



Advanced Registry Operations Curriculum

NAGIOS



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license (<http://creativecommons.org/licenses/by-nc/3.0/>) as part of the ICANN, ISOC and NSRC Registry Operations Curriculum.

Introduction

- A key measurement tool for actively monitoring availability of devices and services.
- Possible the most used open source network monitoring software.
- Has a web interface.
 - Uses CGIs written in C for faster response and scalability.
- Can support up to thousands of devices and services.

Installation

In Debian/Ubuntu

```
# apt-get install nagios3
```

- Files are installed here:

```
/etc/nagios3
```

```
/etc/nagios3/conf.d
```

```
/etc/nagios-plugins/conf
```

```
/usr/share/nagios3/htdocs/images/logos
```

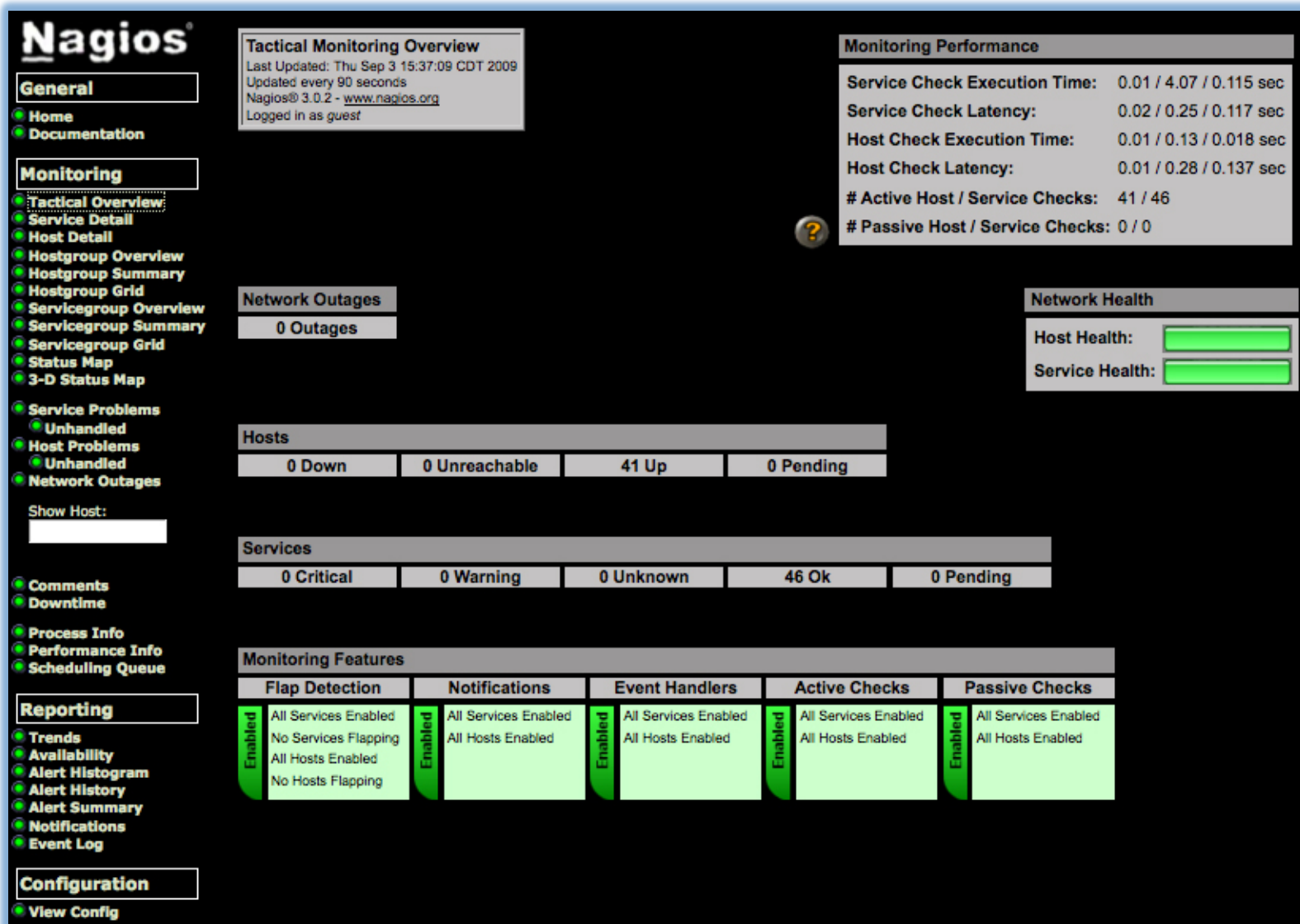
```
/usr/sbin/nagios3
```

```
/usr/sbin/nagios3stats
```

Nagios web interface is here:

<http://localhost/nagios3/>

General View



The screenshot displays the Nagios web interface's 'General View'. On the left is a vertical navigation menu with categories: 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), Reporting (Trends, Availability, Alert Histogram, Alert History, Alert Summary, Notifications, Event Log), and Configuration (View Config). The main content area is divided into several sections: 1. Tactical Monitoring Overview: Shows the last update time (Thu Sep 3 15:37:09 CDT 2009), update frequency (every 90 seconds), Nagios version (3.0.2), and the user is logged in as 'guest'. 2. Monitoring Performance: A table showing execution and latency times for service and host checks, and the count of active and passive host/service checks. 3. Network Outages: A box indicating '0 Outages'. 4. Network Health: Two green progress bars for 'Host Health' and 'Service Health'. 5. Hosts: A table showing 0 Down, 0 Unreachable, 41 Up, and 0 Pending hosts. 6. Services: A table showing 0 Critical, 0 Warning, 0 Unknown, 46 Ok, and 0 Pending services. 7. Monitoring Features: A table with five columns (Flap Detection, Notifications, Event Handlers, Active Checks, Passive Checks) and two rows of status (Enabled/Disabled) for various monitoring features. All features shown are 'Enabled'.

