Network Monitoring Systems

2/19/08
Michael Miller
e-mail: mike.mikemiller@gmail.com
Network Monitoring System

- What is a Network Monitoring System (NMS)?
- What types of devices can you monitor?
- How will a NMS help me in my job daily?
What is a NMS?

Network Monitoring Systems: Allow administrators and support staff to monitor the status of nodes in their network.
What type of devices can you monitor?

- IP Routers
- IP Switches
- Computers
- PBX Systems (Asterisk)
- Class 5 phone switches
How will a NMS Help me in my daily operation

Any NMS should show you the following things at a minimum.

- Health of your network Up / Down status
- Event logging times systems where unavailable
- Alerting of events to via E-mail / Telephone Paging / SMS text messages / Phone call
- Have the ability to customize the NMS product
NMS Systems

- HP OpenView NNM/ITO
- Nagios
- The Dude
- OpenNMS
- Big Brother
Nagios

Where do I get it? http://nagios.org
Nagios

Where do I see examples?

http://www.nagiosexchange.org
Nagios 2.X Install

You can install Nagios several different ways

- Source
- Distribution Package Manager RPM, Ports, APT

**TIP:**
Nagios uses the following dependences
Web Server: Apache (Preferred) lighttpd (lighty should work)

GD Library for Status Maps and Trending
Nagios 2.X Install

Note you need to configure Unix users and groups for Nagios. Nagios should not run as root

groupadd nagios – Nagios Group
groupadd ncmd – Nagios Command Group
useradd -g nagios -M nagios – Add Nagios user to Nagios group no homdir
usermod -G ncmd nagios – Add ncmd to nagios group
usermod -G ncmd apache – Add ncmd to apache group
Nagios 2.X Install

Install from source

./configure --prefix=/usr/local/nagios --with-htmlurl=/nagios/ --with-cgiurl=/nagios/cgi-bin
--with-nagios-user=nagios --with-nagios-group=nagios
--with-command-group-ncmd
make install
make install-init
make install-commandmode
make install-config
Nagios 2.X Install

Additonal Nagios config options

Option
--with-command-user=user
--with-gd-lib=/path/to/gd/lib
--with-gd-inc=/path/to/gd/includes
--enable-event-broker
--enable-embedded-perl
--with-perlcache
--with-mail=/mail/to/mail
--with-init-dir=/path/to/init
--with-lockfile=/path/to/lockfile
Nagios Plugins Install

How-to Install Plugins

./configure –prefix=/usr/local/nagios –with-naigos-user=nagios –with-naigos-group=nagios –with-cgiurl=/nagios/cgi-bin
Nagios Plugins Install

Additional Nagios Plug-in config options

--with-openssl=/path/to/openssl
--without-openssl
--with-ping-command=/path/to/ping command
--with-ping6-command=/path/to/ping6 command
Nagios Apache Config

Some things to think about!
Nagios displays information you may not want other people to have access to. If your Nagios server is on the Internet configure a HTTPS server for Nagios.

Things you don't want others to see:
- Internal IP Addressing (I.E. RFC-1918 Numbering)
- Which machines host which services DNS, HTTP and etc..
- Where your network devices are Printers, Routers, Firewalls and etc..
ScriptAlias /nagios/cgi-bin /usr/lcoal/nagios/sbin

<Directory "/usr/lcoal/nagios/sbin”>
    AllowOverride None
    Options ExecCGI
    Order allow,deny
    Allow from all
    AuthType Basic
    AuthName “Nagios Access”
    AuthUserFile /path/to/htpasswd
    require valid-user
</Directory>
Nagios Apache Config

Alias /nagios /usr/local/nagios/share
<Directory “/usr/local/nagios/share”>
  Options None
  AllowOverride None
  Order allow,deny
  Allow from all
  AuthType Basic
  AuthName “Nagios Access”
  AuthUserFile /path/to/htpasswd
  Require valid-user
</Directory>
Nagios Apache Config

If you are in a company using a class C network internally. You may want to restrict Nagios to a list of IP addresses or subnets. You can use the Allow from Apache directive to restrict access to the Nagios URLs.

Allow from 192.168.1.10 10.50.1.2

Allow from 192.168.1.0/24 10.50.1.0/24
## Nagios 2.X files

<table>
<thead>
<tr>
<th>File name</th>
<th>Description of what the file does.</th>
</tr>
</thead>
<tbody>
<tr>
<td>host.cfg</td>
<td>Hosts are physical devices servers, routers and firewalls.</td>
</tr>
<tr>
<td>hostgroups.cfg</td>
<td>Host groups are collections of hosts.</td>
</tr>
<tr>
<td>services.cfg</td>
<td>Services run on hosts I.E. HTTP or HTTPS or SMTP or SSH.</td>
</tr>
<tr>
<td>servicegroups.cfg</td>
<td>Service groups are collections of services.</td>
</tr>
<tr>
<td>contacts.cfg</td>
<td>Contact groups are collections of contacts I.E. E-mail addresses or Pager Number or Cell Phone Number.</td>
</tr>
<tr>
<td>contactgroups.cfg</td>
<td>Contact groups I.E. group people into teams or groups.</td>
</tr>
<tr>
<td>timeperiods.cfg</td>
<td>Time periods are windows of time. I.E. Business hours or Non-Business hours.</td>
</tr>
</tbody>
</table>
## Nagios 2.X files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>checkcommands.cfg</td>
<td>Commands are processes to perform actions I.E. Nagios Plugins.</td>
</tr>
<tr>
<td>escalations.cfg</td>
<td>Escalation of service notifications for a particular service.</td>
</tr>
<tr>
<td>nagios.cfg</td>
<td>Main configuration file, where you list all configuration files and nagios settings.</td>
</tr>
<tr>
<td>hostdependency.cfg</td>
<td>Defines a host or hosts to be dependent on other hosts.</td>
</tr>
</tbody>
</table>
## Nagios 2.X files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostescalation.cfg</td>
<td>Define escalation process for hosts.</td>
</tr>
<tr>
<td>hostextinfo.cfg</td>
<td>Host extended information allows you to define some documentation and other notes for hosts.</td>
</tr>
<tr>
<td>serviceextinfo.cfg</td>
<td>Service extended information allows you to define some documentation and other notes for services.</td>
</tr>
</tbody>
</table>
Nagios 2.X config files

Example of how Nagios configuration file syntax (Looks kind of like Bind)
This syntax is not used in the naigos.cfg file.

define object_type{
    directive1 setting
    directive2 setting
    directive3 setting
    directive4 setting
    directive5 setting
}

Nagios 2.X config files

hosts.cfg
define host{
    host_name f00.yourdomain.com
    alias bar
    address 10.129.10.1
    check_period 24x7
    max_check_attempts 1
    contact_groups network_team
    notification_interval 30
    notification_period 24x7
    notification_options d,u,r
}


New Installations:

If you have just installed Nagios, read the documentation for instructions on getting everything up and running.

Click here for a brief overview of new features that have been added in this release.

More Information:

Visit the Nagios homepage at http://www.nagios.org for information on bug fixes, upgrades, support, etc.
Nagios Books

Title: Pro Nagios 2.0 (Expert's Voice in Open Source)
Hardcover: 424 pages
Publisher: Apress; 1 edition (April 17, 2006)
ISBN-10: 1590596099

Title: Nagios: System and Network Monitoring [ILLUSTRATED]
Paperback: 464 pages
ISBN-10: 1593270704