Currently, when some issue occurs at the service end we usually have to look at multiple log files stored in different servers to pinpoint the issue. Having a proper centralized log management infra will help us to investigate or debug the problems that arise in the system easily.

The ELK Stack is most commonly used open source tool for this kind of purpose.

ELK is used because it helps in aggregating log and audit data from the different sources, processing and enhancing this data (Logstash, Beats), storing them in one central data store (Elasticsearch), and providing analysis and visualization tools (Kibana).