplicación

Detalles de Vista de recursos

Las tablas de detalles contienen la siguiente información.

Etiqueta	Descripción
CPU	La etiqueta CPU muestra en verde el porcentaje total de la capacidad de la CPU que está en uso, y en azul la frecuencia máxima de la CPU. Algunos equipos portátiles reducirán la frecuencia máxima de la CPU cuando el equipo no esté conectado a un sistema de alimentación de corriente alterna para reducir el uso de la batería.
• Imagen	Aplicación que utiliza recursos de la CPU.
• PID	Identificador de proceso de la instancia de la aplicación.
• Descripción	Nombre de la aplicación.
• Subprocesos	Número de subprocesos actualmente activos de la instancia de la aplicación.
• CPU	Ciclos de la CPU actualmente activos de la instancia de la aplicación.
• Uso medio de CPU	Carga media de la CPU durante los últimos 60 segundos resultante de la instancia de la aplicación, expresada como un porcentaje de la capacidad total de la CPU.

Etiqueta	Descripción
Disco	La etiqueta del disco muestra la E/S total actual en color verde, y el máximo porcentaje de tiempo activo en color azul.
• Imagen	Aplicación que utiliza recursos del disco.

• PID	Identificador de proceso de la instancia de la aplicación.
• Archivo	Archivo que está siendo leído y/o escrito por la instancia de la aplicación.
• Lectura	Velocidad actual (en Bytes/min.) a la que la instancia de la aplicación lee los datos del archivo.
• Escritura	Velocidad actual (en Bytes/min.) a la que la aplicación escribe los datos en el archivo.
• Prioridad de E/S	Prioridad de la tarea de E/S para la aplicación.
• Tiempo de respuesta	Tiempo de respuesta en milisegundos para la actividad del disco.

Etiqueta	Descripción
Red	La etiqueta Red muestra en verde el tráfico de la red total actual (en Kbps), y en azul el porcentaje de la capacidad de la red en uso.
• Imagen	Aplicación que utiliza recursos de la red.
• PID	Identificador de proceso de la instancia de la aplicación.
• Dirección	Dirección de red con la que el equipo local intercambia información. Se puede expresar en forma de nombre de equipo, dirección IP o nombre de dominio completo (FQDN).
• Enviar	Cantidad de datos (en Bytes/min.) que la instancia de la aplicación está enviando actualmente desde el equipo local a la dirección.
• Recibir	Cantidad de datos (en Bytes/min.) que la instancia de la aplicación está recibiendo actualmente desde la dirección.
• Total	Ancho de banda total (en Bytes/min.) que actualmente está enviando y recibiendo la instancia de la aplicación.

Etiqueta	Descripción
Memoria	La etiqueta Memoria muestra en verde los errores severos por segundo actuales, y en azul el porcentaje de la memoria física actualmente en uso.
• Imagen	Aplicación que utiliza recursos de la memoria.
• PID	Identificador de proceso de la instancia de la aplicación.
• Errores severos/min.	Número de errores severos por minuto actualmente procedentes de la instancia de la aplicación.
	Nota



- Un error severo (también denominado error de página) se produce cuando la página de la dirección a la que se hace referencia ha dejado de ser la memoria física y se ha intercambiado y está disponible desde un archivo de copia de seguridad en el disco. No se trata de un error. Sin embargo, un gran número de errores severos puede explicar el tiempo de respuesta lento de una aplicación si debe leer continuamente los datos desde el disco en lugar de desde la memoria física.

• Espacio de trabajo (KB)	Número de kilobytes actualmente residentes en la memoria de la instancia de la aplicación.
• Se puede compartir (KB)	Número de kilobytes del espacio de trabajo de la instancia de la aplicación que puede haber disponible para su uso por parte de otras aplicaciones.
• Privada (KB)	Número de kilobytes del espacio de trabajo de la instancia de la aplicación que se dedica al proceso.

Consideraciones adicionales

Para usar la Vista de recursos, es necesario ser miembro del grupo local Administradores o de un grupo equivalente.

Para iniciar la Vista de recursos, haga clic en Inicio, haga clic en el cuadro Iniciar búsqueda, escriba perfmon y presione ENTRAR.

Si Vista de recursos no muestra datos en tiempo real cuando se inicia el Monitor de confiabilidad y rendimiento de Windows, haga clic en el botón Inicio verde situado en la barra de herramientas.

