Chapter 1: An Overview of Windows Server 2008 Services

In This Chapter

- **Defining how services differ from other application types**
- **Considering the basic Windows services**
- **Using the WMI interface to perform tasks with services**
- **Managing the WMI control properties**

Windows Server 2008 relies on a myriad of services. A *service* is a special kind of application that executes in the background and doesn't normally interact with the user in any way. Often, roles and features rely on services to perform tasks in the background. In most cases, the role or feature starts the service for you, but in a few cases, such as FTP support for IIS 7, you must start the service manually to obtain the functionality provided by the service.

Having an application that can't interact with the user may seem like a limitation, but you might be amazed at the number of tasks that services can perform. For example, when your system needs to access Windows Update, it relies on the Windows Update service to do it. When Windows Update needs to download a file to your system, it uses the Background Intelligent Transfer Service (BITS) to perform the task. Services are constantly performing tasks in the background to make the Windows computing experience better.

You may wonder why you need to worry about services, considering that they work almost automatically. An administrator needs to know about every application executing on Windows Server 2008, even the services. In some cases, Microsoft assumes that you need a particular service enabled when you really don't. For example, when you use some other means of updating your server, you really don't need the Windows Update and Background Intelligent Transfer Service enabled. These services are using processing cycles and can open potential security holes. (Yes, services present security holes too.)

One of the more important management services is the Windows Management Interface (WMI). You can use WMI to query a hierarchical database

containing information about the server. In addition, by changing settings within this database, you can control the configuration of the server to an extent. By understanding how the Windows Management Instrumentation service works, you can begin to see the importance of working with services as an administrator.

Understanding How Services Work

Services are a special kind of application. However, you can't run a service from the command line — at least, not directly. The system normally starts services for you when it starts or in response to a command you provide. Unlike with most applications, you issue commands to a service by using the Services console, described in the "Using the Services Console" section of Book VIII, Chapter 2. Services normally respond to the commands in the following list:

- **Start:** Starts the service after you stop it. The service starts with a fresh copy of itself in memory and without any memory of tasks it performed previously.
- **Stop:** Stops the service from executing any other commands. This action also clears any memory that the service uses.
- **Continue:** Starts the service after you stop it. The service picks up where it left off in the processing cycle.
- **Pause:** Stops the service from executing any other commands. This action doesn't clear memory and lets the service later resume any activity it was performing.
- **Restart:** Performs a combination of a Stop and a Start command. The service restarts any processing it's supposed to perform. You can use this command to restart a service when it has frozen or become corrupted in some other way.

Not all services support all commands in the list. In fact, some services don't support any of the commands — you can't start or stop them. A few services don't provide much in the way of configuration settings either because Microsoft considers them essential to Windows Server 2008 operation. If you see a service that lacks both commands and configuration options, it's safe to assume that you should leave the service alone.

Normally, you never need to know anything more to use a service effectively. In fact, you can safely skip the rest of this section if you want, but you'll also miss out on some very interesting information about how services work.

Some services also support hidden commands. A user application may interact with the service and use these hidden commands to direct service actions. You should never use any technique to issue a hidden command unless directed to do so by a support person.

A service always appears as a DLL. Normally, you can use the RunDLL32 utility to run a DLL file, but services don't rely on this utility. Instead, a service relies on the SvcHost utility to run. Consequently, when working with services, you normally look for the SvcHost utility, rather than the service itself, as a starting point for learning more about the service. You find the SvcHost utility in the `\Windows\System32` folder of your system.

The SvcHost utility relies on registry entries to determine which DLLs to work with. The DLLs normally appear in groups and you tell SvcHost to execute a group by specifying the -k command line switch, along with the group name. For example, the Background Intelligent Transfer Service is part of the `netsvcs` group, which appears as a value in the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost` key of the registry. To start the Background Intelligent Transfer Service using SvcHost, type **%SystemRoot%\system32\svchost.exe -k netsvcs** (where %SystemRoot% is the location of the Windows folder on your system) and press Enter at the command line.

A group contains a number of strings that define registry entries containing additional entries for the service. For example, if you look at the `netsvcs` group, you notice that one of the entries is `BITS`. When you look at the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BITS` key, you find all the information needed to use the Background Intelligent Transfer Service. If you're looking for the DLL used to create the service, check the `Servicedll` value of the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BITS\Parameters` key. You'll discover that the Background Intelligent Transfer Service resides within `QMGR.DLL`. This two-layer approach for working with the SvcHost utility is common in Windows — it's the technique you see most often for working with a service.

