Network Monitoring & Management: Nagios

Network Startup Resource Center

Introduction

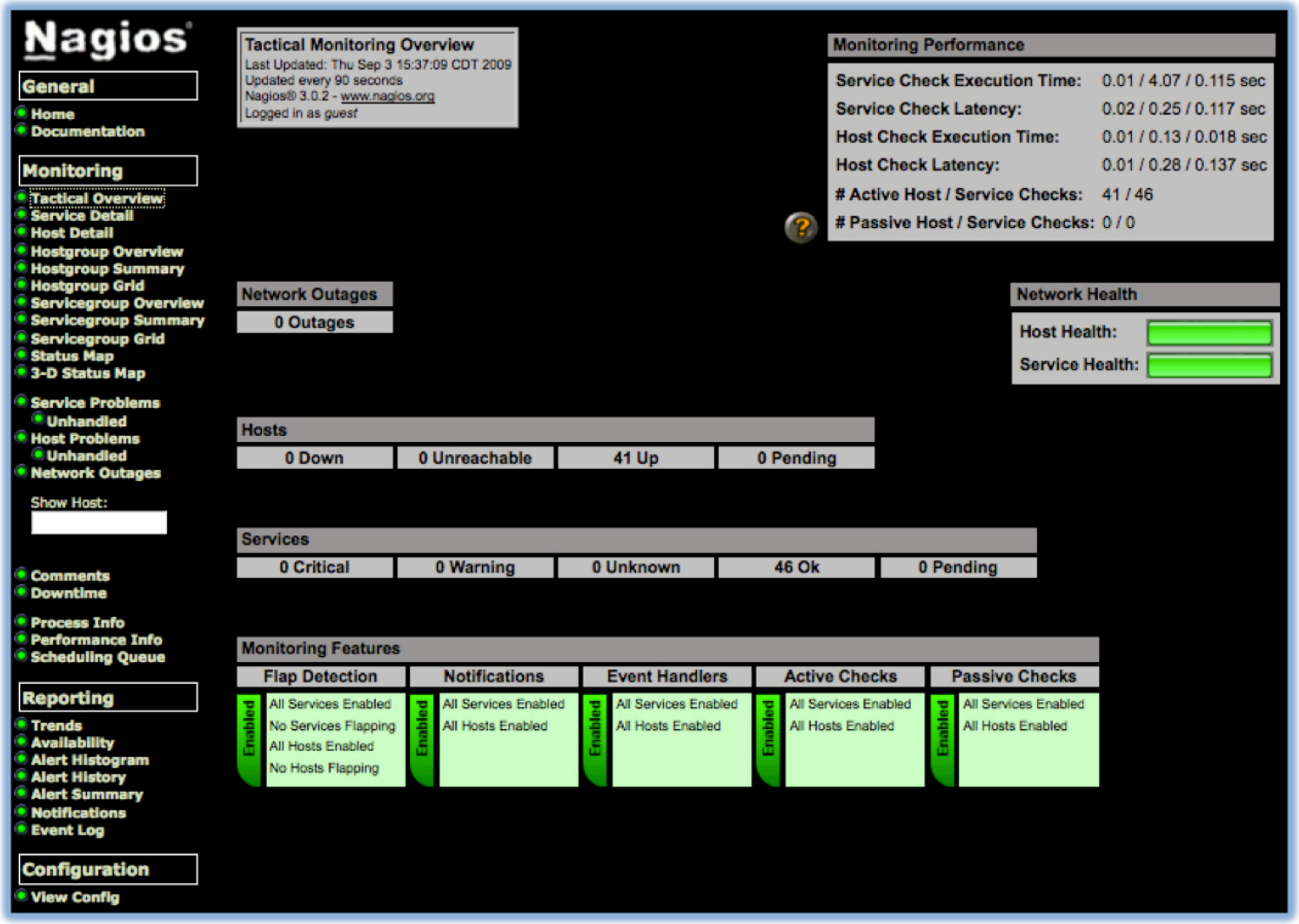
- Possibly the most used open source network monitoring software
- Web interface for viewing status, browsing history, scheduling downtime etc
- Sends out alerts via E-mail. Can be configured to use other mechanisms, e.g. SMS

