



Nagios - introduction

Dhruba Raj Bhandari
(CCNA)

Additions by Phil Regnault

bhandari.dhruba@scp.com.np

Why Nagios?

- Open source
- Relatively scaleable, 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

What one can check

– 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?

Associated node status

Nagios Features

- Nagios
 - host and service monitor designed to inform you of network problems before your clients, end-users or managers do ;
 - Designed to run under the UNIX (Linux, *BSD, Solaris, ...)
 - Monitoring daemon runs intermittent checks on hosts and services
 - uses external "plugins" which return status information to Nagios
 - when problems are encountered, the daemon can send notifications out to administrative contacts in a variety of different ways (email, instant message, SMS, etc.)
 - current status information, historical logs, and reports can all be accessed via a web browser

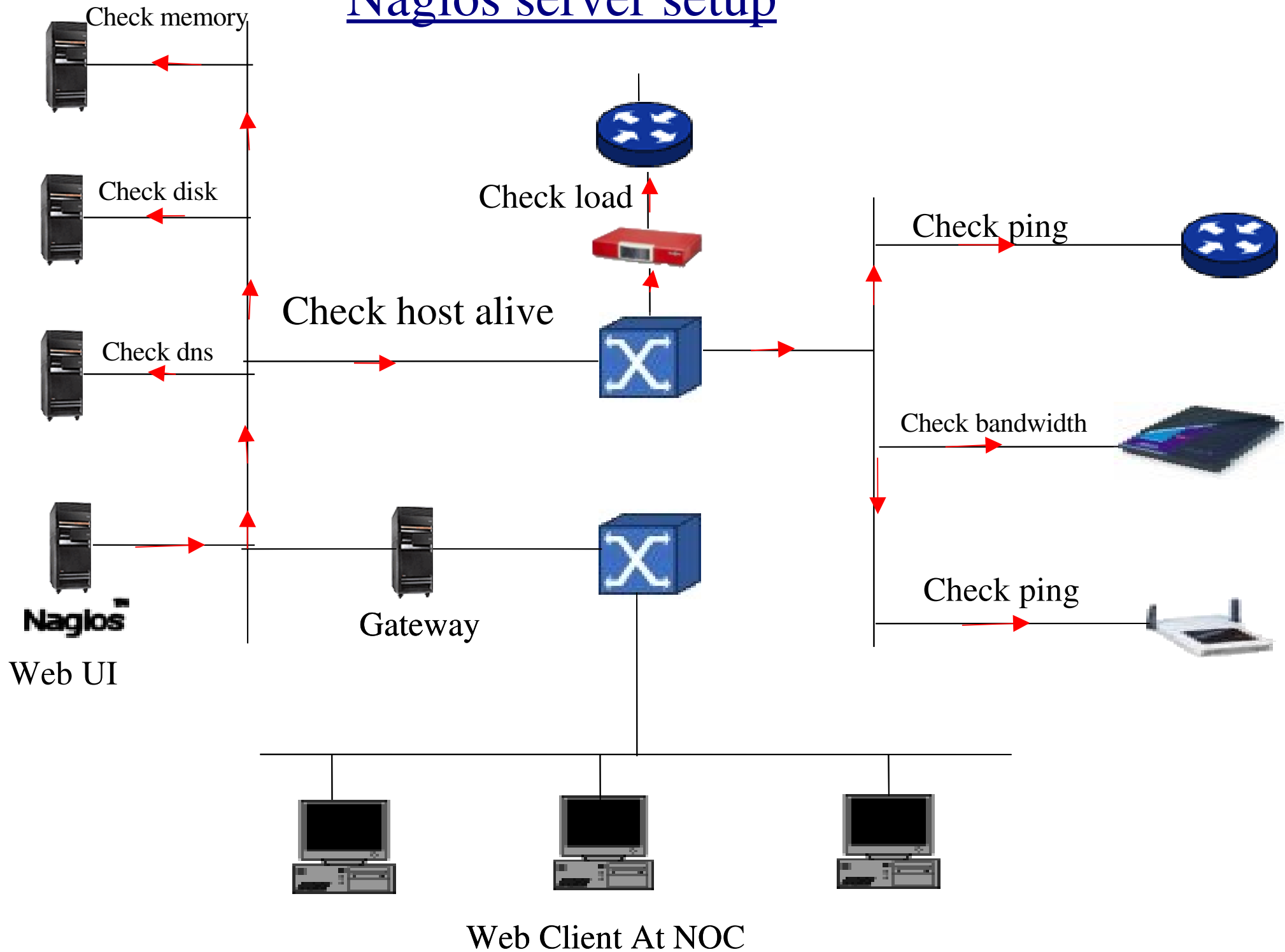
Nagios® is licensed under the terms of the GNU General Public

