An Introduction

Nagios®

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

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)

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
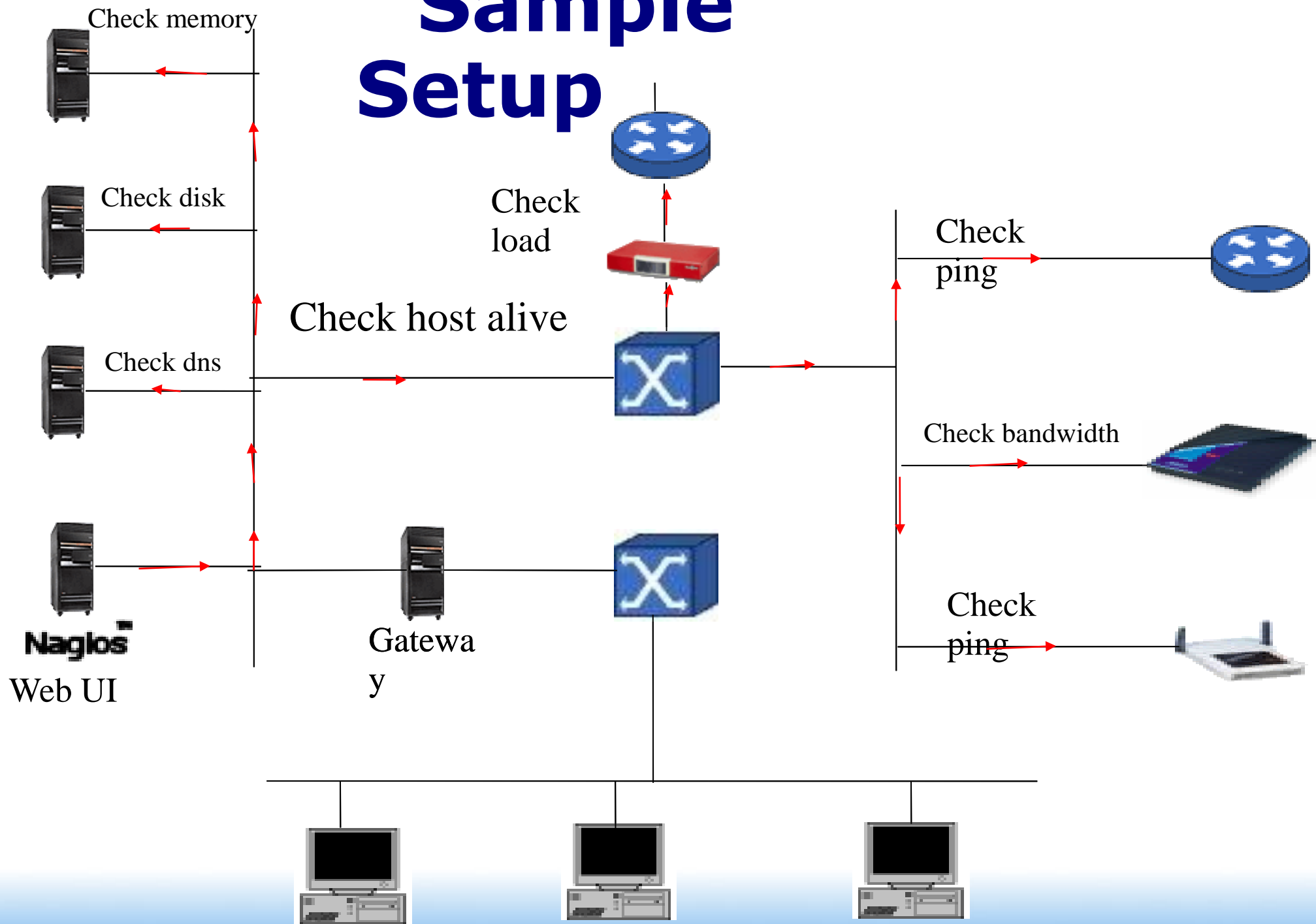
What Can it Do?

