Important Windows Files Folders and Tools

Author: Jialong He
Jialong_he@bigfoot.com
http://www.bigfoot.com/~jialong_he

Time Synchronization

Time Service

On Window NT4, use "TimeServ" from Windows NT Server 4.0 Resource Kit (timeserv.exe, timeserv.dll in c:\winnt\system32 and timeserv.ini in c:\winnt)

On Win2k, W32Time server is preinstalled. Default sync time with domain controller. To make it sync with external NTP server,
net time /setsntp:"192.5.41 209 192.5.41.41"

This make registry change in
HKLM\SYSTEM\CurrentControlSet \Services\W32Time\Parameters

Type=NTP
NtpServer=192.5.41.209 192.5.41.41

Other parameters include:
ReliableTimeSource, TimeSource,

Sync workstation with Windows time server
net time \\timeserver /set /yes

Essential System Files

File Name	Descriptions
Ntoskrnl.exe	Executive and kernel.
Ntkrnlpa.exe	Executive and kernel with support for Physical Address Extension (PAE), which allows addressing of more than 4 gigabytes (GB) of physical memory.
Hal.dll	Hardware abstraction layer.
Win32k.sys	Kernel-mode part of the Win32 subsystem.
Ntdll.dll	Internal support functions and system service dispatch stubs to executive functions.
Kernel32.dll Advapi32.dll User32.dll Gdi32.dll	Core Win32 subsystem DLLs.

Essential Startup Files

File Name	Descriptions
Ntldr	Reads the Boot.ini file, presents the boot menu, and
	loads Ntoskrnl.exe, Bootvid.dll, Hal.dll, and boot-start device drivers.
Boot.ini	Contains options for starting the version of Windows that Setup installs and any preexisting Windows installations.
Ntdetect.com	After the boot selection is made, Ntldr loads and executes this 16-bit real-mode program to query the computer for basic device and configuration information. This information includes the following: · The time and date information stored in the system's CMOS (nonvolatile memory). · The types of buses (for example, ISA, PCI, EISA, Micro Channel Architecture [MCA]) on the system and identifiers for devices attached to the buses. · The number, size, and type of disk drives on the system. · The types of mouse input devices connected to the system. · The number and type of parallel ports configured on the system.
Pagefile.sys	Contains memory data that Windows is unable to fit into physical RAM. During Startup, the virtual memory manager moves data in and out of the paging file to optimize the amount of physical memory available to the operating system and applications.
Ntbootdd.sys	If either the boot or system drives are SCSI-based, Ntldr loads this file and uses it instead of the boot-code functions for disk access.

Default Local Disk Folders

File Name	Descriptions
Documents and Settings	Account information for each user who is granted access on the computer. Each user account is represented by a subfolder assigned the user name. Folders under each user account folder include My Documents, Desktop, and Start Menu.
Program Files	Installed applications, such as Microsoft® Internet Explorer or Microsoft® Office.
WINDOWS or WINNT	Entire operating system.

Windows Folder and Subfolders

File Name	Descriptions
WINDOWS or WINNT	Miscellaneous operating system and application files (for example, Control.ini, Desktop.ini, Notepad.exe, and System.ini files)
Addins	ActiveX controls (.ocx) files
AppPatch	Application compatibility files
Config	Musical Instrument Digital Interface (MIDI) instrument definition files
Connection	Internet connection files that are used when a
Wizard	computer starts Windows for the first time
CSC	Offline files that are used during client-side caching
Cursors	Cursor and icon files
Debug	Log files
Downloaded Program Files	Downloaded program files
Driver Cache	Uninstalled driver files
Fonts	All font files
Help	Help files
Ime	Language files
ime (x86)	Language files for x86-based systems
Java	Java files
Media	Sound and music files (for example: *.wav and *.midi)
MS	Installation folder for Microsoft® Systems Management Server (SMS) client
Msagent	Microsoft Agent files (Microsoft Agent is a set of programmable software services that support the presentation of interactive animated characters within the Microsoft® Windows® interface)
Msapps	Files that support backward compatibility in applications
Mui	Multi-user interface files
Offline Web Pages	Downloaded Web pages for offline reading
PCHEALTH	Help and Support Center files
Prefetch	Data files related to enhancing the speed at which applications start
Registration	COM+ files. COM+ files are enhancements to the Microsoft Component Object Model (COM)
Repair	Registry backup files (these files are updated if you use NTBackup and choose to back up system state files)
Resources	User interface files
SchCache	Schema cache folder
Security	Log files, templates for snap-ins, and security database files
Setupupd	Dynamic Update storage location
Srchasst	Search assistant files
System	Backward compatibility files related to the System folder (for example, applications that look for a System folder)
system32	Core operating system files (for more information, see "System32 Folder" later in this appendix)
Tasks	Scheduled Task files
Temp	Temporary files

twain_32	Imaging files (for scanners)
Web	Printer and wallpaper files
WinSxS	Side by Side (shared components)

