Network Management & Monitoring
Introduction

Network Monitoring Tools

- Availability
- Reliability
- Performance

Nagios actively monitors the availability of devices and services
Introduction

- Possibly the most used open source network monitoring software.
- Has a web interface.
  - Uses CGIs written in C for faster response and scalability.
- Can support up to thousands of devices and services.
Installation

In Debian/Ubuntu

    # apt-get install nagios3

Key directories

/etc/nagios3
/etc/nagios3/conf.d
/etc/nagios-plugins/conf
/usr/lib/nagios/plugins
/usr/share/nagios3/htdocs/images/logos

Nagios web interface is here:

http://pcN.ws.nsrec.org/nagios3/
Plugins

Plugins are used to verify services and devices:

- Nagios architecture is simple enough that writing new plugins is fairly easy in the language of your choice.
- There are many, many plugins available (thousands).
   ✓ http://exchange.nagios.org/
   ✓ http://nagiosplugins.org/
Features

- Configuration done in text files, based on templates.
- Nagios reads its configuration from a directory. You determine how to divide your configuration files.
- Uses parallel checking and forking for scalability.
Features cont.

- Utilizes topology to determine dependencies.
  - Differentiates between what is down vs. what is unreachable. Avoids running unnecessary checks and sending redundant alarms.

- Allows you to define how to send notifications based on combinations of:
  - Contacts and lists of contacts
  - Devices and groups of devices
  - Services and groups of services
  - Defined hours by persons or groups
  - The state of a service.
Notification Options (Host)

Host state:
When configuring a host you have the following notification options:

- d: DOWN
- u: UNREACHABLE
- r: RECOVERY
- f: FLAPPING
- n: NONE
NOTE: The flow will only continue when each of the listed filters are satisfied.
How checks work

- A node/host/device consists of one or more service checks (PING, HTTP, MYSQL, SSH, etc.)
- Periodically Nagios checks each service for each node and determines if state has changed. State changes are:
  - CRITICAL
  - WARNING
  - UNKNOWN
- For each state change you can assign:
  - Notification options (as mentioned before)
  - Event handlers
How checks work continued

Parameters

- Normal checking interval
- Re-check interval
- Maximum number of checks.
- Period for each check

- Node checks only happen when services respond.
  - A node can be:
    - DOWN
    - UNREACHABLE
By default Nagios does a node check 3 times before it will change the node’s state to down.

No response states goes to warning then critical
The concept of “parents”

Nodes can have parents:

• The parent of a **PC** connected to a **switch** would be the **switch**.

• Allows us to specify the dependencies between devices.

• Avoids sending alarms when parent does not respond.

• A node can have multiple parents (dual homed).
Network viewpoint

- Where you locate your Nagios server will determine your point of view of the network.
- The Nagios server becomes the “root” of your dependency tree
Network viewpoint
Demo Nagios
Configuration Files

- Lots!
- Can seem complex at first
- **Object oriented**
  - Objects (devices or services) inherit attributes.
  - Apply functionality to *groups of devices*.
  - Do not apply functionality to individual objects. Does not scale!
  - Once you understand Nagios configs the rest is easy…
Configuration files (Official)
Configuration Files

Located in /etc/nagios3/

Important files include:

- **cgi.cfg** Controls the web interface and security options.
- **commands.cfg** The commands that Nagios uses for notifications.
- **nagios.cfg** Main configuration file.
- **conf.d/*** All other configuration goes here!
Configuration files continued

Under conf.d/*

- contacts_nagios2.cfg  users and groups
- extinfo_nagios2.cfg   make your UI pretty
- generic-host_nagios2.cfg  default host template
- generic-service_nagios2.cfg  default service template
- host-gateway_nagios3.cfg definition
- hostgroups_nagios2.cfg  groups of nodes
- localhost_nagios2.cfg  definition of nagios host
- services_nagios2.cfg  what services to check
- timeperiods_nagios2.cfg  when to check who to notify
Configuration files continued

Under conf.d some other possible config files:

- servicegroups.cfg  Groups of nodes and services
- pcs.cfg  Sample definition of PCs (hosts)
- switches.cfg  Definitions of switches (hosts)
- routers.cfg  Definitions of routers (hosts)
Pre-installed plugins in Ubuntu