Si aparece el siguiente mensaje, seleccione Tomar control de la sesión.

Otra sesión de seguimiento ya está usando el proveedor de seguimiento del kernel de Windows. Si toma control sobre él, el propietario actual puede dejar de funcionar correctamente.

Si se deniega el acceso, significa que está ejecutando el Monitor de confiabilidad y rendimiento de Windows con credenciales insuficientes. Inicie sesión o ejecute el programa como miembro del grupo Administradores.

Uso del Monitor de rendimiento

El Monitor de rendimiento es una herramienta de visualización sencilla pero eficaz que sirve para visualizar datos sobre el rendimiento, en tiempo real y desde archivos de registro. Con él podrá examinar los datos sobre el rendimiento en un gráfico, histograma o informe.

Para completar este procedimiento, lo mínimo que se necesita es pertenecer al grupo local Usuarios del registro de rendimiento, o un grupo equivalente.

Para iniciar el Monitor de rendimiento

1. Haga clic en Inicio, haga clic en el cuadro Iniciar búsqueda, escriba perfmon y presione ENTRAR.
2. En el árbol de navegación, expanda Herramientas de supervisión y, a continuación, haga clic en Monitor de rendimiento.

También puede usar el Monitor de rendimiento ver datos de rendimiento en tiempo real de un equipo remoto.

Para completar este procedimiento, lo mínimo que se necesita es pertenecer al grupo Usuarios del registro de rendimiento, o un grupo equivalente, del equipo de destino.

Para conectarse a un equipo remoto con el Monitor de rendimiento

1. Inicie el Monitor de rendimiento.
2. En el árbol de navegación, haga clic con el botón secundario en Confiabilidad y rendimiento y, a continuación, haga clic en Conectarse a otro equipo.
3. En el cuadro de diálogo Seleccionar equipo, escriba el nombre del equipo que desea supervisar o haga clic en Examinar para seleccionarlo en una lista.
4. Haga clic en Aceptar.

Para agregar los contadores de rendimiento desde un equipo remoto, debe habilitarse la excepción de firewall Registros y alertas de rendimiento en el equipo remoto. Además, los miembros del grupo Usuarios del registro de rendimiento también deben ser miembros del grupo Lectores del registro de eventos en el equipo remoto.

Configurar la pantalla del Monitor de rendimiento

Para completar este procedimiento, lo mínimo que se necesita es pertenecer al grupo local Usuarios del registro de rendimiento o Administradores, o un grupo equivalente.

Para configurar la pantalla del Monitor de rendimiento

1. Haga clic con el botón secundario en el área de la pantalla del Monitor de rendimiento y haga clic en Propiedades.
2. Realice los cambios de configuración deseados.
3. Para ver el efecto de los cambios sin volver a abrir el cuadro de diálogo Propiedades, puede hacer clic en Aplicar después de realizar cualquier modificación.
4. Al finalizar, haga clic en Aceptar.

Puede guardar la información en la pantalla del Monitor de rendimiento actual como una página web o una imagen.

Para guardar la pantalla del Monitor de rendimiento actual como página web

1. Haga clic con el botón secundario en el área de la pantalla del Monitor de rendimiento y haga clic en Guardar configuración como.
2. Elija un directorio en el que desee guardar el archivo.
3. Escriba un nombre para el archivo de visualización guardado y, a continuación, haga clic en Aceptar.



Para guardar la pantalla del Monitor de rendimiento actual como imagen

1. Haga clic con el botón secundario en el área de la pantalla del Monitor de rendimiento y haga clic en Guardar imagen como.
2. Elija un directorio en el que desee guardar el archivo.
3. Escriba un nombre para el archivo de visualización guardado y, a continuación, haga clic en Aceptar.

Consideraciones adicionales

1. También puede obtener acceso a las propiedades del Monitor de rendimiento presionando Ctrl+Q o haciendo clic en el botón Propiedades de la barra de herramientas.
2. Si no hay contadores en la pantalla actual, puede abrir el cuadro de diálogo Agregar contadores seleccionando la ficha Datos y haciendo clic en Agregar.
3. Puede abrir los archivos o las bases de datos de registro desde las propiedades del Monitor del sistema en la ficha Origen. Es posible abrir varios archivos de registro de manera simultánea.