Introduction

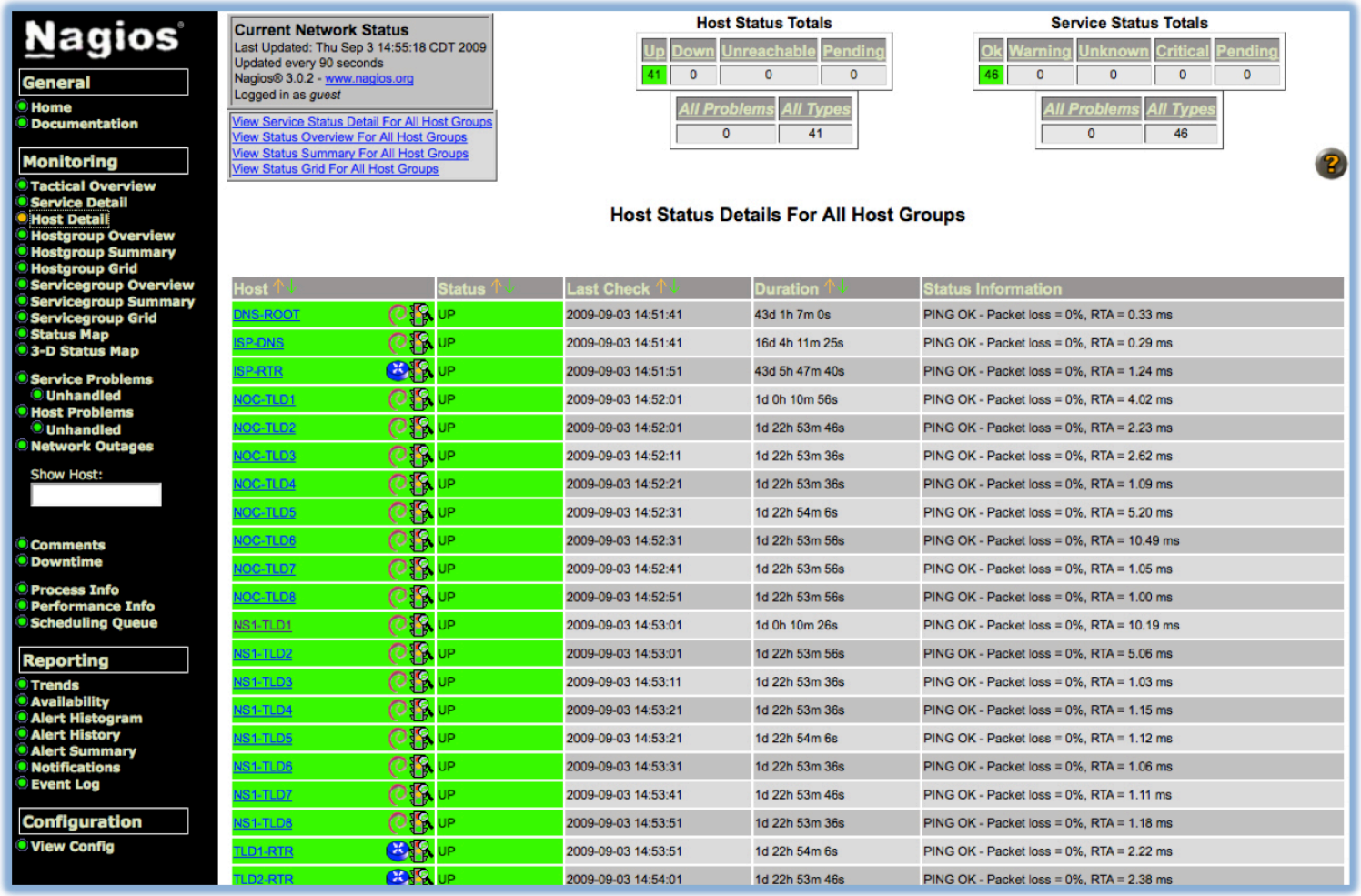
Nagios actively monitors the availability