Features contd.

- Monitoring of network services (SMTP, POP3, HTTP, NNTP, PING, etc.)
- Monitoring of host resources (CPU load, disk and mem usage, etc.)
- Monitoring of environment / temperature
- Simple plugin design that allows users to easily develop their own host and service checks
- Ability to define network host hierarchy, allowing detection of and distinction between hosts that are down and those that are unreachable
- Contact notifications when service or host problems occur and get resolved (via email, pager, or other user-defined method)
- Optional escalation of host and service notifications to different contact groups
- Support for implementing redundant and distributed monitoring servers
- Retention of host and service status across program restarts
- Ability to acknowledge problems via the web interface
- Web interface for viewing current network status, notification and problem history, log file, etc

Simple authorization scheme that allows you restrict what users can see and do

Nagios server setup



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
----	-----

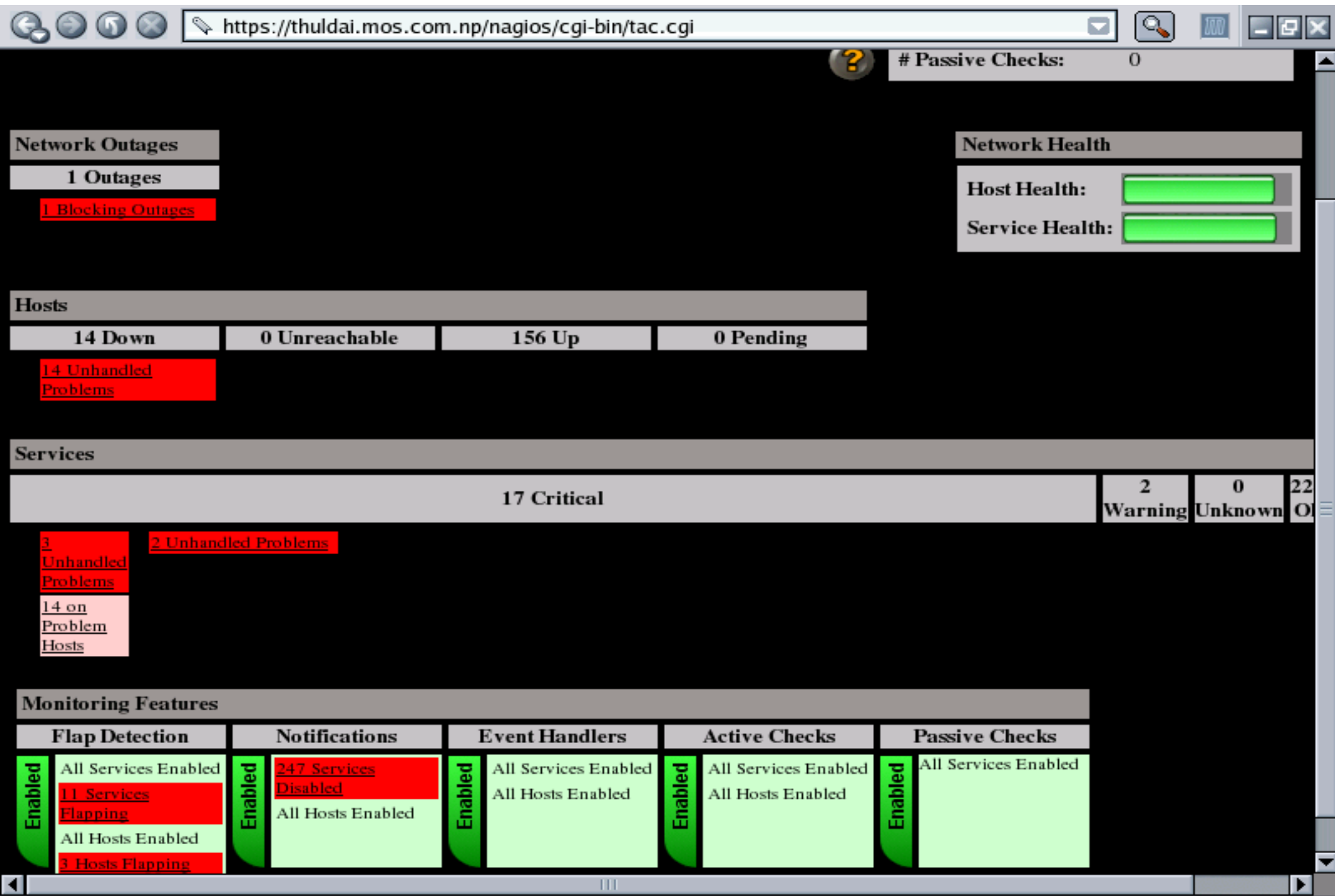
Display Filters:

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 = 100%

Tactical Overview Of Nagios



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>

Search

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	All Types
15	170

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
228	3	0	16	0

All Problems	All Types
19	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 = 2ms
AFP	Ping	OK	02-01-2004 09:55:38	0d 13h 40m 29s	1/3	PING OK - Packet loss = 0%, RTA = 1ms
AGNIPAGE	Ping	OK	02-01-2004 09:55:27	0d 0h 0m 59s	1/3	PING OK - Packet loss = 0%, RTA = 1ms
BRTSCHOOL	Ping	OK	02-01-2004 09:54:06	1d 18h 7m 39s	1/3	PING OK - Packet loss = 0%, RTA = 8ms
Ban-cat	Ping	OK	02-01-2004 09:56:11	0d 22h 44m 39s	1/3	PING OK - Packet loss = 0%, RTA = 1ms

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 Search

Host	Service	Status	Time	Uptime	Version	Output
Kailash	Cpu-usage	OK	02-01-2004 10:21:38	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 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 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 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	Services
Laz-nx1-link1	UP	1 OK
Laz-rt1	UP	1 OK

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

Host	Status	Services	Actions
Bri-gw	UP	1 OK	   
Bri-gw	UP	1 OK	   
Bri-link1	UP	1 OK	   
Bri-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-vsai	UP	1 OK	   
Htd-vsai	UP	1 WARNING	   
Nam-gw	UP	1 OK	   

