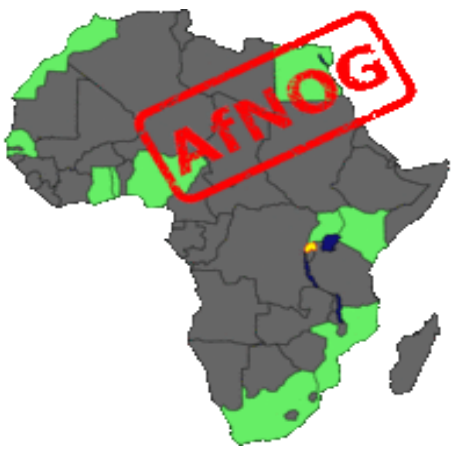
Network Monitoring and Management Conclusions

AfNOG 11, Kigali/Rwanda



Google™

What did we learn?

- We learned some of the advantages of having a well-managed network
- We learned the features of some Open Source Network Management tools
  - Nagios for monitoring network elements and servers
  - RANCID for the backup of configs
  - Cacti for graphing traffic and other statistics
  - SWATCH/Syslog-NG for managing logs
  - Smokeping for measuring latency in your network
- We tried them all in practice and make a simple working setup

What did we not cover

- So much more...

- All this software has many more features and is extensible
  - Read docs, forums, examples
  - Read the source code if you can
  - Ask questions, try it out
- There's commercial alternatives, and alternatives by hardware vendors
  - Compare the features, ask for a test version
  - Only because it costs money, it's not necessarily better/easier to manage (but maybe it is)
  - It all depends on YOUR needs
  - Support is also available for open-source tools

What did we not cover(2)

- There's more network management/monitoring than the tools we covered, you can try the following tools (in no particular order)

- Managing tickets/NOC queues (covered through exercises): **RT (Request Tracker)** is a powerful ticketing tool
- Analyze traffic by type, source destination: Learn about **Netflow** and tools like **NFS**en

More tools we did not cover

- Visualize network designs with tools like **Dia** or **Microsoft Visio** or discover it automatically with **Network Weathermap**
- Manage/secure who has router access with RADIUS or TACACS servers like Shrubbery's **TACACS+** daemon or **Freeradius**
- Sniff and analyze Network traffic using **Wireshark**
- Install intrusion detection systems like **SNORT**
- Use a portscanner like **nmap** to find open ports or a scanner like **Nessus** to find potential vulnerabilities in your network

We're still not done

- Use a Wiki or Content Management system for your documentation like **trac** or **TWiki**
- Use **Netdot** and **Netdisco** to manage your addressing equipment
- Manage code for your tools or other data which changes using a versioning system like **CVS** or **Subversion** (we mentioned it in RANCID)

Some more.....

Performance

- Cricket
- IFPFM
- flowc
- mrtg
- netflow
- NfSen
- ntop
- pmacct
- rrdtool
- SmokePing

SNMP/Perl/ping

Change Mgmt

- Mercurial
- Rancid (routers)
- RCS
- Subversion

Security/NIDS

- Nessus
- OSSEC
- Prelude
- Samhain
- SNORT
- Untangle

Net Management

- Big Brother
- Big Sister
- Cacti
- Hyperic
- Munin
- Nagios*
- Netdisco
- Netdot
- OpenNMS
-
-

What were the main goals of this class

- Depends on you and your users.
- Increase uptime/reliability
- Find errors/faults which increase latency or packet loss
- Decrease amount of manpower needed to manage the network - save you some time
- Easier documentation

- **Most important is that you can take the knowledge home and try the tools which are best for you in your network.**

Thank you for your time

- We hope the last two days have been helpful, and gave you some inspiration
- We hope you learned something
- If you did, give us feedback - if you didn't please tell us too.

- If you have questions or feedback later, please contact us by email!

References

- RT: http://bestpractical.com/rt/
- NSFen: http://nfsen.sourceforge.net/
- Smokeping: http://oss.oetiker.ch/smokeping/
- Dia: http://projects.gnome.org/dia/
- Network Weathermap: http://www.network-weathermap.com/
- TACACS+ daemon: http://www.shrubbery.net/tac_plus/
- Freeradius: http://freeradius.org/
- Wireshark: http://www.wireshark.org/
- Snort: http://www.snort.org/
- nmap: http://nmap.org/
- Nessus: http://www.nessus.org/nessus/
- trac: http://trac.edgewall.org/
- TWiki: http://twiki.org/
- Netdot: https://netdot.uoregon.edu/trac/
- Netdisco: http://netdisco.org
- CVS: http://www.nongnu.org/cvs/ http://ximbiot.com/cvs/cvshome/
- Subversion: http://subversion.apache.org/