Network Monitoring Proposal

Network Monitoring Proposal

General information

We are looking for a Network Monitoring solution to replace our current one, Xymon, with a more robust solution. We will test various solutions until we find one that fits the requirements we outline below.

Meeting Time

- 5:45PM Friday

Faculty

- Chris Allison (cba at ccs)

Students

- **Leader: Thang Nguyen (thang@ccs.neu.edu)**
- Dan calacci (dcalacci@ccs.neu.edu)
- Pasha Sadikov (sigmat@ccs.neu.edu)
- Nick Tinsley (ntinsley@ccs.neu.edu)
- Chris Kohler (ckohler@ccs.neu.edu)
  ### Email List
- Put the email of the group here.
  ...

Freelance Technical Consultant

- Chris McCoy (cmccoy@ccs.neu.edu)

Requirements

Whichever monitoring system(s) we select must (at minimum) be able to:

- Monitor
    - network services (eg: ping, ssh, RDP, http, smtp, imap, etc)
    - host state (eg: CPU/RAM/Disk usage, processes, uptime, etc) on Linux & Windows
    - network devices (eg: SNMP or similar)
    - NetApp(s) (SNMP or ssh)
    - arbitrary conditions on hosts (ie: Custom monitoring of processes/filesystem/etc)
    - arbitrary services (eg: mail round trip time, interactive ssh responsiveness, etc)
    - SSL certs
- Send alerts via at least some of:
    - Email
    - SMS
    - SIP?
- Provide:
    - Graphing & time series data for monitored hosts and services (eg: uptime, response time, resource usage, etc graphs)
- Be:
    - Configurable from external sources (eg: configs can be autogenerated from hostbase, Puppet, etc)

Rationale

The new solution will provide attractive features, including external configurability capable of being automated, useful graphical statistics (uptime, resource usage, etc), among several other requirements highlighted above that are not currently available with our existing Network Monitor.

Goals

By the end of the semester, we hope to find a suitable replacement solution for Xymon, or at the very least narrow down the potential solutions. Additionally, we hope to test out various solutions in hopes of determining the best fit. Ideally we will have a candidate successor for Xymon by the end of the semester configured to Chris A's standards; along with documentation to set it up in the exact same manner. We will have several shorter term goals that will be outlined below, ultimately contributing to this.

Timeline / Deliverables

- 10/21/2011 - Research & narrow down the best contenders. We will rank them, and hold a ~~caucus~~ group vote to determine the best 2, and install them onto machines to begin monitoring various services on the network.
- 10/28/2011 - We will have installed and configured the tools to fill the requirements we outlined. If a tool does not have the functionality we desire, we will replace it in favor of a lower ranked tool that will hopefully fill the niche.
- 11/15/2011 - We will have a demo that will showcase a live demonstration of alert systems for when a service goes offline, along with the various other requirements.
- 12/15/2011 - Wrapping up.

Resources

We will require two blank machines to install the tools we will be testing out, and later on an HTTP server we can turn on/off at our own will.

Notes

There are those who argue (persuasively, in Chris A's view) that monitoring for the purpose of alerting about problems (eg: "wake someone up so they fix it") and monitoring for the purposes of graphing trends over time (eg: track resource consumption, plan new purchases/deployments/etc) are two fundamentally different jobs, and are best served by different systems. It would obviously be easier to only deploy one system that does both tasks, but if the choice is between one system that does two tasks poorly or two systems that each do one task well, we should keep this in mind.

Potential Contenders:

Note: These are options to consider. You should not limit yourself to just these systems, nor should you assume that all of these systems are good options.

- Nagios:
    - Nagios Core (F/OSS)
    - Commercial versions (Nagios XI, Nagios Fusion)
    - Nagios spin-offs, eg Icinga
- Graphite (rrd style graphing used with statsd)
- Zenoss or Zenoss Core
- OpenNMS
- Zabbix
- SolarWinds Orion
- Hyperic
- GroundWork
- Flapjack
- Ganglia