Malware often uses the complex set of registry entries used by services to hide in plain site. The malware creator simply designs the virus or Trojan as a service rather than as an application. Placing the service in a group, such as `netsvcs`, means that finding the rogue service requires a lot of administrator time. You can find out more about how services can appear as malware at `http://www.bleepingcomputer.com/tutorials/tutorial83.html`.

An Overview of the Basic Windows Services

Windows comes with a wealth of services. You must start some services to see basic Windows functionality. For example, you can't use the server as a server without starting the server service. Likewise, if you want to interact with the server, you must start the Workstation service.

In some cases, Windows installs a service as the result of a role or feature you install. For example, you won't see the World Wide Web Publishing Service unless you install the Web Server IIS role. These optional services are part of Windows, so you don't have to do anything special to use them, but Windows won't install them unless you need them.

Microsoft installs some services automatically, but doesn't start them. For example, you don't need the COM+ System Application service running unless you're using a Component Object Model Plus (COM+) application. In fact, Microsoft disables some services because they're dangerous or simply not needed by most people. For example, the Routing and Remote Access service can open a security hole in your system, so Microsoft disables it unless you truly need it. Table 1-1 provides a list of the basic Windows services and describes their use.

Table 1-1 Basic Services Installed on Windows Server 2008

Name	*Startup Type*	*Description*
Application Experience	Automatic	Monitors application launches. When the service detects a launch, it determines whether the application appears within the application compatibility cache and offers advice on using the application with Windows Server 2008. In some cases, you can set this service to manual to save processing cycles, but you may also experience compatibility problems.
Application Information	Manual	Elevates user privileges as needed. Some applications require that you have specific privileges in order to run. This service monitors the system for such applications and provides the required privilege-elevation dialog box when necessary. You can normally keep this service set to Manual on a server.

Name	Startup Type	Description
Application Layer Gateway Service	Manual	Lets you use third-party plug-ins with Internet Connection Sharing (ICS). You need to change only the startup type for this service when you're using third-party plug-ins with ICS.
Application Management	Manual	Helps you manage the installation and removal of applications that you want to distribute using a group policy. The service also lets you obtain a list of available applications. In most cases, you won't need this service on a server unless you plan to distribute server applications using a group policy.
Background Intelligent Transfer Service	Automatic (Delayed Start)	Performs file transfers in the background using idle network bandwidth (which lets the user continue working unimpeded). BITS also provides the means for starting and stopping downloads without losing track of the download status. You can even continue a download between reboots. Other services, such as Windows Update, rely on this service, so you shouldn't disable it without considering the consequences for other services and applications.
Base Filtering Engine	Automatic	Manages firewall and Internet Protocol Security (IPSec) policies. This service also comes into play for filtering user mode requests. It's a bad idea to stop or disable this service.
Certificate Propagation	Manual	Works with smart cards to distribute digital certificates for identification and other purposes. You don't need to start this service unless your organization uses smart cards.
CNG Key Isolation	Manual	Provides Cryptographic Next Generation (CNG) key process isolation. Windows hosts this service within the Local Security Authority (LSA) process. You can learn more about how this service works at `http://msdn2.microsoft.com/en-us/library/bb204778.aspx`.
COM+ Event System	Automatic	Supports the special COM+ application feature System Event Notification Service (SENS), which provides automatic distribution of events to subscribing Component Object Model (COM) components. You can

(continued)

Table 1-1 *(continued)*

Name	*Startup Type*	*Description*
		obtain overviews of SENS at `http://msdn2.microsoft.com/en-us/library/aa377599.aspx`. However, you may find the article about a use for SENS at `http://msdn.microsoft.com/msdnmag/issues/02/08/SENS/` more useful.
COM+ System Application	Manual	Helps you manage and configure COM+ applications. This service also tracks COM+ application status. Most COM+ applications won't run properly without this service, but the COM+ functionality in Windows starts the service automatically as needed, so you shouldn't need to modify this service's configuration.
Computer Browser	Disabled	Creates and maintains a list of computers and other resources (such as printers with direct network connections) on the network. The service supplies this information to other computers that the system designates as browsers. Using this service can speed the spread of resource information on a network. Microsoft disables this service for two reasons. First, this service won't work over an IPv6 network. Second, this service is associated with a named pipe security vulnerability you can read about at `http://www.microsoft.com/technet/security/Bulletin/MS05-007.mspx`.
Cryptographic Services	Automatic	Performs four cryptographic-related management tasks. The Catalog Database Service confirms the signatures of Windows files and lets you install new programs. The Protected Root Service adds and removes Trusted Root Certification Authority certificates from the computer. The Automatic Root Certificate Update Service retrieves root certificates from Windows Update and enables features such as Secure Sockets Layer (SSL). The Key Service helps enroll this computer for certificates. Never stop this service.
DCOM Server Process Launcher	Automatic	Lets the system launch Distributed Component Object Model (DCOM) processes. Never stop this service.

