

An Introduction

Nagios[®]

intERLab at AIT
Network Management Workshop
March 11-15 – Bangkok, Thailand
Hervey Allen & Phil Regnauld



nsro@intERLab
Bangkok, Thailand

Where Does Nagios Fit?

Nagios, in some ways, ties it all together.
We've seen things like:

- SNMP
- MRTG
- RRDTool
- Rancid
- Cacti
- Smokeping

You can and will use all this functionality in Nagios.

It is a monolithic tool:

- Big
- Complex
- Powerful

nsro@intERLab
Bangkok, Thailand

Why Nagios

- Open source
- Relatively scalable, Manageable, Secure and more
- Best documentation available
- Good log and database system
- Nice, informative and attractive web interface
- Very flexible
- Alerts automatically sent if condition changes
- Various notification options (Email, pager, mobile phone)

nsro@intERLab
Bangkok, Thailand

Why Nagios

- Avoidance of “Too many red flashing lights”
 - “Just the facts” – only want root cause failures to be reported, not cascade of every downstream failure.
 - also avoids unnecessary checks
 - e.g. HTTP responds, therefore no need to ping
 - e.g. power outage, no ping response, so don't bother trying anything else
 - Services are running fine no need to do check if the host itself is alive

nsro@intERLab
Bangkok, Thailand

What Can it Do?

- Individual node status
 - ✓ Is it up?
 - ✓ What is its load?
 - ✓ What is the memory and swap usage?
 - ✓ NFS and network load?
 - ✓ Are the partitions full?
 - ✓ Are applications and services running properly?
 - ✓ How about ping latency?
- Aggregated node status
 - ✓ Same info, but across groups of nodes

nsro@interLab
Bangkok, Thailand

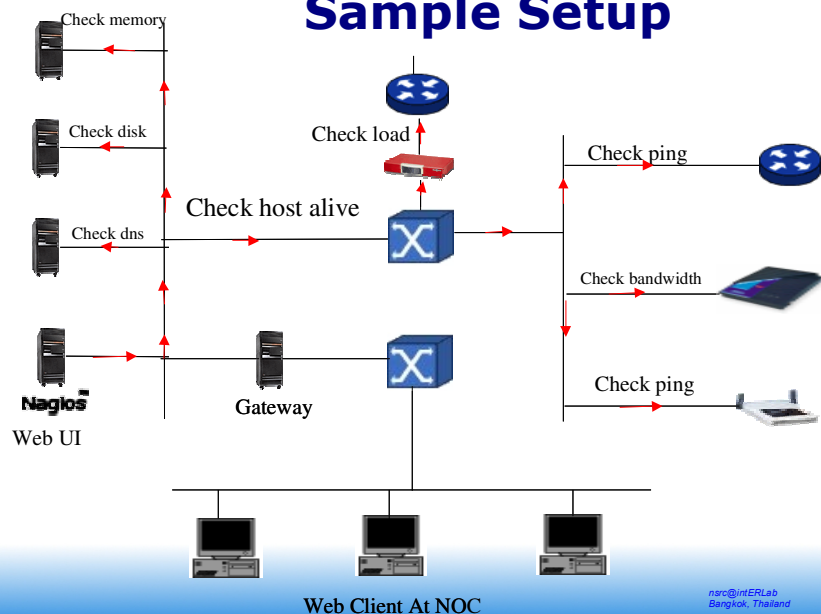
What Can it Do?

A lot, including:

- Service monitoring
- Alerts from SNMP traps
- Monitoring redundancy
- Detection of primary failure to avoid multiple like alerts.
- Notifications via email, pager, etc.
- Notifications to individuals or defined groups
- Log information
- Use databases to store history
- Graph generation from MRTG
- Very extensible via plug-ins, add-ons and local scripts.
- Can scale to large installations
- Allows for redundant monitoring
- Aggregation of like-data across multiple nodes.
- Ability to escalate alerts
- Runs on multiple Unices
- Licensed under GPL v2