Nagios

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
 - Unhandled
- Host Problems
 - Unhandled
- 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

Tactical Monitoring Overview

Last Updated: Thu Sep 3 15:37:09 CDT 2009
Updated every 90 seconds
Nagios® 3.0.2 - www.nagios.org
Logged in as guest

Monitoring Performance

Service Check Execution Time:	0.01 / 4.07 / 0.115 sec
Service Check Latency:	0.02 / 0.25 / 0.117 sec
Host Check Execution Time:	0.01 / 0.13 / 0.018 sec
Host Check Latency:	0.01 / 0.28 / 0.137 sec
# Active Host / Service Checks:	41 / 46
# Passive Host / Service Checks:	0 / 0

Network Outages

0 Outages

Network Health

Host Health:

Service Health:

Hosts

0 Down	0 Unreachable	41 Up	0 Pending
--------	---------------	-------	-----------

Services

0 Critical	0 Warning	0 Unknown	46 Ok	0 Pending
------------	-----------	-----------	-------	-----------

Monitoring Features

	Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
Enabled	All Services Enabled No Services Flapping All Hosts Enabled No Hosts Flapping	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled

Service Detail

Nagios®
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
 - Unhandled
- Host Problems
 - Unhandled
- 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 Sep 3 14:46:07 CDT 2009
Updated every 90 seconds
Nagios® 3.0.2 - www.nagios.org
Logged in as guest

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

Host Status Totals

Up	Down	Unreachable	Pending
41	0	0	0

All Problems	All Types
0	41

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
46	0	0	0	0

All Problems	All Types
0	46

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
DNS-ROOT	SSH	OK	2009-09-03 14:43:51	43d 0h 55m 19s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
ISP-DNS	SSH	OK	2009-09-03 14:41:21	16d 3h 57m 24s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
ISP-RTR	SSH	OK	2009-09-03 14:43:57	43d 5h 35m 13s	1/4	SSH OK - Cisco-1.25 (protocol 2.0)
NOC-TLD1	SSH	OK	2009-09-03 14:41:27	1d 0h 1m 59s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD2	SSH	OK	2009-09-03 14:44:04	1d 22h 44m 22s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD3	SSH	OK	2009-09-03 14:41:34	1d 22h 40m 58s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD4	SSH	OK	2009-09-03 14:44:10	1d 22h 44m 16s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD5	SSH	OK	2009-09-03 14:41:40	1d 22h 41m 46s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD6	SSH	OK	2009-09-03 14:44:17	1d 22h 44m 9s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD7	SSH	OK	2009-09-03 14:41:47	1d 22h 41m 39s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD8	SSH	OK	2009-09-03 14:44:23	1d 22h 44m 3s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD1	SSH	OK	2009-09-03 14:41:53	1d 0h 1m 33s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD2	SSH	OK	2009-09-03 14:44:30	1d 22h 43m 56s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD3	SSH	OK	2009-09-03 14:42:00	1d 22h 41m 26s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD4	SSH	OK	2009-09-03 14:44:36	1d 22h 43m 50s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD5	SSH	OK	2009-09-03 14:42:06	1d 22h 41m 20s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD6	SSH	OK	2009-09-03 14:44:42	1d 22h 43m 42s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)

Host Detail

Nagios®

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

- Unhandled
- Host Problems
- Unhandled
- 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 Sep 3 14:55:18 CDT 2009
Updated every 90 seconds
Nagios® 3.0.2 - www.nagios.org
Logged in as guest

[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
41	0	0	0

All Problems 0 **All Types** 41

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
46	0	0	0	0

All Problems 0 **All Types** 46

Host Status Details For All Host Groups

Host ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Status Information
DNS_ROOT	UP	2009-09-03 14:51:41	43d 1h 7m 0s	PING OK - Packet loss = 0%, RTA = 0.33 ms
ISP-DNS	UP	2009-09-03 14:51:41	16d 4h 11m 25s	PING OK - Packet loss = 0%, RTA = 0.29 ms
ISP-RTT	UP	2009-09-03 14:51:51	43d 5h 47m 40s	PING OK - Packet loss = 0%, RTA = 1.24 ms
NOG-TLD1	UP	2009-09-03 14:52:01	1d 0h 10m 56s	PING OK - Packet loss = 0%, RTA = 4.02 ms
NOG-TLD2	UP	2009-09-03 14:52:01	1d 22h 53m 46s	PING OK - Packet loss = 0%, RTA = 2.23 ms
NOG-TLD3	UP	2009-09-03 14:52:11	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 2.62 ms
NOG-TLD4	UP	2009-09-03 14:52:21	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 1.09 ms
NOG-TLD5	UP	2009-09-03 14:52:31	1d 22h 54m 6s	PING OK - Packet loss = 0%, RTA = 5.20 ms
NOG-TLD6	UP	2009-09-03 14:52:31	1d 22h 53m 56s	PING OK - Packet loss = 0%, RTA = 10.49 ms
NOG-TLD7	UP	2009-09-03 14:52:41	1d 22h 53m 56s	PING OK - Packet loss = 0%, RTA = 1.05 ms
NOG-TLD8	UP	2009-09-03 14:52:51	1d 22h 53m 56s	PING OK - Packet loss = 0%, RTA = 1.00 ms
NS1-TLD1	UP	2009-09-03 14:53:01	1d 0h 10m 26s	PING OK - Packet loss = 0%, RTA = 10.19 ms
NS1-TLD2	UP	2009-09-03 14:53:01	1d 22h 53m 56s	PING OK - Packet loss = 0%, RTA = 5.06 ms
NS1-TLD3	UP	2009-09-03 14:53:11	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 1.03 ms
NS1-TLD4	UP	2009-09-03 14:53:21	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 1.15 ms
NS1-TLD5	UP	2009-09-03 14:53:21	1d 22h 54m 6s	PING OK - Packet loss = 0%, RTA = 1.12 ms
NS1-TLD6	UP	2009-09-03 14:53:31	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 1.06 ms
NS1-TLD7	UP	2009-09-03 14:53:41	1d 22h 53m 46s	PING OK - Packet loss = 0%, RTA = 1.11 ms
NS1-TLD8	UP	2009-09-03 14:53:51	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 1.18 ms
TLD1-RTT	UP	2009-09-03 14:53:51	1d 22h 54m 6s	PING OK - Packet loss = 0%, RTA = 2.22 ms
TLD2-RTT	UP	2009-09-03 14:54:01	1d 22h 53m 46s	PING OK - Packet loss = 0%, RTA = 2.38 ms