Name	Startup Type	Description
Desktop Window Manager Session Manager	Automatic	Provides all the eye candy associated with the new Windows interface. This service provides some theme support, transparency effects, and special features, such as Thumbnail view on the Taskbar. It's unlikely you need these features in a server, so disabling this service can net a small performance gain.
DHCP Client	Automatic	Registers and updates IP addresses. This service also updates Domain Name System (DNS) records for the computer using the Dynamic Host Configuration Protocol (DHCP).
Diagnostic Policy Service	Automatic	Provides policy support for problem detection, troubleshooting, and resolution for Windows components. You manage these policies through group policies on the local system or domain controller. Never stop this service.
Diagnostic Service Host	Manual	Performs the actual task of problem detection, troubleshooting, and resolution for Windows components. Windows automatically starts this service as needed to address errors detected by the Diagnostic Policy Service.
Diagnostic System Host	Manual	Works as part of the Windows Diagnostic Infrastructure (WDI) with the Diagnostic Policy Service and Diagnostic Service Host to present information about problem detection, troubleshooting, and resolution for Windows components. Windows automatically starts this service as needed to address errors detected by the Diagnostic Policy Service. You can learn more about WDI at `http://technet.microsoft.com/en-us/windowsvista/aa905076.aspx`.
Distributed Link Tracking Client	Automatic	Maintains links between NTFS files within a computer or across computers in a network. For example, you can create a file on Computer A and a link to that file on Computer B. When this service detects a change in location for the file on Computer A, it tells Computer B to update its information. Theoretically, you can stop this service if you never use links on your system.

(continued)

Table 1-1 ***(continued)***

Name	*Startup Type*	*Description*
Distributed Transaction Coordinator	Automatic (Delayed Start)	Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. Never stop this service.
DNS Client	Automatic	Performs two DNS-related tasks. First, this service registers the full computer name for the local computer with the DNS server. Second, this service caches DNS information found on the DNS server to the local machine to make locating other network resources easier. Never stop this service.
Extensible Authentication Protocol	Manual	Provides network authentication for various 802.1x wired and wireless connections, Virtual Private Networks (VPNs), and Network Access Protection (NAP). The Extensible Authentication Protocol (EAP) service also provides Application Programming Interfaces (APIs) used by developers to create network applications.
Function Discovery Provider Host	Manual	Hosts the Function Discovery providers for various Windows features, such as Windows Media Center. You normally won't need to enable this service on a server.
Function Discovery Resource Publication	Automatic	Publishes a list of resources available on your computer to other computers on the network. This service helps other computers discover resources located on the local computer. Disabling this service doesn't appear to have any negative effect on network functionality.
Group Policy Client	Automatic	Applies group policy settings to the local computer. If you disable this service, group policies won't have any affect on the local computer. Never stop this service on any network using group policies.
Health Key and Certificate Management	Manual	Provides X.509 certificate and key management services for the Network Access Protection Agent (NAPAgent). Enforcement technologies that use X.509 certificates may not function properly without this service.
Human Interface Device Access	Manual	Supports any Human Interface Device (HID) hardware on your system, such as mice and keyboards. If you disable this service, the hardware still functions, but any special hot buttons or other HID features won't work.