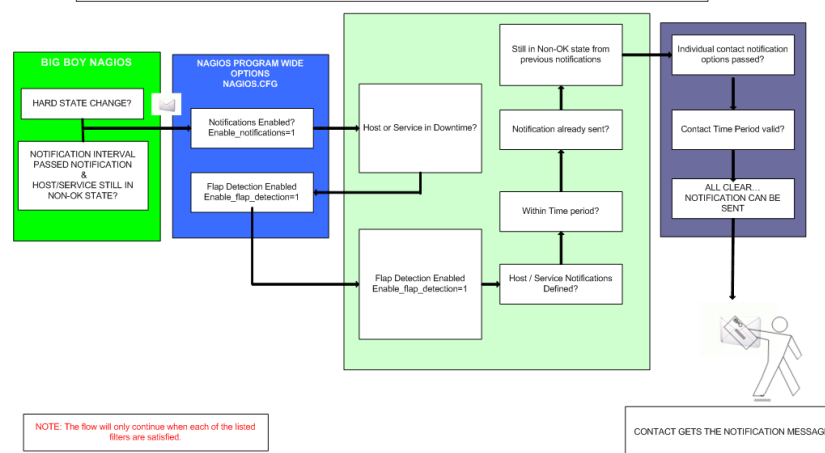
nsro@interLab
Bangkok, Thailand

Sample Setup



nsro@interLab
Bangkok, Thailand

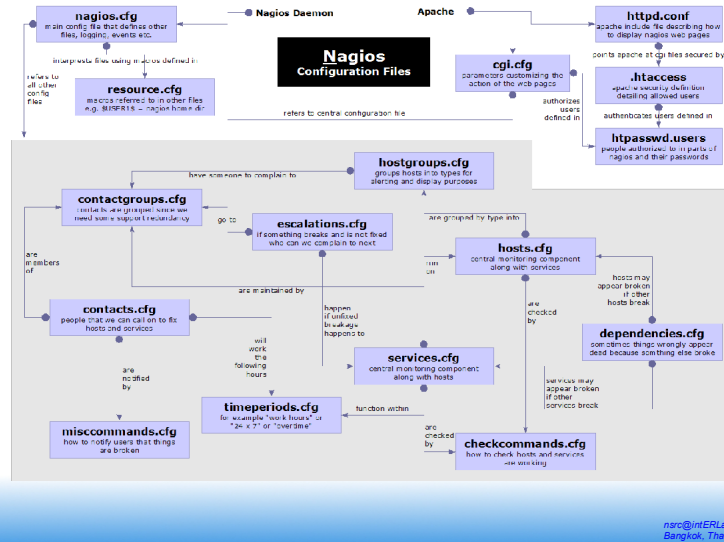
NAGIOS - NOTIFICATION FLOW DIAGRAM



NOTE: The flow will only continue when each of the listed items are satisfied.

nsro@interLab
Bangkok, Thailand

Nagios Configuration



Nagios®

Remaining Slides

Dhruba Raj Bhandari

(CCNA)

Additions by Phil Regnauld

bhandari.dhruba@scp.com.np

nsro@interLab
Bangkok, Thailand

Nagios Status Detail screen

The screenshot shows the Nagios Status Detail screen. The top section displays **Current Network Status** and **Service Status Totals**. Below this, there are links to view service status details for all host groups, status overview, status summary, status grid, status map, and 3-D status map. The main section is titled **Host Status Details For All Host Groups** and includes a table of host status details.

Host	Status	Last Check	Duration	Status Information
CHILDREN-FIRST	DOWN	02-01-2004 12:13:59	1d 19h 10m 33s	PING CRITICAL - Packet loss = 100%
BANIDA	DOWN	02-01-2004 12:15:55	1d 0h 43m 12s	PING CRITICAL - Packet loss = 100%
BASS	DOWN	02-01-2004 12:08:59	4d 0h 40m 42s	PING CRITICAL - Packet loss = 100%
ENCCI	DOWN	02-01-2004 12:12:38	4d 0h 40m 2s	PING CRITICAL - Packet loss = 100%
ITLINK	DOWN	02-01-2004 12:15:55	0d 1h 37m 12s	PING CRITICAL - Packet loss = 100%
ITLXNET	DOWN	02-01-2004 12:12:38	4d 0h 38m 53s	PING CRITICAL - Packet loss = 100%

Tactical Overview Of Nagios

The screenshot shows the Nagios Tactical Overview screen. The top section displays **Network Outages** and **Hosts**. Below this, there are links to view service status details for all host groups, status overview, status summary, status grid, status map, and 3-D status map. The main section is titled **Host Status Details For All Host Groups** and includes a table of host status details.