- 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
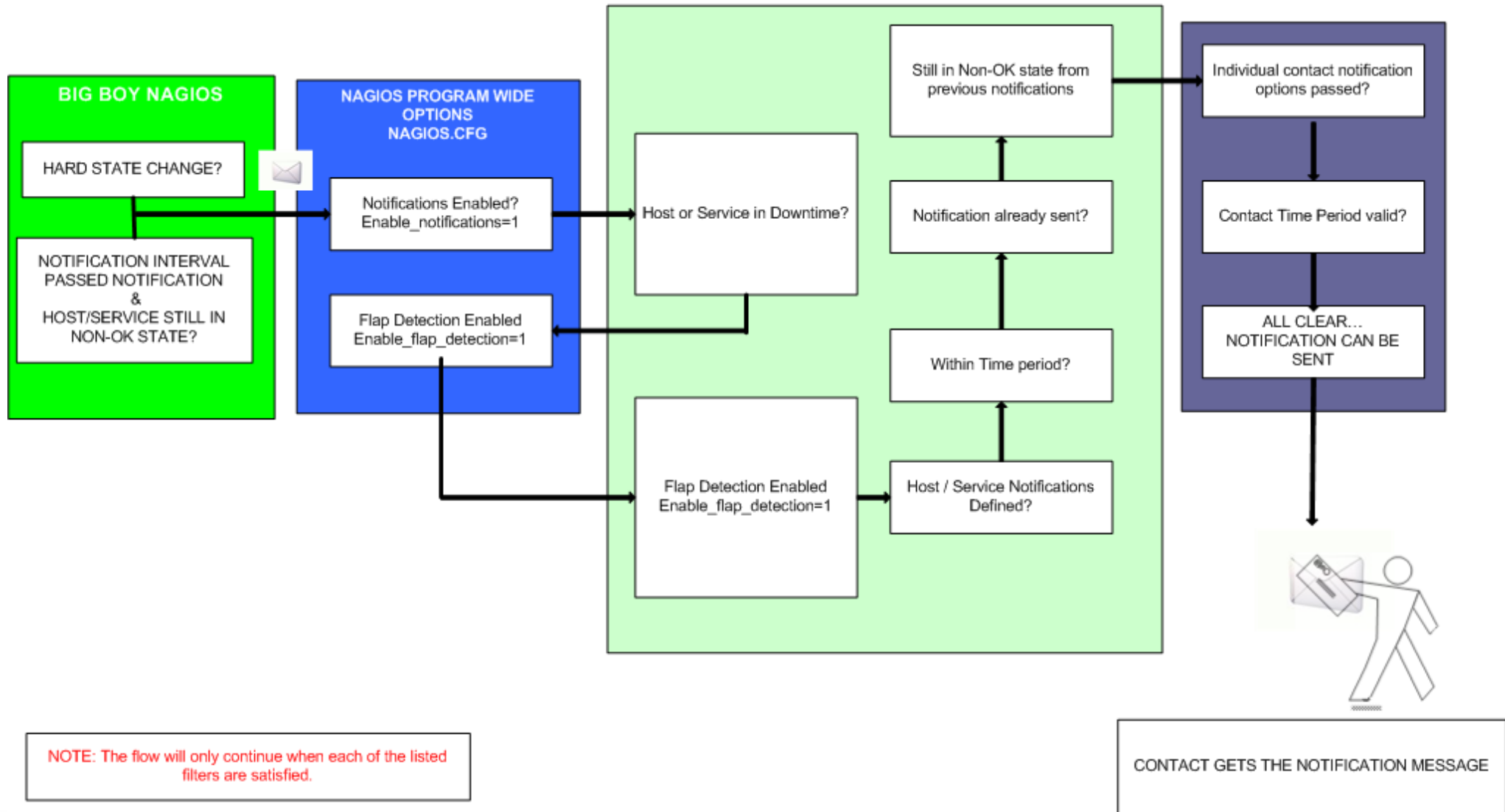
What Can it Do?

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
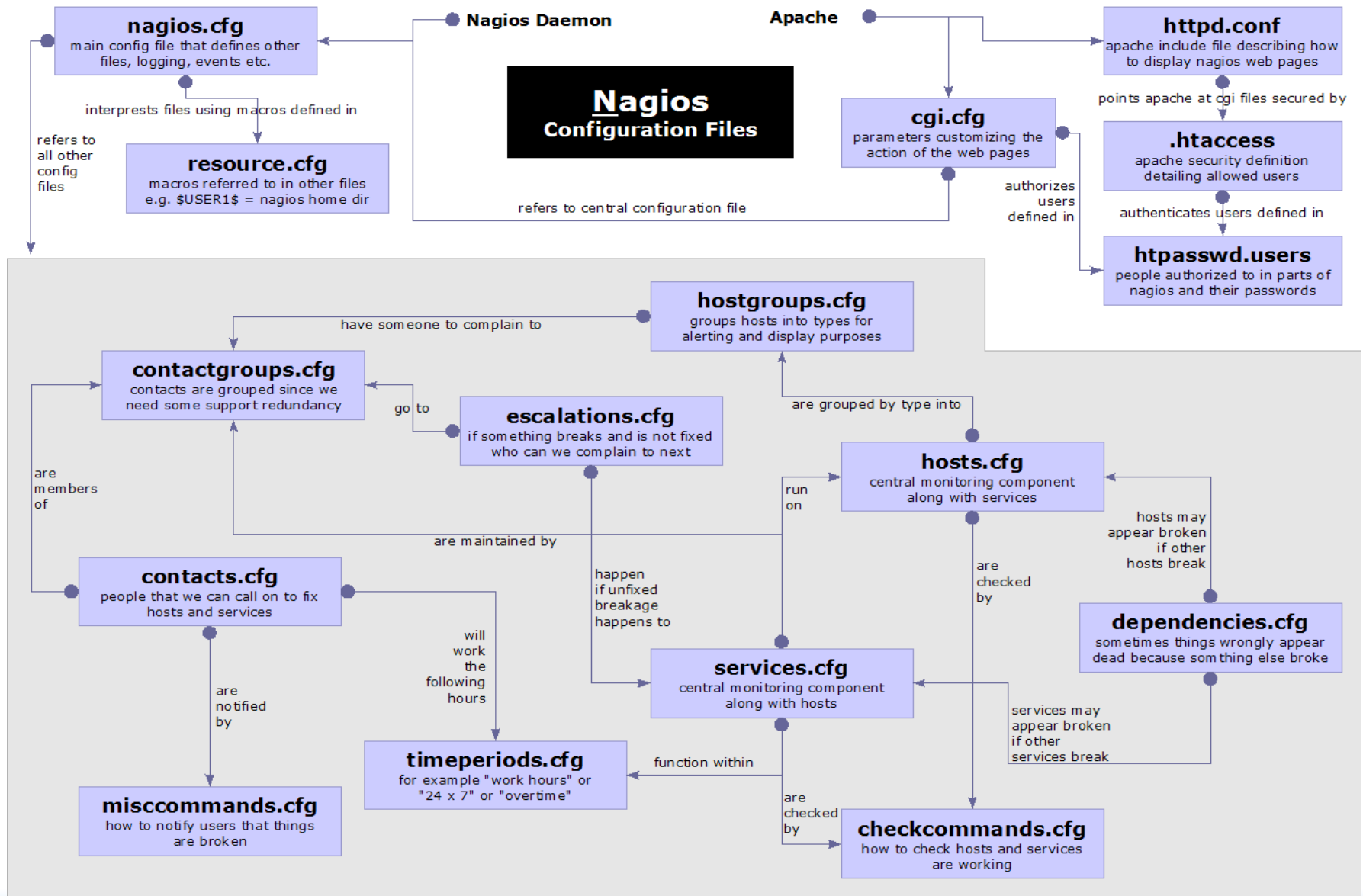
- Licensed under GPL v2

