Requirements for a logtool
Roundtable discussion

2nd SIG-NOC meeting
Vienna
09/11/2015

Belnet
dedicated connectivity

.be

Basic Sections

- Functionalities
- Performance
- Model
- Cost

Functionalities

- Input

  what sources can be collected?
  open API?
  third party apps / modules / daemons
  IPv6 support

- System

  how modular is the system?
  how easy is it to find something?
  what can be searched and in which way?
  Correlation of logs or events: how does it work?

Functionalities

- Legal

  is there a way to anonymize logs ?
  laws about what can be stored where.

- Output

  what are the output methods (files / alarms / reports /webinterface...)
  how is the visualization of the data?
  which reports can be generated?
  which thresholds can be set and how?

Performance

- scalability / extendability
- redundancy
- searching / query times
- number of logs that can be stored / queried
- method of concatenating / aggregation of data / auto-cleanup
- offloading methods for older data
- scheduling

Model

- type
  - centralised or distributed
- data
  - local or remote (can be but not limited to "the cloud")
- philosophy
  - open source
  - closed / proprietary

Cost

- Cost per log
- Cost for installation / initial setup
- Cost for operation / recurring costs
- scalability of costs

Existing solutions

- Graylog / Graylog2
- Splunk
- SumoLogic
- Logentries
- Logstash
- HP Arcsight
- Netwrix
- Alienvault
- Solarwinds

Thanks for participating

2nd SIG-NOC meeting
Vienna
09/11/2015

Belnet
dedicated connectivity

.be