Host	Status	Last Check	Duration	Status Information
CHILDREN-FIRST	DOWN	02-01-2004 12:13:59	1d 19h 10m 33s	PING CRITICAL - Packet loss = 100%
BANIDA	DOWN	02-01-2004 12:15:55	1d 0h 43m 12s	PING CRITICAL - Packet loss = 100%
BASS	DOWN	02-01-2004 12:08:59	4d 0h 40m 42s	PING CRITICAL - Packet loss = 100%
ENCCI	DOWN	02-01-2004 12:12:38	4d 0h 40m 2s	PING CRITICAL - Packet loss = 100%
ITLINK	DOWN	02-01-2004 12:15:55	0d 1h 37m 12s	PING CRITICAL - Packet loss = 100%
ITLXNET	DOWN	02-01-2004 12:12:38	4d 0h 38m 53s	PING CRITICAL - Packet loss = 100%

Service Detail of Nagios

Current Service Status - Mozilla

File Edit View Go Bookmarks Tools Window Help

https://thuldai.mos.com.np/nagios/cgi-bin/status.cgi?host=all

Current Network Status
Last Updated: Sun Feb 1 09:57:47 NPT 2004
Updated every 90 seconds
Nagios® - www.nagios.org
Logged in as dhruba

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
155	15	0	0

All Problems: 15 All Types: 170

Service Status Totals

OK	Warning	Unknown	Critical	Pending
228	3	0	16	0

All Problems: 19 All Types: 247

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
ACTIONAID	Ping	OK	02-01-2004 09:53:07	0d 12h 20m 9s	1/3	PING OK - Packet loss = 0%, RTA = 2 ms
AFP	Ping	OK	02-01-2004 09:55:38	0d 13h 40m 29s	1/3	PING OK - Packet loss = 0%, RTA = 1 ms
AGNIPAGE	Ping	OK	02-01-2004 09:55:27	0d 0h 0m 59s	1/3	PING OK - Packet loss = 0%, RTA = 1 ms
BRTSCHOOL	Ping	OK	02-01-2004 09:54:06	1d 18h 7m 39s	1/3	PING OK - Packet loss = 0%, RTA = 9 ms
Ban-cat	Ping	OK	02-01-2004 09:56:11	0d 22h 44m 39s	1/3	PING OK - Packet loss = 0%, RTA = 9 ms

Transferring data from thuldai.mos.com.np...