Host Groups Overview

Nagios®
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
● Unhandled
● Host Problems
● Unhandled
● 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 Sep 3 14:55:28 CDT 2009
Updated every 90 seconds
Nagios® 3.0.2 - www.nagios.org
Logged in as guest
[View Service Status Detail For All Host Groups](#)
[View Host Status Detail 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
41	0	0	0
All Problems		All Types	
0		41	

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
46	0	0	0	0
All Problems		All Types		
0		46		

Service Overview For All Host Groups

TRTI TLD1 Servers, Virtual Machines, Routers (TLD1)

Host	Status	Services	Actions
NOC-TLD1	UP	1 OK	
NS1-TLD1	UP	1 OK	
TLD1-RTR	UP	1 OK	
TRTI-TLD1	UP	1 OK	

TRTI TLD2 Servers, Virtual Machines, Routers (TLD2)

Host	Status	Services	Actions
NOC-TLD2	UP	1 OK	
NS1-TLD2	UP	1 OK	
TLD2-RTR	UP	1 OK	
TRTI-TLD2	UP	1 OK	

TRTI TLD3 Servers, Virtual Machines, Routers (TLD3)

Host	Status	Services	Actions
NOC-TLD3	UP	1 OK	
NS1-TLD3	UP	1 OK	
TLD3-RTR	UP	1 OK	
TRTI-TLD3	UP	1 OK	

TRTI TLD4 Servers, Virtual Machines, Routers (TLD4)

Host	Status	Services	Actions
NOC-TLD4	UP	1 OK	
NS1-TLD4	UP	1 OK	
TLD4-RTR	UP	1 OK	
TRTI-TLD4	UP	1 OK	

TRTI TLD5 Servers, Virtual Machines, Routers (TLD5)

Host	Status	Services	Actions
NOC-TLD5	UP	1 OK	
NS1-TLD5	UP	1 OK	
TLD5-RTR	UP	1 OK	
TRTI-TLD5	UP	1 OK	

TRTI TLD6 Servers, Virtual Machines, Routers (TLD6)

Host	Status	Services	Actions
NOC-TLD6	UP	1 OK	
NS1-TLD6	UP	1 OK	
TLD6-RTR	UP	1 OK	
TRTI-TLD6	UP	1 OK	

TRTI TLD7 Servers, Virtual Machines, Routers (TLD7)

Host	Status	Services	Actions
NOC-TLD7	UP	1 OK	
NS1-TLD7	UP	1 OK	

TRTI TLD8 Servers, Virtual Machines, Routers (TLD8)

Host	Status	Services	Actions
NOC-TLD8	UP	1 OK	
NS1-TLD8	UP	1 OK	

TRTI Management Virtual Machines (VM-mgmt)

Host	Status	Services	Actions
DNS-ROOT	UP	1 OK	
ISP-DNS	UP	1 OK	

Service Groups Overview

Nagios®
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
 - Unhandled
- Host Problems
 - Unhandled
- 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: Fri Sep 4 13:29:20 CDT 2009
Updated every 90 seconds
Nagios® 3.0.2 - www.nagios.org
Logged in as guest

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

Host Status Totals

Up	Down	Unreachable	Pending
41	0	0	0
All Problems	All Types		
0	41		

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
53	0	0	1	0
All Problems	All Types			
1	54			

Service Overview For All Service Groups

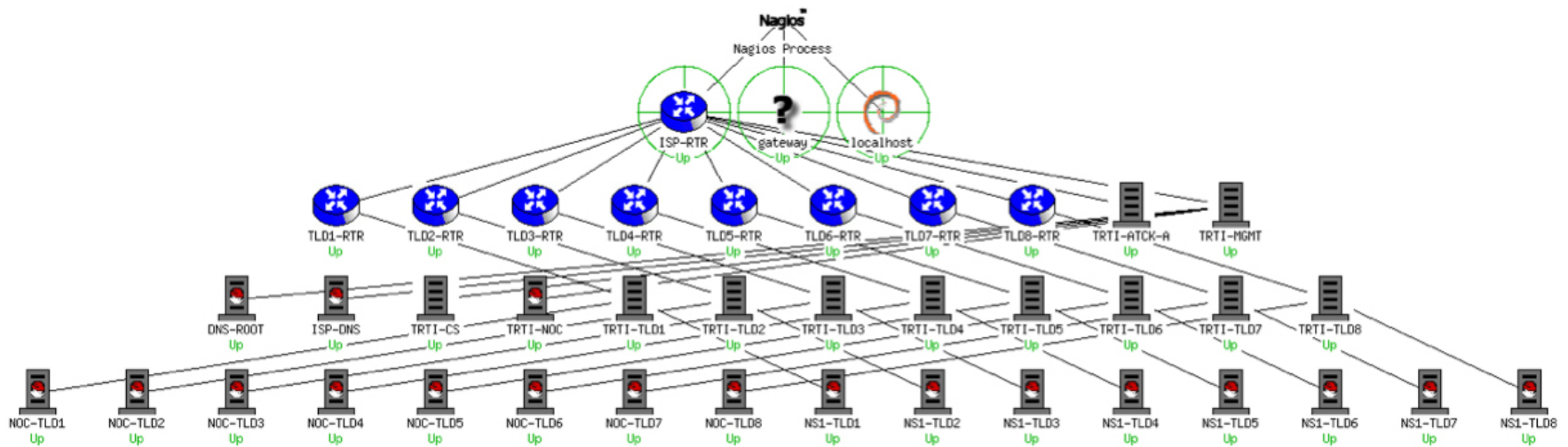
TLD Servers running Nagios (NAGIOS)

Host	Status	Services	Actions
NS1-TLD1	UP	1 OK	
NS1-TLD2	UP	1 OK	
NS1-TLD3	UP	1 OK	
NS1-TLD4	UP	1 OK	
NS1-TLD5	UP	1 OK	
NS1-TLD6	UP	1 OK	
NS1-TLD7	UP	1 OK	
NS1-TLD8	UP	1 OK	