Sample Setup

Check memory

Check disk

Check host alive

Check dns

Check load

Check ping

Check bandwidth

Check ping

Web UI

Gateway

Web Client At NOC

NAGIOS - NOTIFICATION FLOW DIAGRAM

BIG BOY NAGIOS

HARD STATE CHANGE?

NOTIFICATION INTERVAL PASSED NOTIFICATION & HOST/SERVICE STILL IN NON-OK STATE?

NAGIOS PROGRAM WIDE OPTIONS NAGIOS.CFG

Notifications Enabled? Enable_notifications=1

Flap Detection Enabled Enable_flap_detection=1

Host or Service in Downtime?

Flap Detection Enabled Enable_flap_detection=1

Host / Service Notifications Defined?

Within Time period?

Notification already sent?

Still in Non-OK state from previous notifications

Individual contact notification options passed?

Contact Time Period valid?

ALL CLEAR... NOTIFICATION CAN BE SENT

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

CONTACT GETS THE NOTIFICATION MESSAGE

Nagios Configuration

Nagios Daemon

Apache

nagios.cfg
main config file that defines other files, logging, events etc.

httpd.conf
apache include file describing how to display nagios web pages

interprests files using macros defined in

points apache at cgi files secured by

refers to all other config files

resource.cfg
macros referred to in other files e.g. $USER1$ = nagios home dir

Nagios
Configuration Files

cgi.cfg
parameters customizing the action of the web pages

.htaccess
apache security definition detailing allowed users

refers to central configuration file

authenticates users defined in

authorizes users defined in

htpasswd.users
people authorized to in parts of nagios and their passwords

hostgroups.cfg
groups hosts into types for alerting and display purposes

have someone to complain to

contactgroups.cfg
contacts are grouped since we need some support redundancy

go to

are grouped by type into

escalations.cfg
if something breaks and is not fixed who can we complain to next

hosts.cfg
central monitoring component along with services

run on

are members of

are maintained by

hosts may appear broken if other hosts break

contacts.cfg
people that we can call on to fix hosts and services

happen if unfixed breakage happens to

are checked by

dependencies.cfg
sometimes things wrongly appear dead because somthing else broke

will work the following hours

are notified by

services.cfg
central monitoring component along with hosts

services may appear broken if other services break

timeperiods.cfg
for example "work hours" or "24 x 7" or "overtime"

function within

misccommands.cfg
how to notify users that things are broken

are checked by

checkcommands.cfg
how to check hosts and services are working

Nagios Status Detail screen

https://thuldai.mos.com.np/nagios/index.html

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 *dhruba*

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

Host Status Totals

Up	Down	Unreachable	Pending
155	15	0	0

All Problems	All Types
15	170

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
226	5	0	16	0

All Problems	All Types
21	247

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%
FNCCI		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%
Laz-cnet		DOWN	02-01-2004 12:12:38	4d 0h 38m 53s	PING CRITICAL - Packet loss =

Tactical Overview Of Nagios

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

Passive Checks: 0

Network Outages

1 Outages

1 Blocking Outages

Network Health

Host Health:

Service Health:

Hosts

14 Down	0 Unreachable	156 Up	0 Pending

14 Unhandled Problems

Services

17 Critical	2 Warning	0 Unknown	22 O

3 Unhandled Problems

2 Unhandled Problems

14 on Problem Hosts

Monitoring Features

Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
Enabled	Enabled	Enabled	Enabled	Enabled
All Services Enabled	247 Services Disabled	All Services Enabled	All Services Enabled	All Services Enabled
11 Services Flapping	All Hosts Enabled	All Hosts Enabled	All Hosts Enabled	
All Hosts Enabled				
3 Hosts Flapping				

