Network Startup Resource Center

Network Management & Monitoring

Log Management

Why logs?

- Logs are when your devices are trying to tell you something!
- Typically shows *events*, e.g.
  - Link has gone down
  - Power supply has failed
  - Login failure from a particular IP
  - Someone made a config change
  - … etc
- Much of this is not available via SNMP

Log Management and Monitoring

On your routers and switches

```
Sep  1 04:40:11.788 INDIA: %SEC-6-IPACCESSLOGP: list 100 denied tcp
79.210.84.154(2167) -> 169.223.192.85(6662), 1 packet

Sep  1 04:42:35.270 INDIA: %SYS-5-CONFIG_I: Configured from console by pr on
vty0 (203.200.80.75)

%CI-3-TEMP: Overtemperature warning

Mar  1 00:05:51.443: %LINK-3-UPDOWN: Interface Serial1, changed state to down
```

And, on your servers

```
Aug 31 17:53:12 ubuntu nagios3: Caught SIGTERM, shutting down...

Aug 31 19:19:36 ubuntu sshd[16404]: Failed password for root from
169.223.1.130 port 2039 ssh2
```

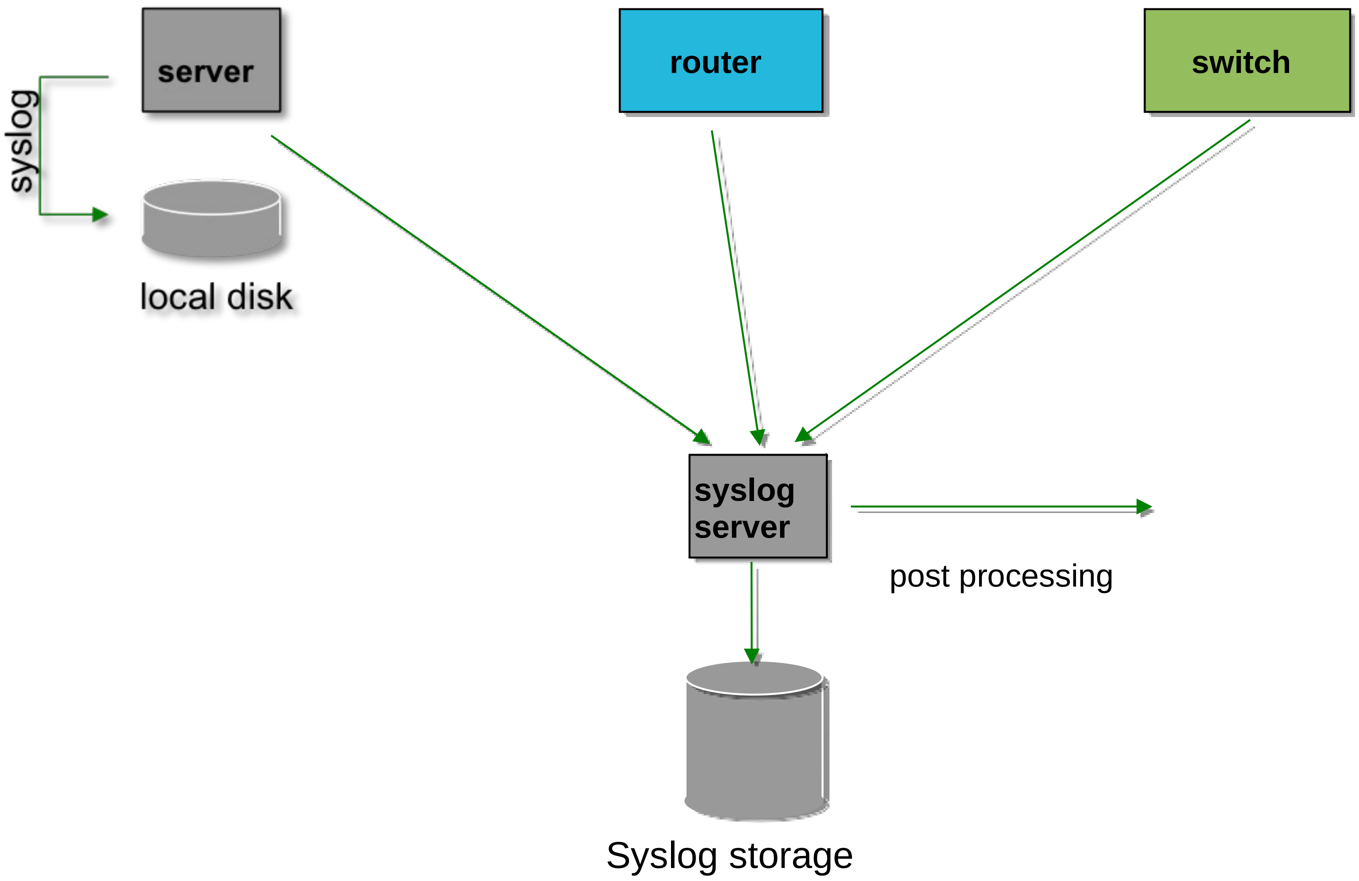
Log Management and Monitoring

- Keep your logs in a secure place where they can be easily inspected.
- Watch your log files.
- They contain important information:
  - Lots of things happen and someone needs to review them.
  - It’s not practical to do this manually.

Log Management

- Centralize and consolidate log files
- Send all log messages from your routers, switches and servers to a single node – a *log server*.
- All network hardware and UNIX/Linux servers can be monitored using some version of *`syslog`*.
- Windows can, also, use syslog with extra tools.
- Save a copy of the logs locally, but, also, save them to a central log server.

Centralized logging



Syslog basics

Uses UDP protocol, port 514

Syslog message have two attributes (in addition to the message itself):

```
Facility                         Level

Auth        Security        |      Emergency  (0)
AuthprivUser                |      Alert      (1)
Console     Syslog          |      Critical   (2)
Cron        UUCP            |      Error      (3)
Daemon      Mail            |      Warning    (4)
Ftp         Ntp             |      Notice     (5)
Kern        News            |      Info       (6)
Lpr                         |      Debug      (7)
Local0 ...Local7            |
```

Configuring centralized logging

Cisco hardware

- At a minimum:
  - logging ip.of.logging.host

Unix and Linux nodes

