Log management

Network Management Workshop

February 18-22, 2009
Manila, Philippines

Log management and monitoring

- What is log management and monitoring ?
- It's about keeping your logs in a safe place, putting them where you can easily inspect them with tools
- Keep an eye on your log files
- They tell you something important...
  - Lots of things happen, and someone needs to keep an eye on them...
  - Not really practictal to do it by hand!

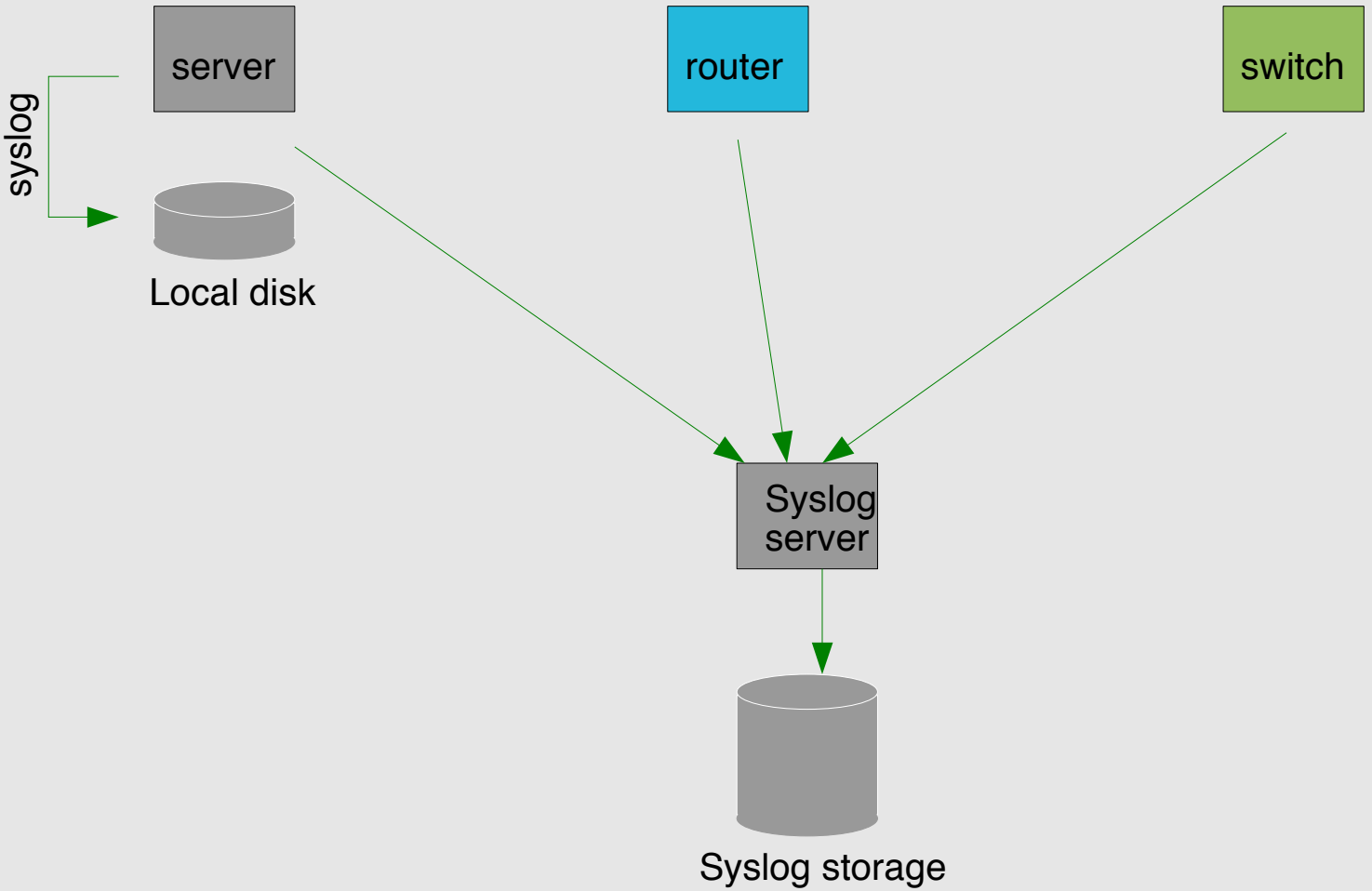
Log management and monitoring

- 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
- On your servers as well
  - Aug 31 17:53:12 ubuntu nagios2: 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

- First, need to centralize and consolidate log files
- Log all messages from routers, switches and servers to a single machine – a logserver
- All logging from network equipment and UNIX servers is done using syslog
- Windows can be configured to use syslog as well, with some tools
- Log locally, but also to the central server

Centralized logging



Configuring centralized logging

- Cisco equipment
  - Minimum:
    - logging ip.of.log.host
- UNIX host
  - Edit /etc/syslog.conf
  - Add a line "*.* @ip.of.log.host"
  - Restart syslogd
- Other equipments have similar options
  - Options to control facility and level

Receiving the messages

- Identify the facility that the SENDING host or device will send their message on
- Reconfigure syslogd to listen to the network (on Ubuntu/Debian: add "-r" to /etc/defaults/syslogd
- Add an entry to syslogd indicating where to write messages:
  - **local7.* /var/log/routers**
- Create the file:
  - **touch /var/log/routers**
- Restart syslogd
  - **/etc/init.d/sysklogd restart**

Syslog basics

- UDP protocol, port 514
- Syslog messages contain:
  - Facility: Auth, Authpriv, Console, Cron, Daemon, Ftp, Kern, Lpr, Mail, News, Ntp, Security, Syslog, User, UUCP, Local0 ...Local7
  - Level: Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Info (6), Debug (7)

Sorting logs

- Using facility and level, sort by category into different files
- With tools like syslog-ng, sort by host, date, ... automatically into different directories
- Grep your way through the logs.
- Use standard UNIX tools to sort, and eliminate, things you want to filter out:
  - `egrep -v '(list 100 denied|logging rate-limited)' mylogfile`
  - Is there a way to do this automatically ?

SWATCH

- Simple Log Watcher
  - Written in Perl
  - Monitors log files, looking for patterns (”regular expressions”) to match in the logs
  - Perform a given action if the pattern is found

Sample config

```
ignore /things to ignore/

watchfor /NATIVE_VLAN_MISMATCH/
        mail=root,subject=VLAN problem
        threshold type=limit,count=1,seconds=3600

watchfor /CONFIG_I/
        mail=root,subject=Router config
        threshold type=limit,count=1,seconds=3600
```

References

- http://www.loganalysis.org/
- Syslog NG
  - http://www.balabit.com/network-security/syslog-ng/
- Windows Event Log to Syslog:
  - https://engineering.purdue.edu/ECN/Resources/Documents/UNIX/evtsys
- SWATCH log watcher
  - http://swatch.sourceforge.net/
  - http://www.loganalysis.org/sections/signatures/log-swatch-skendrick.txt
  - http://www.loganalysis.org/
  - http://sourceforge.net/docman/display_doc.php?docid=5332&group_id=25401

References

- http://www.crypt.gen.nz/logsurfer/
- http://sial.org/howto/logging/swatch/

Questions ?