Log management

AfChix 2011
Blantyre, Malawi

AfNOG

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 practical 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
    deni
    ed tcp 79.210.84.154(2167) -> 169.223.192.85(6662), 1 packet
    ```

  -
    ```
    Sep 1 04:42:35.270 INDIA: %SYS-5-
    CO
    NFIG_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

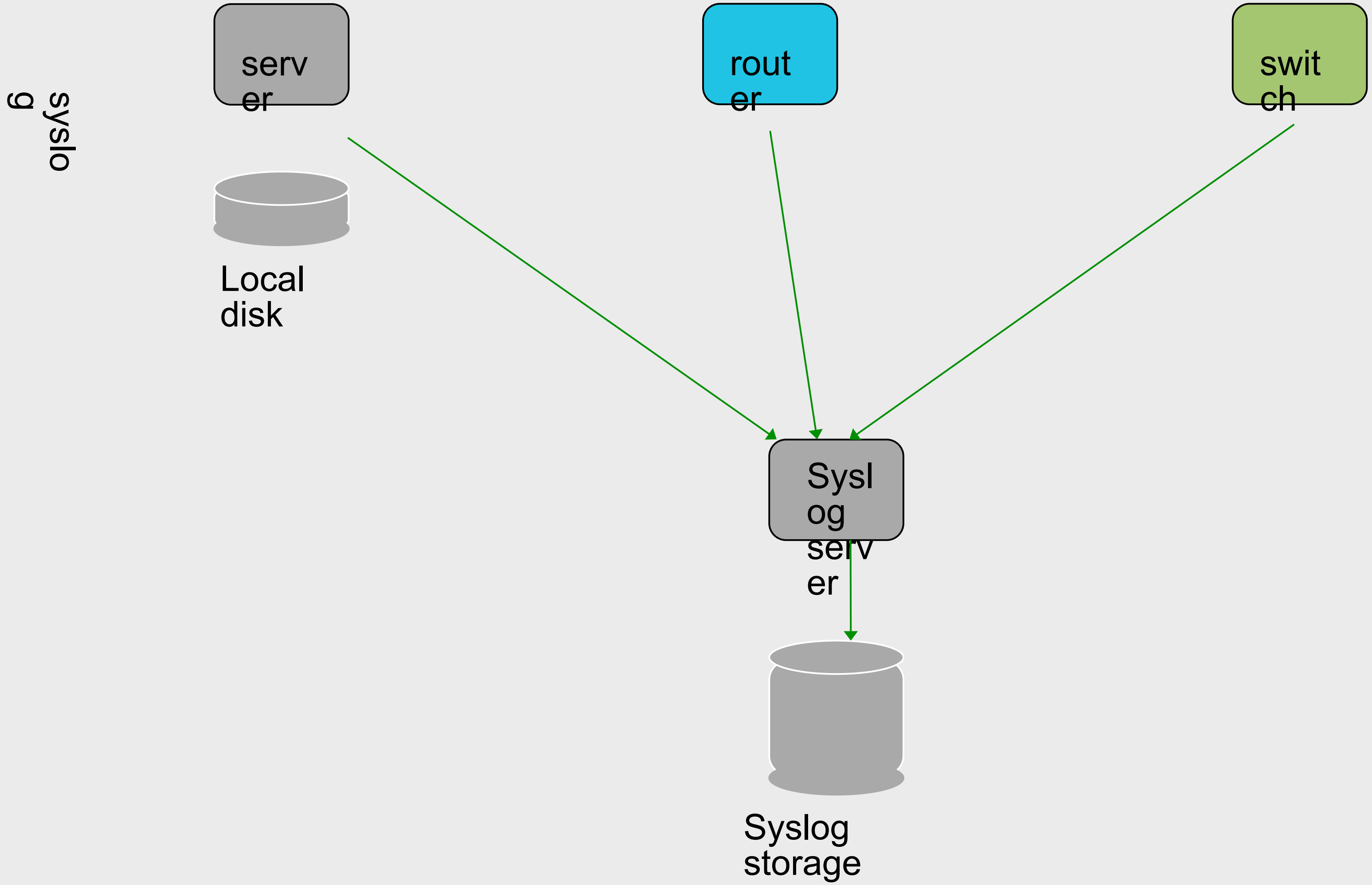
  -
    ```
    Au
    g
    31 17:53:12 ubuntu nagios2: Caught SIGTERM, shutting down...
    ```

  -
    ```
    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 log server
- 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 syslog.conf
  - Add “ip.of.log.host”
  - Restart syslogd

- Other equipments have similar options
  - Options to control facility and level

AfNOG

Receiving the messages

- Identify the facility that the SENDING host or device will send their message on - logger
- Reconfigure syslogd to listen to the network
- Add an entry to syslogd indicating where to write messages:
  - `local7.*                    /var/log/routers`
- Create the file or directory:
  - `touch /var/log/routers`
- Restart syslogd
  - `/etc/rc.d/syslogd restart`

Syslog basics

- UDP protocol, port **514**
- Syslog messages contain:
  - Facility: Auth Level: Emergency (0)

    Authpriv | Alert

    (1)

    Console |

    Critical (2)

    Cron |

    Error (3)

    Daemon |

    Warning (4)

    Ftp |

    Notice (5)

    Kern |

    Info (6)

    Lpr Mail |

    Debug (7)

    News Ntp |

    Security Syslog

    User UUCP

    Local0 ...Local7

Best Practices

* Forward syslog messages from clients to a secure syslog server.

* Enable NTP clock synchronization on all clients and on the syslog server so that logs are all synchronized. Without doing this, it can be difficult or impossible to accurately determine the sequence of events across systems or applications.

* Group “like sources” into the same log file. (i.e. mail server, MTA, spamassassin and A/V scanner all report to one file)

* Use an automated tool to establish a baseline of your logs and escalate exceptions as appropriate.

Best Practices

- Review your records retention policy, if applicable, and determine if anything kept in logs falls under that policy. If so, establish retention periods based on the records policy. Legal requirements for keeping logs vary by jurisdiction and application.

- The “sweet spot” for log retention appears to be one year. Shorter than 1 year, and it is likely that key data would be unavailable in the wake of a long running attack, and longer than one year is most likely wasting disk space.

- Include logs and log archives in a standard backup process for disaster recovery.

- Change read/write permissions on logs files so they are not accessible to unprivileged user accounts.

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
  - Other tools exist, like ”Swatch” to make this automatic

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

```
watchfor /%LINK-3-UPDOWN/
 mail addresses=inst,subject=Link updown throttle 1:00
watchfor /%SEC-6-IPACCESSLOGP/
 exec /usr/bin/echo $* >> /tmp/accesslist.log
watchfor /%SYS-5-CONFIG/
 mail addresses=inst,subject=Configuration of router
```

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

Questions ?

?