LogApp Release 3.6 (Build 3643)

iQSol
Security made in Austria.
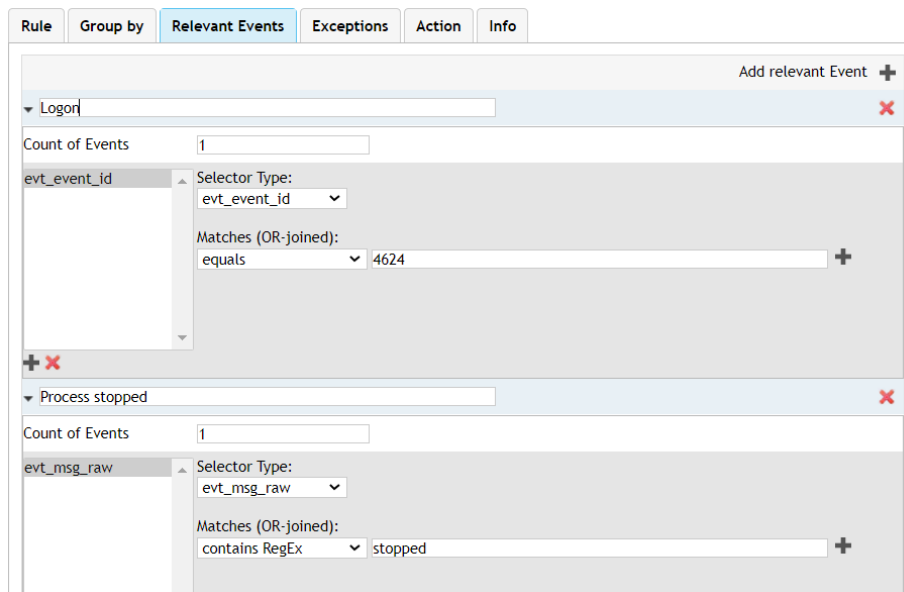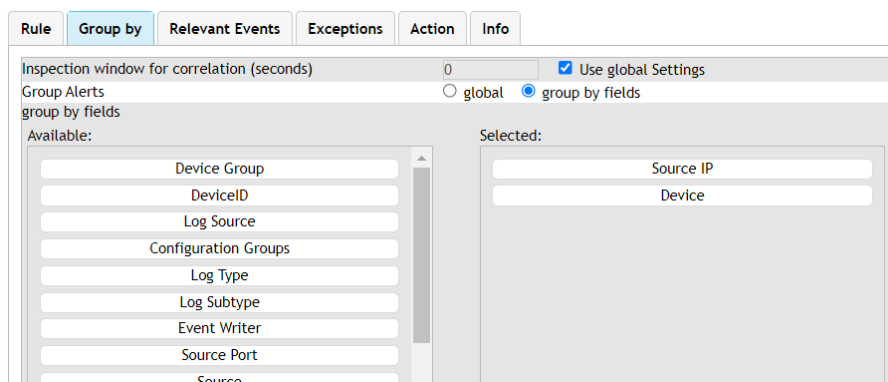
LogApp Release 3.6 (Build 3643)

Release Date 07-12-2021
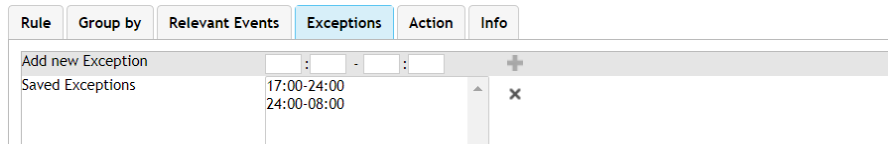
New Features / Enhancements

- Correlation enhancements
    - o new rule type correlation with counters for relevant events necessary for correlation
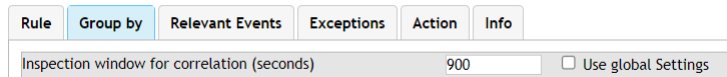

