Nagios SS-E

Slide adapted from 2013 Slides from Ayiteh.

Introduction

- To monitor or monitoring generally means to be aware of the state of a system.
- To observe a situation for any changes which may occur over time, using a monitor or measuring device of some sort.
- The term network monitoring describes the use of a system that constantly monitors a computer network for faults and notifies the network administrator (via email, SMS or other alarms) in case of outages. It is a subset of the functions involved in network management.

What can you monitor?

- Environmental Monitoring
  - Temperature, humidity
- Network Monitoring
  - Device uptime
  - Internet Bandwidth consumption
- System Monitoring
  - Resource usage eg RAM and CPU
- Website Monitoring
  - Number of hits to certain pages

Why do we monitor?

- Deliver on targets (KPIs/SLAs)
  - Is your ISP providing the service as agreed?
  - As an ISP, are you providing your customers what you promised?
- Early detection and fault resolution (MTTR)
  - Packet loss or flapping signifies a problem somewhere
- Are the investments on equipment delivering?
  - Are your devices underutilized?

Some Monitoring Tools

- Nagios
  - Availability of services, servers and network devices.
- Cacti
  - Utilization of resources such as bandwidth, CPU, memory, disk space etc.
- Smokeping
  - Network latency, RTT
- Others: Observium, OpenNMS, Zabbix, Zenoss
- Others:
- For monitoring IP services, we will focus on monitoring availability (Nagios) and reliability (Smokeping)

Perspective on Availability?

Availability %	Downtime per Year	Downtime per Month	Downtime per Week
90% ("one nine")	36.5 days	72 hours	16.8 hours
98%	7.30 days	14.4 hours	3.36 hours
99% ("two nines")	3.65 days	7.20 hours	1.68 hours
99.9% ("three nines")	8.76 hours	43.8 minutes	10.1 minutes
99.99% ("four nines")	52.56 minutes	4.32 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds

Nagios

- Nagios actively monitors the availability of devices and services
- Possibly the most used open source network monitoring software.
- Sends alerts and/or triggers alerts
- Logs history and generates SLA reports
- Can support thousands of devices and services.
- Several plugins available to extend its abilities eg to allow it to monitor CPU or Fan temperature on a router

Dependencies

- Dependencies:
  - Apache & PHP. MySQL depending on what you enable
- Install nagios from ports:

  $sudo pkg install nagios
- Key directories:
  - /usr/local/etc/nagios
  - /usr/local/etc/nagios/objects
  - /usr/local/libexec/nagios
  - /usr/local/www/nagios
- Nagios web interface sample is here:
  - http://pc1.sse.ws.afnog.org/nagios

Nagios Architecture

- Plugins are used to verify the state of devices & services.
- Small, self-contained applications which make a single connection to test a service then quit
- Return OK, Warning, Critical or Unknown
- Many plugins supplied, even more available
  - http://exchange.nagios.org
  - http://nagiosplugins.org
- Data storage: plain text files
- Data visualisation: CGI web interface
- Configuration: plain text files but there are some web based tools for managing it like Nconf, Webmin, Fruity

Configuration Files

- Located in /usr/local/etc/nagios:
- cgi.cfg
  - Controls the web interface and security options
- nagios.cfg
  - Main configuration file
- resource.cfg
  - Used to specify an optional resource file that can contain $USERn$ macro definitions.
- objects/
  - All other configuration files go here.

Config Files

- The /usr/local/etc/nagios/objects directory:
- commands.cfg
  - The commands that nagios uses for notifications
- contacts.cfg
  - Users and groups
- localhost.cfg
  - Definition of the nagios host
- printer.cfg, switch.cfg
  - Definition of printers and switches
- templates.cfg
  - Sample object templates
- timeperiods.cfg
  - Defines when to check the state of objects

Nagios Features

- Allows you to acknowledge an event
  - i.e I am aware of the problem so stop alerting
- A user can add comments via the GUI
  - Useful in a NOC where it will be possible to tell who is working on a problem
- You can define maintenance periods
  - i.e. do not monitor the device at this time
- By device or a group of devices
  - i.e. these devices are similar so group them together on the map
- Maintains availability statistics
- Can detect flapping and suppress additional notifications
- Allows for multiple notification methods:
  - e-mail, pager, SMS, win-popup, audio, etc...
- Allows you to define notification levels for escalation

Nagios Exercise

- Lets install Nagios!