Microsoft

Windows® 2000 Server

Sistema operativo del servidor

Políticas de grupo

Resumen

Este documento describe la Política de grupo Windows® 2000, e incluye información sobre la infraestructura y mecánica de la política de grupo, el editor de políticas de grupo (una herramienta administrativa) y sus capacidades, la ampliación de la funcionalidad de la política de grupo y el uso de la política de grupo en computadoras independientes. También presenta instrucciones para la creación de plantillas administrativas (archivos .adm).

Este documento está diseñado para administradores de informática y administradores del sistema que están interesados en utilizar la política de grupo para administrar ambientes de escritorio de usuarios. Las políticas de grupo se utilizan para especificar configuraciones para grupos de usuarios y computadoras, incluyendo políticas de software, *script* (iniciar y apagar la computadora y conexión y desconexión de usuarios), documentos de usuario y configuraciones, implementación de aplicaciones y configuraciones de seguridad.

Nota: Este texto documenta la funcionalidad de Windows 2000 Server Beta 2 .

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0299

TABLA DE CONTENIDOS

INTRODUCCION

En el sistema operativo Windows® 2000, las políticas de grupo definen las configuraciones para usuarios y computadoras para grupos de usuarios y computadoras. Puede crear una configuración específica de escritorio para cualquier grupo particular de usuarios y computadoras al implementar el *snap-in* del editor de políticas de grupo de Microsoft® Management Console (MMC). Estas configuraciones de políticas de grupo que usted crea se encuentran en el Objeto de políticas de grupo (GPO) que a su vez está asociado con objetos seleccionados de Active Directory (AD) tales como sitios, dominios o unidades organizacionales.

Políticas de grupo y costo total de propiedad

Los estudios recientes sobre el costo total de propiedad (TCO), los costos involucrados en administrar redes distribuidas de computadoras personales, citan productividad perdida en el escritorio como uno de los costos principales para las empresas. La productividad perdida frecuentemente se atribuye a los errores de los usuarios tales como modificar los archivos de configuración del sistema y causar que la computadora se vuelva inservible o a la complejidad tal como la disponibilidad de aplicaciones y funciones no esenciales en el escritorio .

Una manera de abordar el costo total de propiedad es que los administradores utilicen políticas de grupo para crear ambientes de escritorios administrados adaptados a las responsabilidades de trabajo de los usuarios y a nivel de experiencia con las computadoras. En Windows 2000, los administradores pueden administrar de manera central los escritorios utilizando el servicio Active Directory y su soporte de políticas de grupo.

Capacidades de políticas de grupo

Usted utiliza el editor de políticas de grupo y sus extensiones para definir opciones de políticas de grupo para configuraciones de escritorios administradas para computadoras de usuarios. Con el editor de políticas de grupo puede especificar configuraciones para:

- **Políticas de software.** Usted utiliza Políticas de software para controlar configuraciones de registro en el escritorio, incluyendo los componentes y aplicaciones del sistema operativo.
- ***Scripts*** (tales como el iniciar y apagar la computadora y conectarse y desconectarse)**.**
- **Opciones de administración de software** (por ejemplo, las aplicaciones disponibles para usuarios y aquellas que aparecen en sus escritorios)**.**
- **Documentos y configuraciones de usuario** (para implementación de archivos y redireccionamiento de carpetas especiales)**.**
- **Configuraciones de seguridad** (por ejemplo para computadoras locales, dominios y configuraciones de seguridad de red)**.**

Con el uso de las políticas de grupo, usted puede definir el estado del ambiente de trabajo de los usuarios una sola vez y depender del sistema para que éste aplique

las políticas que usted define.

Beneficios de las políticas de grupo

Las políticas de grupo proporcionan las siguientes ventajas:

- Capitalizan los servicios de Windows 2000 Active Directory.
  Las políticas de grupo permiten una administración centralizada o descentralizada de las opciones de políticas.
- Ofrece flexibilidad y escalabilidad.
  Las políticas de grupo manejan una amplia gama de escenarios de implementación que pueden ser aplicados tanto a negocios pequeños como a empresas grandes.
- Proporciona una herramienta simple e integrada para administrar las políticas.
  El editor de políticas de grupo es un *snap-in* MMC que amplía otras herramientas administrativas de Active Directory como el administrador de Active Directory y el administrador de sitio y servicios de Active Directory, además de *snap-in*s de administración de computadoras.
  Los administradores pueden delegar el control de los objetos de Políticas de grupo.
- Cuenta con una interfaz clara y fácil de usar.
- Proporciona una detección de vínculos lentos y una retroalimentación directa y sin obstrucciones.
- Proporciona confiabilidad y seguridad

Las políticas de grupo y Active Directory

Las Políticas de grupo amplían y aprovechan Active Directory. Las configuraciones de las Políticas de grupo se encuentran en los objetos de Políticas de grupo que a su vez están asociados con estos contenedores de Active Directory: Sitios, dominios o unidades organizacionales.

Políticas de grupo y grupos de seguridad

Puede filtrar las Políticas de grupo al usar la membresía en los grupos de seguridad y al configurar los permisos de la Lista de control de acceso (ACL). Al hacerlo, permite procesamiento rápido de los objetos de Políticas de grupo y permite que las Políticas de grupo se apliquen a grupos de seguridad. Al utilizar las ACLs y los grupos de seguridad, puede modificar el alcance de los objetos de Políticas de grupo.

Qué contiene este documento

Este documento describe las políticas de grupo de Windows 2000, incluyendo la infraestructura y mecánica, delegación, filtrado y extensión de las Políticas de grupo y del editor de las mismas. También presenta información sobre migración desde Windows NT® 4.0 a Windows 2000, un resumen general de los conceptos

clave de Windows 2000 Active Directory y la creación de plantillas administrativas (archivos. .adm).

DESCRIPCION GENERAL DE LAS POLÍTICAS DE GRUPO

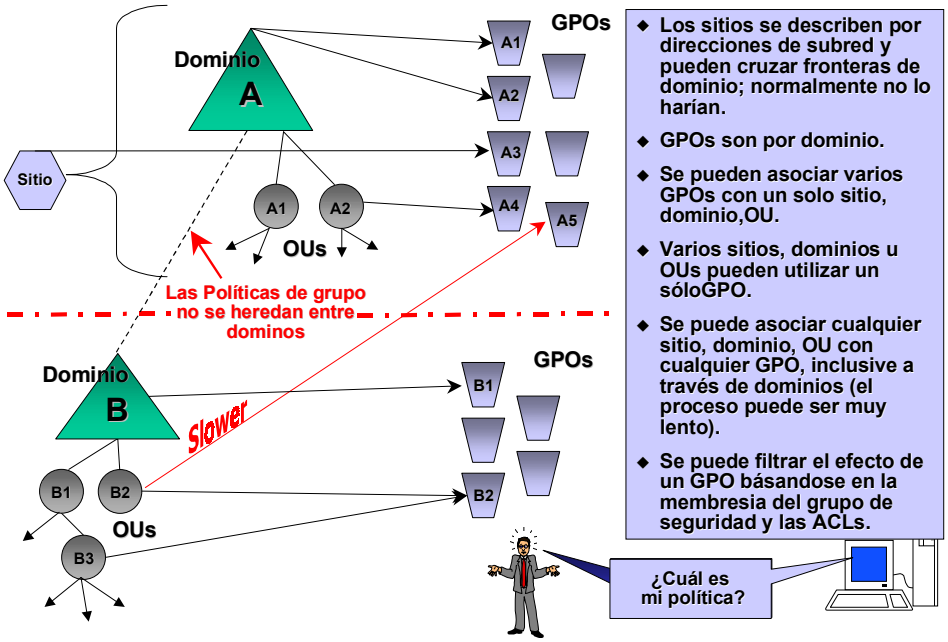
En Windows NT 4.0, utilizó la herramienta del editor de Políticas del sistema para establecer las configuraciones de usuarios y computadoras almacenadas en la base de datos del registro de Windows NT. Con el uso del editor de Políticas del sistema, puede crear una política de sistema para controlar el ambiente y las acciones de trabajo de los usuarios y aplicar las configuraciones del sistema para todas las computadoras que estén ejecutando Windows NT Workstation y Windows NT Server. Las Políticas de sistemas son configuraciones de registro que definen el comportamiento de varios componentes en el ambiente de escritorio.

Windows 2000 introduce el editor de Políticas de grupo como una herramienta que amplía la funcionalidad del editor de Políticas de sistema y proporciona capacidades mejoradas para establecer configuraciones de los usuarios y las computadoras para grupos de computadoras de usuarios. El editor de Políticas de grupo es un *snap-in* de Microsoft Management Console que incluye funciones incorporadas para configurar las Políticas de grupo. Las Políticas de grupo definen los diferentes componentes del ambiente de los usuarios que los administradores del sistema necesitan manejar e incluye configuraciones de software, opciones de implementación de aplicaciones, *scrips*, configuraciones de usuarios además de opciones de documentos y configuraciones de seguridad.

Las configuraciones de la Política de grupo que especifique se encuentran en un objeto de Políticas de grupo que está asociado a su vez con objetos seleccionados de Active Directory (sitio, dominio o unidades organizacionales).

Como se mencionó anteriormente, las Políticas de grupo aprovechan al máximo los contenedores de Windows 2000 Active Directory y los grupos de seguridad. De manera preestablecida, las Políticas de grupo afectan a todas las computadoras y usuarios en un contenedor seleccionado de Active Directory. Sin embargo, puede *filtrar* los efectos de la Política de grupo basándose en la membresía de usuarios o computadoras en un grupo de seguridad Windows 2000. Para filtrar la política de grupo, use la interfaz estándar del editor ACL de seguridad de Windows NT. También puede usar los permisos ACL para delegar el uso de la herramienta de editor de Políticas de grupo.

La siguiente gráfica ilustra un escenario de Políticas de grupo y de Active Directory:



Configuraciones de la computadora y configuración del usuario

En la raíz del espacio para el nombre del editor de Políticas de grupo hay dos nodos principales: Configuración de la computadora y configuración del usuario. Estas son las carpetas principales que utiliza para configurar ambientes de escritorio específicos y para aplicar las Políticas de grupo en las computadoras y usuarios en la red.

Las configuraciones de la computadora incluyen políticas que especifican el comportamiento del sistema operativo, la apariencia del escritorio, la configuración de las aplicaciones, las aplicaciones asignadas, las opciones de implementación de archivo, las configuraciones de seguridad y los *scripts* de iniciar y apagar la computadora. Las Políticas de grupo relacionadas con la computadora se aplican cuando se inicia el sistema operativo.

Las configuraciones del usuario incluyen toda la información específica del usuario tal como el comportamiento del sistema operativo, las configuraciones de escritorio, las configuraciones de aplicaciones, aplicaciones asignadas y publicadas, opciones de implementación de archivos, configuraciones de seguridad y *scripts* de conexión y desconexión de usuarios. Se aplican las Políticas de grupo relacionadas con los usuarios cuando estos se conectan a la computadora.

Nota: Puede especificar que las Políticas de grupo se apliquen a todos los usuarios de computadoras específicas. Esto es útil en ambientes de computación pública tales como bibliotecas o escuelas, por

ejemplo, donde desea proporcionar una configuración específica de escritorio sin importar qué usuario se conecte a la computadora. Para establecer las configuraciones del usuario por computadora, use el nodo de Políticas de software en configuraciones de la computadora.

Políticas de software

El nodo de Políticas de software del editor de Políticas de grupo incluye toda la información de Políticas de grupo basada en registros, eso es lo que controlaban las Políticas del sistema de Windows NT 4.0. Las configuraciones de las Políticas de software incluyen las Políticas de grupo para el sistema operativo Windows 2000 y sus componentes, y para las aplicaciones. Estas configuraciones se escriben ya sea en el usuario o en la parte local del equipo de la base de datos de registro. Las configuraciones de política que son específicas a un usuario que se conecta a una estación de trabajo o servidor se escriben al registro bajo **HKEY_CURRENT_USER (HKCU)** y las configuraciones específicas de la computadora se escriben bajo **HKEY_LOCAL_MACHINE (HKLM)**.

Para generar el espacio de nombre bajo el nodo de Políticas de software del editor de Políticas de grupo, usted puede utilizar ya sea las plantilllas administrativas personalizables (archivos .adm) o un *snap-in* de extensión de MMC en el editor de Políticas de grupo. Para obtener mayor información sobre plantillas administrativas, consulte el Apéndice A.

Administración del software

Puede utilizar la extensión del editor de implementación de aplicaciones para administrar de manera central la distribución de software en su empresa. Puede instalar, asignar, publicar, actualizar, reparar y eliminar software de grupos de usuarios y computadoras.

Usted asigna aplicaciones a grupos de usuarios para que todos los usuarios que requieran las aplicaciones automáticamente cuenten con ellas en sus escritorios, sin requerir que el administrador o personal técnico instale la aplicación en cada escritorio. Cuando asigna una aplicación a un grupo de usuarios, está realmente *anunciando* la aplicación en todos los escritorios de los usuarios. La próxima vez que un usuario se conecte a Microsoft Windows NT, estará anunciada la aplicación. Esto significa que aparece un acceso rápido a la aplicación en el menú **Inicio** y se actualiza el registro con información acerca de la aplicación, incluyendo la ubicación del paquete de la aplicación y la ubicación de archivos fuente para la instalación. Con esta información de publicidad en la computadora del usuario, se instala la aplicación la primera vez que el usuario la activa.

Cuando el usuario selecciona la aplicación desde el menú **Inicio** por primera vez, se instala automáticamente y después se abre.

También puede publicar aplicaciones a grupos de usuarios y ellos pueden decidir si desean o no instalar dichas aplicaciones. Cuando publica una aplicación, no aparecen accesos rápidos a la aplicación en los escritorios de los usuarios y no se

realizan registros locales. En otras palabras, la aplicación no está presente en el escritorio del usuario. Las aplicaciones publicadas guardan su información de publicidad en Active Directory.