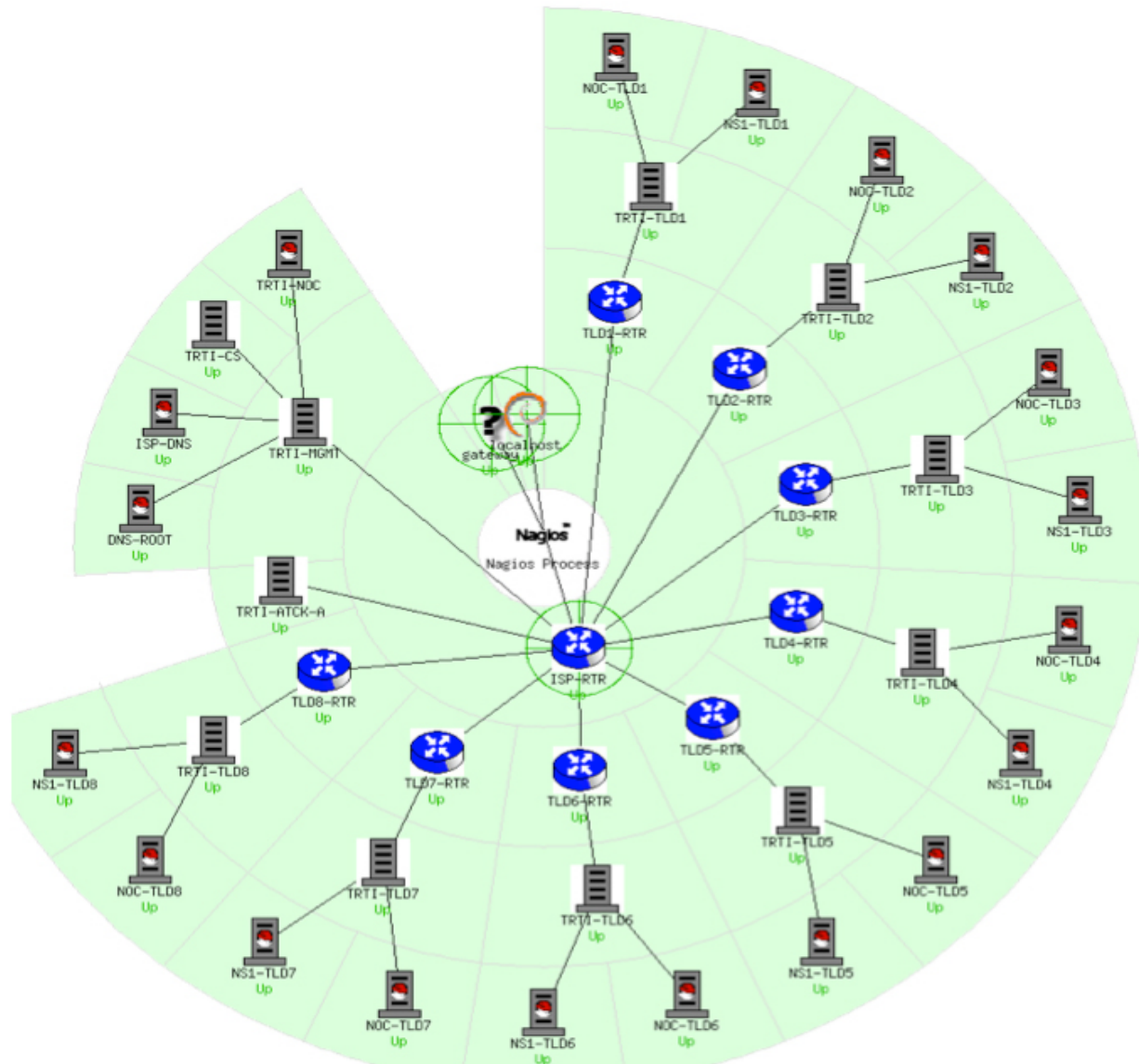
TLD Servers running SSH (SSH)

Host	Status	Services	Actions
NS1-TLD1	UP	1 OK	
NS1-TLD2	UP	1 CRITICAL	
NS1-TLD3	UP	1 OK	
NS1-TLD4	UP	1 OK	
NS1-TLD5	UP	1 OK	
NS1-TLD6	UP	1 OK	
NS1-TLD7	UP	1 OK	
NS1-TLD8	UP	1 OK	