System32 Folder and Subfolders

File Name	Descriptions
system32	Essential system files (for example, Hal.dll and Ntoskrnl.exe files)
1025, 1028, 1031, 1033, 1037, 1041, 1053, 2052, 3076	Localization (language) files for a specific language, corresponding to the number assigned to this folder. This folder remains empty unless Windows XP Professional is localized for this particular language.
CatRoot	Catalog files and signature files
CatRoot2	Catalog files and signature files
Com	Component Object Model (COM) objects
Config	Registry files and event logs
Dhcp	DHCP database files
DirectX	DirectX files
Dllcache	Windows File Protection backup files
Drivers	Installed drivers
Export	Encryption Pack installation files
Ias	Internet Authentication Service files
Icsxml	Universal Plug and Play files
Ime	Language files
Inetsrv	Internet Information Services files
Macromed	Macromedia files
Microsoft	Cryptography files
MsDtc	Microsoft Distributed Transaction Coordinator files
Mui	Multi-user interface files
Npp	Network Monitor and trace files
Oobe	Windows Welcome files
Ras	Remote access server encryption files
Restore	Data files or System Restore related files
Rpcproxy	RPC Proxy files (RPCProxy.dll)
Setup	Optional component manager files
ShellExt	Shell extension components
Smsmsgs	SMS Site Component Manager files
Spool	Print spooling files
Usmt	User State Migration tool
Wbem	Web-based Enterprise Management data files. Windows Management Instrumentation (WMI) is the Microsoft implementation of WBEM.
Wins	WINS database files

Logon Rights

File Name	Descriptions
Access this computer from the network (SeNetworkLogonRight)	Allows a user to connect to the computer from the network. Default setting: Administrators, Power Users, Users, Everyone, and Backup Operators.
Allow logon through Terminal Services (SeRemoteInteractiveLogonRight)	Allows a user to log on to the computer by using a Remote Desktop connection. Default setting: Administrators and Remote Desktop Users.
Log on as a batch job (SeBatchLogonRight)	Allows a user to log on by using a batch-queue facility such as the Task Scheduler service. Default setting: Administrator, System, and Support_xxxxxxxx. When an administrator uses the Add Scheduled Task wizard to schedule a task to run under a particular user name and password, that user is automatically assigned the "Log on as a batch job" right. When the scheduled time arrives, the Task Scheduler service logs the user on as a batch job rather than as an interactive user, and the task runs in the user's security context. The Support_xxxxxxxx account is the logon account for Remote Assistance.
Log on locally (SeInteractiveLogonRight)	Allows a user to start an interactive session on the computer. Default setting: Administrators, Power Users, Users, Guest, and Backup Operators. Users who do not have this right can start a remote interactive session on the computer if they have the "Allow logon through Terminal Services" right.
Log on as a service (SeServiceLogonRight)	Allows a security principal to log on as a service. Services can be configured to run under the Local System, Local Service, or Network Service accounts, which have a built-in right to log on as a service. Any service that runs under a separate user account must be assigned the right. Default setting: Network Service.
Deny access to this computer from the network (SeDenyNetworkLogonRight)	Prohibits a user from connecting to the computer from the network. Default setting: The Support_xxxxxxxx account used by Remote Assistance is denied this right.
Deny logon locally (SeDenyInteractiveLogonRight)	Prohibits a user from logging on directly at the keyboard. Default setting: Guest.
Deny logon as a batch job (SeDenyBatchLogonRight)	Prohibits a user from logging on by using a batch-queue facility. Default setting: Not assigned.
Deny logon as a service (SeDenyServiceLogonRight)	Prohibits a user from logging on as a service. Default setting: Not assigned.
Deny logon through Terminal Services (SeDenyRemoteInteractiveLogonRight)	Prohibits a user from logging on to the computer using a Remote Desktop connection. Default setting: Not assigned.