/usr/lib/nagios/plugins

check_apt  check_file_age  check_jabber  check_nntp  check_procs  check_swap
check_bgpstate  check_flexlm  check_ldap  check_nttps  check_radius  check_tcp
check_breeze  check_ftp  check_lhaps  check_nt  check_real  check_time
check_by_ssh  check_host  check_linux_raid  check_load  check_rpc  check_udp
check_cluster  check_http  check_log  check_mailq  check_rts MULTI  check_users
check_dhcp  check_icalp  check_ntp_peer  check_ntp_time  check_sensors  check_wave
check_dig  check_ide_smart  check_ntp  check_rts_pee  check_simap  check_who
check_disk  check_ifoperstatus  check_ntp_peer  check_rts_time  check_smalp  check_urlize
check_disk_smb  check_ifstatus  check_mysql  check_oracle  check_overcr  check_utils.pm
check_dns  check_imap  check_mrtg  check_overcr  check_psql  check_utils.sh
check_dummy  check_ircd  check_mysql_query  check_ping  check_pop  check_ssnmp
check_nagios  check_swap

/etc/nagios-plugins/config

apt.cfg  disk-smb.cfg  ftp.cfg  ldap.cfg  mysql.cfg  ntp.cfg  radius.cfg  ssh.cfg
breeze.cfg  dns.cfg  hppjd.cfg  load.cfg  netware.cfg  psql.cfg  real.cfg  tcp_udp.cfg
dhcp.cfg  dummy.cfg  http.cfg  mail.cfg  news.cfg  ping.cfg  rpc-nfs.cfg  telnet.cfg
disk.cfg  flexlm.cfg  ifstatus.cfg  mrtg.cfg  nt.cfg  proc.cfg  snmp.cfg  users.cfg
Nodes and services configuration

Based on templates
- This saves lots of time avoiding repetition
- Similar to Object Oriented programming

Create default templates with default parameters for a:
- *generic node*  (generic-host_nagios2.cfg)
- *generic service*  (generic-service_nagios2.cfg)
- *generic contact*  (contacts_nagios2.cfg)
Generic node template

generic-host_nagios2.cfg

```plaintext
define host{
    name generic-host ; The name of this host template
    notifications_enabled 1 ; Host notifications are enabled
    event_handler_enabled 1 ; Host event handler is enabled
    flap_detection_enabled 1 ; Flap detection is enabled
    failure_prediction_enabled 1 ; Failure prediction is enabled
    process_perf_data 1 ; Process performance data
    retain_status_information 1 ; Retain status information across program restarts
    retain_nonstatus_information 1 ; Retain non-status information across program restarts
    check_command check-host-alive
    max_check_attempts 10
    notification_interval 0
    notification_period 24x7
    notification_options d,u,r
    contact_groups admins
    register 0 ; DONT REGISTER THIS DEFINITION - ITS NOT A REAL HOST, JUST A TEMPLATE!
}
```
Individual node configuration

```plaintext
define host{
    use generic-host
    host_name gw-rtr
    alias Main workshop router
    address 192.0.2.1
    contact_groups router_group
}
```
Generic service configuration

generic-service_nagios2.cfg

define service{
    name generic-service
    active_checks_enabled 1
    passive_checks_enabled 1
    parallelize_check 1
    obsess_over_service 0
    check_freshness 1
    notifications_enabled 1
    event_handler_enabled 1
    flap_detection_enabled 1
    process_perf_data 1
    retain_status_information 1
    retain_nonstatus_information 1
    is_volatile 0
    check_period 24x7
    max_check_attempts 5
    normal_check_interval 5
    retry_check_interval 1
    notification_interval 60
    notification_period 24x7
    notification_options c,r
    register 0
}
## Individual service configuration

```plaintext
define service{
    hostgroup_name                servers
    service_description           PING
    check_command                 check-host-alive
    use                           generic-service
    max_check_attempts            5
    normal_check_interval         5
    notification_options          c,r,f
    notification_interval         0 ; set > 0 if you want to be renotified
}
```

**c**: Critical  
**r**: Recovering  
**f**: Flapping
Configuration flow

Items inherit from templates
We start with a host
- Place multiple hosts in a group
- Define parents
- Add a service check to the group
- Add extended info, if any
Another view of configuration

**RTR**
define host {
  use
  generic-host
  rtr
  host_name
  rtr
  alias
  Gateway Router
  address
  10.10.0.254
}

**SW**
define host {
  use
  generic-host
  sw
  host_name
  sw
  alias
  Backbone Switch
  address
  10.10.0.253
  parents
  rtr
}

**RTR3**
define host {
  use
  generic-host
  rtr3
  host_name
  router 3
  alias
  address
  10.10.3.254
  parents
  sw
}

**PC11...**
OoB notifications

A critical item to remember: an SMS or message system that is independent from your network.

