Network Monitoring, Management and Automation

Log Management

INNOG 6

Dec 8 - 12, 2019

Log Management & Monitoring

- Keep your logs in a secure place
- Where they can be easily inspected
- Watch your log file
- They contain important information
  - Many things happen
  - Someone needs to review them
  - It’s not practical to do this manually

Log Management & Monitoring (Contd.)

- On your routers and switches

```
Nov 24 18:49:32 100.68.1.1 %SYS-5-CONFIG_I: Configured from console by lab
 on vty0 (100.68.1.21)
Nov 24 18:53:59 100.68.1.1 %SSH-5-SSH2_SESSION: SSH2 Session request from
 100.68.100.250 (tty = 1) using crypto cipher '', hmac '' Failed
Nov 24 19:01:12 100.68.1.1 %SSH-5-SSH2_CLOSE: SSH2 Session from 100.68.1.21
 (tty = 0) for user 'lab' using crypto cipher 'aes128-cbc', hmac 'hmac-sha1' closed
```

- And, on your servers

```
Nov 30 14:04:01 vm1-g1 sshd[4345]: pam_unix(sshd:auth): authentication failure;
 logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.228  user=lab
Nov 30 14:04:03 vm1-g1 sshd[4345]: Failed password for lab from 192.168.88.228
 port 62338 ssh2
Nov 30 14:04:08 vm1-g1 sshd[4345]: message repeated 2 times: [ Failed password
 for lab from 192.168.88.228 port 62338 ssh2]
Nov 30 14:04:08 vm1-g1 sshd[4345]: Connection closed by authenticating user lab
 192.168.88.228 port 62338 [preauth]
```

Introduction: Syslog

- 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** (we use either ***syslog-ng*** or ***rsyslog*** for this workshop).
- Windows can, also, use syslog with extra tools.
- Save a copy of the logs locally, but, also, save them to a central log server.

