

Taming IIS Logs

Mark Burnett 2000-08-06

Web administrators have a strange relationship with log files. They are an invaluable resource for detecting intrusions and managing security. However, they can also quickly grow out of control and become a burden to monitor. And Windows NT does not make the job any easier. Without a central location for storing logs, a network administrator must look several places using several different tools. If you are monitoring logs on multiple computers it gets even worse. The problem with anything that has to do with security is that if it becomes too much of a burden we stop using it. However, keeping a handle on your logs can greatly enhance your security skills and help you to not look so helpless if you are ever hacked.

Why We Need Logs

Log files allow you to monitor your computer's resources. Those resources include files, applications, network connections, hardware or anything else that someone can use (or abuse) on your computer. Not only do log files tell you that things are being used as they should, they also inform you of abnormal or unauthorized activity. The basic and key elements of a log file are what was used, how it was used, who used it, and when did they use it. The problem with logs is that it is usually up to us to sift through the log entries to identify those entries that require our attention. Although there are tools available to examine log files and create friendly reports, no tool will compensate for poor log management. This article will not explain how to view your logs but will explain a number of log management techniques that can help you keep your log files under control.

Where to Put Logs

In the Unix world, log management has always been very centralized. The main reason is simply because most applications place their logs in the /var/log directory. In Windows NT, logging has never been that centralized. There are EventLogs for Application, System, and Security events, but log files for internet services are placed in C:\WINNT\system32\LogFiles. Other NT services have their own logs strewn about the hard drive and then there are the third-party applications that may keep logs in their own program directories. A network administrator is not going to regularly check logs if that requires looking at several different places using several different viewing applications. What needs to be done is to create a unified and well managed logging strategy.

There is no doubt that log files would be easier to manage if they were all in the same place. Personally, I prefer to create a separate partition just for storing log files. I find that having a separate partition makes it easier to manage ACLs and keeps the logs separated from the applications. I usually make the partition large enough that I will not accidentally run out of log space. Unless I am short on hard drive space, I usually set aside several gigabytes for logs so that I can keep several months online at a time. I then give most groups write access to the drive and only give read access to Administrators. The final step is to create a single directory in that partition named "Current."

Placing logs in a central, secure location is simple task that most NT administrators fail to perform. Even worse, many administrators do relocate logs but put them in a vulnerable location such as a directory named logs or stats under the web root. Because of the sensitive information that log files contain, they should be protected with as much care as any sensitive data files on your computer.

Where to Get the Logs

Now that you have a partition dedicated to log files, the question is what logs are on your system and how do you get all your applications to put their logs on the logs partition? To answer that will take some investigation on your part. Although it is a lot of work up front, it will pay off in time and you will be so much more informed about what is happening on your computer.

To get you started, here are some common log files and how you can relocate them:

EventLogs - These are the built-in NT event logs that are viewed with the Event Viewer. They include logs such as the Application Log, Security Log, System Log, DNS Server, Directory Service, and File Replication Service. They can be relocated by editing the `HKLM\System\CurrentControlSet\Services\Eventlog` registry key. Under that key is a key for each event log and under each of those is a `File` value. Set each file to be saved in the "Current" directory of your log files partition. Edit that value and restart your computer for the changes to take effect.

Internet Services - These are your web, FTP, and other internet log files. These are unique in that they can be set to cycle so that the log file name is based on the cycling period. To change the location of these log files, edit the web or FTP root properties and select the properties for

the log file. From there you can set the logs to be saved in the "Current" directory of your log files partition.

Schedule Logs - An important log that is often overlooked is the one for the Scheduler service. Located at `C:\WINNT\SchedLgU.Txt`, it logs all actions taken by the Scheduler service, including when it was started and stopped. The location of this file can be changed by editing the `LogPath` value in the `HKLM\SOFTWARE\Microsoft\SchedulingAgent` registry key.

Performance Logs - These logs are created by the Performance Monitor counters. They can be changed by editing the `DefaultLogFileFolder` value in the `HKLM\System\CurrentControlSet\Services\SysmonLog` registry key.

In addition, you should not overlook other sources for log files:

Application Logs - If you have a third-party Web, FTP, or mail server you may want to track down their logs and direct them to your new partition.

Modem Logs - If you have enabled logging on your modem connections, it may be a good idea to set those logs to be saved in your logs partition.

Network Device Logs - If your router creates its own logfiles, you may want to periodically collect them and have them stored along with your other logs.

Sent Mail - Although not really a log file, you may want to periodically check or script a list of e-mails sent.

Directory Listings - Again, this is not a traditional log file, but it may be a good idea to schedule a daily directory listing of sensitive directories to be redirected to a file in your logs partition.

For example, you could schedule a command like this:

```
dir C:\InetPub\wwwroot\ /S /B > [LogPartition].
```

If a new file suddenly appears, you will be able to track down when it first appeared.

Processes - Like directory listings, this is not a traditional log file but can be useful to monitor what processes are running on your server. By scheduling `ps.exe`, `tlist.exe`, or a number of freeware process listers and saving the results to a file, you can easily spot trojans or unauthorized applications. Along the same lines, you may want to schedule `NetStat.exe` to run

to view which ports are listening on your computer.

Cycling and Archiving Logs

Now that you have a central location for all your logs and all your important log files are being dumped there, you should come up with a strategy for cycling and archiving your logs. Log cycling is the process of closing up all log files each day (or whatever cycle period you specify) and placing them in a different file or directory. That breaks the log files down in to more manageable chunks and makes them easier to review. Also, when the time comes to track down an entry, you can narrow down your search to a specific day.

Log cycling is best done with a scheduled batch file that moves all the files out of the Current directory into another directory named with the current date. Obviously, the best time to schedule this script is as close to 12:00am as possible to keep the dates in the right place. Bear in mind that some files will not allow being moved and you may have to stop the process in order to move the file. One example is the Scheduler service's log. In order to move the file, you must issue the command `Net Stop Scheduler` then after moving the file use `Net Start Scheduler`. Also, rather than move the NT event logs, you may prefer to dump them to an ASCII format using one of the many event log utilities available. After doing that, you should then clear the event logs so that they are starting the new day clean.

As you collect logs day after day you will eventually want to move them offline. Not only does it save disk space, but if archived properly a log file may be very useful as evidence of misuse of your system. To best accomplish that would be to use a write-once-read-many (WORM) device such as a recordable CD-ROM. As an extra precaution, I like to include a directory listing of all files to be archived that shows the last write and last access times. Finally, you should store your archive CD's in an organized manner, each one well-labeled and in order.

We cannot always protect our web sites from attackers but we can collect information about those attackers. Having our information in a unified logs directory will greatly enhance your ability to monitor or search those logs. Next time when you get that call that the web site has been hacked, you will know exactly where to go and for once, information will be on your side.

Relevant Links

[Logging Section of IIS Security Checklist](#)

Microsoft

[Log section of Secure IIS5 Checklist](#)

Microsoft

[Logging Server Activity](#)

Microsoft

[Dealing with Windows NT Event Logs Part 1](#)

SecurityFocus

[Privacy Statement](#)

Copyright 2006, SecurityFocus