Name	Startup Type	Description
IKE and AuthIP IPsec Keying Modules	Automatic	Hosts the Internet Key Exchange (IKE) and Authenticated Internet Protocol (AuthIP) keying modules. These keying modules provide support for authentication and key exchange in IPSec. Disabling this service will likely cause IPSec to fail on the local system.
Interactive Services Detection	Manual	Notifies users of new interactive services. This service also provides access to the dialog boxes provided by interactive services. If you disable this service, the user may not see required interactive service input and cause problems for the system as a whole.
Internet Connection Sharing (ICS)	Automatic	Lets the user share an Internet connection with others on the network. The ICS service provides Network Address Translation (NAT), addressing, name resolution, and limited intrusion prevention. You should disable this service on a network that has a DNS server.
IP Helper	Automatic	Provides automatic IPv6 connectivity over an IPv4 network. If this service is stopped, the machine has IPv6 connectivity only if it's connected to a native IPv6 network.
IPSec Policy Agent	Automatic	Enforces IPSec policies created through the IP Security Policies console or the NetSH IPSec utility. IPSec provides support for network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. Never stop this service.
KtmRm for Distributed Transaction Coordinator	Automatic (Delayed Start)	Coordinates transactions between the Microsoft Distributed Transaction Controller (MSDTC) and the Kernel Transaction Manager (KTM). Never stop this service.
Link-Layer Topology Discovery Mapper	Manual	Provides support for the new network mapping functionality found in Windows Server 2008 and Vista. You can also add this service to Windows XP machines to obtain a complete map of your network. Windows starts this service automatically as needed.
Microsoft Fibre Channel Platform Registration Service	Manual	Registers the local system with all available Fibre Channel fabrics (used with network storage such as storage area networks or SANs), and maintains the registrations. You can disable this service unless you rely on network storage.

(continued)

Table 1-1 *(continued)*

Name	*Startup Type*	*Description*
Microsoft iSCSI Initiator Service	Manual	Manages Internet Small Computer System Iinterface (iSCSI) sessions from this computer to remote iSCSI target devices. You can disable this service unless you rely on iSCIS storage.
Microsoft Software Shadow Copy Provider	Manual	Manages software-based volume shadow copies taken by the Volume Shadow Copy service. Windows starts this service automatically as needed. Applications such as Backup require this service. In addition, some third-party ghost image applications require this service.
Multimedia Class Scheduler	Manual	Prioritizes the work that the system must perform based on task priorities. The system normally uses this service for multimedia applications, so you won't usually need to enable this service on a server.
Netlogon	Manual	Maintains a secure channel between this computer and the domain controller for authenticating users and services. Never stop this service.
Network Access Protection Agent	Manual	Provides Network Access Protection (NAP) functionality on client computers.
Network Connections	Manual	Manages objects in the Network and Dial-Up Connections folder. These two folders provide views of both local area network (LAN) and remote connections.
Network List Service	Automatic	Creates a listing of connected networks. The service then collects and stores properties for these networks. After the list is complete, the service notifies applications about the connected resource. It also provides application notification whenever the network configuration changes. Never stop this service.
Network Location Awareness	Automatic	Collects and stores configuration information for the network and notifies programs when this information changes. Never stop this service.
Network Store Interface Service	Automatic	Delivers network notifications, such as interface additions and deletions, to user mode clients. Stopping this service causes loss of network connectivity.

Name	Startup Type	Description
Offline Files	Disabled	Performs maintenance activities on the Offline Files cache, responds to user logon and logoff events, and implements the internals of the public API. This service also dispatches interesting events to applications interested in Offline Files activities and changes in cache state.
Performance Logs and Alerts	Manual	Collects performance data from local or remote computers based on a preconfigured schedule. The service then writes the data to a log or triggers an alert. Windows starts this service automatically as needed.
Plug and Play	Automatic	Detects system hardware on startup. This service also registers changes in the hardware configuration. Never stop this service.
PnP-X IP Bus Enumerator	Disabled	Manages the virtual network bus, discovers network connected devices using the Simple Service Discovery Protocol (SSDP) or WS-Discovery protocols (where WS stands for Web Service), and provides access to them through Plug and Play (PnP). You normally keep this service disabled because it can open security holes in your system.
Portable Device Enumerator Service	Manual	Enforces group policy for removable mass-storage devices. Enables applications such as Windows Media Player and Image Import Wizard to transfer and synchronize content using removable mass-storage devices.
Print Spooler	Automatic	Caches data sent to the printer and outputs that data as the printer becomes ready to receive it. You can stop this service if you don't intend to do any printing.
Problem Reports and Solutions Control Panel Support	Manual	Supports viewing, sending, and deletion of system-level problem reports for the Problem Reports and Solutions Control Panel. Windows starts this service automatically as needed.
Protected Storage	Manual	Provides protected storage for sensitive data, such as passwords, to prevent access by unauthorized services, processes, or users. Windows starts this service automatically as needed.