Syslog Basics

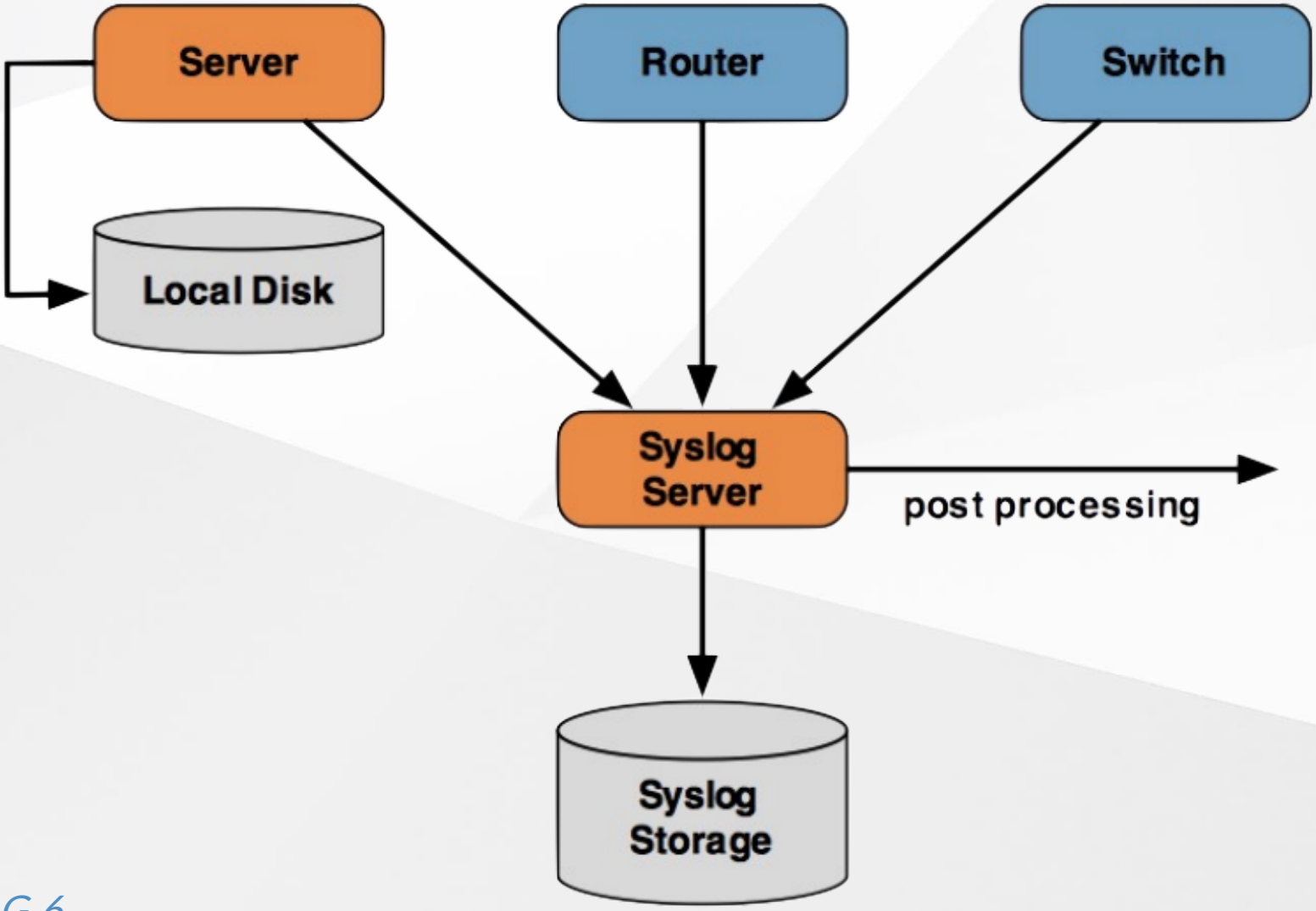
Uses UDP protocol, port 514

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

Facility	
Auth	Security
Authpriv	User
Console	Syslog
Cron	UUCP
Daemon	Mail
Ftp	Ntp
Kern	News
Lpr	Local0 ... Local7

Level	
Emergency	(0)
Alert	(1)
Critical	(2)
Error	(3)
Warning	(4)
Notice	(5)
Info	(6)
Debug	(7)

Centralized Logging



Syslog-ng

Syslog-ng Open Source Edition, is a flexible and simplified log collection and processing solution.

- It extends the original syslogd model with:
  - content-based filtering
  - rich filtering capabilities
  - flexible configuration options
  - adds important features to syslog, like using TCP for transport
- https://www.syslog-ng.com/

Syslog-ng - Receiving Messages

- Identify the facility that the equipment is going to use to send its messages.
- Reconfigure syslog-ng to listen to the network*
  - In Ubuntu update `/etc/syslog-ng/syslog-ng.conf`
- Create the following file*

  `/etc/syslog-ng/conf.d/10-network.conf`
- Create a new directory for logs:

  ```
  # mkdir -p /var/log/remote-syslog
  ```

  or

  ```
  # mkdir -p /var/log/syslog-ng
  ```
- Restart the syslog-ng service:

  ```
  # systemctl restart syslog-ng
  ```

*See logging exercises for details

Configuring Centralized Logging

- **Cisco hardware**
  - At a minimum:

    ```
    logging ip.of.logging.host
    ```
- **Unix and Linux nodes**
  - In syslogd.conf, or in rsyslog.conf, add:

    ```
    *.* @ip.of.log.host
    ```
  - Restart syslogd, rsyslog or syslog-ng
- Other equipment have similar options
  - Options to control `facility` and `level`

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 way to do this automatically?

Syslog-ng Alternative

RSYSLOG

is the **r**ocket-fast **sys**tem for **log** processing.

- It offers high-performance, great security features and a modular design.
- It is included by default in Ubuntu.
- https://www.rsyslog.com/

Tenshi

- Simple and flexible log monitoring tool https://inversepath.com/tenshi.html
- Messages are classified into queues, using regular expressions
- Each queue can be configured to send a summary e-mail within a time period
- E.G. You can tell Tenshi to send you a summary of all matching messages every 5 minutes to avoid cluttering your mailbox

Tenshi- Sample Configuration

```
set uid tenshi
set gid tenshi

set logfile /log/dhcp

set sleep 5
set limit 800
set pager_limit 2
set mailserver localhost
set subject tenshi report
set hidepid on

set queue dhcpd tenshi@localhost lab@srvX.lab.shakya.io [*/10 * * * *]

group ^dhcpd:
dhcpd ^dhcpd: .+no free leases
dhcpd ^dhcpd: .+wrong network
group_end
```

To Learn More About Syslog

- RFC 5424: Syslog Protocol
  https://tools.ietf.org/html/rfc5424
- RFC 5426: Transmission of Syslog Messages over UDP
  https://tools.ietf.org/html/rfc5426
- Transmission of syslog messages over UDP draft-ietfsyslog-transport-udp-00
  https://tools.ietf.org/html/draft-ietf-syslog-transport-udp-00
- Wikipedia Syslog Entry
  https://en.wikipedia.org/wiki/Syslog
- Cisco Press: An Overview of the Syslog Protocol
  http://www.ciscopress.com/articles/article.asp?p=426638