- of Hosts (devices)
- and Services

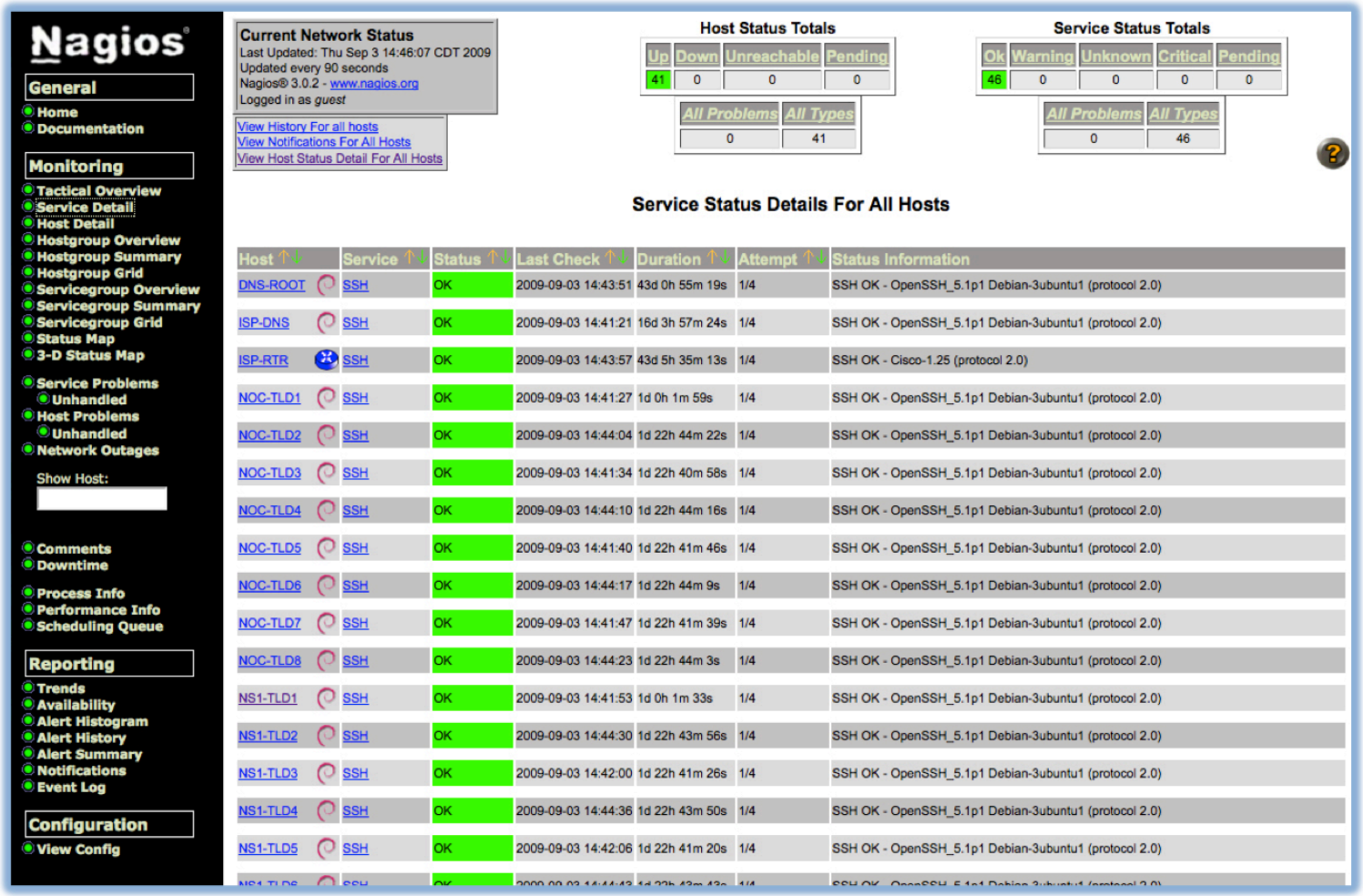
Nagios: General View



Host Detail View



Service Detail View



Features

Utilizes topology to determine dependencies.

- Differentiates between what is *down* vs. what is *unreachable*. Avoids running unnecessary checks and sending redundant alarms

Allows you to define how to 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.