Current S [root@dhr] Sun Feb 01, 9:26 PM

Service Types

Current Service Status - Mozilla

File Edit View Go Bookmarks Tools Window Help

https://thuldai.mos.com.np/nagios/cgi-bin/status.cgi?host=all

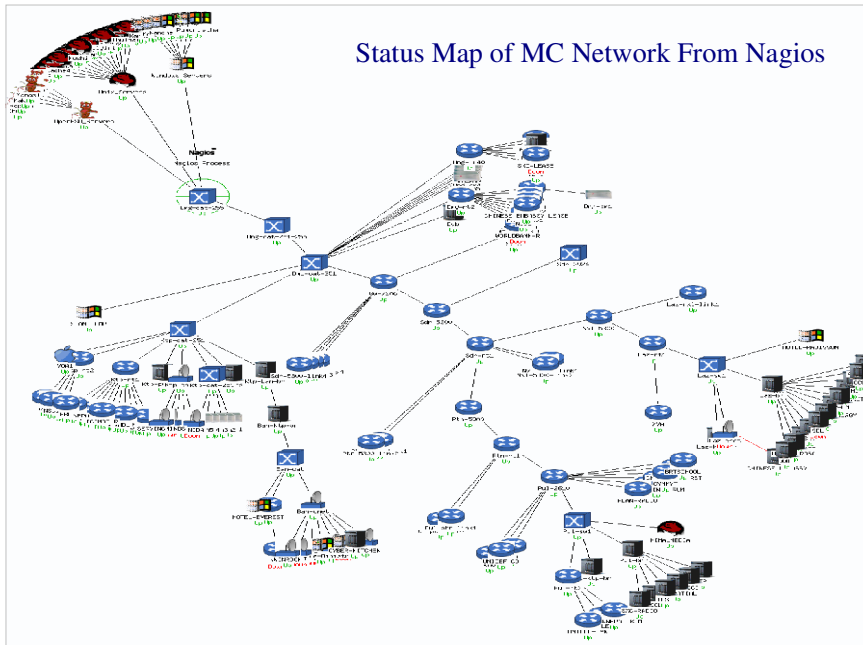
Service Types

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Kantipath	FTP	OK	02-01-2004 10:23:48	3d 22h 46m 38s	1/3	FTP OK - 0.007 second response time port 21 [220 kaillash.mos.com.np FTP server ready.]
Kantipath	Free-Memory	OK	02-01-2004 10:22:15	3d 22h 48m 34s	1/3	SNMP OK: Ram-Free:3100,
Kantipath	HTTP	OK	02-01-2004 10:22:59	3d 22h 46m 38s	1/3	HTTP OK: HTTP/1.1 200 OK - 0.021 second response time
Kantipath	Load	OK	02-01-2004 10:25:17	3d 22h 48m 34s	1/3	SNMP OK: 1MIN-Load:0.08, 5MIN-Load:0.05, 15MIN-Load:0.00,
Kantipath	Ping	OK	02-01-2004 10:25:07	0d 5h 7m 33s	1/3	PING OK - Packet loss = 0%, RTA = 0 ms
Kantipath	disk_usage	OK	02-01-2004 10:22:51	3d 22h 48m 34s	1/3	Disk utilization: All disks OK
Karnali	Ping	OK	02-01-2004 10:25:58	0d 17h 48m 53s	1/3	PING OK - Packet loss = 0%, RTA = 1 ms
Kopila	Cpu-usage	OK	02-01-2004 10:24:07	3d 22h 48m 34s	1/3	SNMP OK: usr-cpu:0, sys-cpu:1,
Kopila	Free-Memory	OK	02-01-2004 10:22:51	3d 22h 46m 38s	1/3	SNMP OK: Ram-Free:3808,
Kopila	Load	OK	02-01-2004 10:22:18	3d 22h 48m 34s	1/3	SNMP OK: 1MIN-Load:0.18, 5MIN-Load:0.19, 15MIN-Load:0.18,
Kopila	POP	OK	02-01-2004 10:23:07	3d 22h 46m 38s	1/3	POP OK - 0.028 second response time port 110 [+OK <8832.1075610415@kopila.mos.com>
Kopila	Ping	OK	02-01-2004 10:25:58	3d 15h 7m 15s	1/3	PING OK - Packet loss = 0%, RTA = 1 ms
Koshi	Ping	OK	02-01-2004 10:22:37	1d 13h 37m 43s	1/3	PING OK - Packet loss = 0%, RTA = 9 ms

Done

Mozilla-bi [root@dhr] Sun Feb 01, 9:56 PM

Status Map of MC Network From Nagios



Status Overview from nagios

https://thuldai.mos.com.np/nagios/cgi-bin/status.cgi?hostgroup=all

All Routers @Durbar Marg-KTM (Routers@DMG)

Host	Status	Services	Actions
Dmg-3640	UP	1 OK	
Dmg-r12	UP	1 OK	
Gw-7206	UP	1 OK	

All Routers @Kantipath-KTM (Routers@KP)

Host	Status	Services	Actions
Kip-r1	UP	1 OK	
Kip-r2	UP	1 OK	

All Routers @Lazim (Routers@LAZ)

Host	Status	Services	Actions
Laz-ns1-link1	UP	1 OK	
Laz-r1	UP	1 OK	

All Routers @POPs w/ Lease Link (Routers@POP)

Host	Status	Services	Actions
Bri-gw	UP	1 OK	
Bri-gw	UP	1 OK	
Bri-link1	UP	1 OK	
Bri-link2	UP	1 OK	
Hkl-boss	DOWN	1 CRITICAL	

All Routers @POPs w/ VSAT Link (Routers@POPv)