- In /etc/syslog.conf, add:

```
*.*            @ip.of.log.host
```

- Restart syslogd

Other equipment have similar options

- Options to control *`facility`* and *`level`*

Receiving syslog messages

- Identify the *facility* that the equipment is going to use to send its messages.
- Reconfigure *syslogd* to listen to the network.
  - Ubuntu: enable ”`imudp`” in `/etc/rsyslog.conf`
- Add an entry to *syslogd* where messages are going to be written:

```
local7.*                /var/log/routers
```

- Create the file

```
touch /var/log/routers
```

- Restart *syslogd*

```
systemctl restart rsyslog
```

Grouping logs

- Using *facility* and *level* you can group by category in distinct files.
- With software such as *rsyslog* you can group by machine, date, etc. automatically in different directories.
- You can use *grep* to review logs.
- You can use typical UNIX tools to group and eliminate items that you wish to filter:

```
egrep -v '(list 100 denied|logging rate-limited)' mylogfile
```

- Is there a better way to do this?

Log databases: Elasticsearch

The "gold standard" for searchable logs

Logs are thoroughly indexed and searchable

Works especially well for structured (JSON) logs

Many data collectors available ("beats")

Dashboard (Kibana)

Downsides of Elasticsearch: it's hungry

uses Java

requires SSDs for speed

indexes consume approx 10x original log space

alerting non-free *(but see elastalert, opensearch)*

Log databases: Loki

Relatively new but exciting

Efficient storage - can be backed by S3 for scale

Partial indexing: fast search by "labels", brute-force search for other queries

Dashboard (Grafana)

Streaming API

Written in Go (compact, fast binaries)

Automated log watching

"Alert me when something bad happens"

Tenshi, Swatch (old)

mtail, grok_exporter, promtail (match patterns and increment counters)

"Host Intrusion Detection Systems"

- OSSEC/Wazuh
- Sagan

All these need rules tuning to your environment

References & links

SyslogNG

    http://www.balabit.com/network-security/syslog-ng/

Rsyslog

    http://www.rsyslog.com/

Windows Log to Syslog

    http://code.google.com/p/eventlog-to-syslog/

    https://nxlog.co/products/nxlog-community-edition

SWATCH log watcher

    http://sourceforge.net/projects/swatch/

Other software

    http://www.crypt.gen.nz/logsurfer

    http://simple-evcorr.github.io/

Questions?

?