Plugins

Plugins are used to verify services and devices:

- Nagios architecture is simple enough that writing new plugins is fairly easy in the language of your choice.
- There are ***many, many*** plugins available (thousands).
  - ✓ http://exchange.nagios.org/
  - ✓ http://nagiosplugins.org/

Pre-installed Plugins for Ubuntu

/usr/lib/nagios/plugins

```
2. nsrc@s1: ~ (ssh)
nsrc@s1:~$ ls /usr/lib/nagios/plugins
check_apt       check_disk      check_hpjd          check_jabber    check_mysql       check_ntp_time  check_real      check_ssh     check_wave
check_breeze    check_disk_smb  check_http          check_ldap      check_mysql_query check_nwstat    check_rpc       check_ssmtp   negate
check_by_ssh    check_dns       check_icmp          check_ldaps     check_nagios      check_oracle    check_rta_multi check_swap    urlize
check_clamd     check_dummy     check_ide_smart     check_load      check_nntp        check_overcr    check_sensors   check_tcp     utils.pm
check_cluster   check_file_age  check_ifoperstatus  check_log       check_nntps       check_pgsql     check_simap     check_time    utils.sh
check_dbi       check_flexlm    check_ifstatus      check_mailq     check_nt          check_ping      check_smtp      check_udp
check_dhcp      check_ftp       check_imap          check_mrtg      check_ntp         check_pop       check_snmp      check_ups
check_dig       check_host      check_ircd          check_mrtgtraf  check_ntp_peer    check_procs     check_spop      check_users
nsrc@s1:~$
```

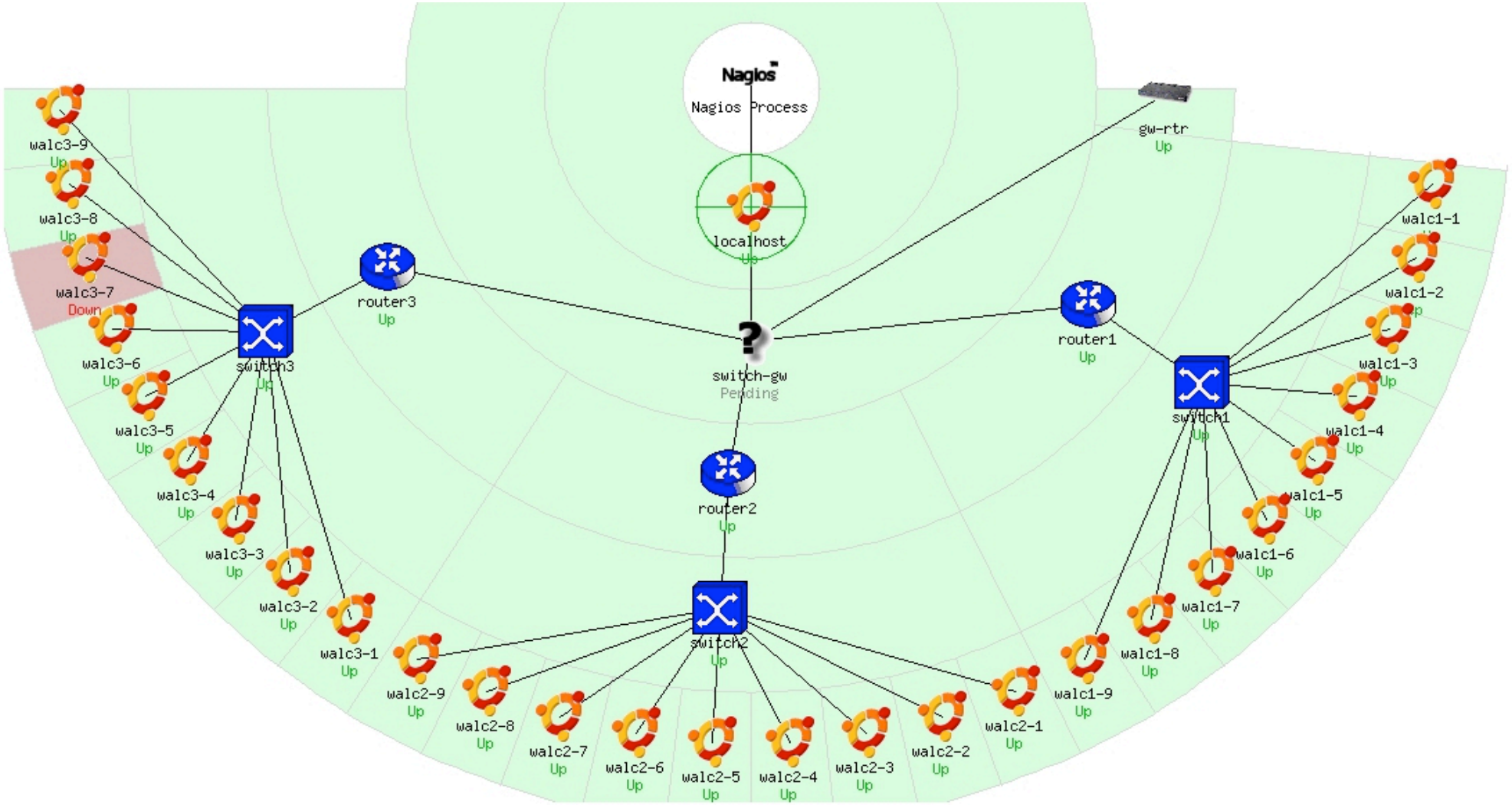
/etc/nagios-plugins/config

```
2. nsrc@s1: ~ (ssh)
nsrc@s1:~$ ls /etc/nagios-plugins/config/
apt.cfg     disk-smb.cfg  fping.cfg  http.cfg      mail.cfg   netware.cfg  pgsql.cfg   real.cfg     tcp_udp.cfg
breeze.cfg  dns.cfg       ftp.cfg    ifstatus.cfg  mailq.cfg  news.cfg     ping.cfg    rpc-nfs.cfg  telnet.cfg
dhcp.cfg    dummy.cfg     games.cfg  ldap.cfg      mrtg.cfg   nt.cfg       procs.cfg   snmp.cfg     users.cfg
disk.cfg    flexlm.cfg    hppjd.cfg  load.cfg      mysql.cfg  ntp.cfg      radius.cfg  ssh.cfg
nsrc@s1:~$
```