Privileges

File Name	Descriptions
Act as part of the operating system (SeTcbPrivilege)	Allows a process to assume the identity of any user and thus gain access to the resources that the user is authorized to access. Typically, only low-level authentication services require this privilege. Default setting: Not assigned.Note that potential access is not limited to what is associated with the user by default; the calling process might request that arbitrary additional privileges be added to the access token. The calling process might also build an access token that does not provide a primary identity for tracking events in the audit log.When a service requires this privilege, configure the service to log on using the Local System account, which has the privilege inherently. Do not create a separate account and assign the privilege to it.
Add workstations to domain (SeMachineAccountPrivilege)	Allows the user to add a computer to a specific domain. For the privilege to take effect, it must be assigned to the user as part of the Default Domain Controllers Policy for the domain. A user who has this privilege can add up to 10 workstations to the domain. Default setting: Not assigned.Users can also join a computer to a domain if they have Create Computer Objects permission for an organizational unit or for the Computers container in Active Directory. Users who have this permission can add an unlimited number of computers to the domain regardless of whether they have been assigned the "Add workstations to a domain" privilege.
Adjust memory quotas for a process (SeIncreaseQuotaPrivilege)	Allows a process that has access to a second process to increase the processor quota assigned to the second process. This privilege is useful for system tuning, but it can be abused. In the wrong hands, it could be used to launch a denial-of-service attack. Default setting: Administrators, Local Service, and Network Service.
Back up files and directories (SeBackupPrivilege)	Allows the user to circumvent file and directory permissions to back up the system. The privilege is selected only when an application attempts access by using the NTFS backup application programming interface (API). Otherwise, normal file and

	directory permissions apply. Default setting: Administrators and Backup Operators. See also "Restore files and directories" in this table.
Bypass traverse checking (SeChangeNotifyPrivilege)	Allows the user to pass through folders to which the user otherwise has no access while navigating an object path in the NTFS file system or in the registry. This privilege does not allow the user to list the contents of a folder; it allows the user only to traverse its directories. Default setting: Administrators, Backup Operators, Power Users, Users, and Everyone.
Change the system time (SeSystemTimePrivilege)	Allows the user to adjust the time on the computer's internal clock. This privilege is not required to change the time zone or other display characteristics of the system time. Default setting: Administrators and Power Users.
Create a token object (SeCreateTokenPrivilege)	Allows a process to create an access token by calling NtCreateToken() or other token-creating APIs. Default setting: Not assigned. When a process requires this privilege, use the Local System (or System) account, which has the privilege inherently. Do not create a separate user account and assign the privilege to it.
Create permanent shared objects (SeCreatePermanentPrivilege)	Allows a process to create a directory object in the object manager. This privilege is useful to kernel-mode components that extend the object namespace. Components that are running in kernel mode have this privilege inherently. Default setting: Not assigned.
Create a pagefile (SeCreatePagefilePrivilege)	Allows the user to create and change the size of a pagefile. This is done by specifying a paging file size for a particular drive in the Performance Options box on the Advanced tab of System Properties. Default setting: Administrators.
Debug programs (SeDebugPrivilege)	Allows the user to attach a debugger to any process. This privilege provides access to sensitive and critical operating system components. Default setting: Administrators.
Enable computer and user accounts to be trusted for delegation (SeEnableDelegationPrivilege)	Allows the user to change the Trusted for Delegation setting on a user or computer object in Active Directory. The user or computer that is granted this privilege must also have write access to the account control flags on the object. Default setting: Not assigned to anyone on member servers and workstations because it has no meaning in those contexts. Delegation of authentication is a capability that is used by multi-tier client/server applications. It allows a front-end service to use the credentials of a client in authenticating to a back-end service. For this

Force shutdown from a remote system (SeRemoteShutdownPrivilege)	Allows a user to shut down a computer from a remote location on the network. Default setting: Administrators.See also "Shut down the system" in this table.
Generate security audits (SeAuditPrivilege)	Allows a process to generate audit records in the security log. The security log can be used to trace unauthorized system access. Default setting: Local Service and Network Service. Local System (or System) has the privilege inherently.See also "Manage auditing and security log" in this table.
Increase scheduling priority (SeIncreaseBasePriorityPrivilege)	Allows a user to increase the base priority class of a process. (Increasing relative priority within a priority class is not a privileged operation.) This privilege is not required by administrative tools supplied with the operating system but might be required by software development tools. Default setting: Administrators.
Load and unload device drivers (SeLoadDriverPrivilege)	Allows a user to install and remove drivers for Plug and Play devices. This privilege is not required if a signed driver for the new hardware already exists in the Driver.cab file on the computer. Default setting: Administrators.Do not assign this privilege to any user or group other than Administrators. Device drivers run as trusted (highly privileged) code. A user who has "Load and unload device drivers" privilege could unintentionally install malicious code masquerading as a device driver. It is assumed that administrators will exercise greater care and install only drivers with verified digital signatures.Note: You must have this privilege and also be a member of either Administrators or Power Users in order to install a new driver for a local printer or manage a local printer by setting defaults for options such as duplex printing. The requirement to have both the privilege and membership in Administrators or Power Users is new to Windows XP Professional.
Lock pages in memory (SeLockMemoryPrivilege)	Allows a process to keep data in physical memory, which prevents the system from paging the data to virtual memory on disk. Assigning this privilege can result in significant degradation of system performance. Default setting: Not assigned.