- You can utilize a cell phone connected to the Nagios server
- You can use packages like:
  gnokii: http://www.gnokii.org/
  qpage: http://www.qpage.org/
  sendpage: http://www.sendpage.org/
References

• Nagios web site
  http://www.nagios.org/

• Nagios plugins site
  http://www.nagiosplugins.org/


• Unofficial Nagios plugin site
  http://nagios.exchange.org/

• A Debian tutorial on Nagios
  http://www.debianhelp.co.uk/nagios.htm

• Commercial Nagios support
  http://www.nagios.com/
Questions?
A few additional slides you may find useful or informative…
Features, features, features…

- Allows you to acknowledge an event.
  - A user can add comments via the GUI
- You can define maintenance periods
  - By device or a group of devices
- Maintains availability statistics.
- Can detect flapping and suppress additional notifications.
- Allows for multiple notification methods:
  - e-mail, pager, SMS, winpopup, audio, etc...
- Allows you to define notification levels for escalation
Main configuration details

Global settings

File: /etc/nagios3/nagios.cfg

• Says where other configuration files are.
• General Nagios behavior:
  - For large installations you should tune the installation via this file.
  - See: Tuning Nagios for Maximum Performance
    http://nagios.sourceforge.net/docs/2_0/tuning.html
CGI configuration

/etc/nagios3/cgi.cfg

- You can change the CGI directory if you wish
- Authentication and authorization for Nagios use:
  - Activate authentication via Apache's .htpasswd mechanism, or using RADIUS or LDAP.
  - Users can be assigned rights via the following variables:
    - authorized_for_system_information
    - authorized_for_configuration_information
    - authorized_for_system_commands
    - authorized_for_all_services
    - authorized_for_all_hosts
    - authorized_for_all_service_commands
    - authorized_for_all_host_commands
Time Periods

This defines the base periods that control checks, notifications, etc.

- Defaults: 24 x 7
- Could adjust as needed, such as work-week only.
- Could adjust a new time period for “outside of regular hours”, etc.

```plaintext
# '24x7'
define timeperiod{
    timeperiod_name 24x7
    alias 24 Hours A Day, 7 Days A Week
    sunday 00:00-24:00
    monday 00:00-24:00
    tuesday 00:00-24:00
    wednesday 00:00-24:00
    thursday 00:00-24:00
    friday 00:00-24:00
    saturday 00:00-24:00
}
```
# 'check-host-alive' command definition
define command{
    command_name    check-host-alive
    command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w 2000.0,60% -c 5000.0,100% -p 1 -t 5
}

- Located in /etc/nagios-plugins/config, then adjust in /etc/nagios3/conf.d/services_nagios2.cfg

- While these are “service” or “host” checks Nagios refers to them as “commands”
**Notification commands**

Allows you to utilize any command you wish. We could use this to generate tickets in RT.

```plaintext
# 'notify-by-email' command definition
define command{
    command_name notify-by-email
    command_line /usr/bin/printf "%b" "Service: $SERVICEDESC$\nHost: $HOSTNAME$\nIn: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState: $SERVICESTATE$\nInfo: $SERVICEOUTPUT$\nDate: $SHORTDATETIME$" | /bin/mail -s
'$NOTIFICATIONTYPE$: $HOSTNAME$/$SERVICEDESC$ is $SERVICESTATE$'
$CONTACTEMAIL$
}
```

From: nagios@nms.localdomain
To: router_group@localdomain
Subject: Host DOWN alert for TLD1-RTR!
Date: Thu, 29 Jun 2006 15:13:30 -0700

Host: gw-rtr
In: Core_Routers
State: DOWN
Address: 192.0.2.100
Date/Time: 06-29-2006 15:13:30
Info: CRITICAL - Plugin timed out after 6 seconds
# check that ssh services are running
define service {
    hostgroup_name ssh-servers
    service_description SSH
    check_command check_ssh
    use generic-service
    notification_interval 0 ; set > 0 if you want to be renotified
}

The “service_description” is important if you plan to create Service Groups. Here is a sample Service Group definition:

define servicegroup{
    servicegroup_name Webmail
    alias web-mta-storage-auth
    members srvr1,HTTP,srvr1,SMTP,srvr1,POP,srvr1,IMAP,
          srvr1,RAID,srvr1,LDAP, srvr2,HTTP,srvr2,SMTP,
          srvr2,POP,srvr2,IMAP,srvr2,RAID,srvr2,LDAP
}
Screen Shots

A few sample screen shots from a Nagios install.
General View
Service Detail

Current Network Status
Last Updated: Thu Sep 3 14:46:07 CDT 2009
Updated every 90 seconds
Nagios® 3.0.2 - www.nagios.org
Logged in as guest
View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