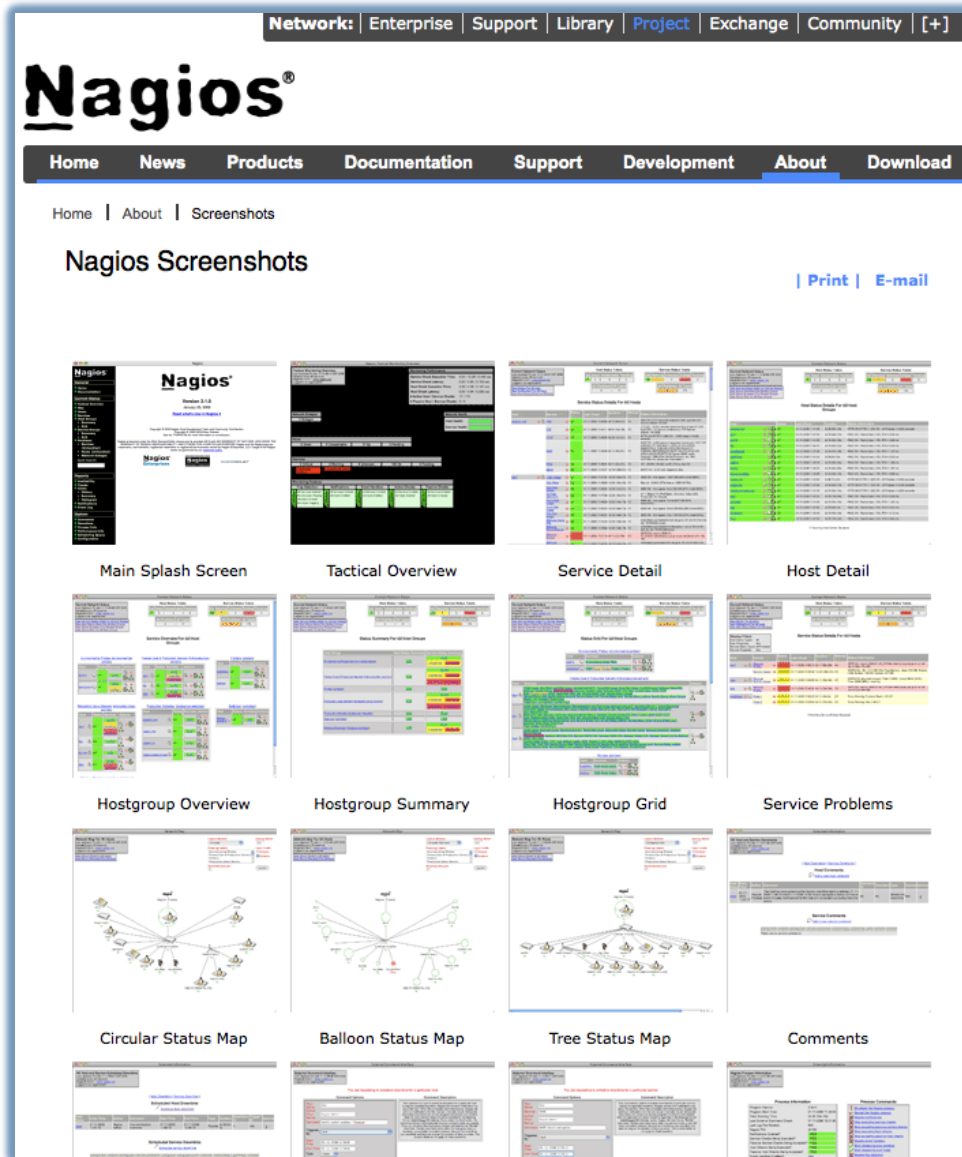
Collapsed tree status map



Marked-up circular status map



More sample screenshots



Many more sample
Nagios screenshots
available here:

[http://www.nagios.org/about/
screenshots](http://www.nagios.org/about/screenshots)

Features

Verification of availability is delegated to plugins:

- The product's architecture is simple enough that writing new plugins is fairly easy in the language of your choice.
- There are many, many plugins available.

Nagios uses parallel checking and forking.

- Version 3 of Nagios does this better.

Features cont.

- Has intelligent checking capabilities. Attempts to distribute the server load of running Nagios (for larger sites) and the load placed on devices being checked.
- Configuration is done in simple, plain text files, but that can contain much detail and are based on templates.
- Nagios reads it's configuration from an entire directory. You decide how to define individual files.

Features cont.

- Utilizes topology to determine dependencies.
 - Nagios differentiates between what is down vs. what is not available. This way it avoids running unnecessary checks.
- Nagios allows you to define how you send notifications based on combinations of:
 - Contacts and lists of contacts
 - Devices and groups of devices
 - Services and groups of services
 - Defined hours by persons or groups.
 - The state of a service.

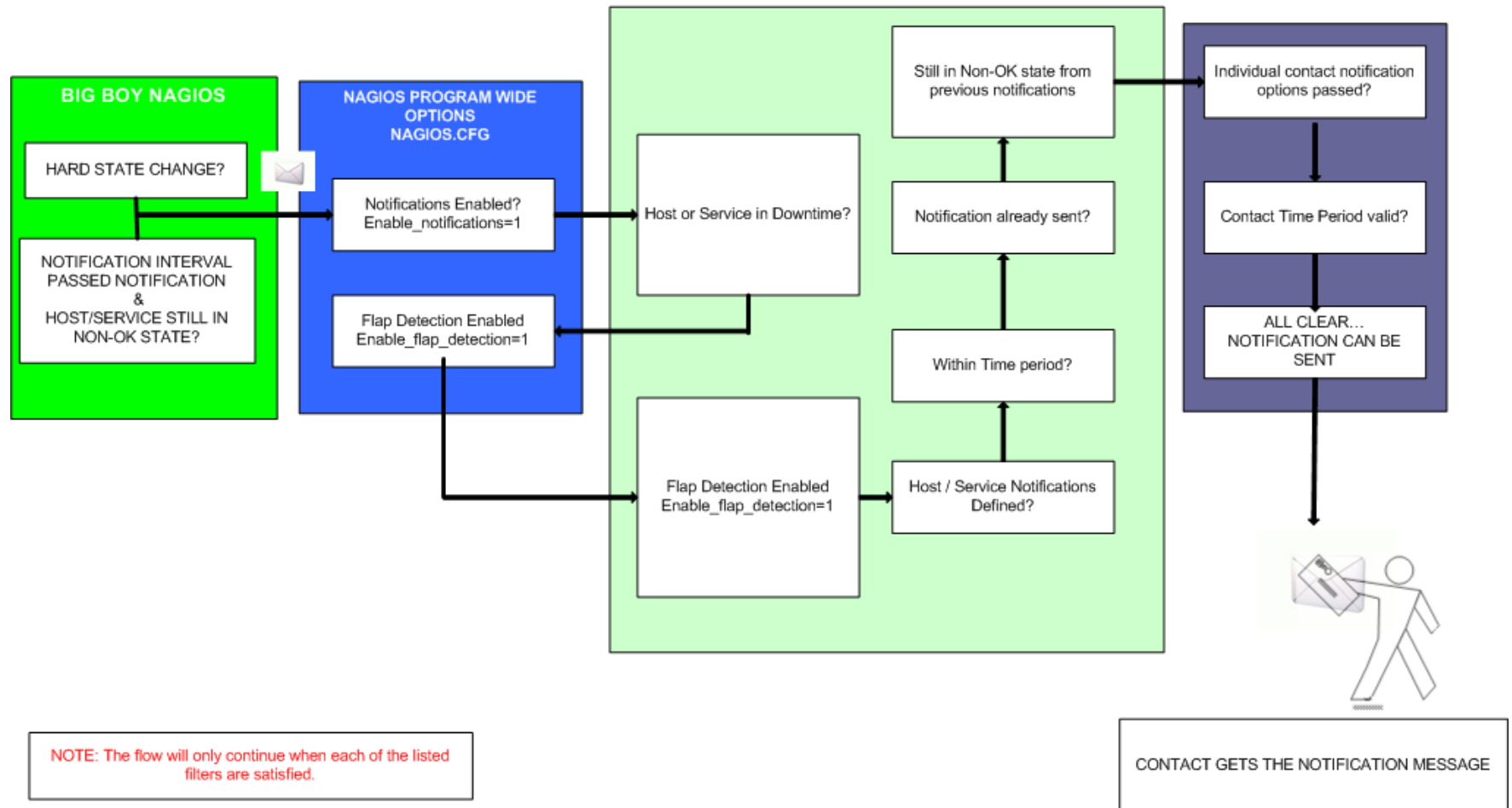
And, even more...