	Local System (or System) has the privilege inherently.
Manage auditing and security log (SeSecurityPrivilege)	Allows a user to specify object access auditing options for individual resources such as files, Active Directory objects, and registry keys. Object access auditing is not performed unless you enable it by using Audit Policy (under Security Settings, Local Policies). A user who has this privilege can also view and clear the security log from Event Viewer. Default setting: Administrators.
Modify firmware environment values (SeSystemEnvironmentPrivilege)	Allows modification of system environment variables either by a process through an API or by a user through System Properties. Default setting: Administrators.
Perform volume maintenance tasks (SeManageVolumePrivilege)	Allows a non-administrative or remote user to manage volumes or disks. The operating system checks for the privilege in a user's access token when a process running in the user's security context calls SetFileValidData(). Default setting: Administrators.
Profile single process (SeProfileSingleProcessPrivilege)	Allows a user to sample the performance of an application process. Default setting: Administrators and Power Users.Ordinarily, you do not need this privilege to use the Performance snap-in. However, you do need the privilege if System Monitor is configured to collect data by using Windows Management Instrumentation (WMI).
Profile system performance (SeSystemProfilePrivilege)	Allows a user to sample the performance of system processes. This privilege is required by the Performance snap-in only if it is configured to collect data by using Windows Management Instrumentation (WMI). Default setting: Administrators.Ordinarily, you do not need this privilege to use the Performance snap-in. However, you do need the privilege if System Monitor is configured to collect data by using Windows Management Instrumentation (WMI).
Remove computer from docking station (SeUndockPrivilege)	Allows the user of a portable computer to undock the computer by clicking Eject PC on the Start menu. Default setting: Administrators, Power Users, and Users.
Replace a process-level token (SeAssignPrimaryTokenPrivilege)	Allows a parent process to replace the access token that is associated with a child process. Default setting: Local Service and Network Service. Local System has the privilege inherently.
Restore files and directories (SeRestorePrivilege)	Allows a user to circumvent file and directory permissions when restoring backed-up files and directories and to set any valid security principal as the owner of an object. Default setting: Administrators and Backup Operators. See also "Back up files and

	directories" in this table.
Shut down the system (SeShutdownPrivilege)	Allows a user to shut down the local computer. Default setting: Administrators, Backup Operators, Power Users, and Users.See also "Force shutdown from a remote system" in this table.
Synchronize directory service data (SeSynchAgentPrivilege)	Allows a process to read all objects and properties in the direct ory, regardless of the protection on the objects and properties. This privilege is required in order to use Lightweight Directory Access Protocol (LDAP) directory synchronization (Dirsync) services. Default setting: Not assigned. The privilege is relevant only on domain controllers.
Take ownership of files or other objects (SeTakeOwnershipPrivilege)	Allows a user to take ownership of any securable object in the system, including Active Directory objects, NTFS files and folders, printers, registry keys, services, processes, and threads. Default setting: Administrators.

Application and Service Tools

File Name	Descriptions
Bootcfg (Bootcfg.exe)	Viewing or editing startup settings in the x86-based Boot.ini file or Itanium-based Boot Manager entries.
Boot logging	Creating a text-based log (Ntbtlog.txt) of listed drivers that loaded or failed at startup.
Dependency Walker (Depends.exe)	Examining a selected application or software component and determining the modules required for it to start.
Device Manager	Viewing and changing hardware and device driver settings.
DirectX Diagnostic Tool (Dxdiag.exe)	Doing the following: ·Viewing information about installed components and drivers for the Microsoft® DirectX® application programming interface (API). · Testing sound, graphics output, and DirectPlay® service providers. · Disabling or enabling DirectX hardware acceleration features.
Dr. Watson (Drwtsn32.exe)	Recording detailed information to a log when application errors occur.
Error Reporting	Monitoring your system for problems that affect Windows XP Professional components and applications. When a problem occurs, you can send a report to Microsoft. An automated process searches the error-reporting database for matching conditions and responds with any