Usar el Monitor de confiabilidad

El complemento Monitor de confiabilidad de Microsoft Management Console (MMC) proporciona una introducción a la estabilidad del sistema y detalles acerca de los eventos que tienen un impacto en la confiabilidad. Calcula el índice de estabilidad mostrado en el Gráfico de estabilidad del sistema durante la vigencia del sistema.

- Iniciar el Monitor de confiabilidad
- Ver el Monitor de confiabilidad en un equipo remoto
- Habilitar la recopilación de datos para el Monitor de confiabilidad
- Descripción del índice de estabilidad del sistema
- Usar el Monitor de confiabilidad para solucionar problemas

Iniciar el Monitor de confiabilidad

El Monitor de confiabilidad forma parte del complemento Monitor de confiabilidad y rendimiento de Windows para Microsoft Management Console (MMC).

Para completar este procedimiento, lo mínimo que se necesita es pertenecer al grupo local Usuarios, o un grupo equivalente.

Para abrir el Monitor de confiabilidad en Microsoft Management Console

1. Haga clic en Inicio, haga clic en el cuadro Iniciar búsqueda, escriba perfmon y presione ENTRAR.
2. En el árbol de navegación, expanda Confiabilidad y rendimiento, expanda Herramientas de supervisión y haga clic en Monitor de confiabilidad.

Ver el Monitor de confiabilidad en un equipo remoto

Puede ver los datos del Monitor de confiabilidad en un equipo remoto con Microsoft Management Console (MMC) si posee suficientes credenciales en el equipo remoto y si el Servicio de Registro remoto está habilitado y está ejecutándose en el equipo al que desea obtener acceso.

- Habilitar el Servicio de Registro remoto
- Abrir el Monitor de confiabilidad en un equipo remoto

La ubicación de los archivos de datos del Monitor de confiabilidad se almacena en el Registro. Sin acceso al Registro remoto, el Monitor de confiabilidad no puede abrir los datos en el equipo remoto.

Para completar este procedimiento, lo mínimo que se necesita es pertenecer al grupo local Administradores, o un grupo equivalente.

Habilitar la recopilación de datos para el Monitor de confiabilidad

El Monitor de confiabilidad utiliza datos que proporciona la tarea programada RACAgent. El Monitor de confiabilidad se iniciará mostrando una valoración del índice de estabilidad del sistema e información del evento concreto 24 horas después de la instalación del sistema.

La tarea programada RACAgent se ejecuta de manera predeterminada después de instalar el sistema operativo. Si está deshabilitada, debe habilitarse manualmente desde el complemento Programador de tareas para Microsoft Management Console (MMC).

Para completar este procedimiento, lo mínimo que se necesita es pertenecer al grupo local Administradores, o un grupo equivalente.

Para habilitar la tarea programada RACAgent

1. Haga clic en Inicio, haga clic en el cuadro Iniciar búsqueda, escriba `taskschd.msc` y, a continuación, presione ENTRAR.
2. En el panel de navegación, expanda Biblioteca del Programador de tareas, Microsoft y Windows y, a continuación, haga clic en RAC.
3. Haga clic con el botón secundario en RAC, haga clic en Ver y en Mostrar tareas ocultas.
4. Haga clic en RACAgent en el panel de resultados.

El nombre de la tarea RACAgent puede que no sea visible completamente. Si no puede encontrarlo, expanda la columna Nombre en el panel de resultados.

En el menú Acción, haga clic en Habilitar

Para llevar a cabo este procedimiento, debe ser miembro del grupo local Administradores, o un grupo equivalente.



Descripción del índice de estabilidad del sistema

En función de los datos recopilados durante la vida útil del sistema, cada fecha del Gráfico de estabilidad del sistema incluye un punto de gráfico que muestra la valoración del índice de estabilidad del sistema de ese día. El índice de estabilidad del sistema es un número que oscila entre 1 (mínima estabilidad) y 10 (máxima estabilidad) y consiste en una medición ponderada derivada del número de errores especificados vistos a lo largo de un período histórico sucesivo. Los eventos de confiabilidad del Informe de estabilidad del sistema describen los errores específicos..