All Routers @Sundhara

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

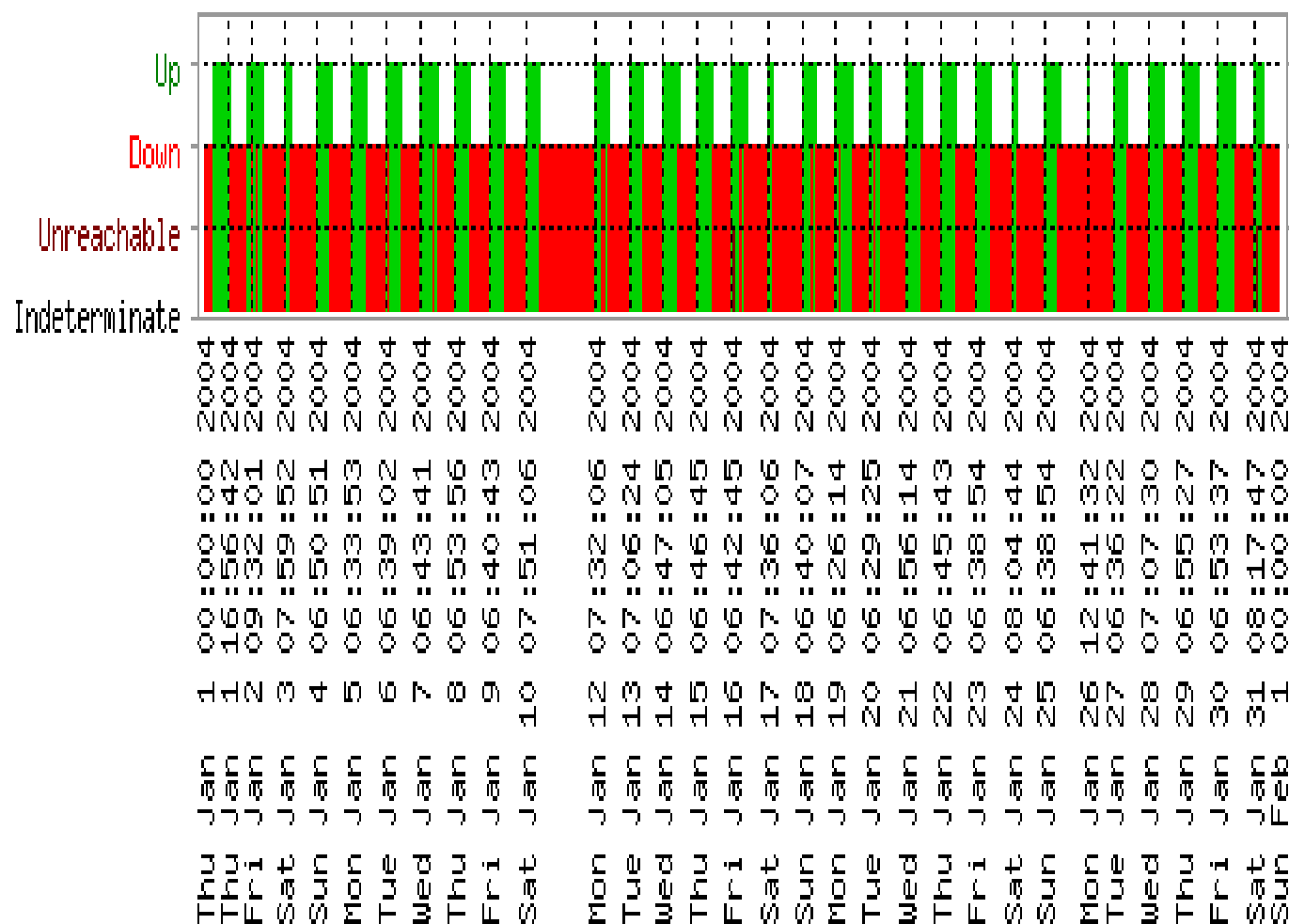
https://thuldai.mos.com.np/nagios/cgi-bin/status.cgi?hostgroup=all&style=summary		
Status Summary For All Host Groups		
Host Group	Host Status Totals	Service Status Totals
Access Servers@KTM (AS@KTM)	11 UP	11 OK
All Routers @KTM (Routers@KTM)	7 UP	7 OK
All Routers @MIX Customers w/ Radio Link (Routers@MIXR)	1 UP	1 OK
All Routers @Xpreway Customers w/ Radio Link (Routers@XprewayR)	19 UP 1 DOWN	19 OK 1 CRITICAL
All Routers @Xpreway Customers w/ Radio Link (Cnet Clients@XprewayR)	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

