A Syslog ETL Process

ETL Threads (Consumer)

ETL Threads (Producer)

MySQL

A single formatted file (ASFF)

Thread 2

Thread N

Thread 1

Thread N

Thread 2

Thread 1

Syslog File

Above diagram is the internal organization of the process. A set of threads (Producer) will read syslog file, format every log message and append that formatted message to a single file (ASFF file). Another set of threads (Consumer) will read every formatted message from ASFF file and write them down into MySQL and delete that message from ASFF file.

Syslog file format:

<Timestamp><Space><IP Address><Space><Process Name><:><Space><Message Text>

Example:  
Feb 9 03:26:05 localhost systemd: Removed slice User Slice of nmonagent.

ASFF file format:

Timestamp: Feb 9 03:26:05

IP-Address: localhost

Process-Name: system

Message: Removed slice User Slice of nmonagent.

<New line [\n]>

Following are the requirements that should be met while implementing the application –

* Programming language: C
* Supported platform: Windows, Linux
* Need to be Thread-safe