(continued)

Table 1-1 ***(continued)***

Name	*Startup Type*	*Description*
Remote Access Auto Connection Manager	Manual	Creates a connection to a remote network whenever a program references a remote DNS or Network Basic Input/Output System (NetBIOS) name or address. Windows starts this service automatically as needed.
Remote Access Connection Manager	Manual	Manages dial-up and virtual private network (VPN) connections from this computer to the Internet or other remote networks. Windows starts this service automatically as needed.
Remote Access Quarantine Agent	Manual	Restricts network access to remote clients until the client meets required authentication requirements. After the client meets these requirements, the service removes the validated client from the quarantine network. Windows starts this service automatically as needed.
Remote Procedure Call (RPC)	Automatic	Serves as an endpoint mapper (the end of a communication stream) for COM application. It also serves as the COM Service Control Manager. Never stop this service.
Remote Procedure Call (RPC) Locator	Manual	Manages the RPC name service database. Windows starts this service automatically as needed.
Remote Registry	Automatic	Lets a remote caller manage the registry settings on the local computer. You should consider disabling this service because it creates a huge security hole.
Resultant Set of Policy Provider	Manual	Provides a network service that processes requests to simulate application of Group Policy settings for a target user or computer in various situations and computes the Resultant Set of Policy settings.
Routing and Remote Access	Disabled	Provides routing services for both LAN and WAN connections. Windows enables this service when you use the Routing and Remote Access features; otherwise, you should keep it disabled for security reasons.
Secondary Logon	Automatic	Lets you start an application or other process using alternate credentials. For example, this service is the one that the RunAs utility uses to let you elevate standard user credentials to administrator credentials. Never stop this service.

Name	Startup Type	Description
Secure Socket Tunneling Protocol Service	Manual	Supports the Secure Socket Tunneling Protocol (SSTP) used to connect the local system to remote computers using VPN. Windows starts this service automatically as needed.
Security Accounts Manager	Automatic	Provides Security Accounts Manager (SAM) support to other applications. This service also signals other services that the SAM is ready to accept requests. Without this feature, applications and services can't perform certain secure tasks on the system. Never stop this service.
Server	Automatic	Supports file, print, and named-pipe sharing over the network for this computer. Never stop this service.
Shell Hardware Detection	Automatic	Provides notifications for AutoPlay hardware events. Never stop this service.
SL UI Notification Service	Manual	Provides Software Licensing activation and notification. If you disable this service, Windows doesn't start in Normal mode. Start Windows in Safe Mode, set the service back to Manual, and then reboot.
Smart Card	Manual	Manages access to smart cards read by this computer. You can disable this service if you don't rely on smart cards.
Smart Card Removal Policy	Manual	Lets you configure the system to lock the user desktop after smart card removal.
SNMP Trap	Manual	Receives trap messages generated by local or remote Simple Network Management Protocol (SNMP) agents and forwards the messages to SNMP management programs running on this computer. Windows starts this service automatically as needed.
Software Licensing	Automatic	Enables the download, installation, and enforcement of digital licenses for Windows and Windows applications. Never stop this service or else Windows will run in reduced functionality mode.
Special Administration Console Helper	Manual	Helps administrators remotely access a command prompt using the Emergency Management Services. Windows starts this service automatically as needed.

(continued)

Table 1-1 *(continued)*

Name	*Startup Type*	*Description*
SSDP Discovery	Disabled	Discovers networked devices and services that use the SSDP discovery protocol, such as Universal Plug and Play (UPnP) devices. This service also announces SSDP devices and services running on the local computer. Microsoft disables this service because UPnP presents security risks. (See the article at `http://research.eeye.com/html/advisories/published/AD20011220.html` for details.)
Superfetch	Disabled	Maintains and improves system performance over time by placing commonly used applications in a cache. This service doesn't provide much value on a server. Read the material at `http://www.tomshardware.com/2007/01/31/windows-vista-superfetch-and-readyboost analyzed/` for additional details on how this service works.
System Event Notification Service	Automatic	Monitors system events and notifies subscribers to COM+ Event System of these events. Never stop this service.
Task Scheduler	Automatic	Lets you configure and schedule automated tasks on this computer. Microsoft has started to use the Task Scheduler for operating system needs. At one time, you could disable this service without a problem, but you may want to check which tasks Microsoft has scheduled before you disable it on Windows Server 2008.
TCP/IP NetBIOS Helper	Automatic	Provides support for the NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution for clients on the network. This service lets users share files, print, and log on to the network by using NetBIOS. You can stop this service if your network doesn't rely on NetBIOS or Windows Internet Naming Service (WINS).
Telephony	Manual	Provides Telephony Application Programming Interface (TAPI) support for programs that control telephony devices on the local computer and through the LAN. When working on a LAN, the remote computer must also run this service.