Para instalar una aplicación publicada, los usuarios pueden usar la herramienta Agregar/eliminar programas, que incluye una lista de todas las aplicaciones publicadas que se encuentran disponibles para su uso. Los usuarios también pueden abrir un archivo de documento asociado con una aplicación publicada (por ejemplo, un archivo .xls para instalar Microsoft Excel).

Documentos y configuraciones del usuario

Puede usar la extensión de documentos y configuraciones del usuario para agregar archivos, accesos rápidos o carpetas especiales que representan el escritorio del usuario. Las carpetas especiales son aquellas que se encuentran bajo la carpeta %Windir%\perfiles (donde %Windir% es la carpeta de Windows NT) y éstas incluyen carpetas tales como Mis documentos, Menú de inicio, Escritorio, Favoritos y otros. Los archivos que especifique se mandan al escritorio del usuario ya sea al inicio del equipo (si se especifica en las configuraciones de la computadora) o cuando el usuario se conecte (si está especificado en las configuraciones del usuario). Los archivos que coloque en el nodo de las configuraciones de la computadora estarán disponibles para todos los usuarios de esa computadora. Los archivos que coloque en el nodo de configuraciones del usuario estarán disponibles sólo al usuario específico, sin importar a qué computadora se conecte la persona.

Note que puede colocar cualquier archivo en la carpeta de Favoritos; sin embargo, el menú Favoritos sólo presentará archivos que son accesos rápidos, en otras palabras, tipos de archivos que están marcados en el registro como “IsShortcut” en la llave **ProgID**. Esto incluye .url, .lnk, .pif y otros.

Puede usar la extensión de documentos y configuraciones del usuario para realizar las siguientes tareas:

- Redireccionar cualquiera de las carpetas especiales en un perfil de usuario a una ubicación alterna (tal como el destino de red). Por ejemplo, podría redireccionar la carpeta Mis documentos de un usuario a \\server\share\%username%. Al redireccionar la carpeta Mis documentos, puede proporcionar las siguientes ventajas:
    - Asegurar que estén disponibles todos los documentos de los usuarios cuando pasean de una computadora a otra.
    - Reducir el tiempo que se requiere para conectarse y desconectarse de la red. En Windows NT 4.0, la carpeta Mis documentos es parte del perfil del usuario *roaming*. Esto significa que la carpeta Mis documentos y su contenido se copian en ambos sentidos entre la computadora del cliente y el servidor cuando se conectan y desconectan los usuarios. La reubicación de la carpeta Mis documentos fuera del perfil del usuario puede reducir de manera significativa ese tiempo.
    - Guardar los datos de los usuarios en la red (en lugar de en una

computadora local).
El departamento de informática administra y protege los datos.

- Hacer que la carpeta Mis documentos basada en la red de los usuarios esté disponible a los usuarios cuando se desconecten de la red corporativa al utilizar las tecnologías de caché del extremo del cliente.

- Publicar accesos rápidos o archivos en cualquier carpeta especial. Por ejemplo, puede utilizar esta función de las siguientes maneras:
  - Puede colocar un acceso rápido URL a la página Web de soporte técnico en el escritorio de todo mundo o entre sus Favoritos de Microsoft Internet Explorer.
  - Un asistente de grupo puede colocar un documento “Bienvenido al grupo Windows NT” en los escritorios de los usuarios.

Las carpetas especiales incluyen:

Computadoras	Usuarios
Datos de aplicación	Datos de aplicación
Escritorio	Escritorio
Menú de Inicio	Favoritos
Programas Arranque	Configuraciones locales
	Mis documentos Mis imágenes
	NetHood
	PrintHood
	Enviar A
	Menú Inicio
	Programas Arranque

Configuraciones de seguridad

Puede utilizar la extensión de configuraciones de seguridad para definir configuración de seguridad para computadoras dentro de un Objeto de políticas de grupo. Una configuración de seguridad consiste en configuraciones aplicadas a cada área de seguridad soportada por Windows NT Workstation o Windows NT Server. Esta configuración se incluye dentro de un Objeto de políticas de grupo. Se aplica entonces esta configuración de seguridad a las computadoras como parte de la vigencia de las Políticas de grupo.

La extensión de configuraciones de seguridad ha sido diseñada para complementar las herramientas de seguridad existentes del sistema tales como el Editor de listas de control de acceso, el Administrador de usuarios locales y el Administrador de

servidores. La extensión de configuraciones de seguridad define un motor que puede interpretar una configuración estándar de seguridad y ejecutar automáticamente las operaciones requeridas en el fondo. Puede continuar utilizando las herramientas existentes para cambiar las configuraciones específicas cuando sea necesario.

Las áreas de seguridad que se pueden configurar para computadoras incluyen:

- **Políticas de cuenta.** Este término se refiere a configuraciones de seguridad de computadoras para políticas de contraseña, políticas de bloqueo y políticas *Kerberos* en dominios Windows NT.
- **Políticas locales.** Estas incluyen configuraciones de seguridad para políticas de auditoría, asignación de derechos a usuarios y acciones de seguridad. La política local le permite configurar quién tiene acceso local desde la red a la computadora y si se auditan o no y cómo los eventos locales.
- **Registro de eventos.** Se controlan las configuraciones de seguridad para aplicación, seguridad y registros de evento del sistema. Puede acceder a estos registros utilizando el Visualizador de eventos.
- **Grupos restringidos.** Esto se refiere a las configuraciones de seguridad de la computadora para grupos incorporados que cuentan con ciertas habilidades predefinidas. Las políticas restringidas de grupo afectan la membresía de estos grupos. Algunos ejemplos de los grupos restringidos son los grupos locales (tales como administradores, usuarios con poder, operadores de impresión y operadores de servidores), así como grupos globales (tales como administradores de dominio).

  Puede agregar categorías que considere sensibles o privilegiadas a la lista de Administración de grupos restringidos, con su información de membresía, y entonces puede rastrear y administrarlas. Además de la membresía de grupo, las políticas restringidas de grupo rastrean y controlan la membresía hacia atrás de cada grupo restringido, los grupos a los cuales pertenece un grupo seleccionado. Puede utilizar la membresía en reversa para controlar exactamente a qué grupos pueden incorporarse sus miembros restringidos o limitar una categoría seleccionada de usuarios a un grupo de membresía y prevenirles que se registren en otras.
- **Servicios del sistema.** Estos controlan las configuraciones de control y opciones de seguridad (ACLs) a los servicios de sistema tales como servicios de red, servicios de archivo e impresión, servicios de telefonía y fax y servicios Internet/intranet y así sucesivamente. Las extensiones de configuraciones de seguridad dan soporte directamente a las configuraciones generales para cada servicio del sistema. Esto incluye modalidad de inicio y seguridad sobre el servicio. Note que el nombre del servicio debe de ser el mismo que el que utilizó el Administrador de control de servicio.
- **Registro.** Este se utiliza para configurar y analizar configuraciones para descriptores de seguridad (incluyendo objetos de propiedad), el ACL e información de auditoría para cada llave de registro.

  Cuando aplica seguridad en llaves de registro, la extensión de

configuraciones de seguridad sigue el mismo modelo de herencia que utilizaron las tres jerarquías estructuradas en Windows 2000 (tales como Active Directory y NTFS). Microsoft recomienda que utilice las capacidades de herencia para especificar la seguridad sólo en objetos de nivel superior y redefinir seguridad sólo para aquellos objetos hijo que lo requieran. Este enfoque simplifica ampliamente su estructura de seguridad y reducirá el gasto administrativo que resultaría de una estructura innecesaria de control de acceso complejo.

- **Sistema de archivos.** Se utiliza para configurar y analizar las configuraciones para descriptores de seguridad (incluyendo objetos de propiedad), el ACL y la información de auditoria para cada objeto (volumen, directorio o archivo) en el sistema de archivo local.

Microsoft proporciona el siguiente conjunto de archivos predefinidos de configuración para escenarios comunes de seguridad:

- Configuraciones para estación de trabajo típica (ideal ws.inf)
- Configuraciones para estación de trabajo segura (securews.inf)
- Configuraciones para controlador de dominio seguro (securedc.inf)
- Configuraciones para estación de trabajo muestra (sample.inf)
- Configuraciones para el controlador de dominio muestra (sampledc.inf)

Por predeterminación, se guardan estos archivos de configuración de seguridad en \%systemroot%\security\templates. Puede utilizar estos o cualquier otra configuración de seguridad como la base de sus configuraciones de seguridad, y después editar las configuraciones de acuerdo a sus necesidades.

Se guardan las configuraciones de seguridad como archivos .inf en formato de texto. Cuando crea y asigna una configuración de seguridad o edita una configuración de seguridad existente, la extensión de configuraciones de seguridad procesa el archivo de configuración y realiza los cambios correspondientes a las computadoras asociadas como parte de las Políticas de grupo.

Scripts

Con las extensiones de *Scripts* puede asignar *scripts* para ejecutarse cuando la computadora se inicia o se apaga o cuando los usuarios se conectan o desconectan de sus computadoras. Para este propósito, puede utilizar Windows® Scripting Host para tipos de *script* Visual Basic®, Scripting Edition (VBScript) y JScript™.

Windows 2000 incluye Windows Scripting Host, un *host de scripting* independiente del lenguaje para plataformas Windows de 32 bits que incluye los motores de *scripting* VBScript y Jscript. Microsoft anticipa que otras compañías de software proporcionaran motores de *scripting* de ActiveX® para otros lenguajes tales como Perl, TCL, REXX y Python. Windows® Scripting Host también proporcionará soporte a esos lenguajes.

Para mayores informes sobre Windows Scripting Host también soporta estos lenguajes, verifique el siguiente URL: http://www.microsoft.com/scripting.

Los nombres de los *scripts* y sus líneas de comando (en forma de llaves de registro y valores) se encuentran guardados en el archivo Registry.pol, que se describe más adelante en este documento.

Requerimientos administrativos de las políticas de grupo

Note que para establecer las Políticas de grupo para un objeto AD seleccionado, debe tener instalado el controlador de dominio Windows NT y debe contar con permiso de leer/escribir para acceder al volumen del sistema de controladores de dominio (carpeta Sysvol) y modificar los derechos en el objeto de directorio actualmente seleccionado. Se crea automáticamente la carpeta de Volumen de sistema cuando instala el controlador de dominio de Windows 2000 (o promueve un servidor a un controlador de dominio).

INFRAESTRUCTURA Y MECANICA DE LAS POLITICAS DE GRUPO

Las siguientes secciones introducen la infraestructura de las Políticas de grupo y ubicaciones de almacenamiento y proporcionan una descripción general de cómo se aplican las Políticas de grupo.

Infraestructura

Se crea una Política de grupo usando el *snap-in* de MMC del Editor de políticas de grupo ya sea como una herramienta independiente o como una extensión al administrador de Active Directory, el sitio de Active Directory y el administrador de servicios usando el verbo Administrar políticas de grupo. (Puede acceder a la extensión del Editor de políticas de grupo desde la consola del Administrador de Active Directory o el sitio de Active Directory y la consola del Administrador de servicios seleccionando un sitio, dominio o unidad organizacional y luego al escoger Administrar políticas de grupo desde el menú **Tareas**).

Todas las configuraciones de las Políticas de grupo se encuentran en los objetos de Políticas de grupo que están asociados con los contenedores de Active Directory (sitios, dominios u OUs), maximizando y ampliando por lo tanto Active Directory.

Puede filtrar los efectos de las Políticas de grupo en computadoras y usuarios utilizando la membresía en los grupos de seguridad y configurando los permisos ACL. Este enfoque asegura un proceso más rápido de los Objetos de políticas de grupo, mientras que permite que las Políticas de grupo se apliquen a grupos de seguridad. Además, puede limitar el alcance del Objeto de políticas de grupo usando los Grupos de seguridad y los ACLs.

Las Políticas de grupo usan un enfoque centrado en documentos. Por ejemplo, por analogía, el Editor de políticas de grupo es en relación a los Objetos de políticas de grupo como Microsoft Word es a los archivos.doc.

Plantillas administrativas (Archivos .Adm)

El Editor de políticas de grupo requiere una fuente para crear las configuraciones de interfaz que establecerá un administrador. Para este propósito, el Editor de políticas de grupo puede emplear ya sea una extensión *snap-in* de MMC del *sanp-in* del Editor de políticas de grupo o un archivo ASCII que se conoce como archivo de plantilla administrativa (.adm). El archivo .adm especifica las configuraciones de registro que se pueden modificar a través de una interfaz del Editor de políticas de grupo. El archivo .adm consiste de una jerarquía de categorías y subcategorías que conjuntamente definen cómo se implementarán las opciones a través de la interfaz del Editor de políticas de grupo. También indica las ubicaciones de registro donde deben realizarse cambios si se realiza una selección específica, cualquier opción o restricción (en valores) que estén asociadas con la selección y en algunos casos, especifica un valor predeterminado a utilizar si la selección es activada.

Para mayores informes sobre archivos .adm, vea el Apéndice A: Plantillas administrativas.

Objeto de políticas de grupo

Cuando utilice el Editor de políticas de grupo, crea configuraciones de Políticas de grupo que se encuentran en el Objeto de políticas de grupo. Estos Objetos de políticas de grupo están asociados a su vez con objetos seleccionados de un directorio tales como sitios, dominios u OUs.

Los Objetos de políticas de grupo guardan información de Políticas de grupo en dos ubicaciones: Un Contenedor de políticas de grupo y una Plantilla de políticas de grupo que se describen en la siguiente sección.

Contenedor de políticas de grupo

El Contenedor de políticas de grupo es un objeto de Active Directory que guarda propiedades del Objeto de políticas de grupo; incluye subcontenedores para información de Políticas de grupos del equipo y de los usuarios. El Contenedor de políticas de grupo cuenta con las siguientes propiedades:

- **Información de la versión.** Se utiliza para asegurar que la información este sincronizada con la información de la Plantilla de políticas de grupo.
- **Información de estado.** Esta indica si el Objeto de políticas de grupo está habilitado o deshabilitado.