Host	Status	Services	Actions
Bri-2501	UP	1 OK	
Bri-vsai	UP	1 OK	
Hkl-vsai	UP	1 WARNING	
Nam-gw	UP	1 OK	

All Routers @Sundhara (Routers@SDR)

Host	Status	Services	Actions
Pul-2610	UP	1 OK	
Pul-pin-link1	UP	1 OK	
Pul-pin-link2	UP	1 OK	
Pul-r2	UP	1 OK	

All Routers @Xpressway (Routers@X)

Host	Status	Services	Actions
AGNIPAGE	UP	1 OK	
BRTSCHOOL	UP	1 OK	

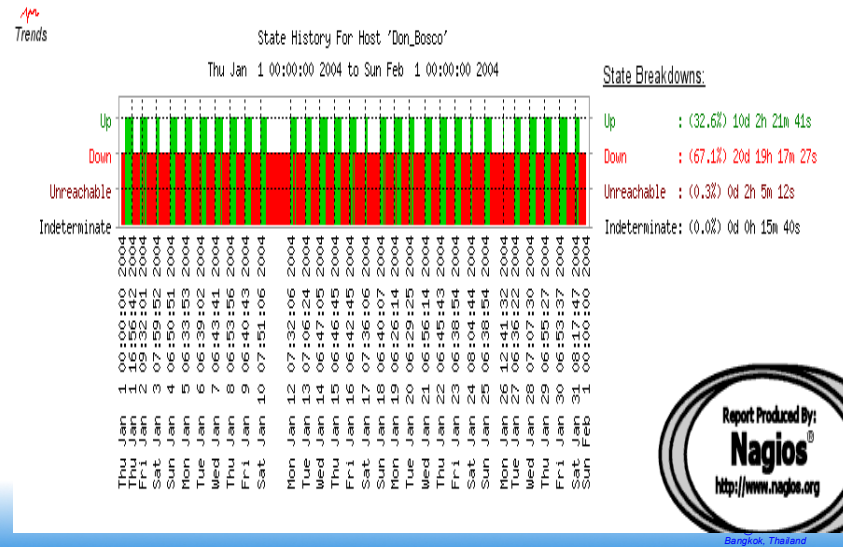
Status Summary Based On Hostgroup

https://thuldai.mos.com.np/nagios/cgi-bin/status.cgi?hostgroup=all&style=summary

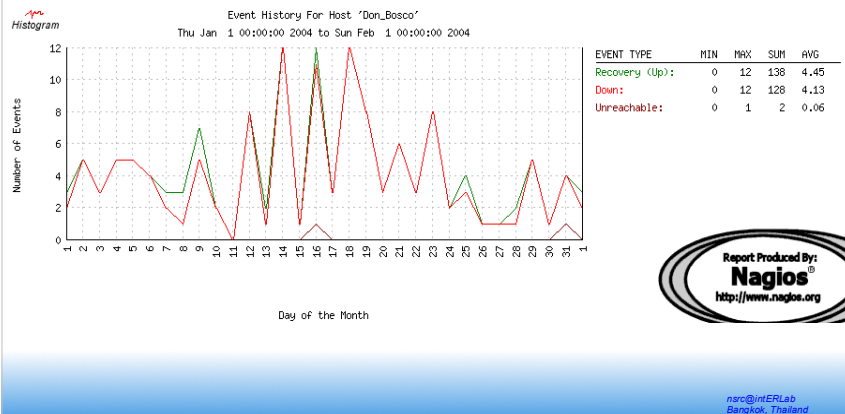
Status Summary For All Host Groups

Host Group	Host Status Totals	Service Status Totals
Access Servers@KTM (AS@KTM)	11 UP	11 OK
All Routers@KTM (Routers@KTM)	9 UP	9 OK
All Routers@MTX Customers w/ Radio Link (Routers@MTXR)	1 UP	1 OK
All Routers@Xpressway Customers w/ Radio Link (Routers@XpresswayR)	19 UP	19 OK
All Routers@Xpressway Customers w/ Radio Link (Cnet Clients@XpresswayR)	6 DOWN	5 CRITICAL
All Routers@Xpressway Customers w/ Radio Link (Cnet Clients@XpresswayR)	6 UP	5 OK
All Routers@Xpressway Customers w/ Radio Link (Cnet Clients@XpresswayR)	4 DOWN	5 CRITICAL
All Cnets@KTM (Cnets@KTM)	2 UP	2 OK
All Co-located Servers (Co-locators)	2 UP	2 OK
Iprico DVB@DMG (DVB@DMG)	1 UP	1 OK
All Email-alert-only Boxes (E-boxes)	1 UP	1 OK
All Livingston Portmasters@Kathmandu (Portmasters@KTM)	10 UP	10 OK
All Livingston Portmasters@MC-POPs (Portmasters@POPs)	1 UP	1 WARNING
All Routers@Banshore (Routers@BAN)	1 UP	1 OK
All Routers@Durbar Marg-KTM (Routers@DMG)	1 UP	1 OK
All Routers@Kantipath-KTM (Routers@KP)	2 UP	2 OK
All Routers@Lazimpat (Routers@LAZ)	2 UP	2 OK
All Routers@POPs w/ Lease Link (Routers@POP.L)	4 UP	4 OK
All Routers@POPs w/ Lease Link (Routers@POP.L)	1 DOWN	1 CRITICAL

Host Trends or Status History



Histogram Of Host



Event Logs

https://thuldai.mos.com.np/nagios/cgi-bin/showlog.cgi

Current Event Log
Last Updated: Sun Feb 1 12:15:31 NPT 2004
Nagios@: www.nagios.org
Logged in as dhruba

Log File Navigation
Sun Feb 1 00:00:00 NPT 2004 to Present..

File: /usr/local/nagios/var/nagios.log

February 01, 2004 12:00