Service Detail of Nagios

Service Types

File   Edit   View   Go   Bookmarks   Tools   Window   Help

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

Kailash		Cpu-usage		OK	02-01-2004 10:21:58	3d 22h 48m 34s 1/3	SNMP OK: usr-cpu:1, sys-cpu:1,
		FTP		OK	02-01-2004 10:23:48	3d 22h 46m 38s 1/3	FTP OK - 0.007 second response time on port 21 [220 kailash.mos.com.np FTP server ready.]
		Free-Memory		OK	02-01-2004 10:22:15	3d 22h 48m 34s 1/3	SNMP OK: Ram-Free:3100,
		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
		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,
		Ping		OK	02-01-2004 10:25:07	0d 5h 7m 33s 1/3	PING OK - Packet loss = 0%, RTA = 0 ms
		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,
		Free-Memory		OK	02-01-2004 10:22:51	3d 22h 46m 38s 1/3	SNMP OK: Ram-Free:3808,
		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,
		POP		OK	02-01-2004 10:23:07	3d 22h 46m 38s 1/3	POP OK - 0.028 second response time on port 110 [+OK <8832.1075610415@kopila.mos.com
		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
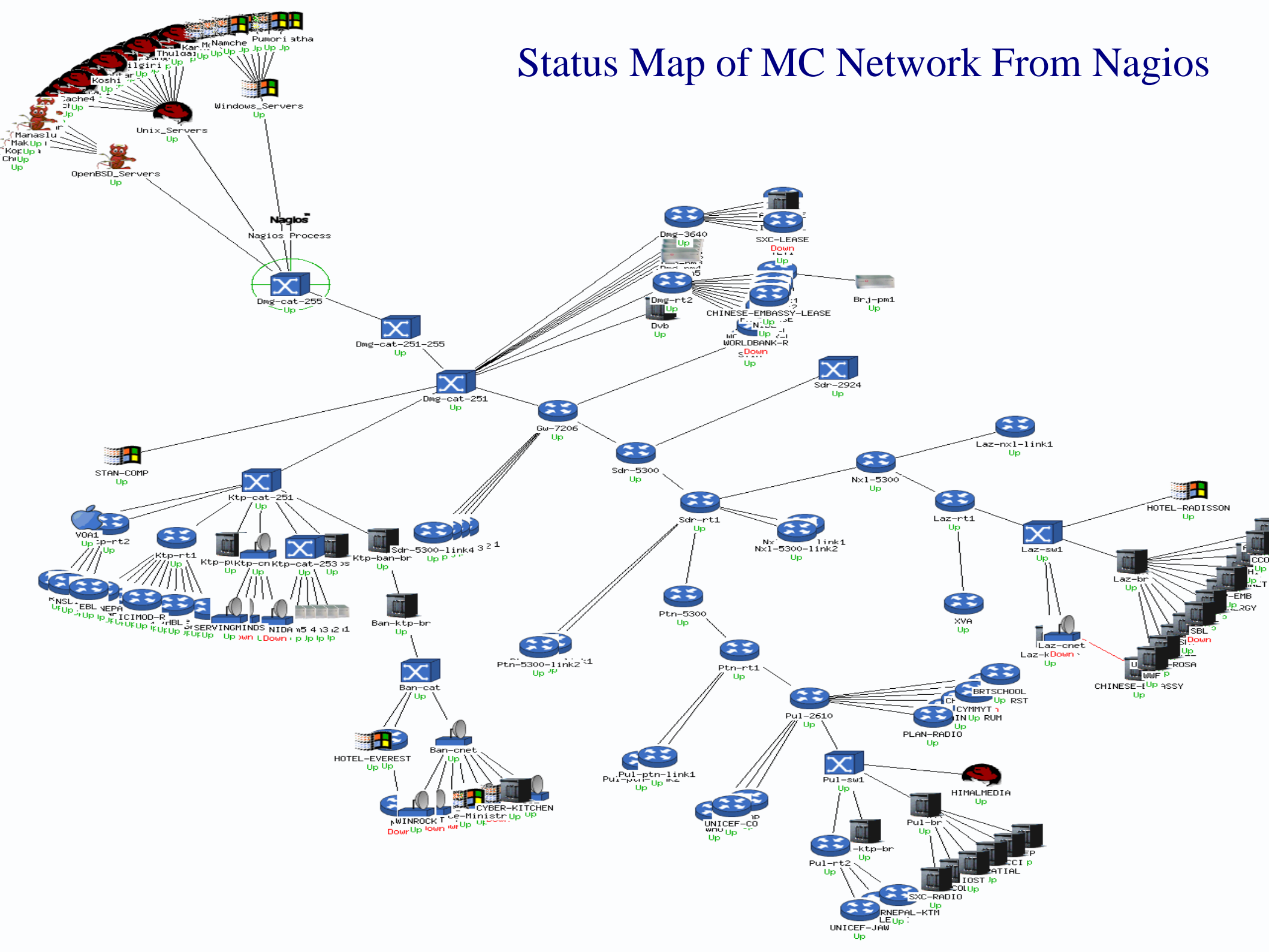
Status Overview from nagios

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

Host	Status	Services	Actions
Dmg-3640	UP	1 OK	
Dmg-rt2	UP	1 OK	
Gw-7206	UP	1 OK	

All Routers @Kantipath-KTM (Routers@KP)

Host	Status	Services	Actions
Ktp-rt1	UP	1 OK	
Ktp-rt2	UP	1 OK	

All Routers @Lazim

Host	Status	Serv
Laz-nxl-link1	UP	1 O
Laz-rt1	UP	1 O

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

Host	Status	Services	Actions
Brj-gw	UP	1 OK	
Brt-gw	UP	1 OK	
Brt-link1	UP	1 OK	
Brt-link2	UP	1 OK	
Htd-lease	DOWN	1 CRITICAL	