How Checks Work

- Periodically Nagios calls a plugin to test the state of each service. Possible responses are:
  - OK
  - WARNING
  - CRITICAL
  - UNKNOWN
- If a service is not OK it goes into a “soft” error state. After a number of retries (default 3) it goes into a “hard” error state. At that point an alert is sent.
- You can also trigger external event handlers based on these state transitions

Network Viewpoint



Demo of Nagios

http://noc.ws.nsrc.org/nagios3/

nagiosadmin: lab_password

Installation

In Debian/Ubuntu

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

Key directories

```
/etc/nagios3
/etc/nagios3/conf.d
/etc/nagios-plugins/config
/usr/lib/nagios/plugins
/usr/share/nagios3/htdocs/images/logos
```

Nagios web interface is here:

http://hostN.ws.nsrc.org/nagios3/

Host and Services Configuration

Based on templates

- This saves lots of time avoiding repetition

There are default templates with default parameters for a:

- *generic host* (generic-host_nagios2.cfg)
- *generic service* (generic-service_nagios2.cfg)

- Individual settings can be overridden
- Defaults are all sensible

Configuration

- Configuration defined in text files
  - /etc/nagios3/conf.d/*.cfg
  - Details at http://nagios.sourceforge.net/docs/3_0/objectdefinitions.html
- The default config is broken into several files with different objects in different files, but actually you can organise it how you like
- Always verify before restarting Nagios – otherwise your monitoring system may die!
  - `nagios3 –v /etc/nagios3/nagios.cfg`

Monitoring a Single Host

pcs.cfg

```
define host {
   host_name host1
   alias     host1 in group 1
   address   host1.ws.nsrc.org
   use       generic-host
}
```

copy settings from this template

- This is a minimal working config
  - You are just pinging the host; Nagios will warn that you are not monitoring any services
- The filename can be anything ending **`.cfg`**
- Organise your devices however you like – e.g. related hosts in the same file

Generic Host Template

generic-host_nagios2.cfg

```
define host {
   name                            generic-host    ; The name of this host template
   notifications_enabled           1  ; Host notifications are enabled
   event_handler_enabled           1  ; Host event handler is enabled
   flap_detection_enabled          1  ; Flap detection is enabled
   failure_prediction_enabled      1  ; Failure prediction is enabled
   process_perf_data               1  ; Process performance data
   retain_status_information       1  ; Retain status information across program restarts
   retain_nonstatus_information    1  ; Retain non-status information across restarts
      check_command                   check-host-alive
      max_check_attempts              10
      notification_interval           0
      notification_period             24x7
      notification_options            d,u,r
      contact_groups                  admins
   register                        0  ; DON'T REGISTER THIS DEFINITION -
                                      ; IT'S NOT A REAL HOST, JUST A TEMPLATE!
}
```