[02-01-2004 12:14:28]	HOST NOTIFICATION: Amod:WORLDBANK-R:DOWN:host-notify-by-email:PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:28]	HOST NOTIFICATION: Amod:WORLDBANK-R:DOWN:host-notify-by-epager:PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:28]	HOST NOTIFICATION: DeepakA:WORLDBANK-R:DOWN:host-notify-by-epager:PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:28]	HOST NOTIFICATION: Krishna:WORLDBANK-R:DOWN:host-notify-by-epager:PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:27]	HOST NOTIFICATION: NirajS:WORLDBANK-R:DOWN:host-notify-by-email:PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:27]	HOST NOTIFICATION: Prabhu:WORLDBANK-R:DOWN:host-notify-by-epager:PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:27]	HOST NOTIFICATION: Ravin:WORLDBANK-R:DOWN:host-notify-by-email:PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:27]	HOST NOTIFICATION: Ravin:WORLDBANK-R:DOWN:host-notify-by-epager:PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:28]	HOST NOTIFICATION: Upendra:WORLDBANK-R:DOWN:host-notify-by-email:PING CRITICAL - Packet loss = 100%
[02-01-2004 12:12:16]	SERVICE ALERT: SDC:Ping:WARNING:HARD:3:PING WARNING - Packet loss = 60%, RTA = 23.73 ms
[02-01-2004 12:12:16]	HOST ALERT: SDC:DOWN:HARD:1:PING CRITICAL - Packet loss = 100%
[02-01-2004 12:11:09]	SERVICE ALERT: Hdd-ysat:Ping:WARNING:HARD:3:PING WARNING - Packet loss = 40%, RTA = 674.22 ms
[02-01-2004 12:10:26]	SERVICE ALERT: Hdd-lease:Ping:WARNING:HARD:3:PING WARNING - Packet loss = 40%, RTA = 385.85 ms
[02-01-2004 12:08:58]	SERVICE FLAPPING ALERT: WORLDBANK-R:Ping:STOPPED: Service appears to have stopped flapping (3.8% change < 5.0% threshold)
[02-01-2004 12:08:49]	HOST NOTIFICATION: Gyanu:Hdd-lease:UP:host-notify-by-email:PING OK - Packet loss = 30%, RTA = 357.24 ms
[02-01-2004 12:08:48]	HOST NOTIFICATION: Ishwar:Hdd-lease:UP:host-notify-by-email:PING OK - Packet loss = 30%, RTA = 357.24 ms
[02-01-2004 12:08:48]	HOST NOTIFICATION: Kedar:Hdd-lease:UP:host-notify-by-epager:PING OK - Packet loss = 30%, RTA = 357.24 ms
[02-01-2004 12:08:48]	HOST NOTIFICATION: MSurya:Hdd-lease:UP:host-notify-by-email:PING OK - Packet loss = 30%, RTA = 357.24 ms