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

Host	Status	Services	Actions
Brj-2501	UP	1 OK	
Btl-vsat	UP	1 OK	
Htd-vsat	UP	1 WARNING	
Nam-gw	UP	1 OK	

All Routers @Sundh

Host	Status	Services
Ptn-rt1	UP	1 OK

All Routers @Pulchowk-KTM (Routers@PUL)

Host	Status	Services	Actions
Pul-2610	UP	1 OK	
Pul-ptn-link1	UP	1 OK	
Pul-ptn-link2	UP	1 OK	
Pul-rt2	UP	1 OK	

All Routers @Sundhara (Routers@SDR)

Host	Status	Services	Actions
Sdr-rt1	UP	1 OK	

All Routers @Xpressway (Routers@X

Host
AGNIPAGE
BRTSCHOOL

Status Summary Based On Hostgroup

Status Summary For All Host Groups

Host Group	Host Status Totals	Service Status Totals
Access Servers@KTM (AS@KTM)	11 UP	11 OK
All Brouters @KTM (Brouters@KTM)	7 UP	7 OK
All Routers @MIX Customers w/ Radio Link (Brouters@MIXR)	1 UP	1 OK
All Brouters @Xprewway Customers w/ Radio Link (Brouters@XpresswayR)	19 UP / 1 DOWN	19 OK / 1 CRITICAL
All Brouters @Xprewway Customers w/ Radio Link (Cnet_Clients@XpresswayR)	6 UP / 4 DOWN	5 OK / 5 CRITICAL
All Cnets @KTM (Cnets@KTM)	2 UP / 1 DOWN	2 OK / 1 CRITICAL
All Co-located Servers (Co-locators)	2 UP	2 OK
Ipricot 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 @Baneshor (Routers@BAN)	1 UP	1 OK
All Routers @Durbar Marg-KTM (Routers@DMG)	3 UP	3 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@POPsL)	4 UP / 1 DOWN	4 OK / 1 CRITICAL

Host Trends or Status History

State History For Host 'Don_Bosco'

