

 **ONE IDENTITY™**

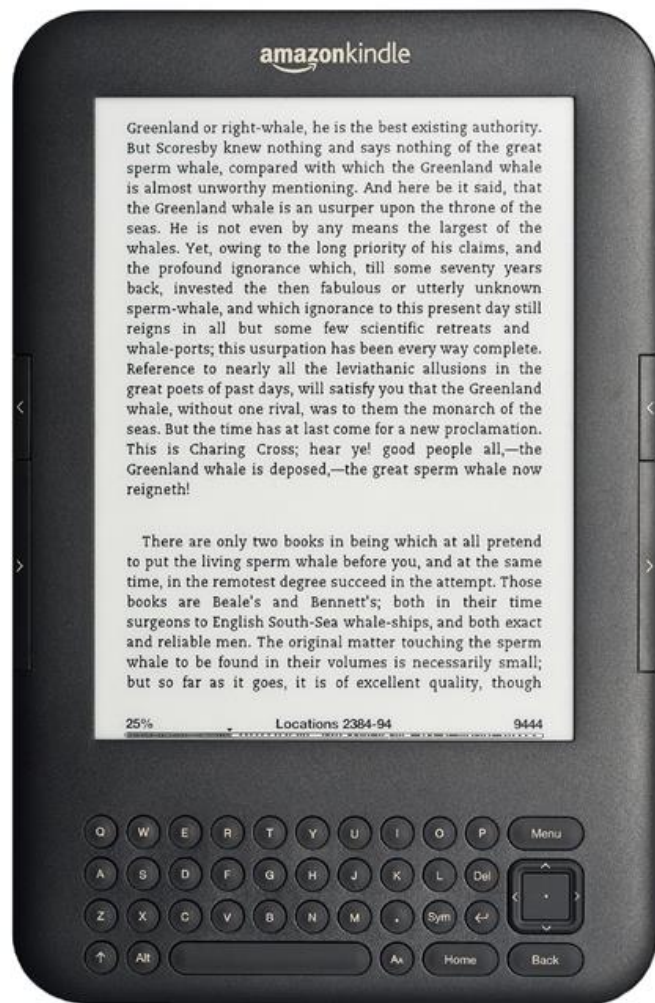
# **Syslog-ng 101, part 3: Syslog-ng editions, and where to get them from**

Peter Czanik

## Question from last time:

- Which is the most used syslog-ng version?

# Was this your answer?



## Version 1.6

- Due to the Kindle e-book reader
- Hundreds of millions of devices

# Syslog-ng editions

- Syslog-ng Open Source Edition (OSE)
  - The focus of this tutorial
- Syslog-ng Premium Edition (PE)
  - Most of my examples also work with PE
- Syslog-ng Store Box (SSB)
  - Not focus at all

# Syslog-ng Open Source Edition (OSE)

- Focus of this tutorial
- “syslog-ng” for open source users, OSE for the rest -> @SNGOSE Twitter user
- This is where syslog-ng is developed
- Source and issue tracking on GitHub
- Includes experimental features
- Part of most Linux distributions, BSD variants
- Community support
- <https://www.syslog-ng.com/products/open-source-log-management/>

# Getting syslog-ng (OSE)

- Starting with this slide syslog-ng refers to syslog-ng OSE
- Syslog-ng is part of most Linux distributions and BSD variants
  - Often an old version with a limited feature set
- Up-to-date unofficial packages
- Up-to-date container images
- Build from source
  - DBLD

# Getting the right feature set

- Usually base package + modules
- RPM distros:
  - Core package: syslog-ng
  - Modules: syslog-ng-`{modulename}`
- DEB distros:
  - Everything: syslog-ng
  - Core package: syslog-ng-core
  - Modules: syslog-ng-mod-`{modulename}`
- FreeBSD:
  - Pkg: JSON + HTTP (curl)
  - Ports: all syslog-ng features available



## For next time

- Install syslog-ng with JSON support
- HTTP (curl) support is optional, if you have Elasticsearch (or compatible)
- GeoIP support is optional, getting a database can be a pain

 **ONE IDENTITY™**