

NOC TOOLS

nagios

AfNOG 2008, SI-E, Friday, 3 of 5

nagios

- How do you know when your routers and switches have a problem?
- How do you know if your ISP stopped working?
- *(hint: “because the customer called us and said so” is not the right answer!)*

nagios

- nagios is a tool for automatically testing whether things are working
 - servers, routers, switches
 - http server processes
 - disk space, CPU load, number of users, etc
 - anything you can write a script to check

When Things Happen

- What happens when a test fails?
 - depends on how nagios is configured
 - maybe make beeping noises
 - show red on the status screen
 - send an SMS to someone

Screenshots

Nagios - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

Bookmarks Go to: What's Related

Nagios

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Status Overview
- Status Summary
- Status Grid
- Status Map
- 3-D Status Map
- Service Problems
- Host Problems
- Network Outages
- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue

Reporting

- Trends
- Availability
- Histogram
- Alert History
- Notifications
- Event Log

Configuration

- View Config

Network Map For All Hosts

Last Updated: Sun Jan 6 20:28:54 CST 2002
Updated every 75 seconds
Nagios™ - www.nagios.org
Logged in as guest
- Monitoring process is running
- Notifications cannot be sent out!
- Service checks are being executed

[View Status Detail For All Hosts](#)
[View Status Overview For All Hosts](#)

Layout Method: Circular (Marked Up) Scaling factor: 0.7

Drawing Layers: Win3x Workstations, Bogus Servers, Linux Servers, Mail Servers

Layer mode: Include Exclude

Suppress popups:

The network map displays a central host 'Nagios' connected to various other hosts. The hosts are organized into layers based on their operating system or role. The green layer contains Linux Servers, the red layer contains Mail Servers, and the grey layer contains Win3x Workstations. The map shows a complex network topology with many connections between hosts. Some hosts have status indicators: 'Up' (green), 'Down' (red), or a question mark (unknown). The map is titled 'Network Map For All Hosts' and is updated every 75 seconds. The Nagios logo is visible in the center of the map.

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Hostgroup Overview
- Hostgroup Summary
- Hostgroup Grid
- Servicegroup Overview
- Servicegroup Summary
- Servicegroup Grid
- Status Map
- 3-D Status Map

- Service Problems
- Host Problems
- Network Outages

Show Host:

- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue

Reporting

- Trends
- Availability
- Alert Histogram
- Alert History
- Alert Summary
- Notifications
- Event Log

Configuration

- View Config

Current Network Status

Last Updated: Thu May 29 10:33:39 WET 2008
 Updated every 30 seconds
 Nagios® - www.nagios.org
 Logged in as sse

[View History For all hosts](#)
[View Notifications For All Hosts](#)
[View Host Status Detail For All Hosts](#)

