Log Analysis – Seeing the Trees in the Forest

Questions and Answers
Februrary 2, 2016

Q: How long did it take you originally and how long does it take now to do the analysis?
A: Initially, the process took 60 minutes or more. This was due to learning and developing the process and having a very long list of lines I was not willing to ignore. Within a few months the time was reduced to 15 to 20 minutes. More importantly, every line of the log was reviewed in some way and I could address any issues uncovered.

Q: What other files have you done this on?
A: Similar methods could be used on any structured log – special or delimited. While the Service Manager logs are the primary logs, I have used similar methods on the Apache Tomcat logs. I analyzed these for about six months and found it not useful.

Q: What are the dangers of ignoring a log entry?
A: You may decide to ignore a line that is important. Be conservative.

Q: Couldn’t you automate more of this?
A: Yes. I could probably automate it to the point of receiving an email with the Cross-tab report and other selected information. If I did that, I would loose contact with the process and probably neglect to add or delete lines to ignore.