Service state:

When configuring a service you have the following notification options:

- **d**: DOWN: The service is down (not available)
- **u**: UNREACHABLE: When the host is not visible
- **r**: RECOVERY: (OK) Host is coming back up
- **f**: FLAPPING: When a host first starts or stops or it's state is undetermined.
- **n**: NONE: Don't send any notifications

NAGIOS - NOTIFICATION FLOW DIAGRAM



Features, features, features...

- Allows you to acknowledge an event.
 - A user can add comments via the GUI
- You can define maintenance periods
 - By device or a group of devices
- Maintains availability statistics.
- ✓ *Can detect flapping and suppress additional notifications.*
- Allows for multiple notification methods:
 - e-mail, pager, SMS, winpopup, audio, etc...
- ✓ *Allows you to define notification levels.*

How checks work

- A node/host/device consists of one or more service checks (PING, HTTP, MYSQL, SSH, etc)
- Periodically Nagios checks each service for each node and determines if state has changed. State changes are:
 - CRITICAL
 - WARNING
 - UNKNOWN
- For each state change you can assign:
 - Notification options (as mentioned before)
 - Event handlers

How checks work continued

Parameters

- Normal checking interval
- Re-check interval
- Maximum number of checks.
- Period for each check
- Node checks only happen when services respond (assuming you've configured this).
 - A node can be:
 - DOWN
 - UNREACHABLE

How checks work continued

In this manner it can take some time before a host change's its state to “down” as Nagios first does a service check and then a node check.

By default Nagios does a node check 3 times before it will change the nodes state to down.

You can, of course, change all this.

The concept of “parents”

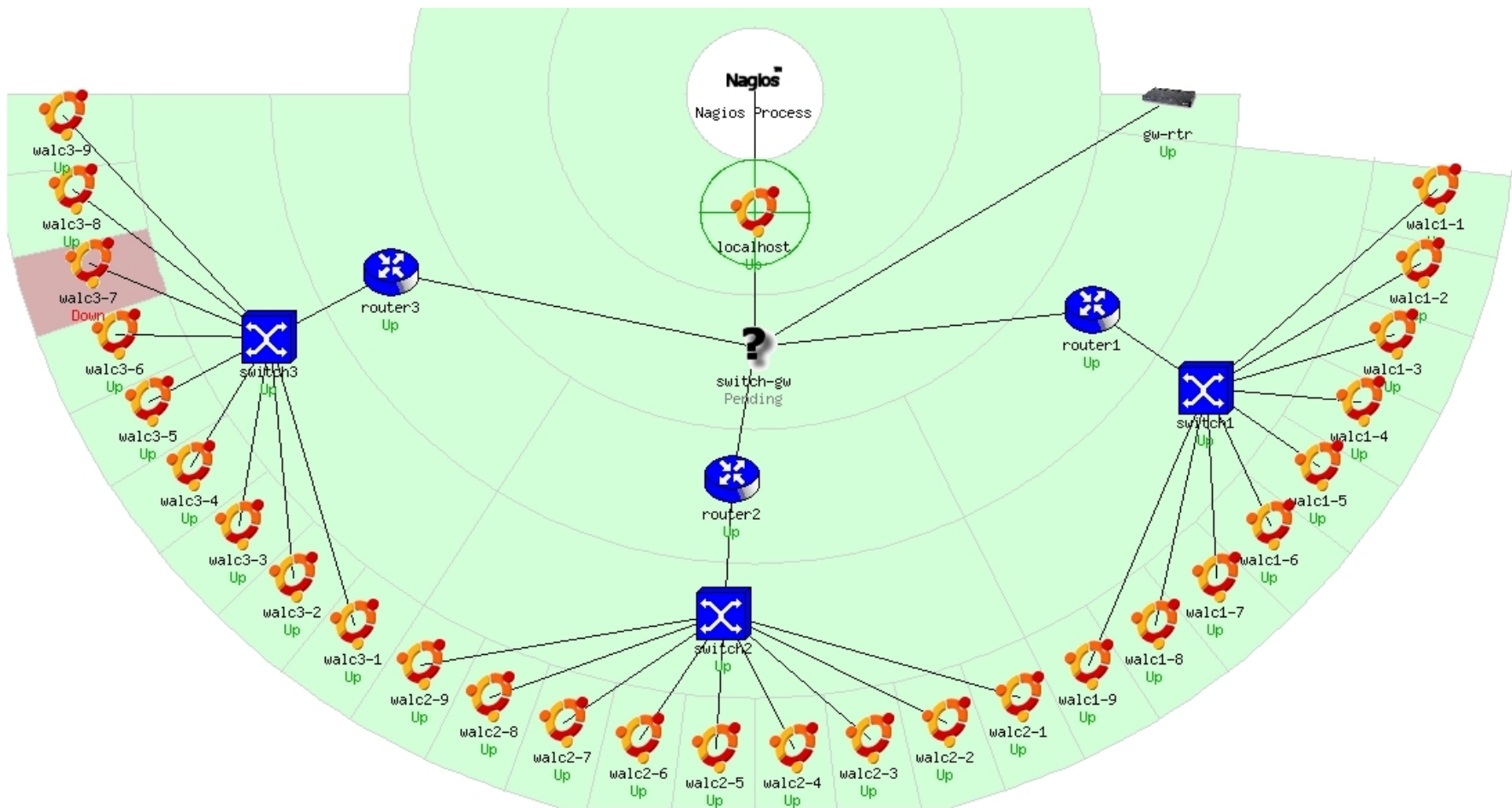
Nodes can have parents:

- For example, the parent of a PC connected to a switch would be the switch.
- This allows us to specify the network dependencies that exist between machines, switches, routers, etc.
- This avoids having Nagios send alarms when a parent does not respond.
- A node can have multiple parents.