Host Status Totals

Up	Down	Unreachable	Pending
26	3	0	0

All Problems	All Types
3	29

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
130	0	0	129	0

All Problems	All Types
129	259

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
noc	DNS	OK	05-28-2008 18:43:46	4d 22h 28m 4s	1/3	DNS OK: 0.091 seconds response time. www.yahoo.com returns 87.248.113.14
	FTP	OK	05-28-2008 18:44:18	4d 21h 52m 28s	1/3	FTP OK - 0.002 second response time on port 21 [220 noc.sse.ws.afnag.org FTP server (Version 6.00LS) ready.]
	HTTP	OK	05-28-2008 18:38:18	5d 21h 7m 10s	1/3	HTTP OK HTTP/1.1 200 OK - 507 bytes in 0.006 seconds
	PING	OK	05-28-2008 18:38:18	5d 21h 6m 34s	1/3	PING OK - Packet loss = 0%, RTA = 0.04 ms
	POP3	OK	05-28-2008 18:38:18	0d 17h 0m 33s	1/3	POP OK - 0.008 second response time on port 110 [+OK Hello there.]
	RADIUS	OK	05-28-2008 18:38:18	0d 16h 59m 43s	1/3	Access GRANTED. (code = 2)
	SMTP	OK	05-28-2008 18:40:19	2d 19h 50m 3s	1/3	SMTP OK - 0.015 sec. response time
pc01	DNS	OK	05-28-2008 18:38:20	1d 23h 32m 33s	1/3	DNS OK: 0.245 seconds response time. www.yahoo.com returns 87.248.113.14
	HTTP	OK	05-28-2008 18:38:52	0d 16h 58m 25s	1/3	HTTP OK HTTP/1.1 200 OK - 330 bytes in 0.001 seconds
	HTTPS	OK	05-28-2008 18:43:47	0d 17h 2m 40s	1/3	OK - Certificate will expire on 05/25/2018 18:43.
	IMAP	CRITICAL	05-28-2008 18:10:09	6d 0h 52m 28s	3/3	Connection refused
	IMAP-S	CRITICAL	05-28-2008 18:44:19	6d 0h 51m 52s	3/3	Connection refused
	PING	OK	05-28-2008 18:38:18	4d 23h 6m 50s	1/3	PING OK - Packet loss = 0%, RTA = 0.17 ms
	POP3	CRITICAL	05-28-2008 18:38:18	6d 0h 50m 40s	3/3	Connection refused
	POP3-S	CRITICAL	05-28-2008 18:38:18	6d 0h 50m 4s	3/3	Connection refused
SMTP	OK	05-28-2008 18:40:19	0d 16h 59m 28s	1/3	SMTP OK - 0.076 sec. response time	
pc02	DNS	OK	05-28-2008 18:38:21	1d 23h 32m 32s	1/3	DNS OK: 0.042 seconds response time. www.yahoo.com returns 87.248.113.14
	HTTP	OK	05-28-2008 18:38:53	0d 16h 58m 24s	1/3	HTTP OK HTTP/1.1 200 OK - 431 bytes in 0.001 seconds
	HTTPS	OK	05-28-2008 18:39:38	0d 17h 2m 39s	1/3	OK - Certificate will expire on 05/25/2018 19:22.
	IMAP	CRITICAL	05-28-2008 18:43:48	6d 0h 52m 26s	3/3	Connection refused
	IMAP-S	CRITICAL	05-28-2008 18:44:20	6d 0h 51m 50s	3/3	Connection refused
	PING	OK	05-28-2008 18:38:18	4d 23h 6m 49s	1/3	PING OK - Packet loss = 0%, RTA = 0.36 ms
	POP3	CRITICAL	05-28-2008 18:38:18	6d 0h 50m 38s	3/3	Connection refused
	POP3-S	CRITICAL	05-28-2008 18:38:18	6d 0h 50m 2s	3/3	Connection refused
SMTP	OK	05-28-2008 18:40:19	0d 16h 59m 27s	1/3	SMTP OK - 0.002 sec. response time	
pc03	DNS	CRITICAL	05-28-2008 18:38:22	0d 16h 5m 17s	1/3	CRITICAL - Plugin timed out while executing system call
	HTTP	CRITICAL	05-28-2008 18:38:54	0d 16h 4m 45s	1/3	CRITICAL - Socket timeout after 10 seconds
	HTTPS	CRITICAL	05-28-2008 18:39:39	0d 16h 9m 0s	1/3	CRITICAL - Socket timeout after 10 seconds
	IMAP	CRITICAL	05-28-2008 18:43:49	6d 0h 52m 24s	1/3	CRITICAL - Socket timeout after 10 seconds
	IMAP-S	CRITICAL	05-28-2008 18:44:21	6d 0h 51m 48s	1/3	CRITICAL - Socket timeout after 10 seconds
	PING	CRITICAL	05-28-2008 18:38:18	0d 16h 5m 21s	1/3	CRITICAL - Plugin timed out after 10 seconds
	POP3	CRITICAL	05-28-2008 18:38:18	6d 0h 50m 36s	1/3	CRITICAL - Socket timeout after 10 seconds
	POP3-S	CRITICAL	05-28-2008 18:38:18	6d 0h 50m 0s	1/3	CRITICAL - Socket timeout after 10 seconds
SMTP	CRITICAL	05-28-2008 18:40:19	0d 16h 8m 48s	1/3	Host is down	
pc04	DNS	OK	05-28-2008 18:38:23	1d 23h 32m 29s	1/3	DNS OK: 0.091 seconds response time. www.yahoo.com returns 87.248.113.14
	HTTP	OK	05-28-2008 18:38:55	0d 16h 58m 22s	1/3	HTTP OK HTTP/1.1 200 OK - 330 bytes in 0.001 seconds
	HTTPS	OK	05-28-2008 18:39:40	0d 17h 2m 37s	1/3	OK - Certificate will expire on 05/25/2018 18:36.

Installing Nagios

- On FreeBSD, it is very easy
 - `cd /usr/ports/net-mgmt/nagios`
 - `make install`
- Packages are available on other platforms, too
- See <http://www.nagios.org/> for details

Configuring nagios?

- The FreeBSD port comes with default configuration, which is good enough to get it running
- Look in `/usr/local/etc/nagios/`

SS-E Nagios

- SS-E uses nagios to monitor student computers, to see which services are up and running
- <http://noc.sse.ws.afnog.org/nagios/>

Demonstration