El Contenedor de políticas de grupo almacena información del Almacén de clase para el Editor de implementación de aplicaciones, una extensión del Editor de políticas de grupo. El Almacén de clase Windows es un depósito basado en Windows 2000 Server para todas las aplicaciones, interfaces y APIs que permiten la publicación y asignación de aplicaciones.

Plantilla de políticas de grupo

Los Objetos de políticas de grupo también guardan información de Políticas de grupo en una estructura de carpeta llamada Plantilla de políticas de grupo que está ubicada en la carpeta del Volumen del sistema de los controladores de dominio (Sysvol) en la subcarpeta /políticas. La Plantilla de políticas de grupo es el contenedor para toda la información de implementación de política de software, *script*, archivos y aplicaciones.

Cuando modifique un GPO, el nombre de carpeta que se le da a la Plantilla de políticas de grupo es el identificador global único del Objeto de políticas de grupo que modificó. Por ejemplo, supongamos que modificó el GPO asociado con un dominio llamado *Seattle*. La carpeta GPT que se crea se llamaría (el GUID es un ejemplo):

```
%systemroot%\sysvol\<SYSVOL>\Seattle.yourcompanyname.com\Policies\{476364
45-af79-11d0-91fe-080036644603}
```

donde el segundo *sysvol* está compartido como SYSVOL. (La ubicación predeterminada para la carpeta Sysvol es %systemroot%).

Archivo Gpt .ini

En la raíz de cada carpeta Plantilla de políticas de grupo existe un archivo llamado

Gpt.ini. Este archivo contiene la siguiente información:

```
[General]
Version=0   //Version number of the Group Policy Object
Disabled=0  // 1=disabled - this is only valid for local Group Policy Object
                    (%systemroot%\system32\GroupPolicy)
```

Objetos locales de políticas de grupo

Un Objeto de políticas de grupo local existe en cada computadora y de manera predeterminada contiene *sólo* políticas de seguridad. Esta guardado en %systemroot%\system32\GroupPolicy y cuenta con los siguientes permisos ACL:

- Administradores: Control total
- Sistema operativo: Control total
- Usuario: Lectura

El archivo Gpt.ini define si el GPO esta habilitado o no; para otros GPOs esta información está guardada en Active Directory.

Subcarpetas de la Plantilla de políticas de grupo

La carpeta Plantilla de políticas de grupo contiene las siguientes subcarpetas:

- **Adm.** Contiene todos los archivos .adm para este GPT.
- **Scripts.** Contiene todos los *scripts* y archivos relacionados para este GPT.
- **Usuario.** Incluye un archivo Registry.pol que contiene las configuraciones de registro a ser aplicadas a los usuarios. Cuando un usuario se conecta a una computadora, el archivo se descarga el archivo Registry.pol y se aplica a la parte **HKEY_CURRENT_USER** del registro. La carpeta Usuario contiene las siguientes subcarpetas:
    - **Apps.** Contiene los archivos de publicidad (archivos .aas) que utiliza Windows Installer. Estos se aplican a los usuarios.
    - **Archivos.** Contiene los archivos a ser implementados. La estructura del directorio iguala a aquella del espacio del nombre. Esta es aplicada a los usuarios.
- **Equipo.** Incluye un archivo Registry.pol que contiene las configuraciones de registros a ser aplicadas a las computadoras. Cuando se enciende una computadora, se descarga el archivo Registry.pol y se aplica a la parte **HKEY_LOCAL_MACHINE** del registro. La carpeta Equipo contiene las siguientes subcarpetas:
    - **Apps.** Contiene los archivos de publicidad (archivos .aas) utilizados por Windows Installer. Estos son aplicados a las computadoras.
    - **Archivos.** Contiene los archivos a ser implementados y la estructura del directorio igual a aquella del espacio del nombre. Estas son aplicables a las computadoras.
    - **\Microsoft\Windows NT\SecEdit.** Contiene el archivo del editor de seguridad GPTTmpl.inf.

Se crean las carpetas Usuario y Equipo al momento de la instalación y las otras

carpetas se crean conforme se requieran cuando se establece la política.

Archivos Registry.pol

La extensión de las Políticas de software del Editor de políticas de grupo guarda información en la Plantilla de políticas de grupo en archivos ASCII que se conocen como archivos Registry.pol. Estos archivos contienen las configuraciones de registro personalizadas que especifica (al usar el editor de políticas de grupo) a ser aplicadas al equipo (**HKLM**) o al usuario (**HKLU**) del registro.

Se crean dos archivos Registry.pol y se guardan en la Plantilla de políticas de grupo, uno para las configuraciones de la computadora, que esta guardada en el subdirectorio \Machine y uno para las configuraciones del usuario, que esta guardado en el subdirectorio \User.

Formato de archivo Registry.pol

El formato de archivo Registry.pol en la Plantilla de políticas de grupo difiere de aquel de versiones previas del sistema operativo Windows NT y Windows 95. Los archivos Registry.pol creados por Windows NT 4.0 y Windows 95 sólo pueden ser aplicados al sistema operativo sobre el cual fueron creados. El archivo Registry.pol creado por el Editor de políticas de sistema de Windows NT 4.0 era un archivo binario, mientras que el archivo Registry.pol que creó el Editor de políticas de grupo de Windows 2000 es un archivo de texto. El archivo Registry.pol de Windows 2000 consiste de valores de encabezado y registro.

El encabezado contiene información sobre la versión y datos de firma, ambos valores de DWORD:

```
REGFILE_SIGNATURE 0x67655250
REGISTRY_FILE_VERSION 00000001 (increments each time changed)
```

Los valores de registro inician con el símbolo “[” y terminan con”]”:

```
[key;value;type;size;data]
```

donde:

key es la ruta a la llave de registro a utilizar para la categoría. No incluya **HKEY_LOCAL_MACHINE** o **HKEY_CURRENT_USER** en la ruta del registro. La ubicación del archivo determina cuáles de estas llaves se utilizarán. Los siguientes valores tienen un significado especial para este campo:

- `**DeleteKeys` — una lista delimitada por puntos y comas de llaves a eliminar. Por ejemplo: `**DeleteKeys NoRun;NoFind`.
- `**SecureKey` — `**SecureKey=1` asegura la llave, dando a los administradores y al sistema control total y a los usuarios acceso de sólo lectura. `**SecureKey=0` reinicia el acceso a la llave según lo que esté establecido en la raíz.

value valor es el nombre del valor del registro. Los siguientes valores tienen un significado especial para este campo:

- ***`**DeleteValues`*** — una lista de valores delimitada por puntos y comas a ser

eliminada. Utilice como un valor de la llave asociada.

*****Del.valuename*** — elimina un valor único. Utilícelo como un valor de la llave asociada.

*****DelVals*** — elimina todos los valores en una llave. Utilícelo como un valor de la llave asociada.

Type / type es un tipo de datos. El campo puede ser uno de los siguientes valores:

REG_BINARY

REG_DWORD

REG_EXPAND_SZ

REG_MULTI_SZ

REG_SZ

Size es el tamaño del campo de datos en bytes. Por ejemplo, 4.

Data es la información en bruto. Por ejemplo, 4 bytes de datos 0x00000001.

Es posible que el *nombre del valor, tipo, dato y tamaño* puedan no estar presentes o estar en ceros. En este caso, sólo se debe de crear la llave.

Este patrón de registros continua hasta el final del archivo.

Las siguientes llaves especiales se utilizan para eliminar llaves y valores:0 DeleteKe**ys // Semi-colon delimited list of keys to deleFor exampl**DeleteKeys REG_SZ NoRun;NoFin**DeleteValu**es // Semi-colon delimited list of values to deleUsed as a value of the designated ke**Del.valuena**me // Deletes a single valuenaUsed as a value of the designated ke**DelVa**ls // Deletes all values in a kUsed as a value of the designated ke**SecureK**ey // Makes the named key securSee the SecureKey section for details.**

El archivo Registry.pol contiene datos a ser escritos en el registro basándose en las configuraciones especificadas con el editor de políticas de grupo y los nombres de cualquier *script* y sus líneas de comandos (en forma de llaves y valores de registros).

*****SecureKey***

Se pueden aplicar los ACLs utilizando una bandera especial que puede ser establecida en el archivo Registry.pol. Cuando el archivo Registry.pol esta siendo analizado, si ese encuentra ****SecureKey=1** se establecen los siguientes permisos en la llave de registro que está siendo modificada actualmente:

Administradores: Control total

Sistema operativo: Control total

Usuario: Lectura

Una bandera reestablecida (****SecureKey=0**) regresa los ACLs a los ACLs que estén establecidos en la raíz de **HKCU**. Los proveedores de terceros pueden implementar esta funcionalidad a través de archivos .adm utilizando la palabra clave **SECUREKEY**. Esto le da al administrador un recuadro de selección en la

interfaz para habilitar la bandera segura. Esto se requiere por razones de legado. Las aplicaciones necesitan esta capacidad para contar con una llave segura cuando la aplicación todavía no utiliza el árbol HKCU\Software\Policies (que es seguro) para guardar sus configuraciones.

Nota: Cualquier aplicación que *no* guarde sus políticas en el árbol HKCU\Software\Policies se romperá cuando se mueve un usuario de una OU a otra con políticas diferentes. Esto se debe a que otras llaves no se encuentran limpias (eliminadas) durante el proceso de política.

Para eliminar llaves o valores, establezca un valor "**" en el archivo Registry.pol. Las llaves con esta designación son llaves especiales escritas en el archivo Registry.pol que le dicen a Winlogon que actúe de manera diferente basándose en estos valores. Vea la sección de formato de archivo Registry.pol para obtener detalles sobre la eliminación de llaves y valores.

Cuando se encuentra la palabra clave **SECUREKEY** una llave tipo DWORD, ****SecureKey**, se escribe en el archivo Registry.pol. El valor es 0 (no seguro) ó 1 (seguro). Esto le dice a Winlogon si debe de asegurar o no la llave correspondiente.

Cómo se crean archivos Registry.pol

La siguiente sección resume cómo formar archivos Registry.pol:

- Cuando inicia el editor de políticas de grupo, se crea un árbol temporal de registros que consiste de dos nodos: **USUARIOS** y **EQUIPOS**.
- Conforme explora el nodo de políticas de software del editor de políticas de grupo, se implementan archivos .adm y nodos de extensión *snap-in*. Los archivos .adm dentro de los nodos del editor de políticas de grupo se cargan dinámicamente cuando se selecciona un nodo específico y entonces se realiza el proceso de caché en el archivo .adm.
- Cuando se selecciona una política en el panel de detalles (el lado derecho de la ventana de la consola MMC), se consulta al registro temporal para determinar si la política seleccionada ya cuenta con valores de registros asignados a la misma; de ser así, estos valores se despliegan en el cuadro de diálogo **Política**.
- Si la política seleccionada no tiene un valor de registro asignado a ella, se utiliza el valor predeterminado del archivo .adm o de la extensión *snap-in* MMC asociada.
- Después de modificar una política, se escriben los valores de registro que especifique en la parte apropiada del registro temporal (ya sea **EQUIPO** o **USUARIO**).
- Cuando cierra el editor de Políticas de grupo, se exportan los enjambres del registro de temporal a los archivos Registry.pol en las carpetas apropiadas de la plantilla de políticas de grupo.
- La siguiente vez que inicia el editor de políticas de grupo para el mismo objeto de políticas de grupo para el cual estableció previamente políticas de grupo, se importa la información de registro de los archivos correspondientes Registry.pol al árbol de registro temporal. Por lo tanto, cuando ve las políticas,

éstas reflejarán el estado actual.

Nota: El editor de políticas de grupo guarda ésta información en dos ubicaciones distribuidas, el AD (contenedor de políticas de grupo) y Sysvol (plantilla de políticas de grupo). Ya que ésta información se guarda en ubicaciones distribuidas, existe la posibilidad de que se sobre escriban las configuraciones de políticas, como se ilustra en el siguiente ejemplo. Si dos administradores lanzarán el GPE enfocado sobre el mismo objeto de políticas de grupo y están actuando sobre diferentes controladores de dominios (DCs), cada uno de los administradores puede realizar modificaciones de políticas que pueden ser sobre escritas una por la otra. Note que en todos los casos, la última modificación de políticas será la que tendría efecto. Una manera de prevenir dicha circunstancia es que los administradores de dominio reduzcan el número de usuarios a los que se les otorga permiso para escribir a cualquier objeto de políticas de grupo.

Cómo se aplican las políticas de grupo

Las Políticas de grupo para computadoras se aplican al inicio de la computadora. Para usuarios, las Políticas de grupo se aplican cuando estos se conectan.

Procesamiento sincrono y asincrono

Puede especificar el procesamiento de Políticas de grupo para que éste sea asincrono o sincrono. Puede configurar esta opción utilizando la política de grupos de la misma manera que lo haría para *scripts* en Windows NT 4.0. La configuración de esta opción aplicará a todo el procesamiento de Políticas de grupo, política de software, implementación de aplicaciones y archivos y *scripts*. La opción predeterminada es procesar de manera asíncrona la política de grupo (de la misma manera en la que los *scripts* de conexión se procesan en Windows NT 4.0 y Windows 2000).

Procesamiento periódico

Puede especificar que se procese periódicamente la política de grupo. De manera predeterminada esto se realiza cada 8 horas y puede configurarse de 7 segundos a 45 días (1,080 horas).

El procesamiento de implementación de aplicaciones ocurre sólo durante el inicio de la computadora o cuando un usuario se conecta, no de manera periódica. Esto se debe a que un procesamiento periódico podría causar resultados indeseables. Por ejemplo, si una aplicación no estuviera asignada todavía, ésta se eliminaría. Si un usuario estuviera utilizando la aplicación mientras que la política de grupo tratará de desinstalarla o se realizara una actualización de una aplicación asignada mientras alguien la está utilizando, podría haber problemas.

