

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

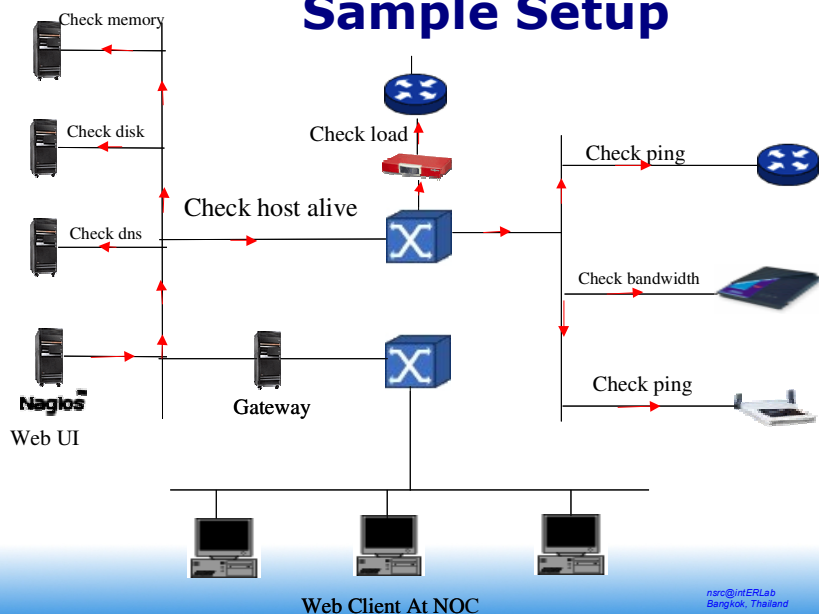
What Can it Do?

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

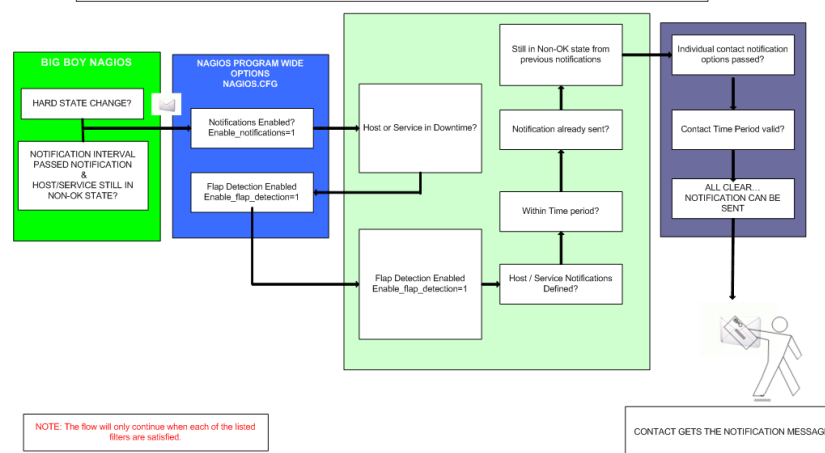
nsro@interLab
Bangkok, Thailand

Sample Setup



nsro@interLab
Bangkok, Thailand

NAGIOS - NOTIFICATION FLOW DIAGRAM



nsro@interLab
Bangkok, Thailand

[illegible]

Nagios®

Remaining Slides

Dhruba Raj Bhandari
(CCNA)

Additions by Phil Regnault
bhandari.dhruba@scp.com.np

nro@INERLab
Bangkok, Thailand

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
- Alert Histogram
- Alert History
- Alert Summary
- Notifications

Current Network Status

Last Updated: Sun Feb 1 12:17:48 NPT 2004
Updated every 90 seconds
Nagios® -
www.nagios.org
Logged in as *dhruvi*

Host Status Totals

Up	Down	Unreachable	Pending
15	15	0	0

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
226	5	0	16	0

All Problems All Types

All Problems	All Types
15	170

[View Service Status Detail For All Host Groups](#)
[View Status Overview For All Host Groups](#)
[View Status Summary For All Host Groups](#)
[View Status Grid For All Host Groups](#)

Display Filters:

Host Status Types: All problems
Host Properties: Any
Service Status Types: All
Service Properties: Any