- Los errores recientes tienen un mayor peso que los errores pasados, lo que permite con el tiempo reflejar una mejora en un Índice de estabilidad del sistema ascendente una vez que se ha resuelto un problema de confiabilidad.
- Los días en los que el sistema está apagado o en un estado de suspensión no se utilizan para calcular el índice de estabilidad del sistema.
- Si no hay suficientes datos para calcular un índice de estabilidad del sistema fijo, la línea del gráfico aparecerá punteada. Cuando se hayan registrado suficientes datos para generar un índice de estabilidad del sistema fijo, la línea del gráfico será sólida.
- Si hay algún cambio significativo en la hora del sistema, aparecerá un icono de información en el gráfico para cada día en el que se haya ajustado la hora del sistema.

Introducción al Programador de tareas

El complemento de MMC Programador de tareas le ayuda a programar tareas automatizadas que realizan acciones a una hora concreta o cuando se produce un determinado evento. Mantiene una biblioteca de todas las tareas programadas, proporcionando una vista organizada de las tareas y un punto de acceso cómodo para administrarlas. Desde la biblioteca, puede ejecutar, deshabilitar, modificar y eliminar tareas. La interfaz de usuario del Programador de tareas es un complemento de MMC que reemplaza la extensión del Explorador de tareas programadas en Windows XP, Windows Server 2003 y Windows 2000

Desencadenadores y acciones

Los dos conceptos clave implicados en la programación de una tarea son los desencadenadores y las acciones. Un desencadenador hace que se ejecute una tarea y la acción es el trabajo que se realiza cuando se ejecuta dicha tarea. Las acciones que puede realizar una tarea incluyen la ejecución de un programa, el envío de un mensaje de correo electrónico y la presentación de un cuadro de mensaje. Por ejemplo, puede enviar un mensaje de correo electrónico cuando se registre una determinada entrada de evento en el registro de eventos o cuando se ejecute un script de mantenimiento cuando un usuario inicie sesión en un equipo. Éstas son algunas de las instancias que pueden desencadenar la ejecución de una tarea: el inicio de un equipo, la entrada de un equipo en un estado de inactividad o el desbloqueo de una estación de trabajo por parte de un usuario. Además, puede programar una tarea para que se ejecute a una hora específica.

Desencadenadores

Al configurar una tarea, primero debe decidir lo que desencadenará el inicio de la misma. Un desencadenador es un conjunto de criterios que, si se cumplen, inicia la ejecución de una tarea. Los desencadenadores de una tarea se muestran en la ficha Desencadenadores del cuadro de diálogo Propiedades de tarea o Crear tarea. Puede usar un desencadenador basado en tiempo o en eventos para iniciar una tarea. Los desencadenadores basados en tiempo incluyen el inicio de una tarea a una hora concreta del día o el inicio de varias tareas de acuerdo con una programación diaria, semanal o mensual. Los desencadenadores basados en eventos inician una tarea en respuesta a unos determinados eventos del sistema. Por ejemplo, los desencadenadores basados en eventos se pueden establecer para que inicien una tarea cuando se inicie el sistema, cuando un usuario inicie sesión en el equipo, o cuando el equipo entre en un estado de inactividad. Cada tarea puede contener uno o más desencadenadores, lo que permite que la tarea pueda iniciarse de muchas maneras. Si una tarea dispone de varios desencadenadores, la tarea se iniciará cuando se active cualquiera de los desencadenadores.

Configuración del desencadenador

Cada desencadenador contiene una configuración que determina los criterios de activación del mismo. Es posible establecer una configuración avanzada adicional para cada desencadenador, lo que se explica en la sección Configuración avanzada incluida a continuación. A la configuración del desencadenador se obtiene acceso desde el cuadro de diálogo Editar desencadenador o Nuevo desencadenador, que se ve haciendo clic en el botón Editar o Nuevo de la ficha Desencadenadores del cuadro de diálogo Propiedades de tarea o Crear tarea.

La siguiente lista describe cada uno de los desencadenadores y su configuración.

- Según una programación
Este desencadenador hace que la tarea se ejecute según una programación y la configuración del desencadenador le permite establecer la programación. Puede elegir programar la tarea a la vez, diaria, semanal o mensualmente. La hora que establezca debe ser relativa a la zona horaria que esté establecida en el equipo que ejecute la tarea. Active la casilla Universal para lograr que la hora sea relativa a la hora universal coordinada (UTC) en lugar de a la zona horaria que esté establecida en el equipo que ejecute la tarea. Utilice la configuración Universal cuando desee coordinar un conjunto de tareas para que se ejecuten simultáneamente en varias zonas horarias.