Mensajes y eventos

Cuando se aplica la política de grupo**,** se envía un mensaje **WM_WININICHANGE** y se avisa un evento. Las aplicaciones que pueden recibir el mensaje lo pueden utilizar para responder a un cambio de políticas de grupo. Aquellas aplicaciones que no cuentan con una ventana para recibir el mensaje (como con la mayoría de los servicios) pueden esperar el evento.

Lectura de registros

Las APIs también existen para permitir que una aplicación reclame (asegure) una sección critica del registro, lea los valores requeridos y entonces libere la sección critica. Si no se libera la sección en 10 minutos, entonces la aplicación se verá forzada a liberarla. Esto asegura que la actualización de fondo de la política de grupo no ocurra durante el proceso de lectura.

Políticas de grupo y conexione de red (vínculos lentos)

Cuando Winlogon detecta un vinculo lento, éste establece la bandera **GPO_INFO_FLAG_SLOWLINK** en la estructura **GPO_INFO** para indicar que está siendo aplicada la política a través de un vinculo lento. Las extensiones individuales *snap-in* pueden determinar si se debe o no aplicar una política sobre un vinculo lento.

Las configuraciones predeterminadas son las siguientes:

- Política de software –encendido (y no puede ser apagado)
- *Scripts* - encendido
- Implementación de aplicaciones - apagado
- Implementación de archivos - apagado

Para los *scripts*, implementación de aplicaciones, configuración de usuario y *snap-in*s de documentos, se proporcionará una política de grupo para jalar las configuraciones.

Procesamiento a solicitud

La política de grupo también será aplicada a solicitud. Para realizar esto, las aplicaciones pueden llamar a la API **RefreshPolicy()** que permite a las aplicaciones solicitar una actualización de política.

Cambio de dominio

Cuando el dominio al cual pertenece una computadora cambia, Winlogon utilizará la API **RefreshPolicy()** para reaplicar la política de grupo. Este proceso ya no requiere una reinicialización

.

Objetos múltiples de políticas de grupo

Puede asociar objetos múltiples de políticas de grupo con un solo sitio, dominio o unidad organizacional y puede establecer prioridades en torno a cómo afectarán estos objetos de política de grupo al objeto de directorio al que están siendo aplicados. Por otro lado, varios sitios, dominios u OUs pueden utilizar un solo objeto de políticas de grupo.

Cualquier sitio, dominio u OU puede ser asociado con cualquier objeto de políticas de grupo, inclusive a través de dominios.

Jerarquía de políticas de grupo

De manera predeterminada, la política de grupo se hereda y es acumulativa y afecta a todas las computadoras y usuarios en un contenedor AD. Se procesa la política de grupo de acuerdo al siguiente orden: sitio, dominio y OU. El método de herencia predeterminado existe para evaluar la política de grupo iniciando con el contenedor AD más lejos de la computadora o del objeto del usuario. El contenedor AD más cerca de la computadora o al usuario puede anular la configuración de política de grupo en un contenedor de nivel más alto.

Existen opciones que le permiten reforzar las políticas de grupo en un objeto específico de políticas de grupo para que el objeto de políticas de grupo en contenedores AD de nivel más bajo no puedan anular esa política. También puede bloquear la herencia de políticas de grupo desde los contenedores AD padre. La opción validada siempre tiene preferencia.

Filtración del alcance del objeto de políticas de grupo

Puede redefinir aún más qué equipos de usuarios influencia un objeto específico de política de grupos al utilizar grupos de seguridad de Windows 2000. Esto significa que por cualquier objeto de política de grupo puede filtrar el efecto del objeto de política de grupo sobre los miembros de grupos específicos de seguridad. Para realizar esto, utilice el editor de la lista de control de acceso estándar. Puede tener acceso al editor ACL seleccionando la página **Propiedad** del objeto de políticas de grupo y después haciendo clic sobre **Seguridad**.

Los administradores también pueden utilizar el editor ACL para determinar qué usuarios pueden modificar un política de grupo.

Soporte de delegación

Usted delega políticas de grupo al crear y guardar consolas MMC del editor de políticas de grupo (archivos .msc), especificando después qué usuarios y grupos cuentan con permisos de acceso al objeto de políticas de grupo o a un contenedor AD específico (sitio, dominio u OU). Define permisos para un cierto objeto de políticas de grupo utilizando el editor ACL; éstos permisos otorgan o rechazan acceso al objeto de políticas de grupo a grupos específicos.

Establecimiento de permiso (ACLs) para políticas de grupo

La página *Propiedades* del Editor de políticas de grupo alberga al editor ACL de seguridad. Para utilizar el editor ACL, haga clic con el botón derecho del ratón en el nodo de raíz del Editor de políticas de grupo, haga clic en **Propiedades** y después haga clic en **Seguridad**. Utiliza la página de propiedad de *seguridad* para configurar permisos de acceso (ACLs) sobre un objeto seleccionado de políticas de grupo para permitir o rechazar acceso al objeto de políticas de grupo por grupos específicos.

Los administradores pueden especificar qué grupos de usuarios y computadoras cuentan con la posibilidad de *Aplicar acceso de registros* de control de acceso de

políticas de grupo (ACE) al GPO. Los grupos que ya cuentan con acceso de aplicación y de lectura de políticas de grupo al GPO reciben las políticas de grupo que se encuentran en éste y los grupos que no cuentan con acceso de aplicación de políticas de grupo o de lectura al GPO no obtienen las política de grupo que se encuentran en éste. De manera prederterminada, los usuarios autenticados tienen tanto los permisos de aplicación de política de grupos como de lectura de ACL. Esto significa que los usuarios no pueden modificar la información en el GPO.

Tome en cuenta que si coloca datos sensibles en un GPO que no desea que los usuarios afectados las puedan leer, es posible que desee cambiar los permisos predeterminados del ACL y otorgar permisos de lectura sólo a aquellos usuarios que requieran esos datos. De manera predeterminada, los administradores de dominio tienen permisos de control total, pero no cuentan con ACLs de aplicación de políticas de grupo. Esto significa que la política GPO no aplicaría de manera predeterminada para prestadores de dominios, pero estos podrán modificar GPOs.

Los administradores de red (miembros de un grupo de administradores de dominios) también pueden utilizar el editor ACL para determinar qué grupos de administradores pueden modificar políticas en GPOs. Para realizar esto, el administrador de red puede definir grupos de administradores (por ejemplo, administradores de mercadotecnia) y después proporcionarles, con acceso lectura/escritura a GPOs seleccionados. Esto permite a los administradores de red delegar control de las políticas GPO. El otorgamiento de acceso lectura/escritura a un GPO le permite a los administradores controlar todos los aspectos de este.

También estará albergado el editor ACL en el cuadro de diálogo administración de **políticas de grupo**. Para acceder el editor ACL haga clic con el botón derecho del ratón en el objeto AD en la consola MMC del administrador de Active Directory, haga clic en tarea, haga clic en **Administrar políticas de grupo** y después haga clic en **Seguridad**. De manera similar, también puede tener acceso al editor ACL en los sitios AD y en la consola MMC del administrador de servicios (al hacer clic primero en un objeto de sitio). Los administradores de dominios pueden entonces utilizar el editor ACL para establecer permisos de lectura/escritura para grupos de administradores como se describió anteriormente.

USO DE POLÍTICAS DE GRUPO EN COMPUTADORAS INDEPENDIENTES BASADAS EN WINDOWS 2000

Puede configurar las políticas para un equipo local para cualquier computadora que no sea miembro de un dominio. Para configurar una política local, utilice el editor de políticas de grupo enfocado en la computadora local. Podrá contar con acceso a la herramienta del Editor de políticas de grupo utilizando el *snap-in* MMC de administración de computadoras para la computadora local.

Objeto local de políticas de grupo

En políticas independientes, el objeto local de políticas de grupo (LGPO) existe—ésta es sólo la parte de la plantilla de la política de grupo. La ubicación del objeto local de políticas de grupo es %SystemRoot%System32\GroupPolicy. Al estar enfocado en un GPO, el Editor de políticas de grupo notifica sus extensiones y éstas se cargan basándose en si son apropiadas o no para un uso local.

La siguiente tabla indica si las extensiones del Editor de políticas de grupo (GPE) abrirán o no cuando el Editor de políticas de grupo esté enfocado en un objeto local de políticas de grupo.

Extensión del Editor de políticas de grupo	Cargado cuando el GPE este enfocado en LGPO
Implementación de aplicaciones	No
Implementación de archivos	No
Scripts	Sí
Política de software	Sí
Configuraciones de seguridad	Sí

Si una computadora no es miembro de un dominio, el Editor de políticas de grupo abrirá automáticamente el objeto local de políticas de grupo.

Prevención de computadoras en un dominio de políticas de grupos heredadas

Los administradores pueden ampliar ciertas computadoras de heredar políticas de grupo del dominio al cual pertenecen (o del sitio, si está configurada la política de la computadora a ese nivel de jerarquía de políticas). En dichos casos, la computadora funcionará como si fuera una computadora independiente con respecto a la política de grupo. Puede habilitar esta opción para cualquier objeto de políticas de grupo utilizando el siguiente interruptor de registro (éste estará incluido en el archivo .adm que viene con el producto):

```
HKLM\Software\Policies\Microsoft\Windows\System  DisableGPO Reg_Dword 1,0
```

Si configura este interruptor de registro, las computadoras afectadas sólo recibirán política del objeto local de políticas de grupo; es decir, no recibirán políticas del dominio. Esta capacidad es útil para computadoras no empresariales, por ejemplo, computadoras personales de empleados o aquellas para las cuales no se desea la política válida.

Siempre se procesan primer los objetos locales de políticas de grupo y después las

políticas de dominio. Si una computadora está participando en un dominio y ocurre un conflicto entre las políticas del dominio y de la computadora local, toma precedencia la política del dominio. Sin embargo, si una computadora ya no esta participando en un dominio, entonces se aplica la política LGPO.

AMPLIACION DE LA FUNCIONALIDAD DEL EDITOR DE POLITICAS DE GRUPO

Los desarrolladores de terceros de aplicaciones pueden aplicar la funcionalidad del editor de políticas de grupo para proporcionar políticas de grupo específicas a sus aplicaciones. Para este objetivo, ellos pueden:

- Crear una plantilla administrativa (archivo .adm). Para mayores informes, vea el Apéndice A: Plantillas administrativas.
- Crear una extensión *snap-in* MMC del Editor de políticas de grupo y proporcionar la interfaz para configurar políticas de grupo específicas a sus aplicaciones. Para guardar y distribuir las políticas, se recomiendan los siguientes mecanismos:
    - Use el API específico al *snap-in* MMC del Editor de políticas de grupo para escribir políticas de grupo basadas en registros en la plantilla de políticas de grupo. Se incluirá la documentación API del Editor de políticas de grupo en el Estuche de desarrollo de software de la plataforma Microsoft. Para mayores informes vea el siguiente URL:http://www.microsoft.com/msdn/sdk/platform.htm.
    - Use la función **GetFileSysPath** para guardar la información de políticas basada no en registro (basada en archivos) en la subcarpeta de la plantilla de políticas de grupo (GPT). Puede utilizar la convención de nombre de compañía/nombre App /Versión para dicha carpeta. Entonces puede colocar los archivos requeridos en esa subcarptea GPT. En el extremo del cliente, Winlogon puede llamar la extensión del extremo del cliente para la herramienta. Esto a su vez procesará la información guardada en el directorio en el GPT. Es decisión de desarrollador de la aplicación utilizar apropiadamente éste mecanismo. Al guardar los datos en la subcarpeta GPT la aplicación aprovecha los mecanismos incorporados en la política de grupos (el GPT y Winlogon) para aplicar políticas especiales basadas no en registros.

Para información sobre Microsoft Management Console vea la documentación de Microsoft Platform SDKpara *componentes para instalación y desarrolladores de servicios de administración de sistemas* en la siguiente URL:http://www.microsoft.com/mdsn/sdk/sysmgmt.htm.

SOPORTE A CLIENTES PARA WINDOWS 2000, WINDOWS 95 Y WINDOWS 98

La herramienta del Editor de políticas de Windows 2000 *no* proporciona soporte a clientes para Windows NT 4.0 y computadoras que estén ejecutando Windows 95 y Windows 98.

El soporte para clientes de Windows NT 4.0 se proporciona soportando totalmente las plantillas administrativas estilo Windows NT 4.0 (archivos .adm) y proporcionando los archivos de la herramienta del Editor de políticas de sistemas de Windows NT 4.0 (Poledit.exe). Sin embargo, la interfaz del Editor de políticas del sistema no aparecerá en la interfaz de Windows 2000.

Podrá instalar la herramienta del Editor de políticas del sistema Poledit.exe, en Windows 2000 profesional utilizando el paquete opcional de herramientas administrativas Windows 2000. Durante la instalación de Windows 2000 Server, puede escoger instalar un componente opcional llamado herramientas administrativas Windows 2000, un paquete de instalación de Windows (archivo .msi) que contiene toda la información necesaria para instalar las aplicaciones opcionales administrativas—este paquete se incluye en el producto Windows 2000 Server. Para información sobre la instalación del Editor de políticas del sistema y el uso del paquete de herramientas opcionales administrativas de Windows 2000 vea la documentación del producto Windows 2000 Server.

Los clientes que están ejecutando Windows 95 y Windows 98 aún requerirán utilizar el Editor de políticas del sistema de Windows NT 4.0, Poledit.exe.

Note que tanto Windows NT Workstations como las computadoras que estén ejecutando Windows 95 y Windows 98 tendrán que copiar el archivo .pol que se genere a la parte Netlogon del dominio (…\system32\Repl\Import\Scripts).