Apex
Trends

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

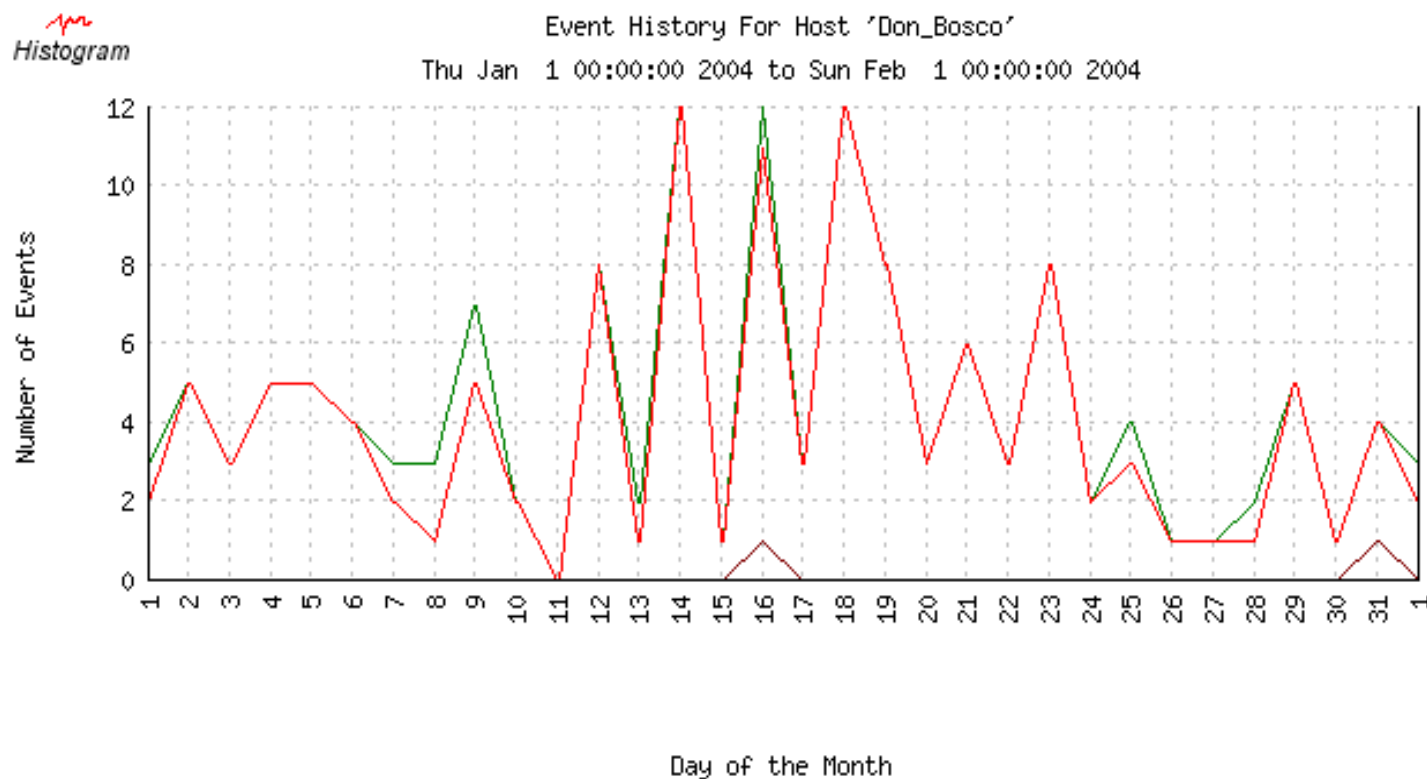
Down : (67.1%) 20d 19h 17m 27s

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

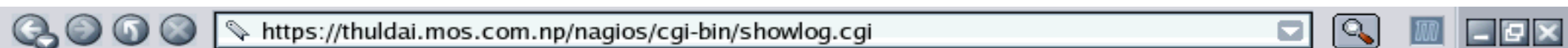
Indeterminate: (0.0%) 0d 0h 15m 40s



Histogram Of Host



Event Logs



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-vsate;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?

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 *dhruba*

All Contacts

Log File Navigation

Sun Feb 1 00:00:00
NPT 2004
to
Present..

Latest
Archive



Notification detail level for all contacts:

All notifications

Older Entries First:



Update



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	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

