What is new in syslog-ng 3.X?

Peter Czanik / BalaBit

About me

- Peter Czanik from Hungary
- Community manager at BalaBit: syslog-ng upstream
- BalaBit is an IT security company with HQ in Budapest, Hungary
- 150 employees
  - over 80% can configure a Linux kernel :)

Topics

- What is syslog? And syslog-ng?
- What is new? + DEMO
  - Patterndb
  - Correlation
  - Modularization
  - Multithreading
  - JSON
  - MongoDB
  - AMQP
- Questions?

What is syslog?

- Logging: recording events
- Syslog:
  - Application: collecting events
  - data: the actual log messages
  - Protocol: forwarding events
- History:
  - Originally developed as a logging tool for sendmail
- Format:
  - <38>2013-02-13T11:43:58 localhost sshd[1234]: Accepted password for root from 192.168.101.1 port 38420 ssh2

What is syslog-ng

- Syslog-ng: “Next Generation” syslog, since 1997
- Focus on central log collection
- “Swiss army knife” of logging
  - High performance
  - More input sources (files, programs, and so on)
  - More destinations (databases, encrypted net, etc.)
  - Better filtering (not only priority, facility)
  - Processing (rewrite, parse, correlate, and so on)

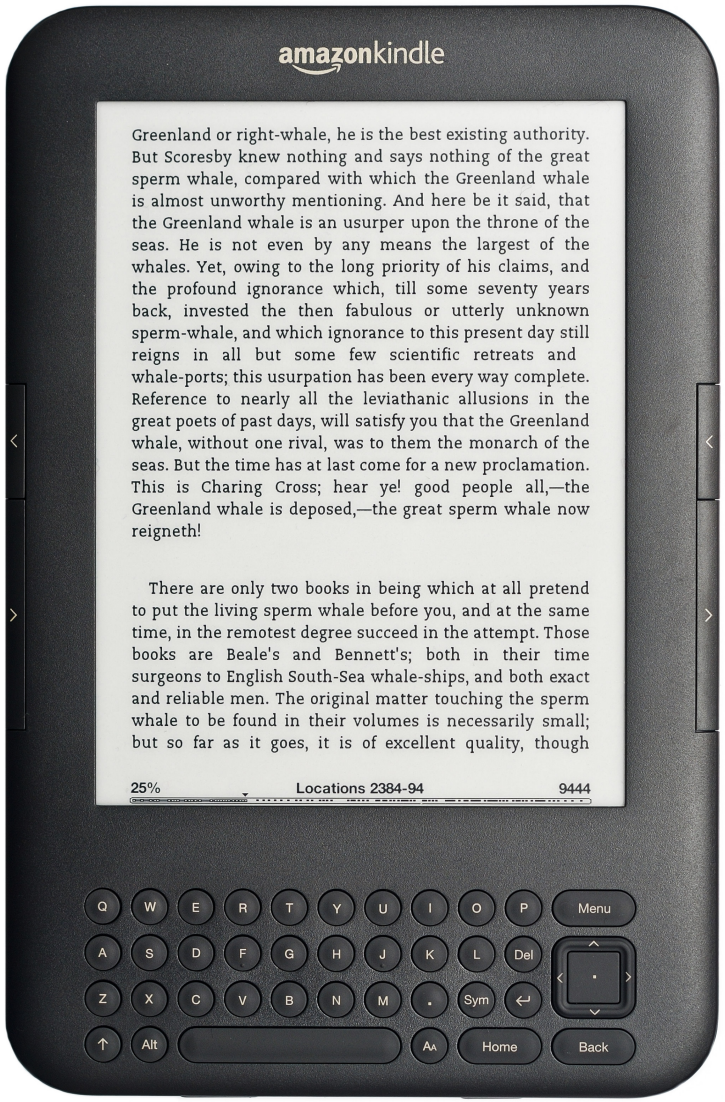
- OSE vs. PE

Which syslog-ng version is the most popular?

- Hints:
  - the current version is v3.4 (2 months old :-))
  - SLES has v2.0
  - Debian has v3.1
  - Gentoo has v3.2
  - Fedora has v3.3
  - openSUSE has v3.4

Version 1.6

- V1.6
- :-)



So what's new?

- 2.0 was a complete rewrite
- 2.1 added SQL destination, TLS/SSL networking
- Major 3.X features in more detail

PatternDB

- syslog-ng: name-value pairs inside
  - Date, facility, priority, program name, pid, etc.
- PatternDB message parser:
  - Can extract useful information into name-value pairs
  - Add status fields based on message text
  - Message classification (like LogCheck)
- Example: an ssh login failure:
  - user=root, action=login, status=failure
  - classified as “violation”
- DEMO: what a patterndb rule looks like

Correlation

- An extension to patterndb
- Create a new event based on the information from previous related events
- Example:
  - First event: ssh login by joe
  - Second event: ssh logout by joe
  - These two could be combined into: user joe was logged in from 8:00 to 16:00 from 192.168.253.253
- Also used for firewall logs, postfix, etc.
- DEMO

Code modularization

- Easier to develop and extend
- More external contributions
  - Patterndb parsers
  - The complete AMQP destination

Multi-threading

- Greatly improved performance
- Under some special circumstances over 800k messages per second
  - Multiple TCP sources with multiple Gigabit connections
  - Flat file destinations with fast SSD storage
  - Only simple filtering (not content based)

MongoDB destination

- The most popular NoSQL
- Easy storage for PatternDB results

- DEMO: http://mojology.madhouse-project.org/

JSON output and parser

- Web 2.0 :)
- CEE / Lumberjack logging standards use it
- Forwarding name value pairs
- Interpreting JSON based logs

- DEMO

AMQP destination

- First major outside code contribution
- Publishes messages using AMQP
- Other message queuing protocols (stomp), sources are also planned

- DEMO

So, why syslog-ng?

- 15 years of open source development
- High performance log management
- Flexible configuration
- Excellent documentation
- PatternDB message parsing

Questions? (and some answers)

- Questions?

- Some useful syslog-ng resources:
  - Syslog-ng: http://www.balabit.com/network-security/syslog-ng
  - Many books at http://oreilly.com/
  - ELSA (log analysis based on syslog-ng's patterndb): http://code.google.com/p/enterprise-log-search-and-archive/

  - My blog: http://czanik.blogs.balabit.com/
  - My e-mail: czanik@balabit.hu

End