MIGRACION DE WINDOWS NT 4.0 A WINDOWS 2000

La migración de clientes basados en Windows NT 4.0-a Windows 2000 Professional y de servidores basados en Windows NT 4.0-a Windows 2000 Server en sus varias combinaciones generará comportamientos diferentes para las políticas de grupo. La siguiente tabla resume el comportamiento esperado, utilizando la siguiente nomenclatura:

LGP = Política local de grupo

LSDOU = Política local de grupo, sitio, dominio, OU

Dominio	Cliente de Windows NT 4.0 recibe ésta política	Cliente de Windows 2000 recibe ésta política
Windows NT 4.0	Windows NT 4.0	LGP + Windows NT 4.0
Windows 2000 AD – Windows 2000 modo nativo.	Windows NT 4.0	LSDOU
Windows 2000 AD – modo mezclado (predeterminado).	Windows NT 4.0	LSDOU + Windows NT 4.0
Windows 2000 DS – modo mezclado. Todos los controladores de dominio de Windows 2000 con el respaldo arriba de DCs de Windows NT 4.0.	Windows NT 4.0	LSDOU + Windows NT [1] Como conectarse con credenciales de caché. Si no esta establecido, entonces LGP + Windows NT 4.0.
Grupo de trabajo/independiente	No hay cambio del actual: 1. Sin política. 2. Si hay instalación, política de Windows NT 4.0 manual. 3. Si el cliente estaba previamente en un dominio Windows NT 4.0 el cliente recibirá la política restante del dominio.	1. LGP. 2. Si existe instalación, la política de Windows NT 4.0 será manual. 3. Si el cliente estaba previamente en un dominio de Windows 2000, el cliente recibirá a alguna política restante del dominio[2].

[1]Para hacer que esto funcione, requiere suponer que el papel de la computadora (cliente basado en Windows 2000-) es el mismo que el del usuario. Note que una excepción es un usuario que *nunca* ha tenido un perfil. En ese caso, el usuario *no* recibirá *política*.

[2]Las políticas restantes se refieren a aquellas políticas que están fuera de las dos ubicaciones de limpieza en el registro, **HKLM** y **HKCU** (\Software\Policies y \Software\Microsoft\Windows\Current Version). Por ejemplo, banderín de conexión.

Nota: Los archivos.adm de terceros que no utilizan el árbol de políticas también dejarán atrás políticas.

CONSIDERACIONES DE DISEÑO DE POLITICAS DE GRUPO

Esta sección resume temas que debe considerar al planear y diseñar su implementación de políticas de grupos.

Estructura de Active Directory e implementación de políticas de grupo

Cuando planea y diseña su estructura de Active Directory, necesita considerar cómo desea implementar las políticas de grupo para su empresa. Esto es muy importante ya que como se aplican las políticas de grupo depende en la estructura de Active Directory que defina. Si construye cuidadosamente su diseño de Active Directory tomando en cuenta las políticas de grupo, entonces podrá aprovechar al máximo su estructura de Active Directory y simplificar su implementación y administración de políticas de grupo.

Se aplica la política de grupo a los objetos de políticas de grupo que a su vez están asociados con contenedores específicos de Active Directory. La política de grupo se procesa de manera jerárquica en el siguiente orden: sitio, dominio y OU; el contenedor de Active Directory más cerca de la computadora o usuario anula la configuración de la política de grupo en un contenedor de Active Directory de nivel más alto. De manera predeterminada, las configuraciones que defina para la política de grupo son acumulativas y son heredadas desde los contenedores padre de Active Directory. Note que éste es el comportamiento predeterminado y que existen mecanismos que le permiten forzar o prevenir que políticas de grupo afecten a usuarios o computadoras en sitios, dominios u OUs. Sin embargo, para lograr un desempeño y simplificación óptimos, es mejor minimizar el uso de éstos mecanismos al aplicar la política de grupo. Para un control adicional, se pueden utilizar una o más membresías de computadoras o usuarios en grupos de seguridad para filtrar el efecto de un GPO. Esto se realiza modificando las ACLs para un GPO de tal manera que sólo los miembros de ciertos grupos de seguridad se vean afectados por un GPO.

El uso de las capacidades de las políticas de grupo en varias combinaciones hacen muy flexibles las políticas de grupo, permitiéndole cumplir con una variedad de requerimientos de negocios. El punto de cuidado más importante es utilizar la combinación más simple de estas capacidades y planear cuidadosamente su uso. La siguiente sección enumera ejemplos específicos de áreas a considerar al realizar la planeación de políticas de grupo.

Minimice el uso de la función de herencia de políticas de bloque

Como se mencionó anteriormente, puede evitar que las configuraciones de políticas de grupo de contenedores AD padres afecten a usuarios y computadoras en contenedores de nivel más bajo. Esto es una función útil y poderosa que debe usar concienzudamente sólo cuando usa situación particular lo requiera. El bloqueo de la herencia de política por parte de contenedores AD padre puede complicar la política de solución de problemas.

Minimice el uso de la función de herencia de política de fuerza

También puede asegurar que las configuraciones de políticas que especifique en un objeto dado de políticas de grupo en un contenedor AD de nivel más alto se

refuerce en contenedores AD de nivel más bajo. Sólo utilice esta función poderosa y de ayuda cuando las circunstancias lo requieran. El sobre uso de ésta función con otras funciones relacionadas tales como la herencia de política de bloqueo puede complicar la política de solución de problemas.

Minimice el número de objetos de políticas de grupo asociados con usuarios en contenedores de Active Directory

Puede asignar más de un objeto de políticas de grupo a un contenedor AD particular si su situación lo requiere; sin embargo, debe notar que el número de objetos de políticas de grupo que asigne pueden afectar el tiempo de proceso de conexión. Durante el tiempo de conexión, cada objeto de políticas de grupo asociado con un contenedor AD (y que el usuario o la computadora tenga que aplicar acceso de aplicación ACE de política de grupos) se procesa, así que entre más sean los objetos de políticas de grupo asociados, mayor será el tiempo de conexión que se requiera para procesarlos.

Una manera de minimizar el número de objetos de políticas de grupo que afectan a los usuarios es utilizar grupos de seguridad como una manera de filtrar GPOs. Si aplica políticas desde varios objetos de políticas de grupo a un contenedor de Active Directory y utiliza filtros de políticas de grupo, haciendo que algunas políticas sean invisibles a algunos usuarios, se mejorará significativamente el rendimiento. Esto se debe a que se procesarán un número menor de objetos de políticas de grupo.

Si su situación requiere que utilice filtros basado en grupos de seguridad, debe asegurarse que los usuarios a los que pretende que reciban políticas desde un *objeto particular de políticas de grupo* tengan acceso de aplicación ACE de política de grupos a ese GPO. Si los usuarios no tienen acceso de aplicación de políticas de grupo a ese GPO, no obtendrán esas políticas.

Anule las políticas de grupo basadas en usuarios con políticas de grupo basadas en computadoras sólo cuando sea necesario

Puede establecer las configuraciones del usuario por computadora y por lo tanto anular las políticas especificas del usuario con políticas especificas de computadora. Esto es útil cuando desea proporcionar una configuración de escritorio específica sin importar que usuario se conecte a la computadora. Para establecer configuraciones de usuario por computadora, debe utilizar el nodo de políticas de software en las configuraciones de computadoras en la consola del Editor de políticas de grupo.

Trate de no utilizar las asignaciones GPO a través de dominios

Aunque puede asignar objetos de políticas de grupo desde diferentes dominios a un solo contenedor AD si una situación particular lo requiere, note que en dichos casos sería mucho más lento el procesamiento de políticas de grupo. Esto se debe a que se cruzan las fronteras de dominio.

Administración de objetos de políticas de grupo

La delegación de autoridad, separación de tareas administrativas, la administración

central contra la distribuida y la flexibilidad en el diseño son factores importantes que necesita considerar al diseñar políticas de grupo y al seleccionar qué escenarios utilizará para su empresa.

Si implementa o no políticas de grupo de manera modular (por ejemplo, creando un objeto de políticas de grupo específico para opciones de administración de software, un objeto de políticas de grupo específico para opciones de configuración de seguridad y así sucesivamente) será determinado por los requerimientos administrativos y los roles en su empresa. Por ejemplo, si los administradores están organizados de acuerdo con sus tareas (tales como administradores de gestión de software, administradores de seguridad, administradores de conexión, etc.),puede resultarle útil definir políticas en los módulos de políticas de grupo.

La delegación o autoridad dependerá en gran parte en si utiliza administración centralizada o distribuida de su empresa. Basándose en los requerimientos particulares de su empresa, los administradores de red pueden utilizar los permisos ACL para determinar qué grupos y administradores pueden modificar políticas en los objetos de políticas de grupo. Los administradores de redes pueden definir grupos de administradores (por ejemplo, administradores de gestión de software) y después proporcionarles acceso lectura/escritura para seleccionar objetos de políticas de grupo, permitiéndole a los administradores de red delegar el control de las políticas de objeto de políticas de grupo. Los administradores que cuentan con acceso lectura/escritura a un objeto de políticas de grupo pueden controlar todos los aspectos de ese objeto de políticas de grupo. Si es un administrador de red que utiliza administración centralizada, puede escoger entre otorgarle a otros administradores acceso de sólo lectura a objetos de políticas de grupo. La realización de esto le permitiría a aquellos administradores ver los objetos de políticas de grupo, pero no podrían cambiarlos.

APENDICE A: PLANTILLAS ADMINISTRATIVAS

Creación de archivos .Adm personalizados

Para definir las configuraciones de interfaz, los administradores pueden configurar el Editor de políticas de grupo que utiliza ya sea las plantillas administrativas (archivos .adm) o los *snap-ins* de extensión MMC sobre el MMC del Editor de políticas de grupo. Puede crear archivos .adm personalizados para ampliar las capacidades del Editor de políticas de grupo. Las siguientes secciones presentan información sobre el lenguaje y los componentes ADM:

El archivo .adm:

- Define una jerarquía de categorías y subcategorías que conjuntamente especifican las configuraciones de registro que se pueden modificar utilizando la interfaz del Editor de políticas de grupo.
- Indica las ubicaciones de registro donde se deben de realizar los cambios en caso de una selección específica.
- Especifica cualquier opción o restricción (en valores) asociada con una cierta selección.
- En algunos casos, especifica un valor predeterminado a utilizar si se activa la selección.

Agregar archivos .adm

Para agregar sus archivos .add seleccione **Políticas de software** el nodo **Configuraciones de la computadora** o **Configuraciones del usuario** en la consola MMC del Editor de políticas de grupo y después seleccione **Agregar/eliminar plantillas** desde el menú **Tareas**.

Cuando agrega un archivo .adm, se agrega ese archivo a la carpeta Sysvol\Policies\GPO_GUID\ADM del objeto de políticas de grupo actualmente seleccionado. El espacio de nombre del Editor de políticas de grupo se define por la jerarquía de los nombres de la categoría y subcategoría especificados en el archivo .adm. Los nombres de nodos que son idénticos pero aparecen en diferentes archivos .adm son desplegados sólo una vez en el espacio del nombre. Esto difiere de la manera en que funciona el Editor de políticas de sistemas en que el Editor de políticas de sistemas los despliega más de una vez en dichos casos.

Convenciones de nombramiento para el espacio del nombre

Cuando crea registros personalizados para el nodo de políticas de software, recomendamos ampliamente que cree el espacio del nombre utilizando \nombre de compañía\producto\versión en la convención de nombramiento (o\nombre de compañía\producto y versión) que también se utiliza en el registro. Por ejemplo, la configuración del sistema operativo para Windows 2000 estaría en \Microsoft\Windows.

Política para ubicaciones de llave de registro

Las siguientes ubicaciones de la llave de registro que serán limpiadas sin la política ya no será aplicada; otras llaves *no* serán limpiadas. Debe asegurarse de que utilice éstas llaves para políticas al escribir archivos .adm personalizados:

HKEY_LOCAL_MACHINE\Software\Policies (para política de computadoras)

HKEY_CURRENT_USER\Software\Policies (para política de usuarios)

También se limpian dos llaves anteriores, pero debe de notar que esto sólo se realiza para proporcionar compatibilidad hacia niveles inferiores. No se deben utilizar estas llaves:

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies

Componentes de lenguaje ADM

ADM proporciona un lenguaje de esquema de trabajo. Un archivo de plantilla (.adm) describe un número de categorías. Cada una de éstas categorías puede contener cero o más políticas y cada política a su vez puede contener cero o más partes. La siguiente sección describe los diferentes componentes del lenguaje ADM.

Nota: Esta sección sólo cubre las políticas obligatorias del sistema y de aplicación que fueron administradas previamente utilizando la herramienta de edición de políticas del sistema Windows NT 4.0. Las versiones posteriores a Beta 2.0 de Windows 2000 presentarán información actualizada sobre la creación de archivos .adm.

Comentarios

Puede agregar comentarios a un archivo .adm precediendo el comentario ya sea con un punto y coma (;) o con dos diagonales hacia adelante (//). Puede comentar comentarios al final de cualquier línea válida.

Extensiones

El Editor de políticas de grupo requiere que se defina una extensión en la sección **[extensiones]** del archivo .adm para cualquier cosa que esté precedida "!!". El propósito de esto es utilizar variables para definir extensiones largas de texto que aparecerán en la interfaz y definir esas extensiones sólo una vez. Esto es útil si las extensiones se utilizan en ubicaciones múltiples en todo el archivo .adm. Este método también permite una conversión más fácil a otros lenguajes (localización). La extensión debe de estar entre comillas.

CATEGORY, **POLICY**, **PART** y **DEFAULT** deben estar siempre definidos utilizando el mecanismo variable [extensiones]. Aunque no se requiere este método (por que las extensiones entre comillas pueden estar codificadas de base), no utilizar el método variable de extensiones imposibilita la reutilización de las extensiones y presenta problemas para la localización del archivo.

De manera opcional, puede poner un nombre variable entre comillas dobles. Los nombres con espacio deben estar entre comillas dobles.

Ejemplo variable [extensiones]

En el cuerpo de un archivo .adm puede describir el nombre **CATEGORY** de la siguiente manera:

```
CATEGORY !!FirstCategory
```

Después en la sección **[extensiones]** puede definir la variable :

```
FirstCategory="My First Category"
```

Resultado: La extensión `My First Category` (sin las comillas) aparecería en la interfaz del Editor de políticas de grupo.