Si selecciona el botón de radio Una vez, debe elegir una fecha y una hora para desencadenar la tarea.

Si selecciona el botón de radio Diariamente, debe elegir el intervalo de periodicidad de la tarea así como la fecha y la hora a la que se iniciará la tarea. Un intervalo de 1 genera una programación diaria y un intervalo de 2 genera una programación del tipo un día sí y otro no. La tarea se iniciará a la hora especificada cada día.

Si selecciona el botón de radio Semanalmente, debe elegir el intervalo de periodicidad de la tarea, la fecha y la hora a la que se iniciará la tarea, y los días



de la semana en los que se iniciará la tarea. Un intervalo de 1 genera una programación semanal y un intervalo de 2 genera una programación del tipo una semana sí y otra no. La tarea se iniciará a la hora especificada en cada uno de los días especificados.

Si selecciona el botón de radio Mensualmente, debe elegir los meses en los que desea iniciar la tarea así como las semanas del mes y los días de la semana de cada mes en los que desea iniciar la tarea. También puede especificar que desea iniciar una tarea el último día de cada mes.

- **Al iniciar la sesión**
Este desencadenador hace que la tarea se ejecute cuando un usuario inicia sesión en el equipo y la configuración del desencadenador le permite especificar la tarea que debe desencadenarse cuando cualquier usuario inicie sesión en el equipo o cuando un usuario concreto o un miembro de un grupo de usuarios inicie sesión.
- **Al iniciar el sistema**
Este desencadenador hace que la tarea se ejecute cuando el equipo se inicia. La única configuración de este desencadenador es la configuración avanzada descrita en la sección Configuración avanzada incluida más adelante.
- **Al estar inactivo**
Este desencadenador hace que la tarea se ejecute después de que el equipo entre en un estado de inactividad; la configuración de la inactividad puede establecerse desde la ficha Condiciones en el cuadro de diálogo Crear tarea o Propiedades de tarea.
- **Al producirse un evento**
Este desencadenador hace que la tarea se ejecute cuando se agregan determinadas entradas de evento a un registro de eventos. Puede elegir entre especificar una configuración de desencadenador de evento básica o una configuración de desencadenador de evento personalizada. Si elige la configuración de desencadenador de evento básica, un solo evento de un registro de eventos específico se encargará de desencadenar la tarea. Elige el registro de eventos que contiene el evento, el nombre del publicador del evento, y especifica el identificador del evento. Si elige la configuración de desencadenador de evento personalizada, puede especificar una consulta de evento XML o un filtro de eventos personalizado con el fin de consultar eventos que desencadenarán la tarea. Este desencadenador no está disponible para tareas configuradas para Windows Server 2003, Windows XP o Windows 2000.
- **Al crear o modificar tarea**

Este desencadenador hace que una tarea se ejecute tan pronto como se cree y cuando se modifica la tarea. La única configuración de este desencadenador es la configuración avanzada descrita en la sección Configuración avanzada

incluida más adelante. Este desencadenador no está disponible para tareas configuradas para Windows Server 2003, Windows XP o Windows 2000.

- Al conectarse a una sesión de usuario

Este desencadenador provoca la ejecución de una tarea cuando se conecta a una sesión de usuario desde un equipo local o desde una conexión de escritorio remoto. Por ejemplo, cuando se conecta a una sesión de usuario en el equipo local mediante el cambio de usuarios en el equipo, este desencadenador hará que se ejecute la tarea. Otro ejemplo que puede desencadenar la ejecución de una tarea es cuando un usuario se conecta a una sesión de usuario mediante el uso del programa Conexión a Escritorio remoto desde un equipo remoto. La configuración del desencadenador le permite especificar que la tarea debe desencadenarse cuando cualquier usuario se conecte a una sesión de usuario o cuando se conecte un usuario o miembro de un grupo de usuarios específico. Este desencadenador no está disponible para tareas que están configuradas para Windows Server 2003, Windows XP o Windows 2000.