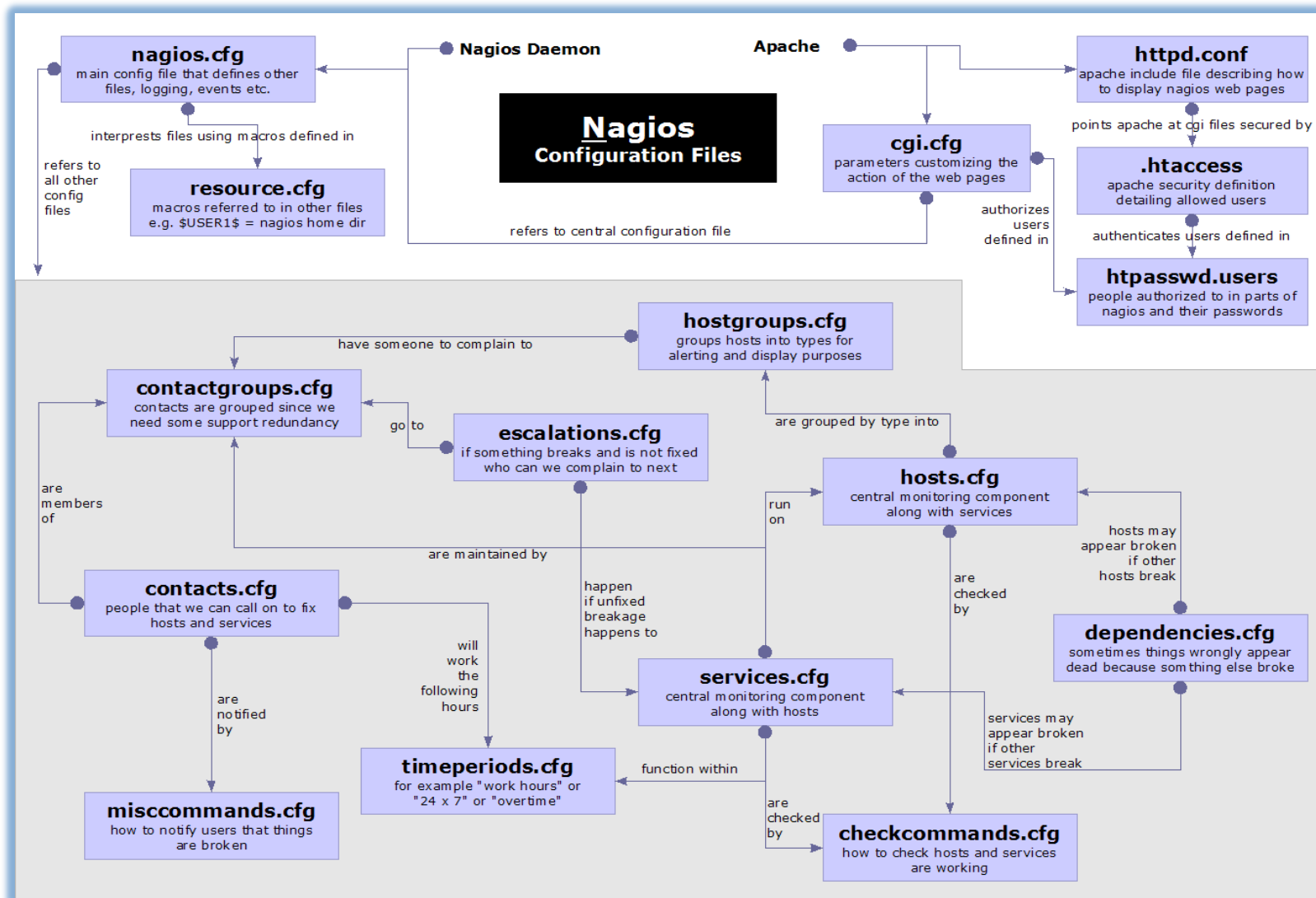
Network viewpoint concept

- Where you locate your Nagios server will determine your point of view of the network.
- Nagios allows for parallel Nagios boxes that run at other locations on a network.
- Often it makes sense to place your Nagios server nearer the border of your network vs. in the core.

Network viewpoint



Nagios configuration files



Configuration Files

Located in /etc/nagios3/

Important files include:

- `cgi.cfg` Controls the web interface and security options.
- `commands.cfg` The commands that Nagios uses for notifications.
- `nagios.cfg` Main configuration file.
- `conf.d/*` All other configuration goes here!

Configuration files continued

Under conf.d/* *(sample only)*

- `contacts_nagios3.cfg` users and groups
- `generic-host_nagios2.cfg` default host template
- `generic-service_nagios2.cfg` default service template
- `hostgroups_nagios2.cfg` groups of nodes
- `services_nagios2.cfg` what services to check
- `timeperiods_nagios2.cfg` when to check and who to notify

Configuration files continued

Under conf.d some other possible configfiles:

- `host-gateway.cfg` Default route definition
- `extinfo.cfg` Additional node information
- `servicegroups.cfg` Groups of nodes and services
- `localhost.cfg` Define the Nagios server itself
- `pcs.cfg` Sample definition of PCs (hosts)
- `switches.cfg` Definitions of switches (hosts)
- `routers.cfg` Definitions of routers (hosts)

Pre-installed plugins in Ubuntu

check_bgpstate	check_hpjd	check_mailq	check_overcr
check_ssmtp	check_breeze	check_http	check_mrtg
check_pgsql	check_swap	check_by_ssh	check_icmp
check_mrtgtraf	check_ping	check_tcp	check_clamd
check_ide_smart	check_mysql	check_pop	check_time
check_cluster	check_ifoperstatus	check_mysql_query	
check_procs	check_udp	check_dhcp	check_ifstatus
check_nagios	check_radius	check_ups	check_dig
check_imap	check_nntp	check_real	check_users
check_disk	check_ircd	check_nntps	check_rpc
check_wave	check_disk_smb	check_jabber	check_nt
check_sensors	check_dns	check_ldap	check_ntp
check_simap	check_dummy	check_ldap	check_ntp_peer
check_smtp	check_file_age	check_linux_raid	check_ntp_time
check_snmp	check_flexlm	check_load	check_nwstat