CLASS

El primer registro en el archivo .adm es **CLASS** xxxx, donde *xxxx* puede ser uno de los siguientes:

- **ACHINE.** Esta sección incluye registros que se encuentran en el nodo de configuraciones de la computadora en el Editor de políticas de grupo.
- **SER.** Esta sección incluye registros que se encuentran en el nodo de configuraciones del usuario en el Editor de políticas de grupo.

Note que sólo existen dos clases válidas dentro de un archivo .adm. Si el archivo .adm contiene una clase que es cualquier otra cosa que no sea una clase válida, se ignoran los errores cuando se carga el Editor de políticas de grupo.

CATEGORY

Se muestra el nombre **CATEGORY** en el Editor de políticas de grupo como un nodo ya sea en las configuraciones de la computadora o en las configuraciones del usuario, dependiendo bajo qué **CLASS** esté la **CATEGORY**.

La sintaxis de **CATEGORY** es la siguiente:

```
CATEGORY !!"variable name"
        [KEYNAME "key name"]
        [... policy definition statements ...]
END CATEGORY
```

donde:

`variable name` es el nombre **CATEGORY** que debe de aparecer en la caja de lista del Editor de políticas de grupo. Opcionalmente puede estar entre dobles comillas. Los nombres con espacios deben de estar entre dobles comillas.

`key name` es un nombre de llave de registro opcional a utilizar para **CATEGORY**. Si se especifica un nombre de llave, éste será usado por todas las categorías, políticas y partes hijo, a menos de que se proporcione específicamente un nombre propio de la llave. Los nombres con espacios deben estar entre dobles comillas.

Puede no aparecer una declaración de definición de política más de una vez en una sola categoría.

A continuación aparece un ejemplo:

```
CATEGORY !!MyNewCategory
```

Para cerrar la categoría después de llenar las opciones, utilice:

```
END CATEGORY ; MyNewCategory
```

Note que éstas pueden estar acopladas para crear subcategorías como en el siguiente ejemplo:

```
CATEGORY !!FirstCategory
   CATEGORY !!SecondCategory
     CATEGORY !!ThirdCategory
     ...
     ...
     END CATEGORY ; ThirdCategory
   END CATEGORY ; SecondCategory
END CATEGORY ; FirstCategory
```

POLICY

Para identificar **POLICY** que puede ser modificada por el usuario, utilice la palabra clave **POLICY**. Esto es similar a la palabra clave **CATEGORY** ya que iniciamos definiendo lo siguiente:

```
POLICY !!MyFirstPolicy
...//Then fill in all the policy specifics.
...//And finish with the following:
END POLICY
```

Puede utilizar varios nombres clave **POLICY** bajo un nombre **CLAVE**. En el ejemplo anterior, debe definir la variable **MyFirstPolicy** en la sección **[extensiones]** del archivo .adm.

VALUENAME

Define las opciones disponibles dentro de una política. Debe identificar primero el valor del registro que debe ser modificado como resultado de utilizar la palabra clave **VALUENAME**. Por ejemplo, **VALUENAME MyFirstValue**.

A menos de que especifique lo contrario, el valor será escrito en el siguiente formato cuando el usuario marque o deje la opción en blanco:

- **Seleccionada. REG_DWORD** con un valor de 1.
- **Sin seleccionar.** Elimine completamente el valor.

Están disponibles otras opciones y están enumeradas en las siguientes secciones. Si la opción a ser seleccionada en el panel inferior del Editor de políticas de grupo entonces **VALUENAME** necesita estar dentro de una **PARTE** (ver la sección PARTE).

VALUEOFF /VALUEON

Puede utilizar **VALUEOFF/VALUEON** para escribir valores específicos basándose en el estado de la opción. Para habilitar esta funcionalidad al escribir el archivo .adm como se describe en los siguientes ejemplos:

```
KEYNAME ....
   POLICY !!MyPolicy
   VALUENAME ValueToBeChanged
   VALUEON "Turned On" VALUEOFF "Turned Off"
   END POLICY
```

o:

```
KEYNAME ....
   POLICY !!MyPolicy
   VALUENAME ValueToBeChanged
   VALUEON 5 VALUEOFF 10
   END POLICY
```

Palabra clave de Ayuda

En cada política, existe una palabra clave **AYUDA** seguida por lo menos por un espacio y la extensión de ayuda en comillas o una referencia a la extensión de ayuda. Por ejemplo:

```
POLICY !!NetCache
    KEYNAME Software\Policies\Microsoft\Windows\NetCache

#if VERSION >= 3
    HELP !!IntelliMirrorHelp
#endif

       .....

[Strings]
IntelliMirrorHelp="Help for Windows NT IntelliMirror\n\nThis policy
allows you to configure the file system caching options."
```

En el ejemplo anterior, se ofrece Ayuda a las opciones de caché del lado del cliente (CSC). La palabra clave `HELP` está envuelta en la versión define para permitir que será utilizado el mismo archivo .adm con el Editor de políticas anterior (que es la versión 2).

#if Version (para una comparación de versiones)

La siguiente sintaxis se utiliza para comparaciones de versiones:

```
#if Version (operator) x
#endif
```

Los operadores válidos se muestran en la siguiente tabla.

Operador	Significa
>	Mayor a,. Por ejemplo, *a* > *b* significa que a es mayor a b.
<	Menor a. Por ejemplo, *a* < *b* significa que a es menor a b.

==	Igual. Por ejemplo, *a* == *b* significa que a es igual a b.
>=	Mayor a o igual a. Por ejemplo, *a* >= *b* significa que a es mayor o igual a b.
<=	Menor a o igual a. Por ejemplo, *a* <= *b* significa que a es menor o igual a b.

PART

Puede utilizar **PART** para especificar varias opciones, incluyendo cuadros de listas desplegables, cuadros de texto y texto en el panel inferior del Editor de políticas de grupo.

La sintaxis de **PART** es:

```
PART [!!]name  PartType
  type-dependent data
  [KEYNAME KeyName ]
  VALUENAME ValueName
END PART
```

donde:

name es el nombre **PART** como debe de aparecer en el cuadro de la lista del Editor de políticas de grupo. Opcionalmente puede estar entre dobles comillas. Los nombres con espacios deben estar entre dobles comillas. Como una extensión de texto visible en la interfaz, debe de utilizar la variable **[EXTENSIONES]!!**.

PartType es la bandera de la parte de la política. Las banderas se analizan de manera individual en la sección **PartTypes**.

type-dependent data es información a cerca de la parte.

KeyName es un nombre clave opcional a ser utilizado. Si no se especifica un nombre clave, se utiliza el nombre clave anterior en la jerarquía.

ValueName es el nombre del valor a utilizar para establecer los datos para esta parte.

A continuación aparece un ejemplo del uso de **PART**:

```
PART !!MyVariable     FLAG(s)  {one or more, defined later}
...
       FIN DE PARTE
```

o:

```
PART !!MyVariable     FLAG(s)        END PART
```

PartTypes

El lenguaje ADM básico permite la creación de un archivo .adm simple que crea un **VALUENAME** de tipo **REG_DWORD** con un valor de 1, o elimina completamente el valor. El uso de los siguientes modificadores puede proporcionar opciones adicionales. **PartType** referenciada anteriormente en la sección **PART** puede ser uno de los siguientes:

TEXT

Muestra una línea de texto estático (etiqueta). No existe valor de registro asociados para este tipo de parte. El tipo de parte **TEXT** acepta datos que no son específicos a cierto tipo. Este es útil para mostrar un mensaje descriptivo en el panel inferior.

EDITTEXT

Muestra un campo de edición que acepta texto alfanumérico. Se establece el texto en el registro con el tipo **REG_SZ**. El tipo de parte **EDITTEXT** acepta las siguientes opciones:

- Valor **DEFAULT**. Especifica la extensión inicial a colocar en el campo de edición. Si no se especifica ésta opción, el campo esta vacío inicialmente.
- Valor **MAXLEN**. Especifica la longitud máxima de una extensión. La extensión en el campo de edición está limitada a ésta longitud.
- **REQUIRED**. Especifica que el Editor de políticas de grupo no permitirá una política que contenga la habilitación de ésta parte, a menos de que se haya registrado un valor para ésta parte.
- **OEMCONVERT**. Establece el estilo **ES_OEMCONVERT** en el campo de edición para que el texto escrito sea correlacionado desde ANSI a OEM y de viceversa.

COMBOBOX

Muestra una caja combo. El tipo de parte **COMBOBOX** acepta las mismas opciones que **EDITTEXT** así como la opción **SUGGESTIONS** que inicia una lista de sugerencias a ser colocada en una lista desplegable. **SUGGESTIONS** están separadas con espacio y deben estar entre comillas cuando un valor incluye espacios. La lista termina con **END SUGGESTIONS**.

Por ejemplo:

```
SUGGESTIONS
  Alaska Alabama Mississippi "New York"
END SUGGESTIONS
```

CHECKBOX

Muestra una caja de selección. Se establece este valor en el registro con el tipo **REG_DWORD**. El valor debe de ser diferente a cero si el usuario selecciona la caja, y cero en caso contrario. El tipo de parte **CHECKBOX** acepta las siguientes opciones:

- **ACTIONLISTOFF.** Especifica una lista de acciones opcionales a utilizar si está apagada la caja de selección.
- **ACTIONLISTON.** Especifica una lista de acciones opcionales a utilizar si está encendida la caja de selección.
- **DEFCHECKED.** Genera que esté seleccionada inicialmente la caja de selección.
- **VALUEOFF.** Anula el comportamiento preestablecido "apagado" de la caja de selección, si está especificado.

- **VALUEON.** Anula el comportamiento preestablecido “encendido” de la caja de selección, si está especificado.

El comportamiento preestablecido de una caja de selección es describir el valor 1en el registro si está seleccionada y 0 si no está seleccionada. **VALUEON** y **VALUEOFF** se utilizan para anular este comportamiento. Por ejemplo, la siguiente opción escribe “Fred” en el registro cuando está seleccionada la caja de selección:

```
VALUEON “Fred”
```

La siguiente opción describe el valor 12 en el registro cuando no está seleccionada la caja de selección:

```
VALUEOFF NUMERIC 12
```

DROPDOWNLIST

Muestra una caja combo con un estilo de lista desplegable. El usuario sólo puede escoger uno de los registros proporcionados. La ventaja principal de una caja combo con una lista desplegable es que se pueden especificar varias ediciones de registro adicionales, basadas en la selección del usuario. El tipo de parte **DROPDOWNLIST** acepta las opciones **ITEMLIST** y **REQUIRED**.

ITEMLIST inicia una lista de artículos en la lista desplegable, que debe de terminar con **END ITEMLIST**.

Cada **ITEMLIST** en la opción de lista de artículos se debe especificar de la siguiente manera:

```
NAME name VALUE value
[ACTIONLIST actionlist]
...
```

donde

name es el texto a mostrarse en la lista desplegable para este artículo.

Value es el valor a escribir como el valor de la parte si se selecciona este artículo. Se supone que los valores son extensiones, a menos que estén precedidos por **NUMERIC**. El siguiente ejemplo muestra tanto valores de extensión como numéricos:

```
VALUE “Some value”
VALUE NUMERIC 1
```

Si **VALUE** está seguido por **DELETE** (por ejemplo, **VALUE DELETE**), el nombre del valor de registro y el par del valor se eliminarán.

ACTIONLIST es una lista de acción opcional a ser utilizada si se selecciona el valor.

REQUIRED especifica que el editor de políticas de grupo no permitirá una política que contenga la habilitación de esta parte a menos que se registre un valor para la parte.

LISTBOX

Muestra una caja de lista con los botones **Add** y **Remove**. Este es el único tipo de parte que puede ser utilizado para administrar varios valores bajo una llave. La opción **VALUENAME** no se puede utilizar con el tipo de parte **LISTBOX,** ya que no existe ningún nombre de valor asociado con este tipo. De manera preestablecida, sólo aparece una columna en la caja de lista y se crea un valor por cada registro cuyo nombre y valor sean los mismos. Por ejemplo, un registro “Fred” en la caja de lista crearía un valor llamado “fred” cuyos datos serian “fred”.

El tipo de parte **LISTBOX** acepta las siguientes opciones:

- **ADDITIVE**. De manera predeterminada, el contenido de las cajas de lista anula cualquier valor establecido en el registro meta. Esto significa que se inserta un valor de control en el archivo de políticas que causa que los valores existentes sean eliminados antes de que se fusione el conjunto de valores en el archivo de políticas. Si se especifica esta opción, no se eliminan los valores existentes y los valores establecidos en la caja de lista existirán además de cualquier otro valor que exista en el registro meta.
- **EXPLICITVALUE**. Esta opción causa que el usuario especifique los datos de valor y el nombre del valor. La caja de lista muestra dos columnas, una para el nombre y otra para los datos. Note que no se puede utilizar esta opción con la opción **VALUEPREFIX**.
- Prefijo **VALUEPREFIX**. El prefijo que especifica se usa para determinar los nombres de valor. Si se especifica un prefijo, el prefijo y un número íntegro incremental se utilizan en lugar del esquema de nombres de valor previamente descrito. Por ejemplo, un prefijo “SomeName” generará nombres de valor “SomeName1”, “SomeName2”, y así sucesivamente. El prefijo puede estar vacío (“”), lo que causaría que los nombres de valor fueran “1”, “2”, y así sucesivamente.

NUMERIC

Presenta un campo de edición con un control opcional (un control hacia arriba y hacia abajo) que acepta un valor numérico. Se establece el valor en el registro con el tipo **REG_DWORD** .

El tipo de parte **NUMERIC** acepta las siguientes opciones:

- Valor **DEFAULT**. Especifica el valor numérico inicial para el campo de edición. Si no se especifica esta opción, el campo está inicialmente vacío.
- Valor **MAX**. Especifica el valor máximo para el número. El valor preestablecido es 9999.
- Valor **MIN**. Especifica el valor mínimo para el número. El valor preestablecido es 0.
- **REQUIRED**. Especifica que el Editor de políticas de grupo no permitirá una política que contenga la habilitación de esta parte a menos que se haya registrado un valor para esta parte.
- Valor **SPIN**. Especifica incrementos a utilizar para el control *spinner*.

