Managing logs with syslog-ng and SWATCH

AfNOG 11, Kigali/Rwanda

Google™

What is log management?

- Keeping your logs central + backed up
- Monitoring your logs regularly
- Filter your logs for important stuff
  - Important for you might be something different then for other people/the vendor
  - Most of the time, you want to keep some data for searching through, but be notified of some logs immediately

Example logs

- Cisco routers

Apr 18 03:28:57.506 UTC: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to down
Apr 18 03:29:30.876 UTC: %SEC-6-IPACCESSLOGP: list 112 denied tcp 172.16.150.2(23) -> 172.16.150.4 (11004), 1 packet
Apr 18 03:42:41.892 UTC: %FAN-3-FAN_FAILED: Fans had a rotation error reported.

- Juniper routers

Apr 18 08:36:46 kigali mib2d[152]: SNMP_TRAP_LINK_DOWN: ifIndex 79, ifAdminStatus down(2),ifOperStatus down(2), ifName fe-3/0/0
Apr 18 08:40:43 kigali mgd[4334]: UI_COMMIT: User 'jens' requested 'commit' operation (comment: test)
Apr 18 08:45:56 Modifying fan speed as high temp is now 53 C

- Unix Servers

Apr 18 09:19:44 ubuntu sudo: pam_unix(sudo:session): session opened for user root by jens(uid=0)
Apr 18 09:33:45 ubuntu nagios3: caught SIGTERM, shutting down..

Centralize logs

- Syslog server collects all logs, splits them up in files, but groups several devices in files
- All routers/switches and Unix boxes can use Syslog, Windows can with extra tools

- Uses UDP Port 514 by default, some implementations can do TCP

- Because UDP is unreliable, best to keep local logs as well - in times of failures, you might not be able to send out messages

Syslog packet format

- Syslog protocol is very simple: PRI, HEADER, MSG
- PRI: Severity and Facility
  - Severities: Emergency(0), Alert(1), Critical(2), Error(3), Warning(4), Notice(5), Info(6), Debug(7)
  - Facilities: Kern, User, Mail, Daemon, Auth, Syslog, Lpr, News, Uucp, Cron, Authpriv, Ftp, Local0-7
- HEADER: Timestamp and Hostname
- MSG: The real message
- Packet must be <1024 bytes

How to send logs

- From Cisco:
  logging 196.200.208.3
- From UNIX/Ubuntu:
  Edit /etc/syslog.conf - add:
  . @196.200.208.3
  Restart the syslog server
- Other devices are similarly easy. You can sometimes specify facility and priority levels

How to receive logs

- Login to machine which receives the syslog
- Install syslog-ng (apt-get install syslog-ng)
- Reconfigure the syslog-ng daemon to listen. Edit /etc/syslog-ng/syslog-ng.conf and uncomment the line:
  `# udp();`
  it should look like
  `udp();`
- If you use old syslogd, you need to start it with the -r command

How to receive logs (2)

- Tell the facility mapping to files. Syslog-ng uses filters and destinations. Edit /etc/syslog-ng/syslog-ng.conf

```
filter f_routers { facility(local5); };
destination df_routers { file("/var/log/routers.log"); };
log {
        source(s_all);
        filter(f_routers);
        destination(df_routers);
}
```

- In old syslogd configuration file this is simpler:

```
local5.*                /var/log/routers.log
```

- Restart syslog-ng

Reading / sorting logs

- You can add more complicated rules to add one logfile per router/day or similar. You can split up by facilities

- Many people use standard UNIX tools, like grep and sed to filter out log messages they might like or not like and then watch the files (with tail -f). Something like:
  tail -f mylogfile | egrep -v "(list 337 denied|rate-limited)"
- This can get very complicated very quickly - solution?

Use a tool

- SWATCH (Simple log Watcher) does this for you. Monitors incoming logs, searches for specific expressions
- Written in perl
- Takes action if pattern is found.
- Sample config:
- ignore /my-test-router/
-
- watchfor /FAN_FAILED/
  mail=root,subject=Fan error again
  threshold type=limit,count=1,seconds=3600

References

- Syslog-NG: http://www.balabit.com/network-security/syslog-ng/
- SWATCH: http://swatch.sourceforge.net
  Sample configs: http://www.campin.net/newlogcheck.html
- General sites: http://www.loganalysis.org