Thu Jan 1 00:00:00 2004 to Sun Feb 1 00:00:00 2004
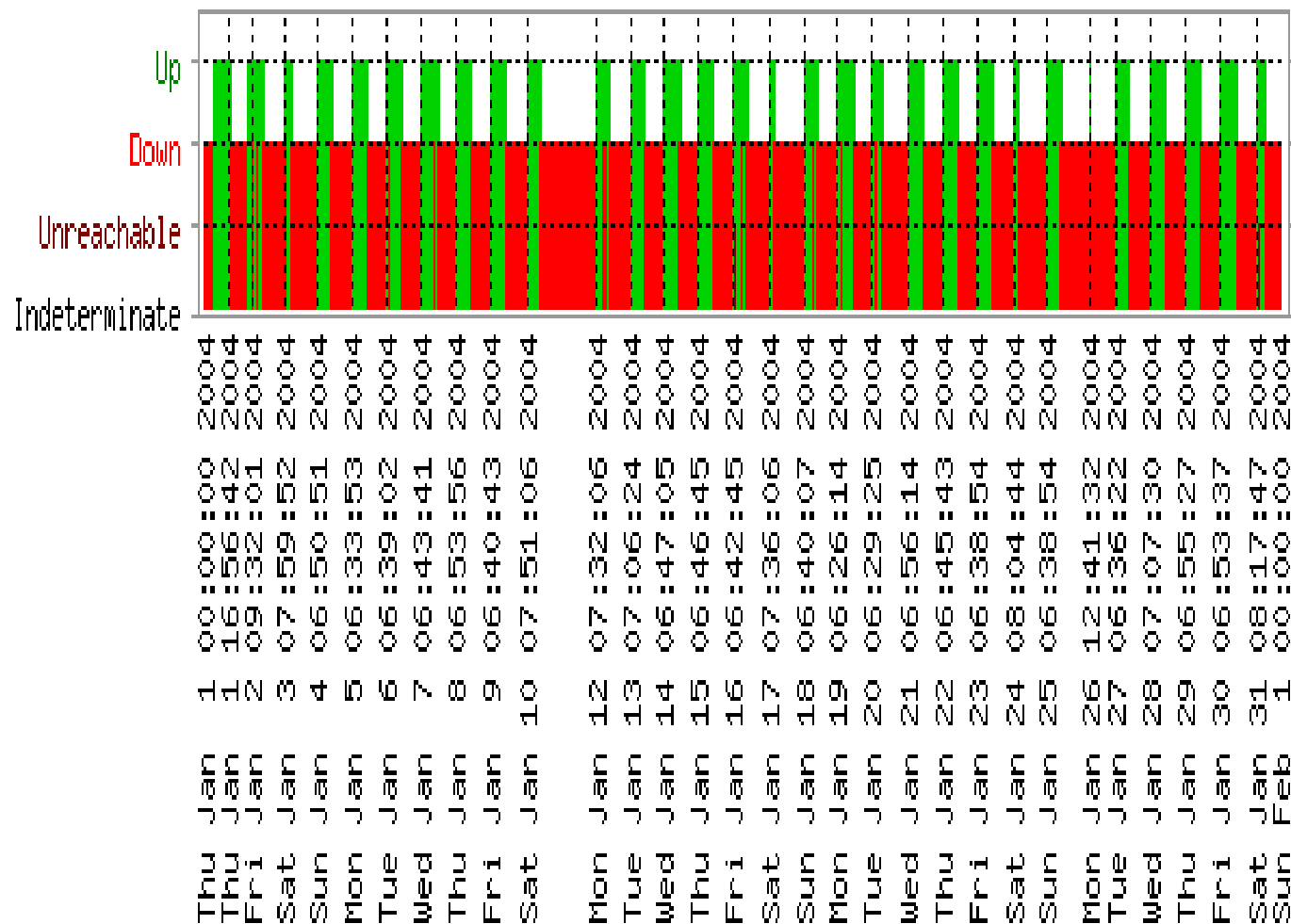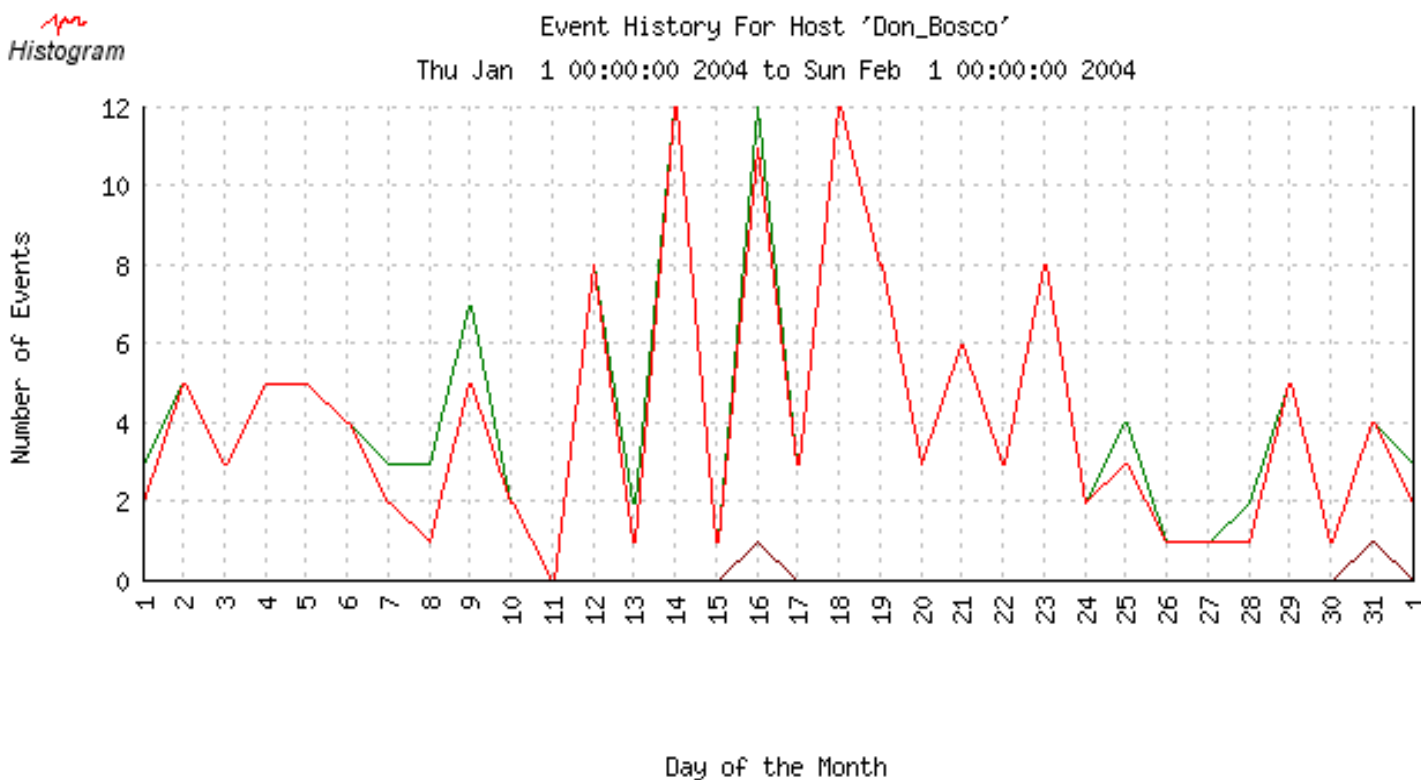
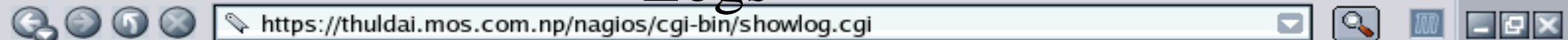State Breakdowns:

Up   : (32.6%) 10d 2h 21m 41s

Down   : (67.1%) 20d 19h 17m 27s

Unreachable : (0.3%) 0d 2h 5m 12s

Indeterminate: (0.0%) 0d 0h 15m 40s

Histogram Of Host

Event History For Host 'Don_Bosco'
Thu Jan 1 00:00:00 2004 to Sun Feb 1 00:00:00 2004

