



# Network Management & Monitoring

## Log Management



# Log Management and Monitoring

## What is log management and monitoring?

- Keeping your logs in a secure place where they can be easily inspected.
- Watching 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 and Monitoring

## On your routers and switches

```
ep 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
```

```
ep 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
```

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

## And, your servers

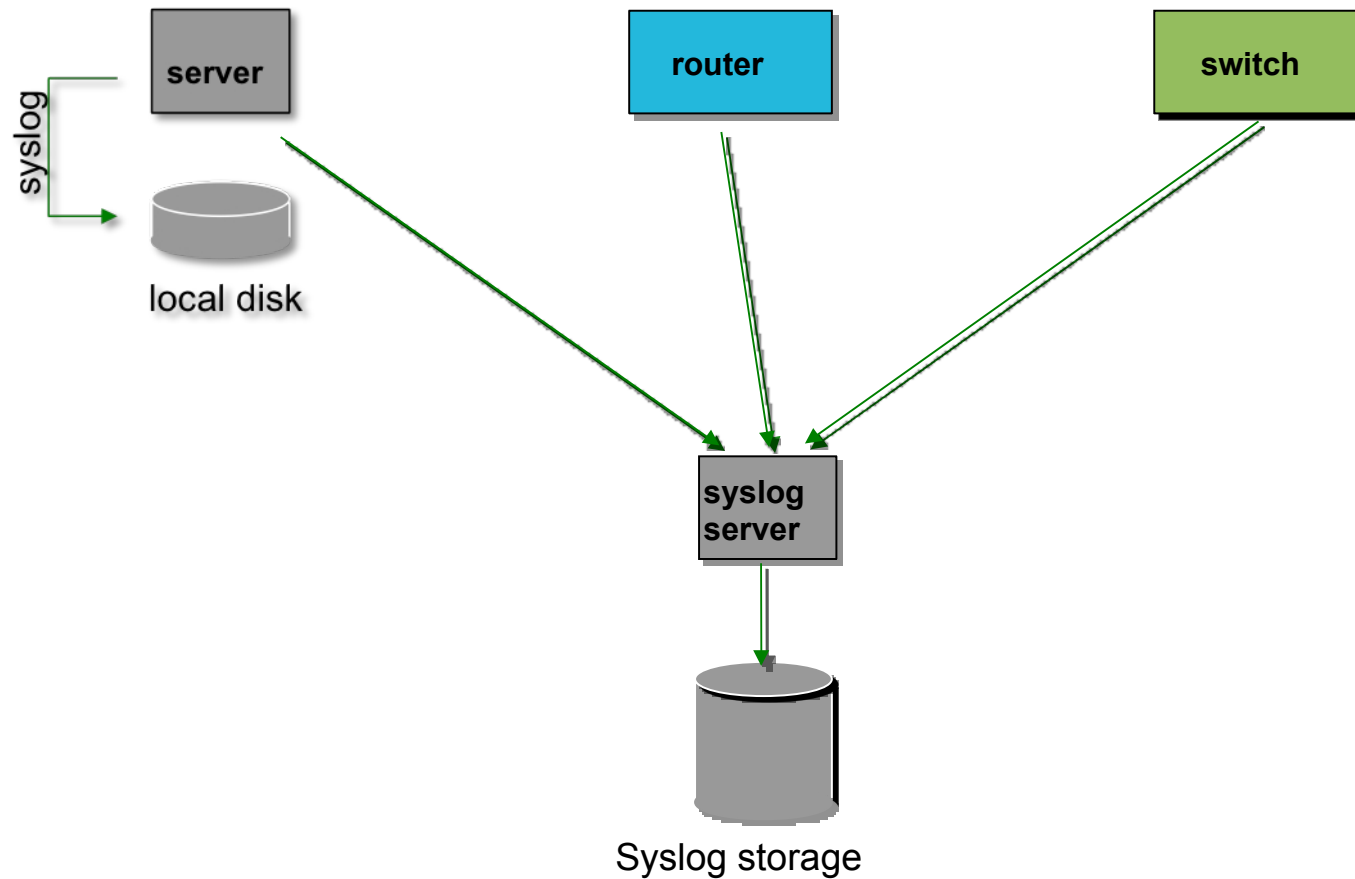
```
ug 31 17:53:12 ubuntu nagios3: Caught SIGTERM, shutting down...
```

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

# 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 logs locally, but, also, save them to a central log server.

# Centralized logging



# 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: add "-r" to `/etc/default/syslogd`
- 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*

```
/etc/init.d/syslogd restart
```

# Syslog basics

## Uses UDP protocol, port 514

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

<u>Facility</u>		<u>Level</u>	
Auth	Security		Emergency (0)
Authpriv	User		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		



# Grouping logs

- Using *facility* and *level* you can group by category in distinct files.
- With software such as *syslog-ng* 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?

# SWATCH

## Simple Log Watcher

- Written in Perl
- Monitors logs looking for patterns using regular expressions.
- Executes a specific action if a pattern is found.
- Can be any pattern and any action.
- Defining the patterns is the hard part.

# Sample configuration

```
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
```

What are these? What does it mean?

# References

<http://www.loganalysis.org/>

## Syslog NG

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

## Windows Event Log a 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](http://sourceforge.net/docman/display_doc.php?docid=5332&group_id=25401)

# References cont.

- <http://www.crypt.gen.nz/logsurfer>
- <http://sial.org/howto/logging/swatch/>
- <http://www.occam.com/sa/CentralizedLogging2009.pdf>
- <http://ristov.users.sourceforge.net/slct/>

# Questions?