Main configuration details

Global settings

File: `/etc/nagios3/nagios.cfg`

- Says where other configuration files are.
- General Nagios behavior:
 - For large installations you should tune the installation via this file.
 - See: *Tunning Nagios for Maximum Performance*
http://nagios.sourceforge.net/docs/2_0/tuning.html

CGI configuration

`/etc/nagios3/cgi.cfg`

- You can change the CGI directory if you wish
- Authentication and authorization for Nagios use:
 - Activate authentication via Apache's .htpasswd mechanism, or using RADIUS or LDAP.
 - Users can be assigned rights via the following variables:
 - `authorized_for_system_information`
 - `authorized_for_configuration_information`
 - `authorized_for_system_commands`
 - `authorized_for_all_services`
 - `authorized_for_all_hosts`
 - `authorized_for_all_service_commands`
 - `authorized_for_all_host_commands`

Time Periods

This defines the base periods that control checks, notifications, etc.

- Defaults: 24 x 7
- Could adjust as needed, such as work week only.
- Could adjust a new time period for “outside of regular hours”, etc.

```
# '24x7'
define timeperiod{
    timeperiod_name 24x7
    alias            24 Hours A Day, 7 Days A Week
    sunday           00:00-24:00
    monday           00:00-24:00
    tuesday          00:00-24:00
    wednesday        00:00-24:00
    thursday         00:00-24:00
    friday           00:00-24:00
    saturday         00:00-24:00
}
```

Configuring service/host checks:

Definition of “host alive”

```
# 'check-host-alive' command definition
define command{
    command_name    check-host-alive
    command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w 2000.0,60% -c
5000.0,100% -p 1 -t 5
}
```

- Located in /etc/nagios-plugins/config, then adjust in /etc/nagios3/conf.d/services_nagios2.cfg
- While these are “service” or “host” checks Nagios refers to them as “commands”

Notification commands

Allows you to utilize any command you wish.
We'll use this to generate tickets in RT.

```
# 'notify-by-email' command definition
define command{
    command_name    notify-by-email
    command_line    /usr/bin/printf "%b" "Service: $SERVICEDESC$\nHost:
$HOSTNAME$\nIn: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState: $SERVICESTATE$
\nInfo: $SERVICEOUTPUT$\nDate: $SHORTDATETIME$" | /bin/mail -s
'$NOTIFICATIONTYPE$: $HOSTNAME$/$SERVICEDESC$ is $SERVICESTATE$'
$CONTACTEMAIL$
}
```

```
From: nagios@nms.localdomain
To: router_group@localdomain
Subject: Host DOWN alert for TLD1-RTR!
Date: Thu, 29 Jun 2006 15:13:30 -0700
```

```
Host: TLD1-RTR
In: Core_Routers
State: DOWN
Address: 111.222.333.444
Date/Time: 06-29-2006 15:13:30
Info: CRITICAL - Plugin timed out after 6 seconds
```

Nodes and services configuration

Based on templates

- This saves lots of time avoiding repetition
- Similar to Object Oriented programming

Create default templates with default parameters for a:

- generic node
- generic service
- generic contact

Generic node template

```
define host{
    name                generic-host
    notifications_enabled 1
    event_handler_enabled 1
    flap_detection_enabled 1
    process_perf_data     1
    retain_status_information 1
    retain_nonstatus_information 1
    check_command          check-host-alive
    max_check_attempts     5
    notification_interval  60
    notification_period     24x7
    notification_options    d,r
    contact_groups          nobody
    register                0
}
```

Individual node configuration

```
define host{
    use                generic-host
    host_name          TLD1-RTR
    alias              TLD1_router
    address            192.168.101.1
    parents            ISP-RTR.MGMT
    contact_groups     router_group
}
```

Generic service configuration

```
define service{
    name                generic-service
    active_checks_enabled 1
    passive_checks_enabled 1
    parallelize_check    1
    obsess_over_service  1
    check_freshness      0
    notifications_enabled 1
    event_handler_enabled 1
    flap_detection_enabled 1
    process_perf_data    1
    retain_status_information 1
    retain_nonstatus_information 1
    is_volatile          0
    check_period         24x7
    max_check_attempts   5
    normal_check_interval 5
    retry_check_interval 1
    notification_interval 60
    notification_period   24x7
    notification_options  c,r
    register              0
}
```

Individual service configuration

```
define service{
    host_name          TLD1-RTR
    use                 generic-service
    service_description PING
    check_command       check-host-alive
    max_check_attempts 5
    normal_check_interval 5
    notification_options c,r,f
    contact_groups      router_group
}
```

Group service configuration

```
# check that ssh services are running
define service {
    hostgroup_name      ssh-servers
    service_description SSH
    check_command        check_ssh
    use                  generic-service
    notification_interval 0 ; set > 0 if you want to be renotified
}
```

The “service_description” is important if you plan to create Service Groups. Here is a sample Service Group definition:

```
define servicegroup{
    servicegroup_name  Webmail
    alias               web-mta-storage-auth
    members             svr1,HTTP,svr1,SMTP,svr1,POP,svr1,IMAP,
                      svr1,RAID,svr1,LDAP, svr2,HTTP,svr2,SMTP,
                      svr2,POP,svr2,IMAP,svr2,RAID,svr2,LDAP
}
```

Beeper and sms messages

- It's important to integrate Nagios with something available outside of work
 - Problems occur after hours... (unfair, but true)
- A critical item to remember: an SMS or message system should be independent from your network.
 - You can utilize a modem and a telephone line
 - Packages like sendpage, qpage or gnokii can help.

References

- **Nagios web site**
<http://www.nagios.org/>
- **Nagios plugins site**
<http://sourceforge.net/projects/nagiosplug/>
- *Nagios System and Network Monitoring*, by Wolfgang Barth. Good book about Nagios.
- **Unofficial Nagios plugin site**
<http://www.nagiosexchange.org/>
- **A Debian tutorial on Nagios**
<http://www.debianhelp.co.uk/nagios.htm>
- **Commercial Nagios support**
<http://www.nagios.com/>