    - o new rule type missing any
    - o new rule type missing all
    - o group by: correlating and aggregating events grouped by selected event fields
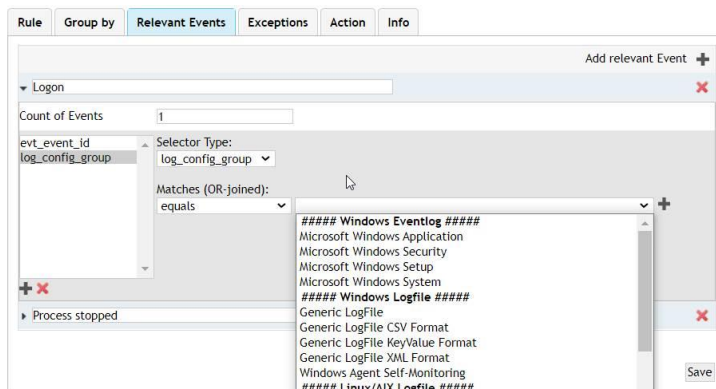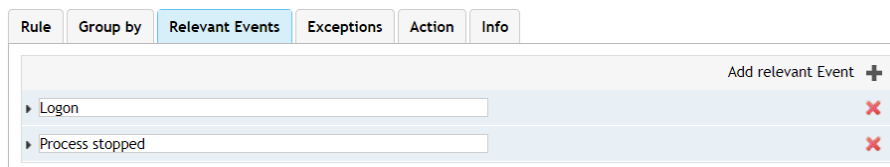
- o time frame exceptions: correlation and aggregation is paused for defined time frames (e.g. at night)
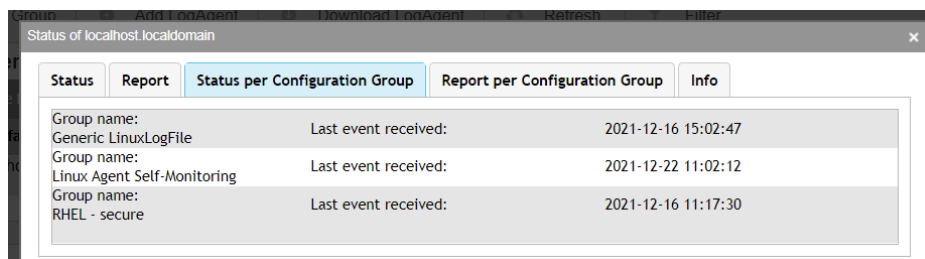

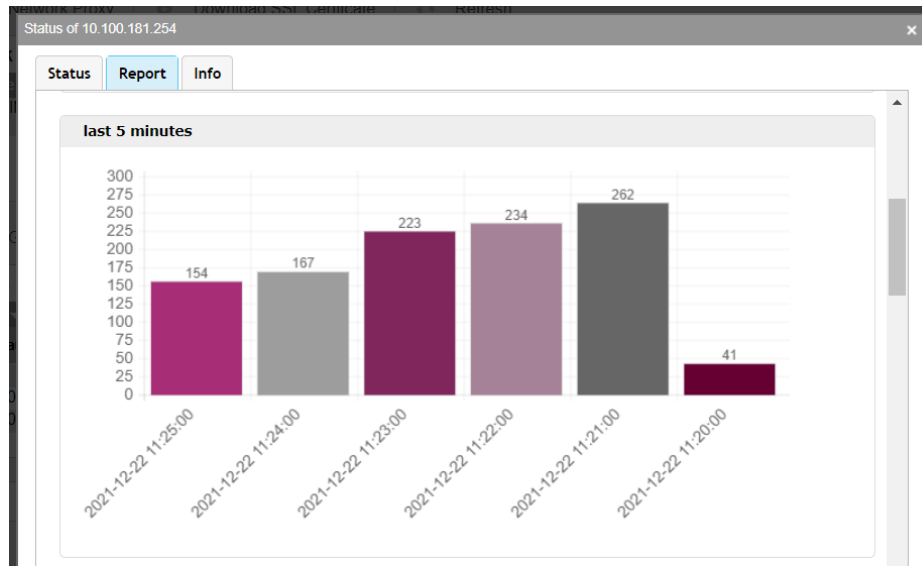- o individual inspection window per rule

- Alert rules simplification (relevant events not sticking to configuration groups any more)

- Agent health and event transmission stats enhancements
  - o event transmission stats for agent and agent configuration groups at GUI and via SNMP
  - o event transmission stats for network devices at GUI and via SNMP
  - o event transmission stats for forwarding devices at GUI and via SNMP

- syslog via TCP octet counting mode (e.g. for Fortinet)
- exporting configuration audit data to Enterprise Reporting Server
- editable FIM path, whitelist and blacklist entries

- improvement of counters of network and forwarding devices
- additional page navigation for event and alert views

- CSR SAN capable of multiple values