- Al desconectarse de una sesión de usuario

Este desencadenador provoca la ejecución de una tarea cuando una sesión de usuario se desconecta del equipo local o de una conexión de escritorio remoto. Por ejemplo, cuando se desconecta de una sesión de usuario en el equipo local mediante el cambio de usuarios en el equipo, este desencadenador hace que se ejecute la tarea. Otro ejemplo que puede desencadenar la ejecución de una tarea es cuando un usuario se desconecta de una sesión de usuario mediante el uso del programa Conexión a Escritorio remoto desde un equipo remoto. La configuración del desencadenador le permite especificar que la tarea debe desencadenarse cuando cualquier usuario se desconecte de una sesión de usuario o cuando se desconecte un usuario o miembro de un grupo de usuarios específico. Este desencadenador no está disponible para tareas configuradas para Windows Server 2003, Windows XP o Windows 2000

- Al bloquear la estación de trabajo

Este desencadenador hace que la tarea se ejecute cuando el equipo se bloquee. La configuración del desencadenador le permite especificar que la tarea debe desencadenarse cuando cualquier usuario bloquee el equipo o cuando un usuario o miembro de un grupo de usuarios específico bloquee el equipo. Este desencadenador no está disponible para tareas configuradas para Windows Server 2003, Windows XP o Windows 2000.

- Al desbloquear la estación de trabajo

Este desencadenador hace que la tarea se ejecute cuando el equipo se desbloquea. La configuración del desencadenador le permite especificar que la tarea debe desencadenarse cuando cualquier usuario bloquee el equipo o cuando un usuario o miembro de un grupo de usuarios específico bloquee el equipo.



Este desencadenador no está disponible para tareas configuradas para Windows Server 2003, Windows XP o Windows 2000.

Configuración avanzada

La siguiente lista describe la configuración avanzada del desencadenador.

Retrasar la tarea durante o Retrasar la tarea durante un máximo de (retraso aleatorio): esta configuración le permite especificar una cantidad de tiempo para demorar la ejecución de la tarea después de que ésta se desencadene. Si está usando un desencadenador basado en tiempo (Según una programación), será un tiempo de retraso aleatorio entre el tiempo en el que la tarea está desencadenada y el tiempo especificado en esta configuración. Si se programa una tarea para que se desencadene a la 1:00 p.m. y la configuración Retrasar la tarea durante un máximo de (retraso aleatorio) está establecido en 5 minutos, la tarea se ejecutará a una hora comprendida entre la 1:00 p.m. y la 1:05 p.m.

Repetir la tarea cada: esta configuración le permite establecer un intervalo de tiempo de repetición para la tarea. De este modo, la tarea se ejecutará, esperará el intervalo de tiempo especificado y se volverá a ejecutar. Este ciclo continuará hasta que finalice el tiempo de duración.

Detener las tareas que se ejecuten durante más de: esta configuración le permite detener tareas en ejecución largas mediante el establecimiento de un límite de tiempo en la cantidad de tiempo que se permite para la ejecución de la tarea (es decir, en ejecutarse la acción).

Activar: esta configuración le permite establecer una fecha y una hora para la activación del desencadenador.

Una vez que se activa un desencadenador, el desencadenador puede provocar la ejecución de la tarea. La hora es relativa a la zona horaria que esté establecida en el equipo que ejecute la tarea. Active la casilla Universal para lograr que la hora sea relativa a la hora universal coordinada (UTC) en lugar de a la zona horaria que esté establecida en el equipo que ejecute la tarea. Use la configuración Universal cuando desee coordinar un conjunto de tareas para que se activen simultáneamente en varias zonas horarias.

Expirar: esta configuración le permite establecer una fecha y una hora para la expiración del desencadenador. Al expirar un desencadenador, no puede producirse la ejecución de la tarea. La hora es relativa a la zona horaria que esté establecida en el equipo que ejecute la tarea. Active la casilla Universal para lograr que la hora sea relativa a la hora universal coordinada (UTC) en lugar de a la zona horaria que esté establecida en el equipo que ejecute la tarea. Use la configuración Universal cuando desee coordinar un conjunto de tareas para que expiren simultáneamente en varias zonas horarias.

Habilitada: esta configuración le permite habilitar o deshabilitar la tarea. Una tarea que está habilitada puede ejecutarse y una tarea que está deshabilitada no puede ejecutarse hasta que se habilite.