Name	Startup Type	Description
Terminal Services	Automatic	Helps users connect interactively to a remote computer. Remote Desktop and Terminal Server depend on this service. Clear the check boxes on the Remote tab of the System Properties applet of the Control Panel to disable this feature.
Terminal Services Configuration	Manual	Provides configuration support for Terminal Services and Remote Desktop functionality. It also supports session maintenance activities that require SYSTEM context, such as per-session temporary folders, TS themes, and TS certificates.
Terminal Services UserMode Port Redirector	Manual	Redirects printers, drives, and ports for Remote Desktop Protocol (RDP) connections.
Themes	Disabled	Provides user experience theme management.
Thread Ordering Server	Manual	Provides ordered execution for a group of threads within a specific timeframe.
TPM Base Services	Automatic (Delayed Start)	Provides access to the Trusted Platform Module (TPM) that offers hardware-based cryptographic services to system components and applications. You can normally disable this service if your motherboard lacks a TPM.
UPnP Device Host	Disabled	Lets the system host UPnP devices.
User Profile Service	Automatic	Loads and unloads user profiles. Never stop this service. If you stop or disable this service, users can no longer successfully log on or log off, applications may have problems obtaining user data, and components registered to receive profile event notifications will not receive them.
Virtual Disk	Manual	Provides management services for disks, volumes, file systems, and storage arrays.
Volume Shadow Copy	Manual	Manages the Volume Shadow Copies used for backup and other purposes. Windows starts this service automatically as needed.
Windows Audio	Manual	Manages audio for Windows-based programs. Unless your server has a sound card installed, you can disable this service.
Windows Audio Endpoint Builder	Manual	Manages audio devices for the Windows Audio service. Unless your server has a sound card installed, you can disable this service.

(continued)

Table 1-1 *(continued)*

Name	*Startup Type*	*Description*
Windows Color System	Manual	Hosts the third-party Windows Color System color device model and gamut map model plug-in modules. These plug-in modules are vendor-specific extensions to the Windows Color System baseline color device and gamut map models. Disabling this service may result in poor color rendering between the screen and attached devices.
Windows Driver Foundation - User-mode Driver Framework	Manual	Manages user-mode driver host processes in managed environment. This is the next-generation driver model for Windows. You can learn more about this model at `http://whitepapers.techrepublic.com.com/whitepaper.aspx?docid=166001`. Windows starts this service automatically as needed.
Windows Error Reporting Service	Automatic	Reports errors when programs stop working or responding and delivers any existing solutions. This service also generates logs for diagnostic and repair services. Windows starts this service automatically as needed.
Windows Event Collector	Manual	Manages persistent subscriptions to events from remote sources that support WS-Management protocol, such as Windows Vista event logs, hardware and Intelligent Platform Management Interface (IPMI)-enabled event sources. The service stores forwarded events in a local event log. Windows starts this service automatically as needed.
Windows Event Log	Automatic	Manages events and event logs. This service supports logging events, querying events, subscribing to events, archiving event logs, and managing event metadata. It can display events in both XML and plain-text format. Never stop this service.
Windows Firewall	Automatic	Helps prevent unauthorized users from gaining access to your computer through the Internet or a network. Never stop this service.
Windows Installer	Manual	Adds, modifies, and removes applications provided as a Microsoft Installer (MSI) package. Windows starts this service automatically as needed.

Name	Startup Type	Description
Windows Management Instrumentation	Automatic	Provides a common interface and object model to access management information about operating system, devices, applications, and services. Think of this service as a kind of database manager. Never stop this service.
Windows Modules Installer	Manual	Installs, modifies, and removes Windows updates and optional components. Windows starts this service automatically as needed.
Windows Process Activation Service	Manual	Provides process activation, resource management, and health management services for message-activated applications. Windows starts this service automatically as needed.
Windows Remote Management (WS-Management)	Automatic (Delayed Start)	Implements the WS-Management protocol for remote management. WS-Management is a standard Web services protocol used for remote software and hardware management. (See `http://www.dmtf.org/standards/wsman` for details.) You must configure the Windows Remote Management (WinRM) Service using the `WINRM.CMD` command line tool or through Group Policy for it to listen over the network. The WinRM service provides access to WMI data and enables event collection. Event collection and subscription to events require that the service be running. WinRM messages use HTTP and HTTPS as transports. The WinRM service does not depend on IIS but is preconfigured to share a port with IIS on the same machine. To prevent conflicts with IIS, administrators should ensure that any Web sites hosted on IIS do not use the `/wsman` URL prefix. You can disable this service if your network doesn't rely on WS-Management.
Windows Time	Automatic	Maintains date and time synchronization on all clients and servers in the network. Make sure that you synchronize at least one server to an external time source. Never stop this service, or else you may have Kerberos security problems on the network.
Windows Update	Automatic (Delayed Start)	Detects, downloads, and installs updates for Windows and other programs. Disable this service if you use another method of updating your server.

