Sahil Patel (159-065-176)
Abdulbasid Guled (156-024-184)
Andre Jenah (134-901-180)

DPS912: Assignment 2 Reflection

1. **Generally, what are syslog and rsyslog? Specifically, name three features of syslog/rsyslog and compare them to your embedded debug logging. Will there be any overlap of information?**

   Syslog is a standard network-based logging protocol from the 1980's which has many applications that can work on a number of different devices and applications. It allows these devices/applications to send text-formatted log messages to a central server.

   Rsyslog is a rocket-fast system for log processing which was first introduced in 2004. It encompasses excellent features for security combined with its high performance and modular design. It's essentially an upgrade from the regular syslog. It can accept a number of inputs coming from a wide range of devices/applications, go onto transform them, and then output the final results to a number of destinations. Alongside these features, it's also been updated to be able to listen to TCP/UDP connections and filter through the generated log by one of the three following methods: source, message, and pid.

   As per our implementation of the embedded debug logging, we don't have the very complex and finite details that the rsyslog boasts. However, we encompass the basic concepts that both of these loggers possess. Therefore, there will be an overlap of both the Syslog and Rsyslog in our implementation. An example is the timestamp that we included and the priority level which we had specified.

2. **Name five features of syslog-ng.**

   The five features of the syslog-ng are as follows:

   - Content and level based message filtering
   - TCP for transport
   - Options for flexible configuration
   - Remote logging
   - Fast searching capabilities

3. **Name five ways syslog-ng is an improvement over syslog/rsyslog.**

   The five ways that syslog-ng is an improvement over the syslog/rsyslog are as follows:

   - Offers a commercial variant (Advantage for corporate users)
   - It is enhanced/supported for multi-threading
   - Able to receive logs from a number of sources at once
   - The filers that are available have the option to be nested which in turn allows them to be reused for a number of destinations. This makes it easier to maintain and provides flexibility.
   - It is compatible with databases such as MySQL & MongoDB making it superior for storage related solutions for DB's

Sahil Patel (159-065-176)
Abdulbasid Guled (156-024-184)
Andre Jenah (134-901-180)

4. **Consider a Log Server that has to manage embedded logs for a massive amount of processes on a massive amount of machines. Name three ways the server could manage the connections to each process.**

   The three ways that the server could manage the connections to each process are as follows:

   - To balance out the massive amount of processes, could have more threads to deal with that.
   - Investing in larger and more servers (expanding) for hardware to process more massive amounts of processes while also having a high speed.
   - We can use thread pools to maintain a list of threads that are ready to receive a client connection each time a new client connects, which allows the server to maintain each connection through each thread in the thread pool.

5. **Consider a Log Server that has to manage embedded logs for a massive amount of processes on a massive amount of machines. With such a large amount of data in the logs, name three ways a user could extract useful information from them (be general).**

   The three ways a user could extract useful information from them are as follows:

   - We can use more traditional methods such as awk to read the logs or use grep to provide the type of patterns that are being used.
   - The tools available on the syslog-ng commercial variant are an excellent method.
   - We can take a large amount of data and then parse it by utilizing loops.

6. **Explain how gdb could be used on a Linux machine to attach to a process and get thread information. Is this also useful in debugging?**

   GDB can be used on a linux machine to attach itself to a process during runtime. It helps an application that’s running to debug. Therefore, it is useful in debugging as it can let you debug while it's running. The command is as follows: $ gdb <PROCESS NAME> <PROCESS ID>