EVENT TYPE	MIN	MAX	SUM	AVG
Recovery (Up):	0	12	138	4.45
Down:	0	12	128	4.13
Unreachable:	0	1	2	0.06

Event Logs

URL: 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*

Latest Archive

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

☐ **Older Entries First:**
Update

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 12:14:27] 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;1;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: Htd-vsat;Ping;WARNING;HARD;3;PING WARNING - Packet loss = 40%, RTA = 674.22 ms

[02-01-2004 12:10:26] SERVICE ALERT: Htd-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;Htd-lease;UP;host-notify-by-email;PING OK - Packet loss = 30%, RTA = 357.24 ms

[02-01-2004 12:08:48] HOST NOTIFICATION: Ishwar;Htd-lease;UP;host-notify-by-email;PING OK - Packet loss = 30%, RTA = 357.24 ms

[02-01-2004 12:08:48] HOST NOTIFICATION: Kedar;Htd-lease;UP;host-notify-by-epager;PING OK - Packet loss = 30%, RTA = 357.24 ms

[02-01-2004 12:08:48] HOST NOTIFICATION: MSurya;Htd-lease;UP;host-notify-by-email;PING OK - Packet loss = 30%, RTA = 357.24 ms

Who is Notified?

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

All Contacts

Latest Archive

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

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

Notification detail level for all contacts:

All notifications

Older Entries First:

Update

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%
Htd-lease	N/A	HOST DOWN	02-01-2004 10:56:06	Gyanu	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Htd-lease	N/A	HOST DOWN	02-01-2004 10:56:06	Ishwar	host-notify-by-email	PING CRITICAL - Packet loss = 100%