(continued)

Table 1-1 ***(continued)***

Name	*Startup Type*	*Description*
WinHTTP Web Proxy Auto-Discovery Service	Manual	Implements the client HTTP stack. This service also provides developers with a Win32 API and COM Automation component for sending HTTP requests and receiving responses. In addition, WinHTTP provides support for auto-discovering a proxy configuration using its implementation of the Web Proxy Auto-Discovery (WPAD) protocol. Windows starts this service automatically as needed.
Wired AutoConfig	Manual	Performs IEEE 802.1X authentication on Ethernet interfaces. Windows starts this service automatically as needed.
WMI Performance Adapter	Manual	Provides performance library information from Windows Management Instrumentation (WMI) providers to clients on the network. This service runs only when Performance Data Helper is activated.
Workstation	Automatic	Creates and maintains client network connections to remote servers by using the Server Message Block (SMB) protocol. Never stop this service.

Understanding the Windows Management Instrumentation (WMI)

Not everyone uses Windows systems, and not everyone manages a network that relies solely on Microsoft technology. Because networks often contain a host of machine types using different operating systems and configured with differing hardware, it's important to have some common way to manage them. The eventual result of a lot of discussion about the topic is Web-Based Enterprise Management (WBEM). (See `http://www.dmtf.org/standards/wbem/` for details.)

WMI is Microsoft's version of WBEM. It implements all the features required by the standard, including the Common Information Model (CIM). The *CIM* is essentially a hierarchical database that provides information about the system configuration. When someone needs to know about a particular system, they query the WMI database to discover the information.

The WMI database also includes configuration information. Consequently, when the system needs to perform a task, it consults the WMI database to discover how to do it. The WMI database may not contain every piece of configuration information about the system, but it contains most of the information that an administrator needs, such as the IP configuration of a network interface card (NIC).

WMI treats every entry in the database as an object. Of course, different objects have different characteristics. A NIC has different characteristics from a disk drive. In addition, a disk drive can have a quote assigned to it as well as security. Consequently, WMI must provide the means to interact with these various objects. The solution is to use a WMI provider — a special piece of software that understands the object and can act as an intermediary between it and WMI.

Any application that understands WMI can access the WMI database. You find WMI in many common administrator utilities, such as Systems Microsoft Management Server, Microsoft Health Monitor, and Microsoft Operations Manager. It's also possible to access the WMI database directly with command line utilities, such as Windows Management Instrumentation Command line (WMIC).

Interestingly enough, one of the many Windows features you can manage with WMIC is services. The Service object helps you interact with services in a lot of ways. Using WMIC, you can start, stop, pause, continue, and restart services. It's even possible to change some service characteristics when you have the proper rights. You'll discover that knowing about WMIC can save you considerable time because you can use WMIC to fully script many configuration activities.

Configuring the WMI Control Properties

There are two levels of WMI configuration: the WMI Control and the WMI database. The database contains all the information that describes the system. The WMI Control controls how WMI works — how it manages the WMI database.

The WMI Control appears as part of the Computer Management console in the `Computer Management\Services and Applications\WMI Control` folder. You can also access this control directly by using the WMIMgmt.MSC console. No matter how you access the WMI Control, you don't see anything at first because the pane normally containing information is blank. Instead, you right-click the control entry and choose Properties to display the WMI Control properties dialog box. The General tab of this dialog box tells you about your system. The remaining tabs help you perform specific tasks, as described in the following sections.

Performing a backup

The Backup/Restore tab contains two buttons that let you back up the WMI database and restore it later as needed. Creating a backup is important if you make substantial changes to your server, because restoring the WMI database can significantly reduce recovery time for a failed server. The following steps describe how to perform a backup:

1. **Click Back Up Now on the Backup/Restore tab.**

   You see a Specify a Name for Your Backup File dialog box. Even though Microsoft recommends placing the file in the `\Windows\System32\WBEM\Repostory` folder on your hard drive, it's unlikely that your daily backup includes this file. Make sure to place the file in a folder that you back up regularly.

2. **Choose a folder for the backup.**

3. **Type a name for the backup file in the File Name field.**

   Choose a filename that makes the purpose of the backup clear. Don't give the file an extension — the backup feature performs that task for you.

