COMMONWEALTH OFFICE OF TECHNOLOGY

Risk and Compliance
Informational Paper

Microsoft IIS Logging and Log Archiving
October 23, 2015

Objective:

This paper will address the recommendation that IIS event logging and log archiving be enabled and performed in every web service instance. This paper applies to Microsoft IIS, but the concepts apply to Apache daemons and any other general purpose web service provider. It is intended to apply to the procedures level of operations.

Overview:

Configuring an IIS Web Service to properly maintain activity logs and then archiving those log files is considered a Best Practice that should be followed in every web service instance unless there is a clear business or security reason not to do so.

This appears to be the only relevant Enterprise policy statement:

"*The level of filtering, supplemental authentication, audit logging, and associated access restrictions must be based on the risk posed by the attached computer systems and applications on both sides of the network connection*."
https://gotsource.ky.gov/docushare/dsweb/Get/Document-329691

Recommendations:

From an incident response perspective, there is the assumption that logging is enabled, specifically during an incident. The IIS logs, along with the event longs in Windows, are a primary source of information during a forensic investigation. Keep in mind that if the incident was malicious the logs would be a primary target for "covering their tracks".

Each IIS service (or any web service) should have logging enabled. The record format would be up to the agency to decide based on how the logs would be reviewed and what software would be used, but the default is typically adequate. There is very little granularity to the logging features of IIS, nor do you know to what degree of detail a log should contain until you have an incident. So the best practice is to “enable fill logging” rather than fine tuning it to a “minimal” level.

The directory containing the log files should be located on the data volume, that is to say any volume other than the SYSTEM volume which is bootable and contains the Operating System. This is important because the log file directory is on the system volume by default and exhausting that volume's space will possibly abend a server and likely keep even administrators from logging in or restarting the server without taking extreme measures such as booting with Linux, mounting the SYSTEM volume and moving the log files to a non-SYSTEM volume. The issue here is that the Windows OS will not boot unless there is adequate free space on the SYSTEM volume for logging and registry manipulation.

IIS log files can eventually use significant disk space, so there should be a routing in place to archive them off of the system to free-up disk space and to remove them from any remote attack vector.

A reasonable configuration would include;

- IIS 7.0 services typically ship with logging enabled, but not IIS 7.5. The configuration should be reviewed to verify that logging is enabled.

- Archiving the directory quarterly, moving the files off the server and into an off-line archived state.

- Review the logs prior to archiving using any of several open source log analysis tools that are available to determine if any significant attacks have occurred. There will be many insignificant attacks/probes as opposed to an actual breach. It is recommended that these logs be reviewed regularly and possibly more often than the archiving routine.

- The archived logs should be zipped to save significant disk space (in production, they are regular CSV ASCII files).

It is also recommend that the directory that contains the log files should be protected by setting its permissions to allow access (RW) only to the IIS service and system administrators.

References and Supplemental Information:

Configuring Logging in IIS 7
https://technet.microsoft.com/en-us/library/cc732079(v=ws.10).aspx (10/23/2015)

Default Log File Settings for Web Sites <logFile>
https://www.iis.net/configreference/system.applicationhost/sites/sitedefaults/logfile

How to Change the Log File Directory in IIS7
https://exchangeserverpro.com/change-log-file-directory-iis7/