- **SPIN 0**. Quita el control *spinner*. **SPIN 1** es el valor preestablecido.
- **TXTCONVERT**. Escribe valores como extensiones **REG_SZ** (“1”, “2” ó “128”) en lugar de valores binarios.

Por ejemplo:

```
PART !!MyVariable      NUMERIC
VALUENAME ValueToBeChanged
END PART
```

TEXT

Sólo presenta texto.

Por ejemplo:

```
PART !!MyVariable      TEXT
END PART
```

NUMERIC

Escribe valores en el registro con tipos de datos **REG_DWORD**. Este es el valor preestablecido a menos que se especifique otro.

Por ejemplo:

```
PART !!MyVariable      NUMERIC
VALUENAME ValueToBeChanged
END PART
```

EXPANDABLETEXT

Escribe un valor en el registro con el tipo de datos **REG_EXPAND_SZ**.

Por ejemplo:

```
PART !!MyVariable      EDITTEXT EXPANDABLETEXT
VALUENAME ValueToBeChanged
END PART
```

EDITTEXT

Describe valores en el registro con tipos de datos **REG_SZ**.

Por ejemplo:

```
PART !!MyVariable      EDITTEXT
VALUENAME ValueToBeChanged
END PART
```

REQUIRED

Genera un error si el usuario no ha registrado un valor cuando se requiere.

Por ejemplo:

```
PART !!MyVariable      EDITTEXT REQUIRED
VALUENAME ValueToBeChanged
END PART
```

MAXLEN

Especifica la longitud máxima del texto.

Por ejemplo:

```
PART !!MyVariable      EDITTEXT
VALUENAME ValueToBeChanged
MAXLEN 4
END PART
```

PRESET

Especifica un valor preestablecido. Se puede utilizar para datos de texto o numéricos.

Por ejemplo:

```
PART !!MyVariable      EDITTEXT
DEFAULT !!MySampleText
VALUENAME ValueToBeChanged
END PART
```

o:

```
PART !!MyVariable      NUMERIC
DEFAULT 5
VALUENAME ValueToBeChanged
END PART
```

MIN/MAX

Especifica los valores validos más bajos y más altos.

Por ejemplo:

```
PART !!MyVariable      NUMERIC
MIN 100 MAX 999 DEFAULT 55
VALUENAME ValueToBeChanged
END PART
```

DROPDOWNLIST

Despliega una caja de lista con opciones entre las cuales se puede escoger.

Por ejemplo:

```
PART !!MyVariable      DROPDOWNLIST
VALUENAME ValueToBeChanged
  ITEMLIST
NAME "First"   VALUE NUMERIC 1
    NAME "Second" VALUE NUMERIC 2
    NAME "Third"       VALUE NUMERIC 3
    NAME "Fourth"      VALUE NUMERIC 4
  END ITEMLIST
END PART
```

Line Breaks

Para crear un salto de línea, utilice la siguiente sintaxis:

```
\n
```

APENDICE B: DESCRIPCION GENERAL DE ACTIVE DIRECTORY

En Windows 2000, se aplican las configuraciones de las políticas de grupo a un objeto de políticas de grupo (GPO), el que a su vez está asociado con objetos seleccionados de Active Directory (AD) tales como sitios, dominios o unidades organizacionales (OUs). Está sección presenta los conceptos clave relacionados con el nuevo Active Directory de Windows 2000 y es importante que los entienda antes de proceder con los conceptos de políticas de grupo.

Windows 2000 introduce Active Directory, un servicio de directorio que es seguro, distribuido, está separado en particiones y duplicado. Active Directory amplía la funcionalidad previa del directorio basada en Windows y también proporciona funciones nuevas.

Un directorio es una estructura jerárquica de información que guarda información acerca de objetos en la red. Un servicio de directorio, como Active Directory, incluye el directorio mismo y los servicios que ponen a disposición la información.

Active Directory proporciona a los usuarios de red acceso a recursos en cualquier parte de la red utilizando una sola conexión. También proporciona a los administradores un punto único de administración para todos los objetos en la red que se puede organizar en una estructura intuitiva y jerárquica. Además, Active Directory proporciona los siguientes beneficios:

Consultas

Active Directory genera un catálogo global que pueden usar los usuarios y administradores para encontrar cualquier objeto en la red, utilizando cualquier atributo de ese objeto. Por ejemplo, puede encontrar un usuario por su primer nombre, apellido, alias de correo electrónico, ubicación de oficina u otro atributo de la cuenta de usuario de esa persona.

Las computadoras que estén ejecutando un cliente soportado por Active Directory proporcionan opciones de menú que le permiten al cliente consultar el catálogo global para obtener información.

Administración mejorada

Una lista mejorada de control (ACL), o permisos, controla qué usuarios pueden ver y acceder a los objetos en Active Directory. Una ACL de un objeto enumera qué usuarios pueden ver o utilizar el objeto y qué acciones especificas se pueden realizar sobre ese objeto. Se puede otorgar acceso específicamente a cada atributo individual de un objeto.

La seguridad de Active Directory soporta tanto herencia como delegación de autoridad. La herencia permite que se copie el conjunto de permisos de un objeto específico a todos sus objetos hijos. Los administradores pueden delegar autoridad y otorgar derechos administrativos específicos para contenedores y subárboles a otros individuos y grupos.

Información sobre seguridad

Para proporcionar mecanismos más fuertes y efectivos de seguridad;

interoperabilidad con entidades externas tales como Internet y compatibilidad con los clientes existentes; Windows NT Server soporta una variedad de protocolos de seguridad de red.

Kerberos versión 5, un estándar de seguridad de Internet, es el protocolo preestablecido para la autenticación de red en Windows NT Server. Windows 2000 también soporta los siguientes:

- Protocolos basados en llave pública, incluyendo Secure Sockets Layer 3.0
- Autenticación de contraseña distribuida
- Protocolo de Windows NT LAN Manager (NTLM) que utiliza Windows NT versión 4.0 y anteriores

Duplicación

Dentro de cada dominio, se duplica el directorio en cada servidor que esté ejecutando Active Directory. Si el dominio contiene varios servidores Active Directory (también conocidos como controladores de dominio), se duplica el directorio a varios servidores. Cada uno de éstos guarda y mantiene una copia completa del directorio del dominio. Los beneficios de la duplicación incluyen tolerancia de fallas, balance de carga y rendimiento mejorado.

Active Directory utiliza duplicación multimaestra, que le permite cambiar información en cualquier servidor que contenga el directorio y copiar automáticamente los cambios a los otros servidores.

Particiones de información

Con Active Directory, el directorio de cada dominio guarda información sólo acerca de los objetos ubicados en ese dominio, en lugar de utilizar un almacén masivo.

Active Directory permite el uso de varias particiones de directorio para la escalación de compañías muy pequeñas a muy grandes.

Facilidad de ampliación del directorio

Active Directory es totalmente ampliable. Esto significa que puede agregar tipos de objetos nuevos al directorio y atributos nuevos a tipos de objetos existentes utilizando ya sea la herramienta del administrador de esquema del directorio activo o escribiendo un programa. También puede escribir *scripts* de líneas de comando para administrar objetos de Active Directory. Los *scripts* utilizan el lenguaje de *script* que proporcionan las interfaces de servicio de Active Directory.

Integración con DNS

Active Directory utiliza el sistema de nombres de dominios (DNS), un conjunto de protocolos y servicios que se utiliza a través de Internet y otras redes de protocolo de control de transporte/Protocolo de Internet (TCP/IP). DNS proporciona registro de nombres y servicios de resolución de nombres a dirección, que permite la identificación de conexión de computadoras y usuarios en redes TCP/IP.

DNS permite el uso de nombres “amigables” de estructura jerárquica. Por ejemplo, DNS permite que se refiera a una computadora por medio de un nombre tal como **oficinascentrales.sucompañía.com**, en vez de la dirección TCP/IP de la computadora.

Active Directory implementa un modelo de nombres de dominios y objetos basado en el sistema de nombres de dominio. Los nombres de dominio de Windows 2000 corresponden a los nombres preestablecidos del dominio DNS.

Windows 2000 soporta DNS *dinámico*, que permite a los servidores actualizar las bases de datos DNS mientras ejecutan el sistema operativo. DNS dinámico se describe en el documento Requerimientos de Internet para comentarios 2136.

Interoperación con otros directorios

Active Directory soporta otros estándares de la industria, tales como la versión 2 y 3 del Protocolo de acceso de directorio ligero (LDAP), la Interfaz del proveedor de servicio de nombres (NSPI) y el Protocolo de transferencia de hipertexto (HTTP).

LDAP es el protocolo central de Active Directory. Es un protocolo de servicio de directorio estándar de la industria que permite a Active Directory compartir información con cualquier otro servicio de directorio que soporte LDAP.

Al soportar esos estándares, Active Directory puede ampliar sus servicios a través de varios espacios de nombres y lidiar con información y recursos ubicados en Internet, otros sistemas operativos u otros directorios.

Espacio de nombre de Active Directory

Active Directory incluye un nuevo modelo de dominio y espacio de nombre jerárquico.

Dominios

La unidad central de Active Directory de Microsoft Windows 2000 es el dominio. Todos los objetos de la red [1] existen dentro de un dominio. Para controlar el acceso a los objetos, se utilizan las listas de control de acceso (ACLs) pobladas con registros de control de acceso (ACEs). Los permisos de acceso son acumulativos dentro de un dominio, a menos que se hayan denegado explícitamente. De manera preestablecida, los derechos de administración están limitados a las fronteras de dominio.

Los dominios también son unidades de duplicación. Un solo dominio puede abarcar varias ubicaciones o sitios físicos. A diferencia del modelo único maestro que utiliza Windows NT 3.*x* y 4.0, con los Controladores de dominio primario (PDCs) y Controladores de dominio de respaldo (BDCs), Active Directory utiliza un modelo multimaestro de “controlador de compañeros”. Así pues, todos los controladores de dominio (DCs) tienen autoridad para que un cierto dominio pueda recibir cambios

[1] Los objetos de servicio de directorio no son “objetos” verdaderos. No contienen métodos ampliables. Por el contrario, son representaciones atribuidas de varios recursos que existen en la red.

directamente y propagarlos, permitiendo que ocurra la duplicación intersitio dentro de un dominio (inclusive si cualquier DC se encuentra caído).

Arboles de dominio

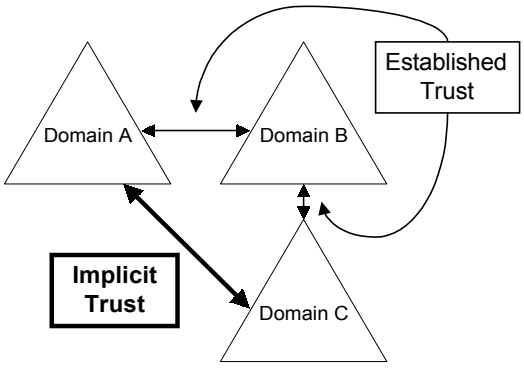
Un árbol de dominio consiste en varios dominios que comparten un esquema y configuración común y forman un espacio de nombre adyacente. Los dominios en un árbol están vinculados por relaciones de confianza. Active Directory es un conjunto de uno o más árboles.

Puede ver estos árboles de una de dos maneras: La relación de confianza entre dominios y el espacio de nombre de un árbol de dominio.

Ver relaciones de confianza

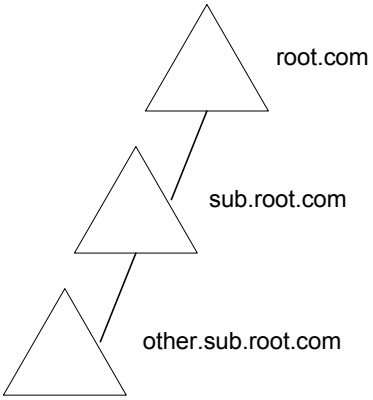
Puede dibujar una imagen de un árbol de dominio con base en los dominios individuales y las relaciones de confianza entre ellos.

Windows NT establece relaciones de confianza entre dominios basándose en el protocolo de seguridad Kerberos. La confianza Kerberos es transitiva y jerárquica, si el dominio A confía en el dominio B y el dominio B confía en el dominio C, el dominio A también confía en el dominio C. La siguiente figura ilustra este concepto.



Visualizar dl espacio de nombre

Puede dibujar una imagen del árbol de dominio basado en el espacio de nombre y después determinar el nombre especifico del objeto siguiendo la ruta del espacio de nombre del árbol de dominio. Esta vista es útil para agrupar objetos en una jerarquía lógica. La ventaja principal del espacio de nombre contiguo es que se realiza una búsqueda profunda desde la raíz del espacio de nombre en toda la jerarquía. La siguiente figura ilustra este concepto:

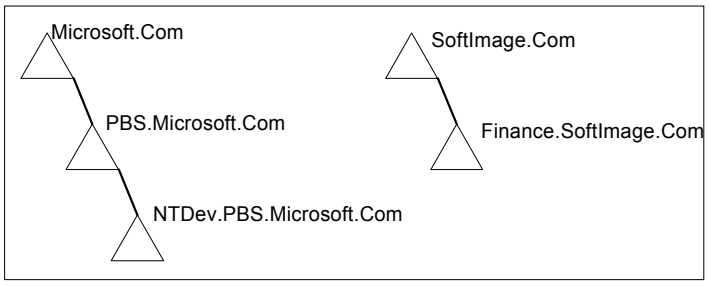


Aunque Active Directory no limita la formación de espacio de nombre contiguo de dominios y directorios discontiguos, puede ser ventajosa para formar árboles contiguos con espacio de nombre correspondiente para asegurar que la estructura de nombre siga la misma lógica que presenta el espacio de nombre.

