LOG
ANALYSIS TOOL
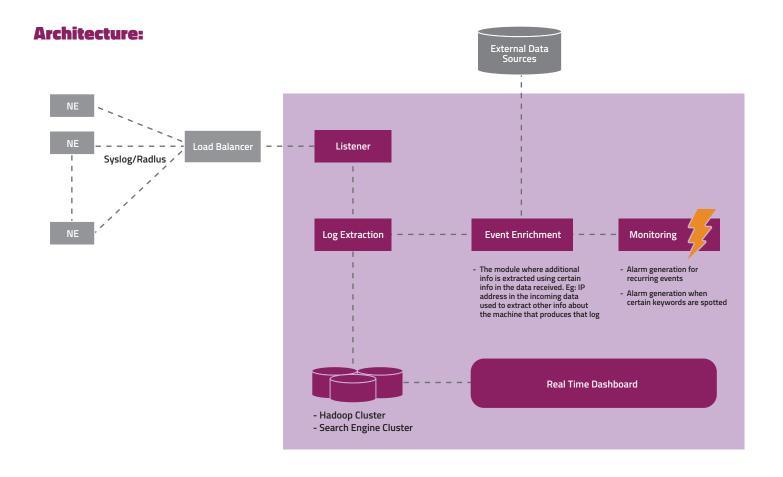

Communication networks have various smart devices producing data continously. Log Analysis Tool collects such data, correlates and compares with related historic data. Based on specified rules, it creates alerts for the responsible units, for a healty and effective network generation.

Architecture:

NE

NE

Syslog/Radlus

NE

Load Balancer

Listener

External Data Sources

Log Extraction

Event Enrichment

Monitoring

- The module where additional info is extracted using certain info in the data received. Eg: IP address in the incoming data used to extract other info about the machine that produces that log

- Alarm generation for recurring events

- Alarm generation when certain keywords are spotted

Real Time Dashboard

- Hadoop Cluster
- Search Engine Cluster

Key Features:

- Monitoring the logs created by the switches and routers in the network and providing a guidance in finding the possible causes of various events

- Processing, recording real-time log records and indexing for high performance queries

- Scalable performance (horizontal growth with increasing log amount)

- Correlating logs from different sources to help finding the causes of various events

- Detecting alarm creating events in the network and sending notification (Sending notice via E-mail following the execution of critical commands on routers and switches, sending notifications to relevant departments when the same alarm occurs 10 times in 5 minutes)

- Logs queries according to various criteria and the related user interfaces