4. **Click Save.**

   You see a dialog box telling you that the system is creating a backup. This dialog box disappears after a few moments. The backup is complete at this point. Make sure to include the file in your normal backup routine.

Performing a restoration

At some point, you need to restore the WMI database. The system may have failed, or a rogue application may have caused damage to your system. As with any database, you can also see damage from a number of other causes. The following steps tell you how to restore the backup:

1. **Click Restore Now on the Backup/Restore tab.**

   You see a Specify Backup File to Restore dialog box.

2. **Choose the folder that contains the restore file.**

3. **Highlight the restore file in the dialog box.**

   Remember that the file will have an REC extension. Consequently, if the original backup name is MyBackup, the file you want to restore is `MyBackup.REC`.

4. **Click Open.**

   You see a dialog box telling you that the system is restoring the backup. The dialog box disappears after a few moments.

5. **Reboot your system.**

   Theoretically, the changes made by the restoration process should take effect immediately. However, rebooting your system ensures that the restoration actually works as intended.

Setting WMI security

The Security tab of the WMI Control Properties dialog box lets you set the security of the individual levels of the WMI database. Figure 1-1 shows a typical view of this database. Each of the folders shown in the dialog box is a separate storage level within the database, and you can control each level separately.

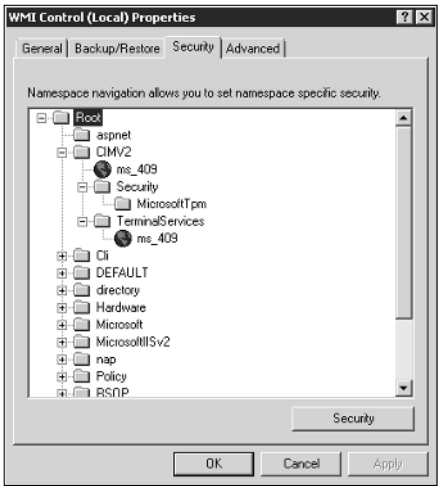

Figure 1-1: The WMI database contains multiple levels, each of which can have different security.

To set security for a particular WMI database level, highlight that level in the dialog box and click Security. You see a Security dialog box such as the one shown in Figure 1-2. This dialog box looks and acts just like any other Security dialog box for Windows.

The rights you assign at each level determine who can perform a particular task. The following list describes the various rights you can assign:

- **Enable:** Lets the user read objects within the namespace.
- **Execute Methods:** Lets the user run objects that are exported from the CIM Object Manager.
- **Full Control:** Grants full read/write/delete access to all CIM objects, classes, and instances.

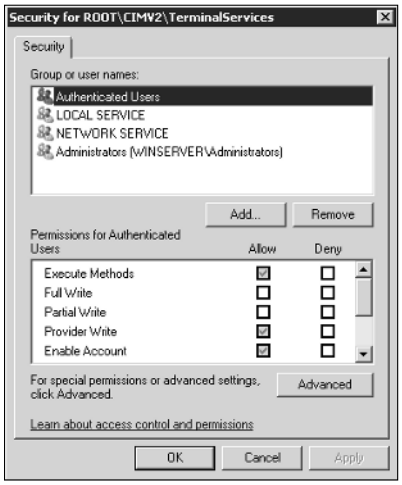

Figure 1-2: Set the security for a particular level by using this Security dialog box.

- **Partial Write:** Grants write access to static objects in the repository.
- **Provider Write:** Grants write access to objects that are made available by the provider.
- **Read Security:** Provides read-only access to WMI security information.
- **Edit Security:** Grants read/write access to WMI security information.
- **Remote Access:** Grants remote computers the same rights that are allowed when connecting from a local computer.

Changing the default namespace for scripting

Most administrators interact with the WMI database through some form of scripting. In fact, you'll find a host of scripts on the Internet. All these scripts have one thing in common: They help you configure your system in a particular way. The namespace that a script uses determines its starting point within the WMI database hierarchy. Look again at Figure 1-1 and you'll see this hierarchy — it begins at the root object and ends wherever the script needs to perform work.

Setting the default namespace to the correct location can make it easier to write scripts because you don't need to include the entire path for an object every time you try to do something. Most scripts rely on the default WMI setting of `Root\CIMV2` as the default namespace. Consequently, you should never have to change the default. However, if you choose to change the default for some reason, click Change on the Advanced tab of the WMI Control Properties dialog box to display the Browser for Namespace dialog box. Highlight the namespace you want to use as a default and click OK.