Event Query (Eventquery.vbs)	Displaying events and properties from the event logs.
Event Triggers (Eventtriggers.exe)	Setting triggers based on event log events.
Event Viewer (Eventvwr.msc)	Viewing the Event log, which contains information about application, security, and system events for your computer.
Global Flag Editor (Gflags.exe)	Enabling or disabling advanced internal system diagnostics and troubleshooting tests.
Group Policy Snap-in (Gpedit.msc)	Viewing, creating, deleting, or editing user and computer Group Policy object (GPO) settings.
Group Policy Results (Gpresult.exe)	Displaying information about the cumulative effect that Group Policy objects have on computers and users.
Group Policy Update (Gpupdate.exe)	Refreshing GPOs so that changes takes effect immediately. GPUpdate replaces the Windows 2000 tool Secedit.exe, and provides increased control and flexibility.
Kernel Debugger	Analyzing computer memory or a memory dump file written to disk when a Stop message occurs.
Memory Pool Monitor (Poolmon.exe)	Detecting and analyzing memory leaks.
OpenFiles (Openfiles.exe)	Listing or closing connections to files and folders opened remotely through a shared folder.
Online Crash Analysis	Sending kernel memory dump files to a Web site hosted by Microsoft Corporation for evaluation. An automated process searches a database of known issues for matching conditions. You can optionally receive e-mail updates about your problem.
Performance Monitor (Perfmon.msc)	Obtainin g data that is useful for detecting and diagnosing bottlenecks and changes in overall system performance.
Process and Thread Status (Pstat.exe)	Viewing the status of threads, processes, and drivers.
Program Compatibility Wizard	Testing and resolving compatibility problems regarding running programs that worked correctly on an earlier version of Windows.
Registry Editor (Regedit.exe)	Searching, viewing, and editing the contents of the registry.
Resultant Set of Policy (Rsop.msc)	Viewing information about the cumulative effect that Group Policy objects have on computers and users.
Runas.exe	Running tools and programs with different permissions than the user's current logon provides.

Runas (GUI feature)	Running tools and programs with different permissio ns than the user's current logon provides.
SC (Sc.exe)	Viewing, stopping, starting, pausing, and disabling services, or changing service startup types for diagnostic purposes from the command-line.
Services snap-in (Services.msc)	Viewing, stopping, starting, pausing, and disabling services, or changing service startup types for diagnostic purposes.
Shutdown Event Tracker	Recording information to the System log, describing the reason for shutting down or restarting the computer.
System Configuration Utility (Msconfig.exe)	Enabling or disabling various settings for troubleshooting and diagnostic purposes.
System Information in Help (Msinfo32.exe)	Collecting and displaying system configuration information about hardware, system components, and software. You can start System Information as a stand-alone tool or by using Windows XP Professional Help and Support Center.
System Information (Systeminfo.exe)	Viewing computer configuration information. This is the character-mode version of the GUI-mode System Information tool.
Task Killing Utility (TsKill.exe)	Ending one or more active tasks or processes.
Task Lister (Tasklist.exe)	Listing active tasks and processes.
Task Manager (Taskman.exe)	Viewing and ending active processes running on your system. In addition, you can use Task Manager to view system information, such as CPU and memory usage statistics.
Uninstall Windows XP Professional	Uninstalling Windows XP Professional and reverting to the previous operating system.

Network and Diagnostic Tools

File Name	Descriptions
GetMac (Getmac.exe)	Displaying media access control (MAC) control information for network adapters and protocols installed on a computer.
IP Configuration (Ipconfig.exe)	Displaying the current configuration of the installed IP stack on a networked computer by using TCP/IP.
IP Security Monitor	Confirming that secured communications are successfully established by displaying the active security associations on local or remote computers.
NetBT Statistics (Nbtstat.exe)	Displaying protocol statistics and current TCP/IP connections by using NetBIOS over TCP/IP (NetBT), including NetBIOS name

	resolution to IP addresses.
Netsh(Netsh.exe)	Viewing or modifying TCP/IP network configuration for a computer. Netsh also provides scripting features.
Network Connectivity Tester (NetDiag.exe)	Viewing network-client health by running a wide range of connectivity tests.
Netstat	Displaying protocol statistics and current TCP/IP connections.
Network Diagnostics	Viewing network-related information such as network adapter status, and IP addresses for DHCP and Domain Name System (DNS) servers.
Network Monitor Capture Utility (Netcap.exe)	Monitoring network traffic and capturing information to a log file.
Nslookup.exe	Performing DNS queries and examining content zone files on local and remote servers.
Path Ping (Pathping.exe)	Obtaining network performance statistics. Path Ping displays information for the destination computer and all routers along the way.