<table>
<thead>
<tr>
<th>Status</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up</td>
<td>41</td>
</tr>
<tr>
<td>Down</td>
<td>0</td>
</tr>
<tr>
<td>Unreachable</td>
<td>0</td>
</tr>
<tr>
<td>Pending</td>
<td>0</td>
</tr>
</tbody>
</table>

Service Status Totals

<table>
<thead>
<tr>
<th>Status</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Problems</td>
<td>0</td>
</tr>
<tr>
<td>All Types</td>
<td>41</td>
</tr>
</tbody>
</table>

Service Status Details For All Hosts

<table>
<thead>
<tr>
<th>Host</th>
<th>Service</th>
<th>Status</th>
<th>Last Check</th>
<th>Duration</th>
<th>Attempt</th>
<th>Status Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS-ROOT</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:43:51</td>
<td>43d 0h 55m 19s</td>
<td>1/4</td>
<td>SSH OK - OpenSSH_5.1p1 Debian-3-jun09u1 (protocol 2.0)</td>
</tr>
<tr>
<td>ISP-DNS</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:41:21</td>
<td>16d 3h 57m 24s</td>
<td>1/4</td>
<td>SSH OK - OpenSSH_5.1p1 Debian-3-jun09u1 (protocol 2.0)</td>
</tr>
<tr>
<td>ISP-RTR</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:43:57</td>
<td>43d 5h 35m 13s</td>
<td>1/4</td>
<td>SSH OK - Cisco-1.25 (protocol 2.0)</td>
</tr>
<tr>
<td>NOC-TLD1</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:41:27</td>
<td>1d 0h 1m 50s</td>
<td>1/4</td>
<td>SSH OK - OpenSSH_5.1p1 Debian-3-jun09u1 (protocol 2.0)</td>
</tr>
<tr>
<td>NOC-TLD2</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:43:04</td>
<td>1d 22h 44m 22s</td>
<td>1/4</td>
<td>SSH OK - OpenSSH_5.1p1 Debian-3-jun09u1 (protocol 2.0)</td>
</tr>
<tr>
<td>NOC-TLD3</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:41:34</td>
<td>1d 22h 40m 58s</td>
<td>1/4</td>
<td>SSH OK - OpenSSH_5.1p1 Debian-3-jun09u1 (protocol 2.0)</td>
</tr>
<tr>
<td>NOC-TLD4</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:44:10</td>
<td>1d 22h 44m 16s</td>
<td>1/4</td>
<td>SSH OK - OpenSSH_5.1p1 Debian-3-jun09u1 (protocol 2.0)</td>
</tr>
<tr>
<td>NOC-TLD5</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:41:40</td>
<td>1d 22h 41m 46s</td>
<td>1/4</td>
<td>SSH OK - OpenSSH_5.1p1 Debian-3-jun09u1 (protocol 2.0)</td>
</tr>
<tr>
<td>NOC-TLD6</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:44:17</td>
<td>1d 22h 44m 9s</td>
<td>1/4</td>
<td>SSH OK - OpenSSH_5.1p1 Debian-3-jun09u1 (protocol 2.0)</td>
</tr>
<tr>
<td>NOC-TLD7</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:41:47</td>
<td>1d 22h 41m 39s</td>
<td>1/4</td>
<td>SSH OK - OpenSSH_5.1p1 Debian-3-jun09u1 (protocol 2.0)</td>
</tr>
<tr>
<td>NOC-TLD8</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:44:23</td>
<td>1d 22h 44m 3s</td>
<td>1/4</td>
<td>SSH OK - OpenSSH_5.1p1 Debian-3-jun09u1 (protocol 2.0)</td>
</tr>
<tr>
<td>NS1-TLD1</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:41:53</td>
<td>1d 0h 1m 33s</td>
<td>1/4</td>
<td>SSH OK - OpenSSH_5.1p1 Debian-3-jun09u1 (protocol 2.0)</td>
</tr>
<tr>
<td>NS1-TLD2</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:44:30</td>
<td>1d 22h 43m 56s</td>
<td>1/4</td>
<td>SSH OK - OpenSSH_5.1p1 Debian-3-jun09u1 (protocol 2.0)</td>
</tr>
<tr>
<td>NS1-TLD3</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:42:00</td>
<td>1d 22h 41m 26s</td>
<td>1/4</td>
<td>SSH OK - OpenSSH_5.1p1 Debian-3-jun09u1 (protocol 2.0)</td>
</tr>
<tr>
<td>NS1-TLD4</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:44:36</td>
<td>1d 22h 43m 60s</td>
<td>1/4</td>
<td>SSH OK - OpenSSH_5.1p1 Debian-3-jun09u1 (protocol 2.0)</td>
</tr>
<tr>
<td>NS1-TLD5</td>
<td>SSH</td>
<td>OK</td>
<td>2009-09-03 14:42:06</td>
<td>1d 22h 41m 20s</td>
<td>1/4</td>
<td>SSH OK - OpenSSH_5.1p1 Debian-3-jun09u1 (protocol 2.0)</td>
</tr>
</tbody>
</table>
Host Status Details For All Host Groups