Who is Notified?

https://thuldai.mos.com.np/nagios/cgi-bin/notifications.cgi?contact=all

Contact Notifications
Last Updated: Sun Feb 1 12:07:59 NPT 2004
Nagios® - www.nagios.org
Logged in as *dmrba*

All Contacts

Notification detail level for all contacts:
All notifications
Older Entries First: ☐ Update

Log File
Navigation
Sun Feb 1 00:00:00
NPT 2004
to
Present..

File: /usr/local/nagios/var/nagios.log

Host	Service	Type	Time	Contact	Notification Command	Information
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:12	Amol	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:12	Amol	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Deepak	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Krishna	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Nira	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Prabu	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Ravin	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:10	Ravin	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:08	Upendra	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Amol	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Amol	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Deepak	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Krishna	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Prabu	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:48	Ravin	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:48	Ravin	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:48	Upendra	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Hid-lease	N/A	HOST DOWN	02-01-2004 10:56:06	Gyanu	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Hid-lease	N/A	HOST DOWN	02-01-2004 10:56:06	Ishwar	host-notify-by-email	PING CRITICAL - Packet loss = 100%

Sun Feb 01, 11:37 PM

Notification Email Sample

From: nagios@thuldai.mos.com.np
 To: "ishwars@mos.com.np" <ishwars@mos.com.np>
 Subject: Host DOWN alert for WORLDBANK-L!
 Date: 05/02/04 11:09

***** Nagios *****

Notification Type: PROBLEM

Host: WORLDBANK-L

State: DOWN

Address: 202.52.239.70

Info: PING CRITICAL - Packet loss = 100%

Date/Time: Thu Feb 5 11:06:38 NPT 2004

nsro@interLab
Bangkok, Thailand

Nagios configuration files

- Located in /etc/nagios2/
- Important files:
 - cgi.cfg controls the Web Interface options security
 - commands.cfg commands that Nagios uses to notify
 - nagios.cfg main Nagios configuration file
 - conf.d/* the core of the config files

nsro@interLab
Bangkok, Thailand

Nagios configuration files

- Under conf.d/*, files "xxxx_nagios2.cfg":
- contacts users and groups
- generic-host "template" host (default)
- generic-service "template" service
- hostgroups host group definitions
- services which services to check
- timeperiods when to check and notify

nsro@interLab
Bangkok, Thailand

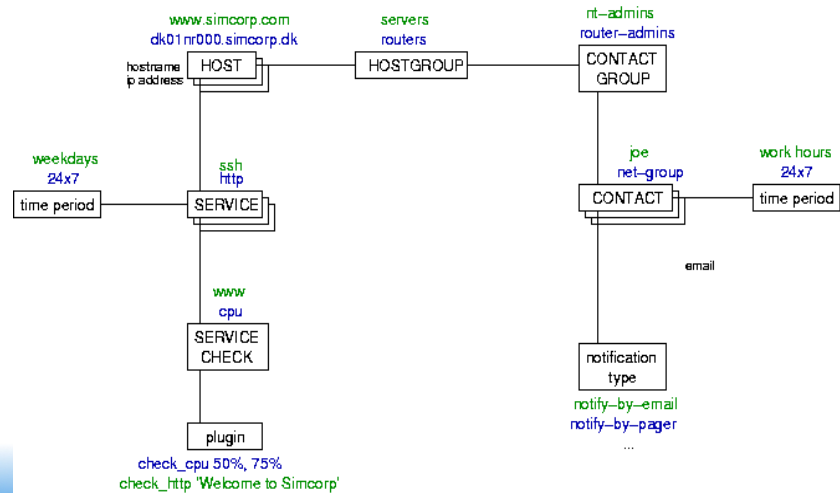
Nagios plugin configuration

• /etc/nagios-plugins/config/

apt.cfg ntp.cfg dhcp.cfg ping.cfg
disk.cfg procs.cfg dummy.cfg real.cfg
ftp.cfg ssh.cfg http.cfg tcp_udp.cfg
load.cfg telnet.cfg mail.cfg users.cfg
news.cfg

