

Server Log Books and Event Monitoring

A server Log Book performs the same type of duties as a log book for a vehicle. It holds information regarding every system maintenance action taken on the computer system and when it occurred. The log is essential for troubleshooting and tracking changes and updates. If you maintain a log book, not only will a visiting support technician be extremely grateful but you will probably save money in support costs, mainly through less wasted time trying to track faults caused by undocumented system updates.

Ideally you should have a logbook for every computer, which contains information about the computer's configuration, but it is essential for your server, where all data should be stored and backed up. Having current system information makes it easier to rebuild your computer in the event of a serious system crash.

The type of information to keep includes:

- Computer type, model number, and serial number.
- Computer BIOS, CMOS and other Hardware configuration information.
- Partition information, such as the size of the partitions and the file system used for each one.
- Which versions of Operating System (Windows NT/200x/XP) are installed, and the partitions on which they are installed.
- Details of any device drivers or other system level software that did not come in the Windows retail package. This software would include such things as a Network File System (NFS) provider, network protocol, or network management software.
- Troubleshooting history for any system failures (or Kernel STOP errors – commonly called blue screens). This information should include:
 - The time and date the problem occurred.
 - Any error messages, or events posted to the event log (see below).
 - Any troubleshooting done and the outcome.
- Update/modification history. All updates made to the system (ie. User account creation/modification, printer added/deleted, patches applied, Windows updates, upgrades to clinical and billing software etc). This information should include:
 - The modification made to the system.
 - Who made the modification.
 - Date/time of the modification.
 - Reason for modification.
 - Any known issues created and/or fixed by the modification.
- Whether the backup ran correctly or not.
- Any power disturbances
- Details of routine maintenance, eg. Creating emergency repair disks, running chkdsk, running defragmentation programs, cleaning up archived files, running cleaning tapes etc.

How do you get all of this information?

There is a simple way to generate the majority of the information above by using a printed report. On Windows 200x and XP this is through Start, Control Panel, System, Hardware tab, Device Manager, View, Print.

You will still need to add other information such as troubleshooting history, modification history and any hardware settings if necessary. Most of this additional information is written manually onto a printed spreadsheet or table with the appropriate columns and attached to the rest of the documentation. This way all relevant documentation is available in one place and in hard copy format for easy access by any support personnel that may require it.

Windows Event logs should be checked daily to see if there are any errors listed. Refer to the section below on how to check your Events.

How and where do you store the information?

The usual practice is to purchase a foolscap sized plastic envelope which can hold both floppy disks, reports and other useful summary documentation, then attach it to your Computer System case. Most newsagents stock these with Velcro stickers attached.

An offsite copy is not usually required but it may be useful in some emergencies (eg. Fires, Floods, etc).