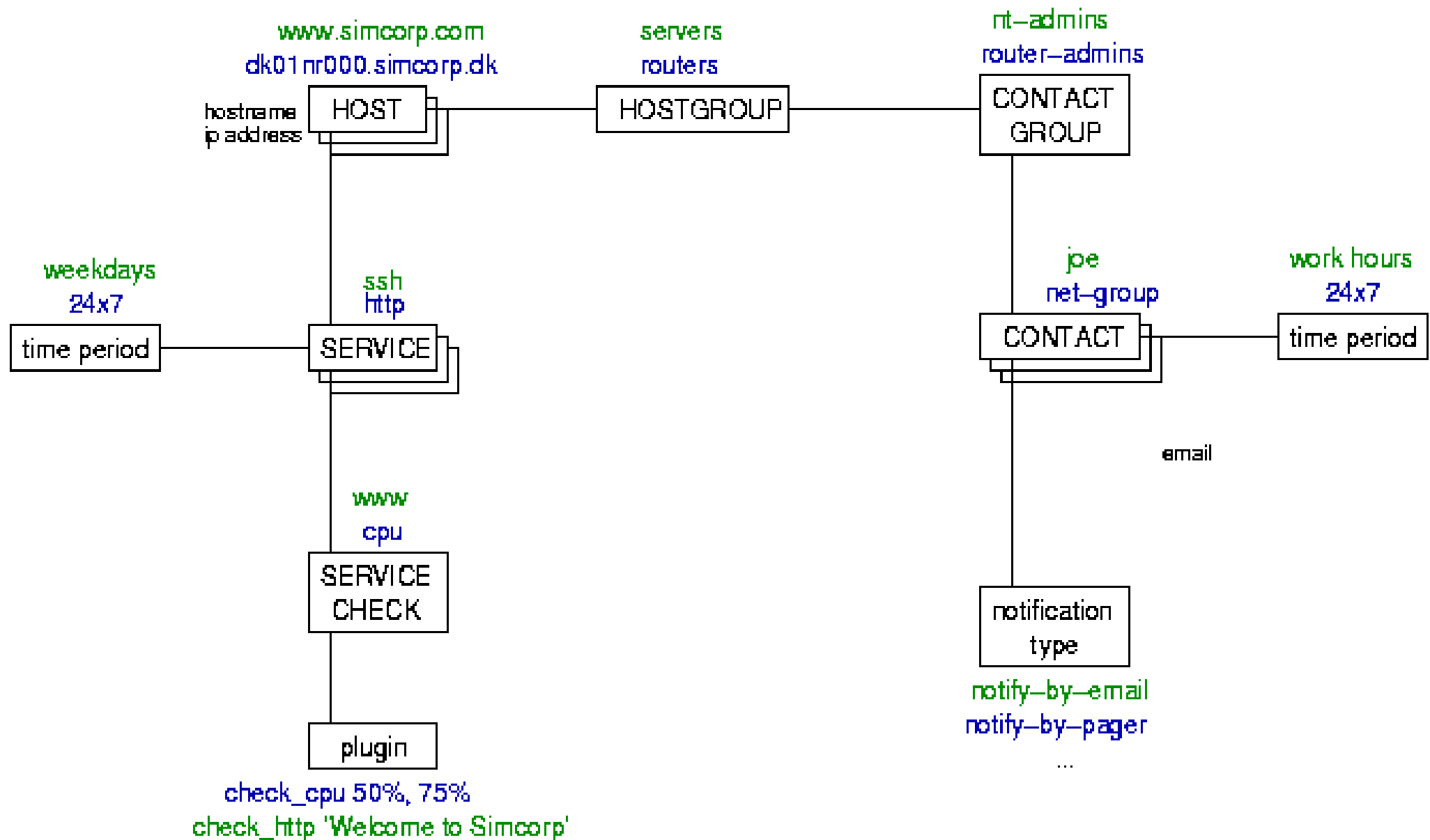
Nagios plugin configuration

- /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 configuration walkthrough

