Log Server Lab Assignment

Choose one of those assignments. The harder it is, the higher the grade you can get.

In your report log, show the relevant command lines and configuration parameters you went through, and most importantly, show the PoC results, logs and acceptance testing.

Graylog [medium]

Setup a graylog collector agent, filebeat agent, and a Graylog server. Make sure a few logs end-up on the server using this method.

Alternatively, you can setup Graylog Server to listen on standard syslog UDP port. Show a sample log and make sure it ended-up there using that alternate method.

ELK [hard]

Same as for Graylog but with ELK.

LogZilla [hard]

Same as for Graylog but with LogZilla.

No Web Required - visualize the logs [medium]

The idea here is to have some kind of replacement of an UI. Setup a traditional log server (sysklogd / rsyslog / syslog-ng / bsd syslogd) so that it writes logs to files depending on parameters. For exemple depending on what host is sending a log, write the log to a different file. Do we now have a CLI-based dashboard and can we easily navigate through logs with lnav? What are the pros and cons for this solution?

https://man.netbsd.org/syslog.conf.5

No Web Required - spot abnormal logs [medium]

Same as above but we rather want to show logs (or get alerts) in case something strange happened. A simple way to make some DIY alert system would be to grep out any known-OK logs. Setup your own blacklist based on a reverse grep filter.

Redis as an error log server [full-blown-project]

Redis can be setup so it stores data not only in memory, but also on disk. However the entire db remains in memory anyhow so we need to handle that use-case:

- send only errors to that log server
- clean-up old logs frequently

Elaborate on that and make a few tests.

https://redis.com/ebook/part-2-core-concepts/chapter-5-using-redis-for-application-support/5-1-logging-to-redis/