Bosques

Un bosque es un conjunto de uno o más árboles que no forman un espacio de nombre contiguo. Todos los árboles en un bosque comparten un esquema, configuración y catálogo global comunes. Todos los árboles en un bosque cualquiera tienen confianza entre si por medio de relaciones de confianza Kerberos, de manera jerárquica y transitiva. A diferencia de un árbol, un bosque no necesita un nombre distinto. Un bosque existe como un conjunto de objetos de referencia cruzada y las relaciones de confianza Kerberos que conocen los árboles miembros. Los árboles en un bosque forman una jerarquía para lograr el objetivo de la confianza Kerberos; se puede utilizar el nombre del árbol que se encuentra en la raíz del árbol de confianza para referirse a un bosque cualquiera.

La siguiente figura ilustra un bosque:



Sitios

Un sitio es una ubicación en la red que contiene servidores de Active Directory. Se define un sitio como una o más subredes TCP/IP. La definición de un sitio como un conjunto de subredes permite a los administradores configurar rápida y fácilmente el acceso a Active Directory y la topología de duplicación para aprovechar la red física. Cuando un usuario se conecta, el cliente de Active Directory encuentra los servidores de Active Directory en el mismo sitio en el que está el usuario. Esto se logra fácilmente, ya que la estación de trabajo del usuario ya conoce en qué subred

TCP/IP está y las subredes se traducen directamente a los sitios del directorio activo.

Unidades organizacionales

Un tipo de objeto de directorio contenido dentro de los dominios es una *unidad organizacional.* Las OUs son contenedores lógicos simples en las que puede colocar usuarios, grupos, computadoras e inclusive otras unidades organizacionales.

Catálogo global

El catálogo global es un servicio en un almacén que contiene información de directorio de todos los dominios en su empresa. Su objetivo es responder consultas acerca de objetos en cualquier parte de la empresa, a través de árboles de dominios. Los usuarios pueden utilizar el catálogo global para encontrar un objeto, sin importar en qué dominio se encuentre, buscando cualquier número de atributos.

El catálogo global se guarda en servidores específicos a través de la empresa y *sólo* en controladores de dominio que pueden servir como servidores de catálogo global. Los administradores usan los sitios del directorio activo y el administrador de servicios para indicar si un controlador de dominio dado puede retener un catalogo global. Active Directory genera automáticamente el contenido del catálogo global desde los dominios que forman el directorio utilizando el proceso normal de duplicación.

Para más información acerca de Active Directory, vea la documentación de Windows 2000 Server.

GLOSARIO

Esta sección introduce terminología que se utiliza en este documento.

Listas de control de acceso

Una lista de registros que otorga o niega derechos específicos de acceso a individuos o grupos. Las ACLs asociadas con cada recurso determinan los usuarios válidos a través del servicio de registro y define los tipos de operaciones que puede realizar un usuario.

Active Directory

El servicio de directorio de Windows 2000 que guarda la información acerca de todos los objetos en la red de computadoras y facilita la búsqueda y aplicación de esta información para los administradores y los usuarios . Con Active Directory, los usuarios pueden acceder a recursos en cualquier parte de la red con una simple conexión. De manera similar, los administradores cuentan con un solo punto de administración para todos los objetos en la red, que pueden ver en una estructura jerárquica. Para más información sobre el directorio activo, vea el Apéndice B: Resumen general de Active Directory.

Plantillas administrativas (archivos .adm)

Los archivos de plantilla que proporcionan configuraciones pertenecientes al sistema operativo Windows NT 4.0, Windows 95, 98 y 2000 y a la estructura de registro. El archivo .adm especifica las configuraciones de registro que se pueden modificar a través de la interfaz del editor de políticas de grupos. El archivo .adm consiste en una jerarquía de categorías y subcategorías que conjuntamente definen cómo se mostrarán las opciones a través de la interfaz del editor de políticas de grupos. También indica las ubicaciones de registro dónde se deben de realizar los cambios si se realiza una selección especifica, especifica cualquier opción o restricción (en valores), que estén asociadas con la selección y, en algunos casos, especifica el valor preestablecido a utilizar si está activada la selección.

Asignación de aplicaciones

En Windows 2000, puede utilizar la extensión del editor de implementación de aplicaciones del editor de políticas de grupos para *asignar* aplicaciones a usuarios para que las aplicaciones parezcan estar instaladas y disponibles en el escritorio del usuario cuando éste se conecta.
Se asignan aplicaciones a objetos específicos de políticas de grupo (GPO), que a su vez se asocian con objetos seleccionados de directorio (sitio, dominio o unidad organizacional). Cuando se asignan aplicaciones, se *publican* a todos los usuarios administrados por el GPOLa publicación de la aplicación instala sólo suficiente información acerca de la aplicación para que aparezcan accesos rápidos a la aplicación en el menú **Inicio** y aparezcan en el registro las asociaciones necesarias de archivoCuando un usuario administrado por el GPO se conecta a una computadora que está ejecutando Windows 2000, la aplicación aparece en su menú **Inicio**Cuando el usuario selecciona la aplicación desde el menú **Inicio** por primera vez,

ésta se instala. También se pueden instalar las aplicaciones publicadas haciendo clic en el documento que administra la aplicación (ya sea la extensión de archivo o la activación basada en COM).

Publicación de aplicaciones

En Windows 2000, puede utilizar la extensión del editor de implementación de aplicaciones en el editor de políticas de grupo para *publicar* aplicaciones a usuarios. Las aplicaciones publicadas son aquellas que el administrador pone a disposición para un uso a solicitud.
Las aplicaciones publicadas no cuentan con presencia en la computadora de los usuarios. En otras palabras, no existen accesos rápidos o referencias en el menú **Inicio** a la aplicación en el escritorio. Se anuncia una aplicación publicada en el almacén de clase de Active Directory (AD). Los programas realizan esto al guardar la información de publicidad en el almacén de clase del contenedor AD. Estos atributos anunciados se utilizan para ubicar la aplicación y toda la información requerida para su instalación. Después que se anuncia la aplicación en el almacén de clase, ésta puede ser activada por asociación de documento como una aplicación asignada. Los usuarios también pueden instalar el programa utilizando la herramienta **Agregar/quitar programas** en su escritorio.

Archivo .cab

Un archivo .cab contiene uno o más archivos que se descargan conjuntamente en un único archivo comprimido de gabinete. Dentro del gabinete existe un archivo .inf que proporciona más información sobre la instalación. El archivo .inf puede referirse a archivos en el .cab o a otros archivos en otros Localizadores de recursos uniformes (URLs).

Almacén de clase

El depósito para la notificación de información correspondiente a aplicaciones y componentes que se encuentran disponibles a usuarios de un contenedor de Active Directory de Windows 2000, tal como una unidad organizacional. El almacén de clase proporciona información clave acerca de esas aplicaciones para que las computadoras de estaciones de trabajo puedan encontrar las aplicaciones conforme las solicitan los usuarios.

Dominio

Un grupo de servidores y otros objetos de red bajo un solo nombre. Los dominios proporcionan los siguientes beneficios:

- Puede agrupar objetos en dominios para ayudarle a reflejar la organización de su compañía en la red informática.
- Cada almacén guarda sólo la información acerca de los objetos ubicados en aquel dominio. Al partir la información de directorio de esta manera, Active Directory escala a cuántos objetos se requieran para guardar información en su red.
- Cada directorio es una frontera de seguridad—esto significa que las

políticas y configuraciones de seguridad (tales como derechos administrativos, políticas de seguridad y ACLs) no cruzan de un dominio a otro. El administrador de un dominio cuenta con derechos absolutos para establecer políticas sólo dentro de ese dominio.

Arboles de dominio

Una organización jerárquica de dominios. Se utiliza la herramienta *snap-in* MMC del administrador de Active Directory para unir dominios a árboles y cuando realiza esto los dominios se juntan transparentemente a través de relaciones de confianza Kerberos transitivas bidireccionales. Ya que estas relaciones de confianza van en ambos sentidos y son transitivas, un dominio que se une a un árbol tiene establecidas relaciones de confianza inmediatamente con cualquier dominio en el árbol. Estas relaciones de confianza hacen que todos los objetos de los dominos de un árbol estén disponibles a todos los demás dominios en el árbol. Por ejemplo, se le pueden otorgar permisos para cualquier objeto en otros dominios en un árbol a un usuario o grupo en cualquier dominio. Esto también permite una conexión única a red de un usuario para acceder a cualquier parte de la red.

Identificadores únicos globales

Un identificador único global (GUID) consiste en un número entero de 128 bits que identifica una clase e interfaz específica de objeto. Los GUIDs están virtualmente garantizados a ser únicos. Se puede generar un GUID utilizando ya sea la utilidad **uuidgen** del estuche de desarrollo de Software Win32®, o la herramienta **guidgen** que viene en el ambiente de desarrollo de Visual C++®. Para más información acerca de los GUIDs, vea la referencia del programador *OLE*, *Volumen uno*; la documentación del estuche de desarrollo software Win32, e *Inside OLE*, 2ª edición, por. Brockschmidt, Redmond, Wash.: Microsoft Press, 1995.

Política de aseguramiento

Una política de aseguramiento es el uso selectivo de cinco diferentes tipos de políticas de grupo. Puede utilizar el editor de políticas de grupo para crear ambientes asegurados de usuarios donde un usuario tiene acceso limitado a archivos en el sistema. El aseguramiento también requiere que especifique configuraciones de seguridad de sistema tales como archivo, carpetas o restricciones de acceso a registros. Para realizar esto se utilizan las ACLs y las opciones de configuración de seguridad.

Microsoft Management Console (MMC)

Un esquema de consola común para aplicaciones de administración de sistema. La meta principal de Microsoft Management Console es proporcionar soporte de administración simplificada y reducir los costos de propiedad a través de la integración de herramientas, orientación de tareas, soporte para delegación de tareas y una simplificación general de interfaz. La consola MMC alberga las herramientas administrativas (éstas se

conocen como *snap-ins* MMC); la consola misma *no* proporciona funcionalidad de administración.

Snap-in MMC

Herramientas que amplían la funcionalidad de la consola MMC y proporcionan funcionalidad administrativa. Un *snap-in* funciona de manera independiente de otros *snap-in*s.

Extensión snap-in MMC

Una herramienta que mejora la funcionalidad de un *snap-in* padre. Una extensión depende del *snap-in* padre para datos contextuales.

Unidad organizacional

Un tipo de objeto de directorio contenido dentro de los dominios. Las OUs son contenedores lógicos en los cuales puede ubicar usuarios, grupos, computadoras e inclusive otras unidades organizacionales.

Paquetes (archivos .msi)

Los paquetes contienen toda la información necesaria para describir a Windows Installer cómo instalar una aplicación en cada escenario posible: Varias plataformas, diferentes conjuntos instalados previamente, versiones anteriores de un producto y varias ubicaciones preestablecidas de instalación.

Registro

Una base de datos en donde se guarda información de configuración interna de Windows NT y configuraciones específicas del equipo y de los usuarios.

Enjambre de registro

Una sección de registro que se guarda como un archivo. El subárbol del registro se divide en enjambres (llamados así por su similitud a la estructura celular de un enjambre de abejas). Un enjambre es un cuerpo discreto de llaves, subllaves y valores.

Esquema

Se puede guardar en el directorio la definición formal de todas las clases de objetos y los atributos que conforman esas clases de objetos. Active Directory incluye un esquema preestablecido, que define varias clases de objetos tales como usuarios, grupos, computadoras, dominios, unidades organizacionales y políticas de grupo. El esquema de Active Directory es ampliable de manera dinámica; esto significa que puede modificar el esquema definiendo nuevos tipos de objetos y sus atributos, y definiendo atributos nuevos para objetos existentes. Puede hacer esto con la herramienta *snap-in* del administrador de esquemas que se incluye en Windows NT Server o a través de programación.

Scripts

Archivos de lote (.bat) o archivos ejecutables (.exe) que se ejecutan cuando

la computadora se inicia o apaga o cuando el usuario se conecta o desconecta desde cualquier computadora en la red. Windows 2000 proporciona soporte a Windows Scripting Host Visual Basic Scripting Edition (VBScript) y JScript (.js), mientras continua proporcionando soporte a *scripts* de comandos MS-DOS y archivos ejecutables.

Aplicación cargadas al servidor

Esta es una aplicación de red. La aplicación vive en el servidor y se ejecuta desde el servidor.

Sitio

En Windows 2000, se registra la topología física de la red definiendo sitios. Se define un sitio como una o más subrredes IP. Windows 2000 utiliza la información de sitio para dirigir solicitudes de una computadora a ser satisfechas por otra en el mismo sitio. Por ejemplo, cuando se conecta una computadora, Active Directory utiliza la dirección TCP/IP de la estación de trabajo, así como la información de sitio que se registró, para determinar un controlador de dominio en el sitio local. Se utiliza este controlador local para dar servicio a los requerimientos de la estación de trabajo. Para más información acerca de la estructura lógica del dominio y la estructura física, vea el capítulo"Introducción a Active Directory", en la documentación de Windows 2000 Server.

Costo total de propiedad (TCO)

Se refiere al costo administrativo asociado con las compras de hardware y software de computadora, implementación y configuración, actualizaciones de hardware y software, capacitación, mantenimiento y soporte técnico.

Cero administración de Windows

La solución de Microsoft para reducir el costo total de propiedad es una iniciativa llamada Cero administración de Windows. Las metas más amplias de la iniciativa Cero administración de Windows son reducir significativamente el costo de la configuración inicial de los niveles actuales y reducir el gasto general administrativo cuando la red está funcionando de manera estable. Después de la configuración inicial de la computadora, una combinación de instalaciones automáticas de aplicación, *scripts* y políticas de escritorio reducen significativamente los costos asociados con la administración de estaciones de trabajo.

PARA MAYORES INFORMES

Para obtener la información más reciente sobre Windows 2000 Server, visite nuestro sitio en el World Wide Web en //www.microsoft.com/ntserver.