IBM z Systems

Anomaly Detection Engine for Linux Logs: Open Source Contribution

February 9, 2016

IBM

Project Overview

- Aug 17, 2015 Announcement at LinuxCON : IBM to contribute the Linux log anomaly detection technology to the Linux Foundation under the Open Mainframe Project

  Improves resiliency for Linux environments and provides ability to analyze Linux logs enabling faster problem determination

- Open Source License - GPL V3: Determined by the IBM legal team and IBM Open Source Steering Committee board for the following reasons

  1. protection of high value patents associated with the contribution
  2. protection against 3rd parties creating proprietary solutions that include this contribution without contributing any enhancements back
  3. contribution includes Apache V2 components

- Contributions accepted under Corporate Contributor License Agreement (CLA)
- Repository for the new open source code will be *github*
- *Sizing: 50K*

Open source Linux log Analytics

- Value / Support for
  - Faster problem determination
  - Root cause analysis and system health
- Functional Content
  - Analytics Framework
  - Linux syslogd anomaly detection
- Pre-requisites:
  - JDBC compliant database