Acciones

La acción de una tarea es el trabajo que se realiza cuando se ejecuta la tarea. Una tarea puede tener una sola acción o un máximo de 32 acciones. Cada acción contiene la configuración que determina cómo se realiza la acción. Las acciones de una tarea se muestran en la ficha Acciones del cuadro de diálogo Propiedades de tarea o Crear tarea. Cuando se especifican varias acciones, éstas se ejecutan en orden secuencial comenzando por la acción situada en la parte superior de la lista en la ficha Acciones y finalizando por la acción situada en la parte inferior de la lista. Puede cambiar el orden en el que se ejecutan las acciones seleccionando una acción y haciendo clic en el botón de flecha arriba o abajo para mover la acción en la lista.

La siguiente lista contiene la descripción y configuración de cada acción.

- Iniciar un programa

Esta acción inicia un programa o script. En el cuadro de texto Programa o script, escriba el nombre del programa o script que desea iniciar. Si el programa o script toma argumentos de la línea de comandos, puede proporcionar estos argumentos en el cuadro de texto Agregar argumentos (opcional). En el cuadro de texto Iniciar en (opcional), puede especificar el directorio de trabajo de la línea de comandos que ejecuta el programa o script. Éste debería ser la ruta de acceso al programa o archivo de script o la ruta de acceso a los archivos que utiliza el archivo ejecutable.

- Enviar correo electrónico

Esta acción envía un mensaje de correo electrónico cuando se desencadena una tarea. En la configuración de la acción se especifica la dirección de correo electrónico de la que procede el correo electrónico, la dirección de correo electrónico a la que se envía el correo, el asunto del correo electrónico, el texto del mensaje de correo electrónico y datos adjuntos de correo electrónico opcionales. También debe especificar el servidor SMTP desde el que envía el correo electrónico. Esta acción no está disponible para tareas configuradas para Windows Server 2003, Windows XP o Windows 2000.

- Mostrar un mensaje

Esta acción muestra un cuadro de mensaje con un mensaje y título especificados. La configuración de la acción especifica el texto del título del cuadro de mensaje y el texto del mensaje. Esta acción únicamente se iniciará si la opción de seguridad Ejecutar sólo cuando el usuario haya iniciado la sesión está activada en la ficha General del cuadro de diálogo Propiedades de tarea o Crear tarea. Esta acción no está disponible para tareas configuradas para Windows Server 2003, Windows XP o Windows 2000.

Inicio de un programa

Si una acción inicia un programa cuando se activa una tarea, necesita escribir el nombre del programa o script y los argumentos de línea de comandos necesarios para ejecutar el programa o script. La siguiente lista contiene programas de uso común que una tarea puede ejecutar. Para que se muestre más información acerca de cada programa y los argumentos disponibles para cada programa, escriba el nombre del programa seguido de /? en el símbolo del sistema.

Un programa puede requerir privilegios elevados para ejecutarse correctamente.



Configuración de tareas

La configuración de la tarea especifica cómo se ejecuta, detiene o elimina una tarea. La configuración de una tarea se muestra en la ficha Configuración del cuadro de diálogo Propiedades de tarea o Crear tarea. La siguiente lista contiene las descripciones de la configuración de la tarea.

Permitir que la tarea se ejecute a petición

Puede especificar si una tarea se puede ejecutar manualmente antes o después del momento para el que se esté programada su ejecución permitiendo para ello que la tarea se ejecute a petición. La configuración predeterminada permite a un usuario ejecutar la tarea en otro momento a petición. Esta configuración no está disponible para tareas configuradas para Windows 2003, Windows XP o Windows 2000.

Ejecutar la tarea de inmediato si se pasó por alto algún inicio programado

Si se activa esta configuración, el servicio Programador de tareas iniciará la tarea si la ejecución de ésta se programó para una determinada hora pero, por algún motivo (por ejemplo, se desactivó el equipo o el servicio Programador de tareas estaba ocupado), la tarea no se activó. El servicio Programador de tareas no iniciará la tarea inmediatamente después de que la tarea se pasara por alto. El servicio espera de manera predeterminada diez minutos antes de iniciar la tarea que se pasó por alto. Esta configuración no está disponible para tareas configuradas para Windows 2003, Windows XP o Windows 2000.

Si la tarea no se ejecuta, reiniciarla cada: <período de tiempo>

Use esta configuración para reiniciar una tarea si la tarea no se ejecuta (el resultado de la última ejecución de la tarea no fue el correcto). En este caso especifica el intervalo de tiempo que transcurre entre los intentos de reinicio de la tarea y el número de veces que debe intentarse el reinicio de la tarea. Esta configuración no está disponible para tareas configuradas para Windows 2003, Windows XP o Windows 2000.