Host Status Details For All Host Groups

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%
DANIDA	DOWN	02-01-2004 12:15:55	1d 0h 43m 12s	PING CRITICAL - Packet loss = 100%
DASS	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%
TELINK	DOWN	02-01-2004 12:15:55	0d 1h 37m 12s	PING CRITICAL - Packet loss = 100%
Unset	DOWN	02-01-2004 12:12:38	4d 0h 38m 53s	PING CRITICAL - Packet loss = 100%

Tactical Overview Of Nagios

The screenshot displays the Nagios web interface with the following components:

- Browser Address Bar:** `https://thuldai.mos.c.m.np/nagios/cgi-bin/tac.cgi`
- Passive Checks:** 0
- Network Outages:**
 - 1 Outages
 - 1 Blocking Outages
- Network Health:**
 - Host Health: OK
 - Service Health: OK
- Hosts:**

Hosts			
14 Down	0 Unreachable	156 Up	0 Pending

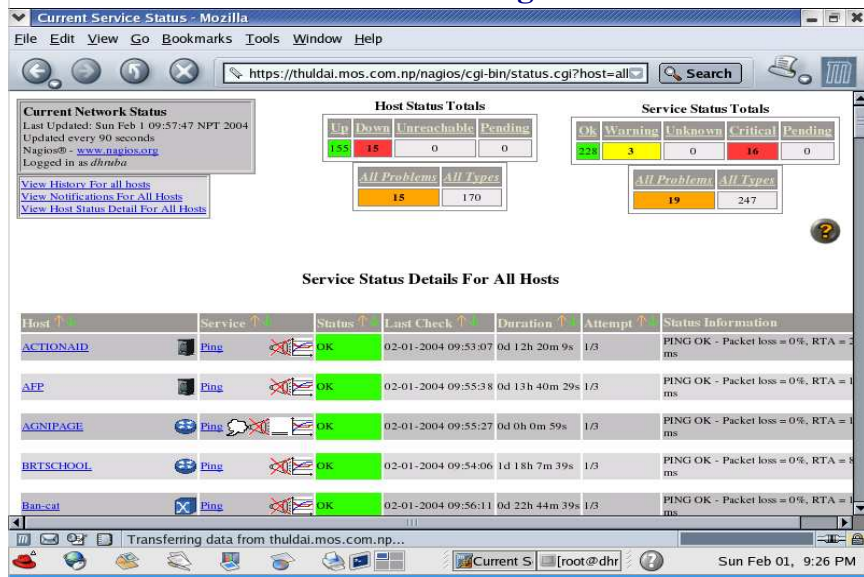
 - 14 Unhandled Problems
- Services:**

Services		
17 Critical	2 Warning	0 Unknown

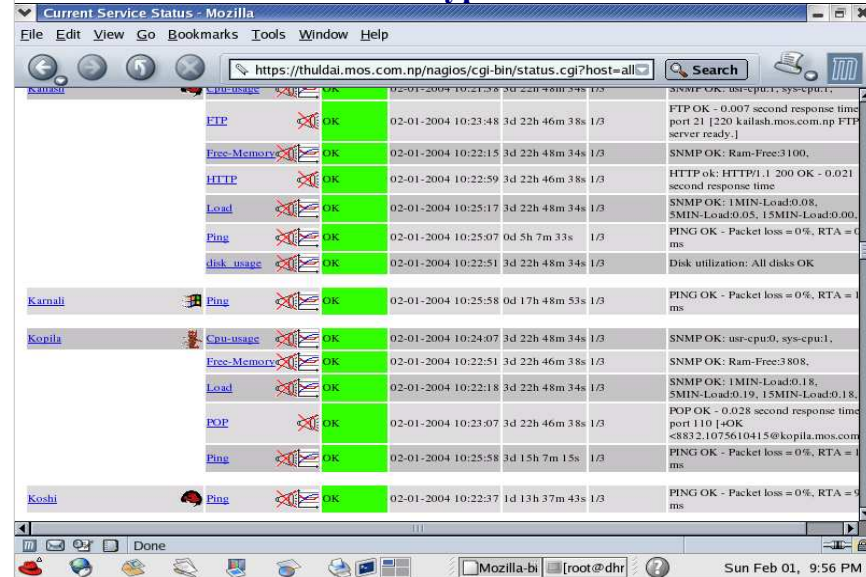
 - 2 Unhandled Problems
 - 14 on Problem Hosts
- Monitoring Features:**

Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
<div style="background-color: green; color: white; text-align: center;">Enabled</div> All Services Enabled 11 Services Warning All Hosts Enabled 3 Hosts Warning	<div style="background-color: red; color: white; text-align: center;">Disabled</div> 212 Services Disabled All Hosts Enabled	<div style="background-color: green; color: white; text-align: center;">Enabled</div> All Services Enabled All Hosts Enabled	<div style="background-color: green; color: white; text-align: center;">Enabled</div> All Services Enabled All Hosts Enabled	<div style="background-color: green; color: white; text-align: center;">Enabled</div> All Services Enabled

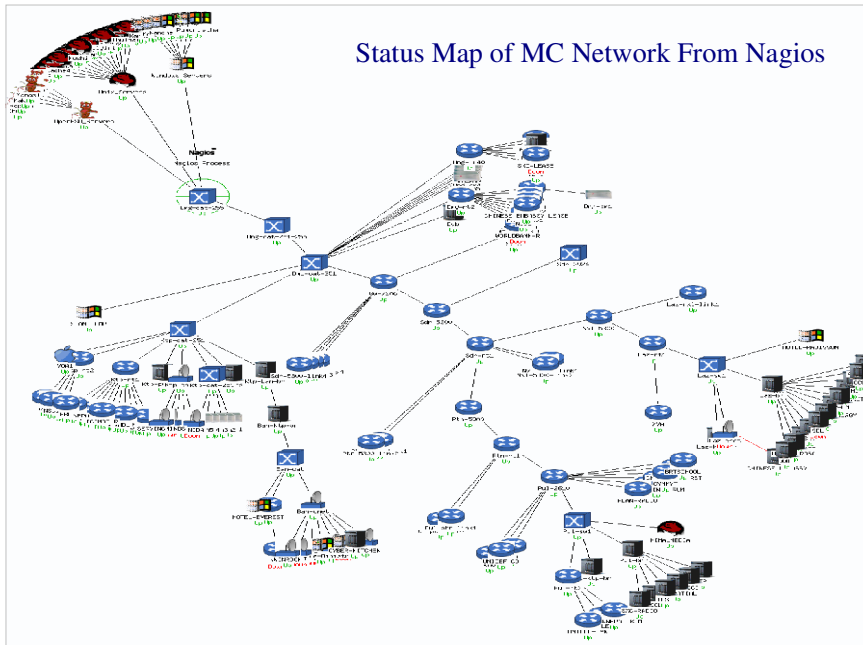
Service Detail of Nagios



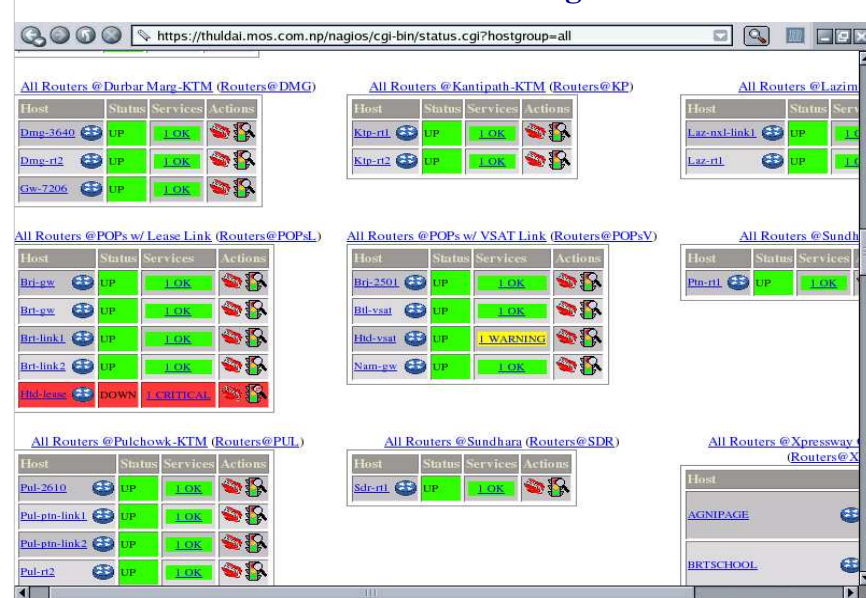
Service Types



Status Map of MC Network From Nagios



Status Overview from nagios



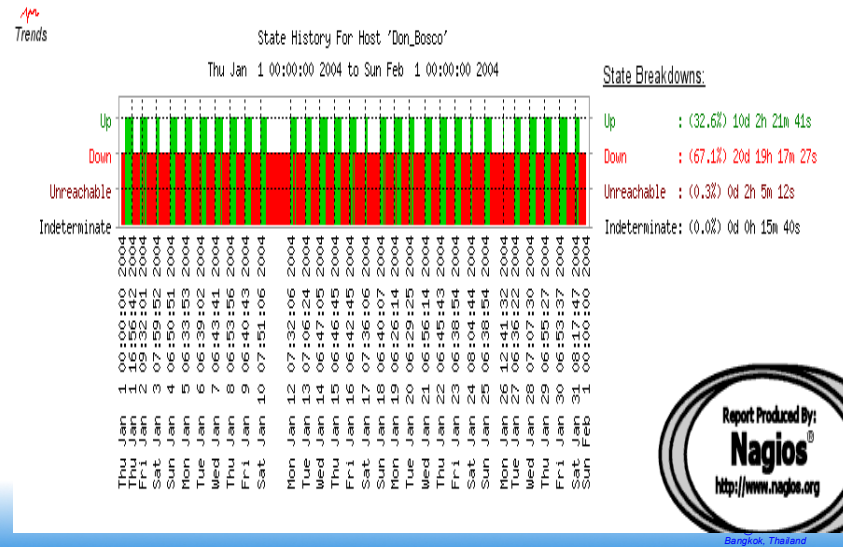
Status Summary Based On Hostgroup

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

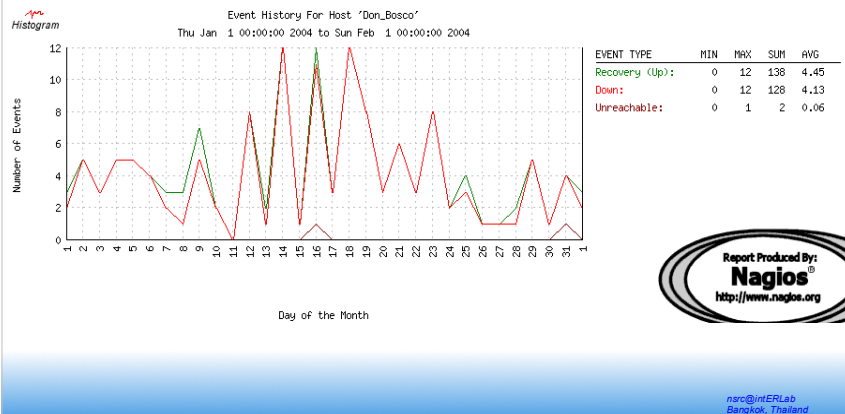
Status Summary For All Host Groups

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?

The screenshot shows the Nagios web interface at <https://thuldai.mos.com.np/nagios/cgi-bin/notifications.cgi?contact=all>. The page displays a list of contacts notified for a host down event. The table below is a representation of the data shown in the screenshot.

Host	Service	Type	Time	Contact	Notification Command	Information
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:12	Amod	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:12	Amod	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	DeepakA	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Krishna	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	NirajS	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Prabhu	host-notify-by-epager	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-epager	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	Amod	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Amod	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	DeepakA	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Krishna	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Prabhu	host-notify-by-epager	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-epager	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%