nsro@interLab
Bangkok, Thailand

NAGIOS schema

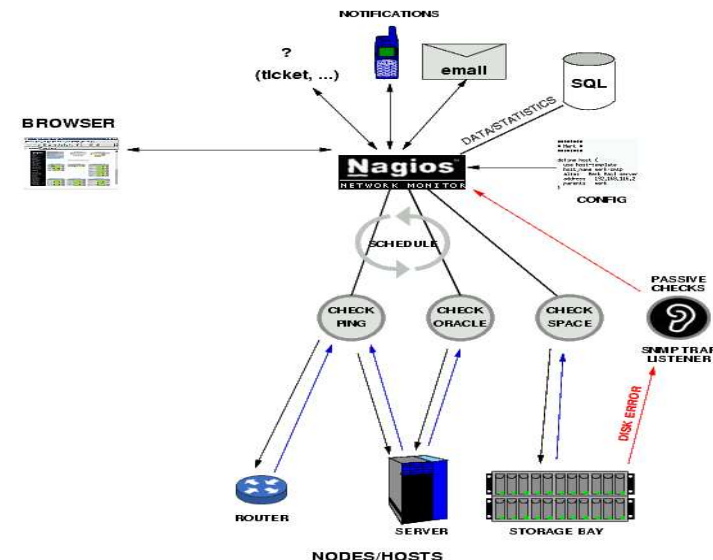


nsro@interLab
Bangkok, Thailand

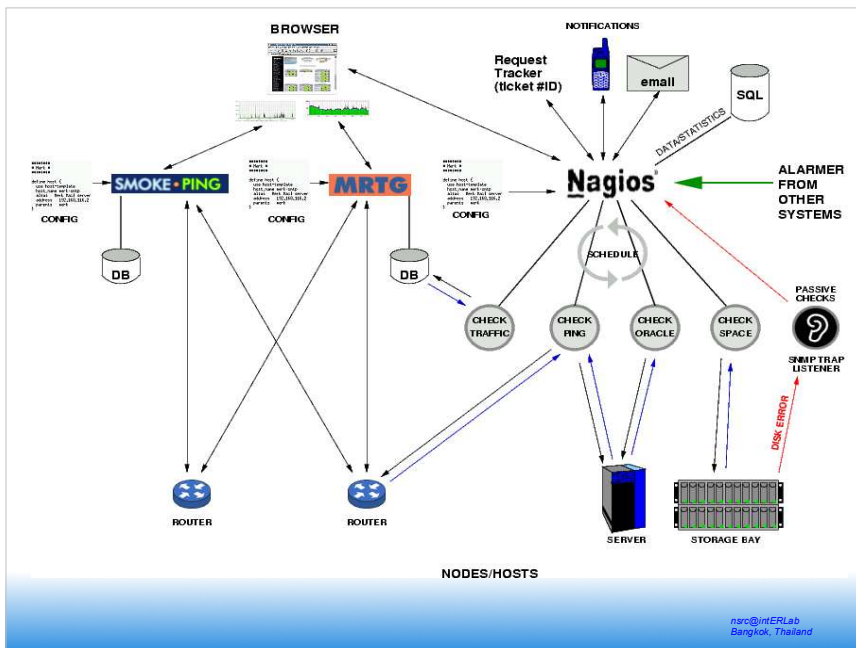
Concepts: parents

- Hosts can have parents
 - Allows one to specify which dependencies there are in the network
 - Avoid sending alarms if we cannot know the state of a host...

nsro@interLab
Bangkok, Thailand



nsro@interLab
Bangkok, Thailand



Nagios Resources

Nagios Home

<http://www.nagios.org/>

Nagios Plugins and Add Ons Exchange

<http://www.nagiosexchange.com/>

Nagios Tutorial for Debian

<http://www.debianhelp.co.uk/nagios.htm>

Nagios Commercial Support

<http://www.nagios.com/>

nsro@interLab
Bangkok, Thailand

Questions?

nsro@interLab
Bangkok, Thailand