Detener la tarea si se ejecuta por más: <período de tiempo>

Esta configuración le permite limitar la cantidad de tiempo que se permite la ejecución de una tarea. Use esta configuración para limitar las tareas cuya ejecución se puede alargar durante un período de tiempo, provocando situaciones incómodas para el usuario.

Hacer que la tarea se detenga si no finaliza cuando se solicite

Si se selecciona esta configuración, la tarea se verá obligada a detenerse si ésta no responde a una solicitud de detención. Esta configuración no está disponible para tareas configuradas para Windows 2003, Windows XP o Windows 2000.

Eliminar la tarea si no está programada para ejecutarse de nuevo después de: <período de tiempo>

Si se activa esta configuración, el servicio Programador de tareas eliminará automáticamente la tarea si no está programada para volverse a ejecutar. El servicio

Programador de tareas esperará durante el período de tiempo especificado antes de eliminar la tarea. Si no se selecciona esta configuración, el servicio Programador de tareas no eliminará automáticamente la tarea. La tarea debe incluir al menos un desencadenador con una fecha de expiración para poder seleccionar esta configuración.

Aplicar la siguiente regla si la tarea ya está en ejecución:

Debe especificar cómo el servicio Programador de tareas debe ejecutar la tarea si ya se está ejecutando otra instancia de la tarea:

No iniciar una instancia nueva: el servicio Programador de tareas no ejecutará la nueva instancia de la tarea y no detendrá la instancia que ya esté ejecutándose.

Ejecutar una instancia nueva en paralelo: el servicio Programador de tareas ejecutará la nueva instancia de la tarea en paralelo con la instancia que ya esté ejecutándose.

Poner en cola una instancia nueva: el servicio Programador de tareas agregará la nueva instancia de la tarea a la cola de tareas que ejecutará el servicio y el servicio no detendrá la instancia de la tarea que ya se esté ejecutando.

Detener la instancia existente: el servicio programador de tareas detendrá la instancia de la tarea que ya esté ejecutándose y ejecutará la nueva instancia de la tarea.

El valor de esta configuración es No iniciar una instancia nueva para tareas configuradas para Windows 2003, Windows XP o Windows 2000.

Iniciar el Programador de tareas

Puede iniciar el complemento de MMC Programador de tareas mediante un solo comando desde la línea de comandos o mediante la interfaz de Windows. El Programador de tareas también se puede iniciar haciendo doble clic en el archivo Taskschd.msc en la carpeta %SYSTEMROOT%\System32.

Para ejecutar el Programador de tareas mediante la interfaz de Windows

1. Haga clic en el botón Inicio.
2. Haga clic en Panel de control.
3. Haga clic en Sistema y mantenimiento.
4. Haga clic en Herramientas administrativas.
5. Haga doble clic en Programador de tareas.

Para ejecutar el Programador de tareas desde la línea de comandos

1. Abra un símbolo del sistema. Para abrir un símbolo del sistema, haga clic en Inicio, seleccione Todos los programas, Accesorios y, a continuación, haga clic en Símbolo del sistema.
2. En el símbolo del sistema, escriba Taskschd.msc.

La herramienta de línea de comandos Schtasks.exe permite a un usuario completar muchas de las mismas operaciones que se pueden completar con el complemento de MMC Programador de tareas. Esta herramienta permite a un usuario crear, eliminar, realizar consultas, cambiar, ejecutar y finalizar tareas programadas en un equipo local o remoto. Esta herramienta se encuentra en la carpeta %SYSTEMROOT%\System32. Escriba Schtasks.exe /? desde una ventana del símbolo del sistema para ver la ayuda de esta herramienta.



Preguntas de Repaso

1. Investigación:
 - a. Qué herramientas están disponibles para realizar una recuperación del sistema operativo en caso de desastres.
 - b. Cómo se realiza un backup de archivos específicos
 - c. Cómo se establece un monitoreo al adaptador de red
2. Desarrollar:
 - a. Implemente una red completa, con Servidor de Directorio, DNS, Archivos e Impresión. Para ello basará su trabajo en un proyecto de empresa "modelo", que incluya sucursales a nivel mundial. El proyecto será desarrollado en grupo de 3 personas. Implemente las carpetas compartidas, y establezca los permisos pertinentes para una correcta configuración de seguridad.