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
  
```

nsr@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

nsr@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

nsr@interLab
Bangkok, Thailand

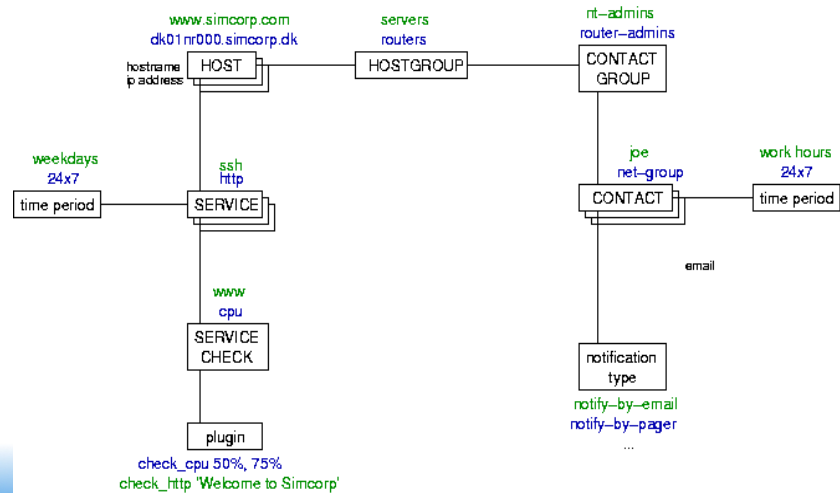
Nagios plugin configuration

• /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

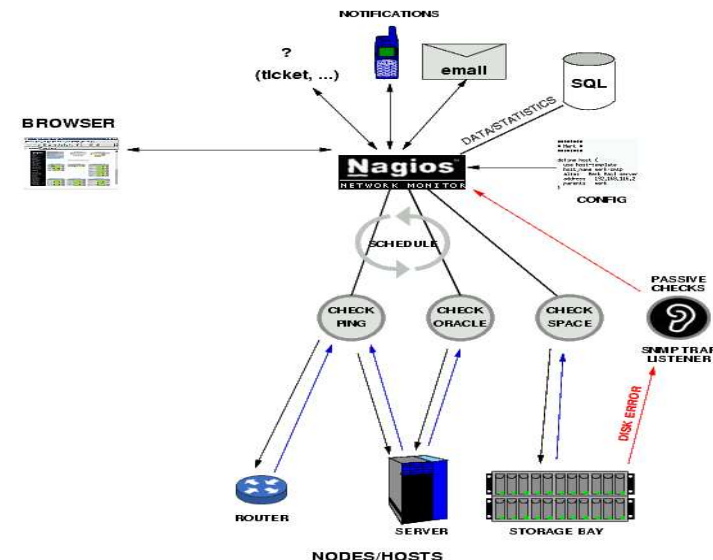


nsro@interLab
Bangkok, Thailand

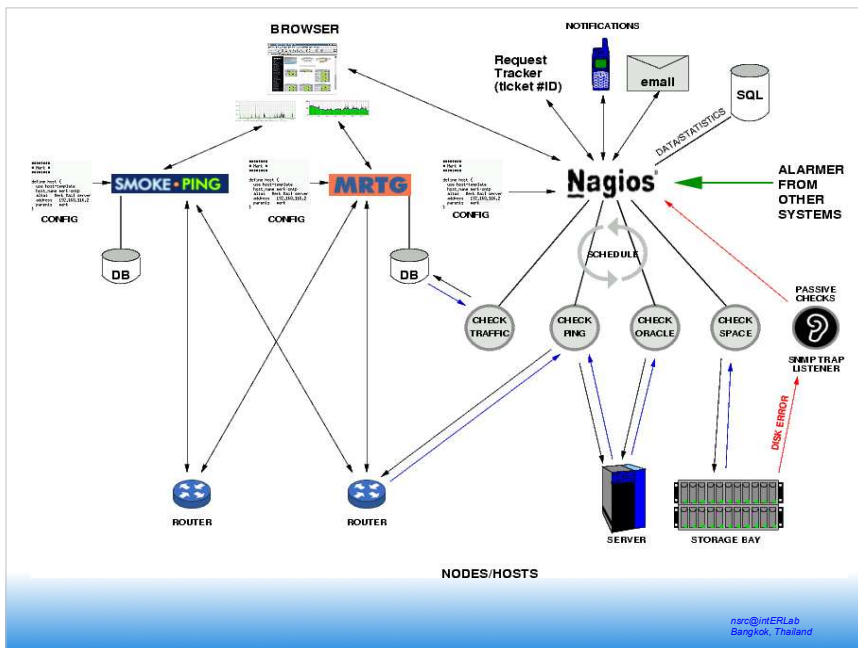
Concepts: parents

- 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/>

Questions?