

WHY `GREP` ISN'T ALWAYS THE BEST CHOICE?

- ▶ You can't reliably share your query
- ▶ You might not have the level of access required to dump the logs from a target machine
- ▶ It's hard to correlate logs across multiple micro services / sources
- ▶ It is simply not possible if you have 100+ GB of logs across thousands of machines

LOG INGESTION PIPELINE