<table>
<thead>
<tr>
<th>Host</th>
<th>Status</th>
<th>Last Check</th>
<th>Duration</th>
<th>Status Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1-01</td>
<td>U</td>
<td>2009-09-03 14:51:41</td>
<td>4h 3m</td>
<td>PING OK - Packet loss = 0%, RTA = 0.33 ms</td>
</tr>
<tr>
<td>M1-02</td>
<td>U</td>
<td>2009-09-03 14:51:41</td>
<td>4h 3m</td>
<td>PING OK - Packet loss = 0%, RTA = 0.29 ms</td>
</tr>
<tr>
<td>M1-03</td>
<td>U</td>
<td>2009-09-03 14:51:41</td>
<td>4h 3m</td>
<td>PING OK - Packet loss = 0%, RTA = 1.24 ms</td>
</tr>
<tr>
<td>M1-04</td>
<td>U</td>
<td>2009-09-03 14:52:01</td>
<td>1d 2h 53m</td>
<td>PING OK - Packet loss = 0%, RTA = 4.02 ms</td>
</tr>
<tr>
<td>M1-05</td>
<td>U</td>
<td>2009-09-03 14:52:01</td>
<td>1d 2h 53m</td>
<td>PING OK - Packet loss = 0%, RTA = 2.83 ms</td>
</tr>
<tr>
<td>M1-06</td>
<td>U</td>
<td>2009-09-03 14:52:01</td>
<td>1d 2h 53m</td>
<td>PING OK - Packet loss = 0%, RTA = 1.09 ms</td>
</tr>
<tr>
<td>M1-07</td>
<td>U</td>
<td>2009-09-03 14:52:01</td>
<td>1d 2h 53m</td>
<td>PING OK - Packet loss = 0%, RTA = 5.20 ms</td>
</tr>
<tr>
<td>M1-08</td>
<td>U</td>
<td>2009-09-03 14:52:01</td>
<td>1d 2h 53m</td>
<td>PING OK - Packet loss = 0%, RTA = 10.49 ms</td>
</tr>
<tr>
<td>M1-09</td>
<td>U</td>
<td>2009-09-03 14:52:01</td>
<td>1d 2h 53m</td>
<td>PING OK - Packet loss = 0%, RTA = 5.95 ms</td>
</tr>
<tr>
<td>M1-10</td>
<td>U</td>
<td>2009-09-03 14:52:01</td>
<td>1d 2h 53m</td>
<td>PING OK - Packet loss = 0%, RTA = 1.93 ms</td>
</tr>
<tr>
<td>M1-11</td>
<td>U</td>
<td>2009-09-03 14:52:01</td>
<td>1d 2h 53m</td>
<td>PING OK - Packet loss = 0%, RTA = 1.15 ms</td>
</tr>
<tr>
<td>M1-12</td>
<td>U</td>
<td>2009-09-03 14:52:01</td>
<td>1d 2h 53m</td>
<td>PING OK - Packet loss = 0%, RTA = 1.12 ms</td>
</tr>
<tr>
<td>M1-13</td>
<td>U</td>
<td>2009-09-03 14:52:01</td>
<td>1d 2h 53m</td>
<td>PING OK - Packet loss = 0%, RTA = 1.08 ms</td>
</tr>
<tr>
<td>M1-14</td>
<td>U</td>
<td>2009-09-03 14:52:01</td>
<td>1d 2h 53m</td>
<td>PING OK - Packet loss = 0%, RTA = 1.11 ms</td>
</tr>
<tr>
<td>M1-15</td>
<td>U</td>
<td>2009-09-03 14:52:01</td>
<td>1d 2h 53m</td>
<td>PING OK - Packet loss = 0%, RTA = 1.18 ms</td>
</tr>
<tr>
<td>M1-16</td>
<td>U</td>
<td>2009-09-03 14:52:01</td>
<td>1d 2h 53m</td>
<td>PING OK - Packet loss = 0%, RTA = 2.22 ms</td>
</tr>
</tbody>
</table>
Collapsed tree status map
Marked-up circular status map
More sample screenshots

Many more sample Nagios screenshots available here:

http://www.nagios.org/about/screenshots