nautil | Mozil | [root | 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

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

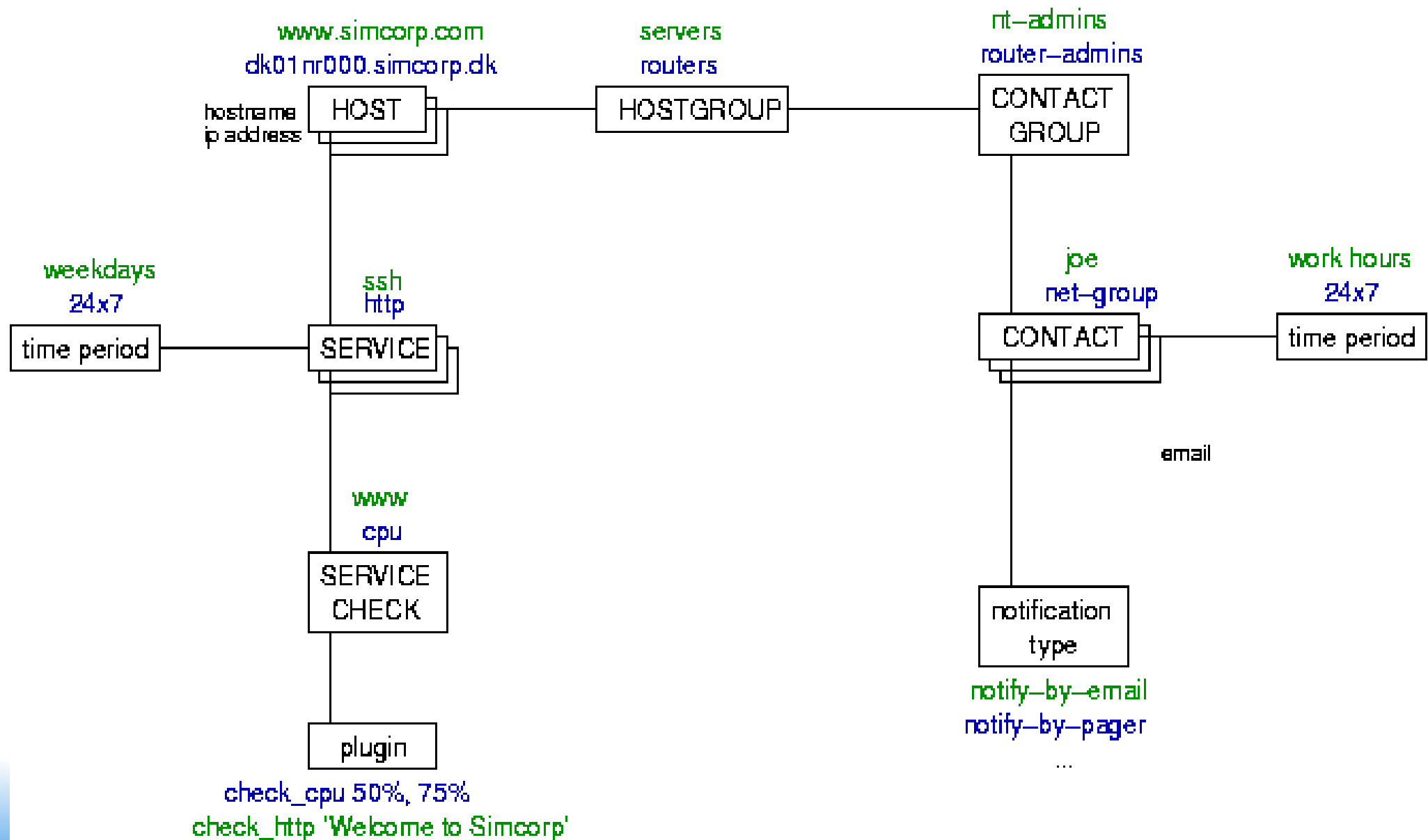# Nagios configuration files

- 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

Nagios plugin configuration

- /etc/nagios-plugins/config/

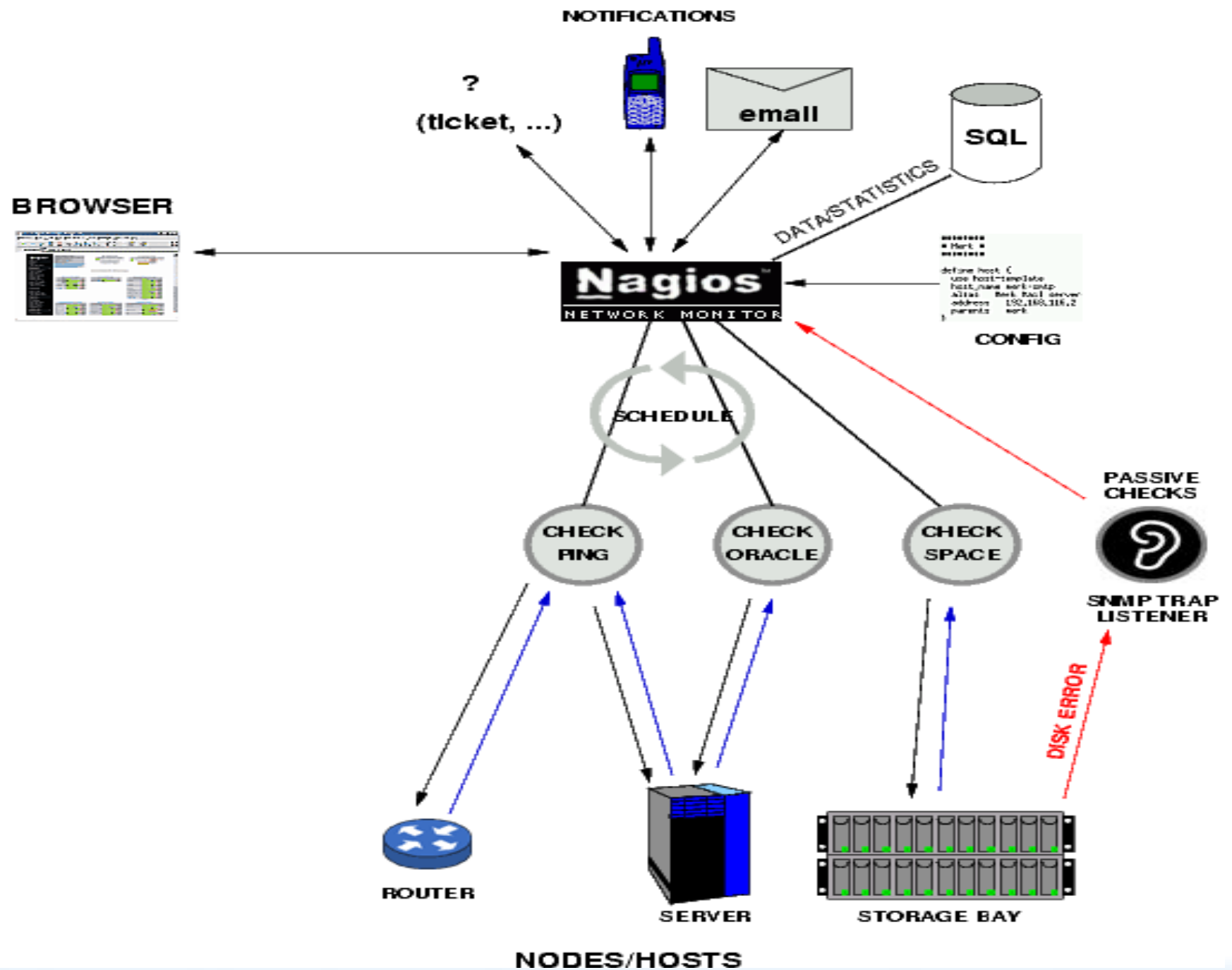apt.cfg   ntp.cfg   dhcp.cfg   ping.cfg

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

NAGIOS schema

www.simcorp.com
dk01nr000.simcorp.dk

HOST

hostname
ip address

servers
routers

HOSTGROUP

nt-admins
router-admins

CONTACT
GROUP

weekdays
24x7

time period

ssh
http

SERVICE

joe
net-group

CONTACT

work hours
24x7

time period

email

www
cpu

SERVICE
CHECK

notification
type

plugin

check_cpu 50%, 75%
check_http 'Welcome to Simcorp'

notify-by-email
notify-by-pager

...

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...

BROWSER

NOTIFICATIONS

Request Tracker (ticket #ID)

email

SQL

SMOKE·PING

CONFIG

MRTG

CONFIG

CONFIG

Nagios®

DATA/STATISTICS

ALARMER FROM OTHER SYSTEMS

DB

DB

SCHEDULE

CHECK TRAFFIC

CHECK PING

CHECK ORACLE

CHECK SPACE

PASSIVE CHECKS

SNMP TRAP LISTENER

DISK ERROR

ROUTER

ROUTER

SERVER

STORAGE BAY

NODES/HOSTS

nsrc@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?