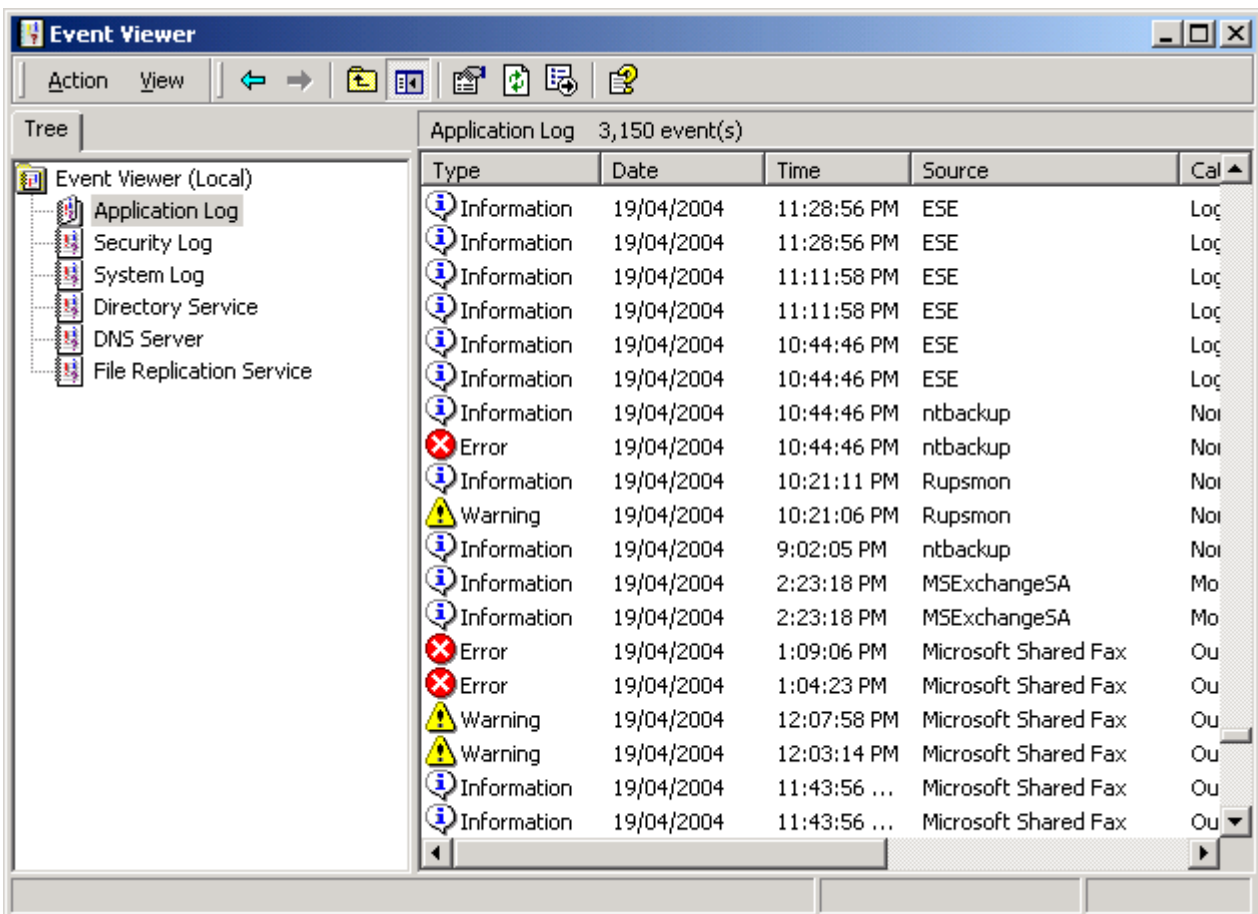
Event Monitor

There are times when significant events occur in your computer system that require you to be notified. For example, you may run out of disk space or your power supply may be interrupted. If a critical event like this occurs, you will receive a message on your screen notifying you. If a less serious event occurs, it is recorded in an event log file, which you can view at your convenience. It is recommended that the Event Logs are checked on a daily basis so that any problems can be fixed as soon as possible.

To view and manage these less serious event logs, use Event Viewer.

To start Event Viewer

1. Point to **Programs**, then **Administrative Tools**, and then click **Event Viewer**.
2. The Event Viewer screen appears:



There may be more or fewer items in the left pane, depending on whether the computer is a workstation or a domain controller and what services are running on the machine. The three major ones to check are:

- The system log records events logged by the Windows system components. For example, the system log records the failure of a driver or other system component that should have been loaded during startup.
- The application log records events logged by applications. For example, a database program might record a file error in the application log.
- The security log records security events. This log helps track changes to the security system and identifies any attempts to breach security. For example, attempts to log on to the system may be recorded in the security log. The security log is not enabled by default, but can be activated through the Security Policy Settings in Active Directory Users and Computers. Use the Help to find instructions on how to do this for your particular machine.

You can use Event Viewer to view, sort, filter, and search for details about events. You can also archive logs in various file formats.

If an error or warning appears, the details can be viewed by double-clicking the event in the right pane. The event ID and text can be used to identify the error to an IT Professional who can assist with fixing any problems. Note that not all error codes are a problem, it may just mean that a service or device was unavailable during startup and that is normal for the startup sequence. Also, if you are using the backup program and use the option to Verify the data, the end of verification shows an error event, which can be safely ignored.

It is recommended that you change the way that the security logs retain their data. This is a simple change that can avoid the problems of computer instability and crashes due to event logs that are full. This is particularly important if you have activated security logging as inability to write another event to this log may mean the PC crashes, potentially to thwart attempts to log on to a machine that cannot record that transaction.

The default setting is to overwrite in 7 days, but if there are a lot of events being logged, this can mean the event logs are full very quickly. To implement 'circular logging', means changing the default setting to Overwrite Events as Needed. This will mean that when the logs become full, the oldest record is removed to make way for the latest event. The size of the event log determines how many events can be recorded.

To change the way Event Logs retain data, in the console tree (left pane), click the log you want to change.

1. Log on as an administrator or a member of the Administrators group.
2. On the Action menu, click Properties.
3. If you would like to increase the size of the log, on the General tab, in Maximum log size, specify the new log size in kilobytes.
4. Change the default setting to Overwrite Events as Needed
5. To put the new setting in effect, click Clear Log.
6. If you want to retain the information currently in the log, click Yes when a message appears, asking if you want to save the original log before clearing it, and then click OK.