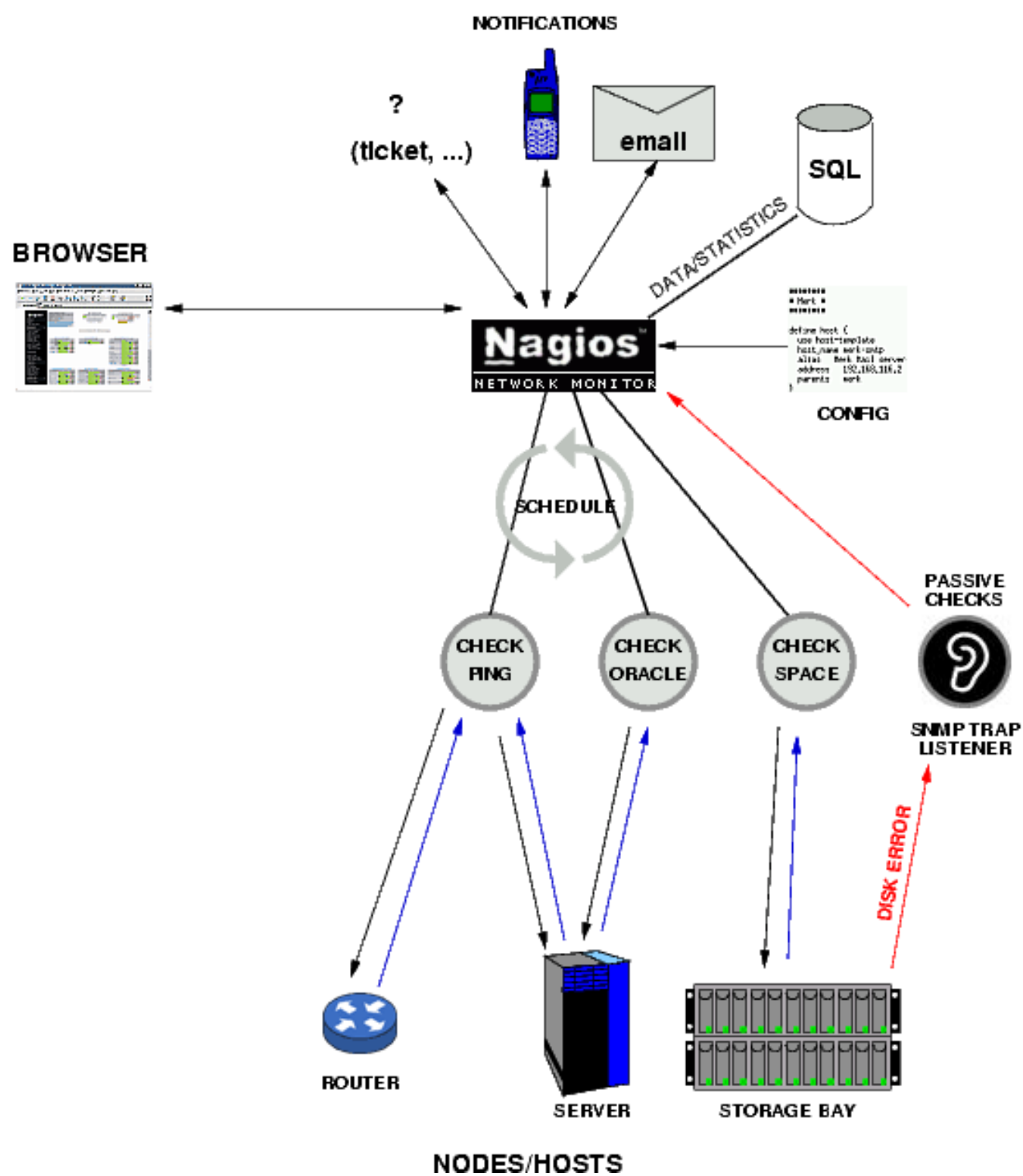
- Let's review the configuration files...

NAGIOS schema

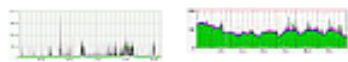


Concepts: parents

- 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...

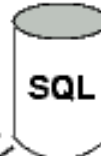


BROWSER



NOTIFICATIONS

Request Tracker
(ticket #ID)



DATA/STATISTICS

ALARMER
FROM
OTHER
SYSTEMS

Nagios

SCHEDULE

PASSIVE CHECKS



SNMP TRAP
LISTENER

DISK ERROR



SERVER



STORAGE BAY

NODES/HOSTS

SMOKE • PING

MRTG

CHECK
TRAFFIC

CHECK
PING

CHECK
ORACLE

CHECK
SPACE

ROUTER

ROUTER



```
define host {
  use host-template
  host_name work-smp
  alias    Real Pail server
  address  192.168.118.2
  parents  work
}
```

CONFIG

```
define host {
  use host-template
  host_name work-smp
  alias    Real Pail server
  address  192.168.118.2
  parents  work
}
```

CONFIG

```
define host {
  use host-template
  host_name work-smp
  alias    Real Pail server
  address  192.168.118.2
  parents  work
}
```

CONFIG

Questions?