Overriding Defaults

All settings can be overridden per host

hosts.cfg

```
define host {
   host_name                host1
   alias                    host1 in group 1
   address                  host1.ws.nsrc.org
   use                      generic-host
   notification_interval    120
   contact_groups           admins,managers
}
```

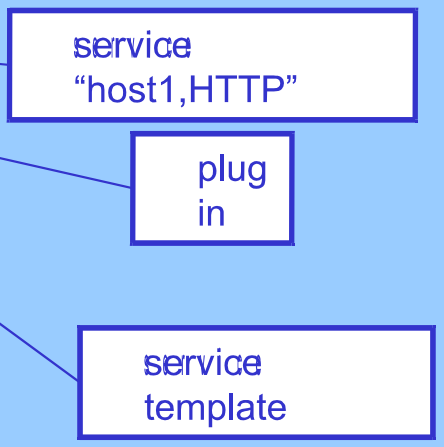
Defining Services: Direct Way

pcs.cfg

```
define host {
    host_name host1
    alias host1 in group 1
    address host1.ws.nsrc.org
    use generic-host
}

define service {
    host_name host1          host1
    service_description      HTTP
    check_command check_http
    use generic-service
}

define service {
    host_name host1          host1
    service_description      SSH
    check_command check_ssh
    use generic-service
}
```



Service Checks

- The combination of host + service is a unique identifier for the service check, e.g.
  - “pc1,HTTP”
  - “pc1,SSH”
  - “pc2,HTTP”
  - “pc2,SSH”
- *check_command* points to the plugin
- *service template* pulls in settings for how often the check is done, and who and when to alert

Generic Service Templates

```
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
        failure_prediction_enabled      1
        process_perf_data               1
        retain_status_information       1
        retain_nonstatus_information    1
          notification_interval           0
          is_volatile                     0
          check_period                    24x7
          normal_check_interval           5
          retry_check_interval            1
          max_check_attempts              4
          notification_period             24x7
          notification_options            w,u,c,r
          contact_groups                  admins
        register                        0    ; DONT REGISTER THIS DEFINITION
        }
```

generic-service_nagios2.cfg

(comments have been removed)

Overriding Defaults

Again, settings can be overridden per service

services_nagios2.cfg

```
define service {
    host_name               host1
    service_description     HTTP
    check_command           check_http
    use                     generic-service
    contact_groups          admins,managers
    max_check_attempts      3
}
```

Repeating Service Checks

- Often we are monitoring an identical service on many hosts
- To avoid duplication, a better way is to define a service check for all hosts in a *hostgroup*

Creating Hostgroups

hostgroups_nagios2.cfg

```
define hostgroup {
   hostgroup_name   http-servers
   alias            HTTP servers
   members          host2,host3
}

define hostgroup {
   hostgroup_name   ssh-servers
   alias            SSH servers
   members          host1,host2,host3,host4
}
```

Monitoring Services in Hostgroups

```
define service {
    hostgroup_name          http-servers
    service_description     HTTP
    check_command           check_http
    use                     generic-service
}

define service {
    hostgroup_name          ssh-servers
    service_description     SSH
    check_command           check_ssh
    use                     generic-service
}
```

services_nagios2.cfg

if hostgroup "http-servers" contains pc1 & pc2 then Nagios creates HTTP service checks for both hosts. The service checks are called "pc1,HTTP" and "pc2,HTTP"

Alternative View

- “this hostgroup contains these PCs”

or:

- “this PC belongs to these hostgroups”
- No need for “members” line in hostgroups file

Optional: Servicegroups

- Services can be grouped into a “servicegroup”
- This is so related or dependent services can be viewed together in the web interface
- The services themselves must already exist

servicegroups.cfg

```
define servicegroup {
   servicegroup_name   mail-services
   alias         Services comprising the mail platform
   members       host2,HTTP,host2,HTTP,host3,MYSQL
}
```

Out of Band (OOB) Notifications

A critical item to remember: an SMS or message system that is independent from your network.

- You can utilize a cell phone connected to the Nagios server, or a USB dongle with SIM card
- You can use packages like:

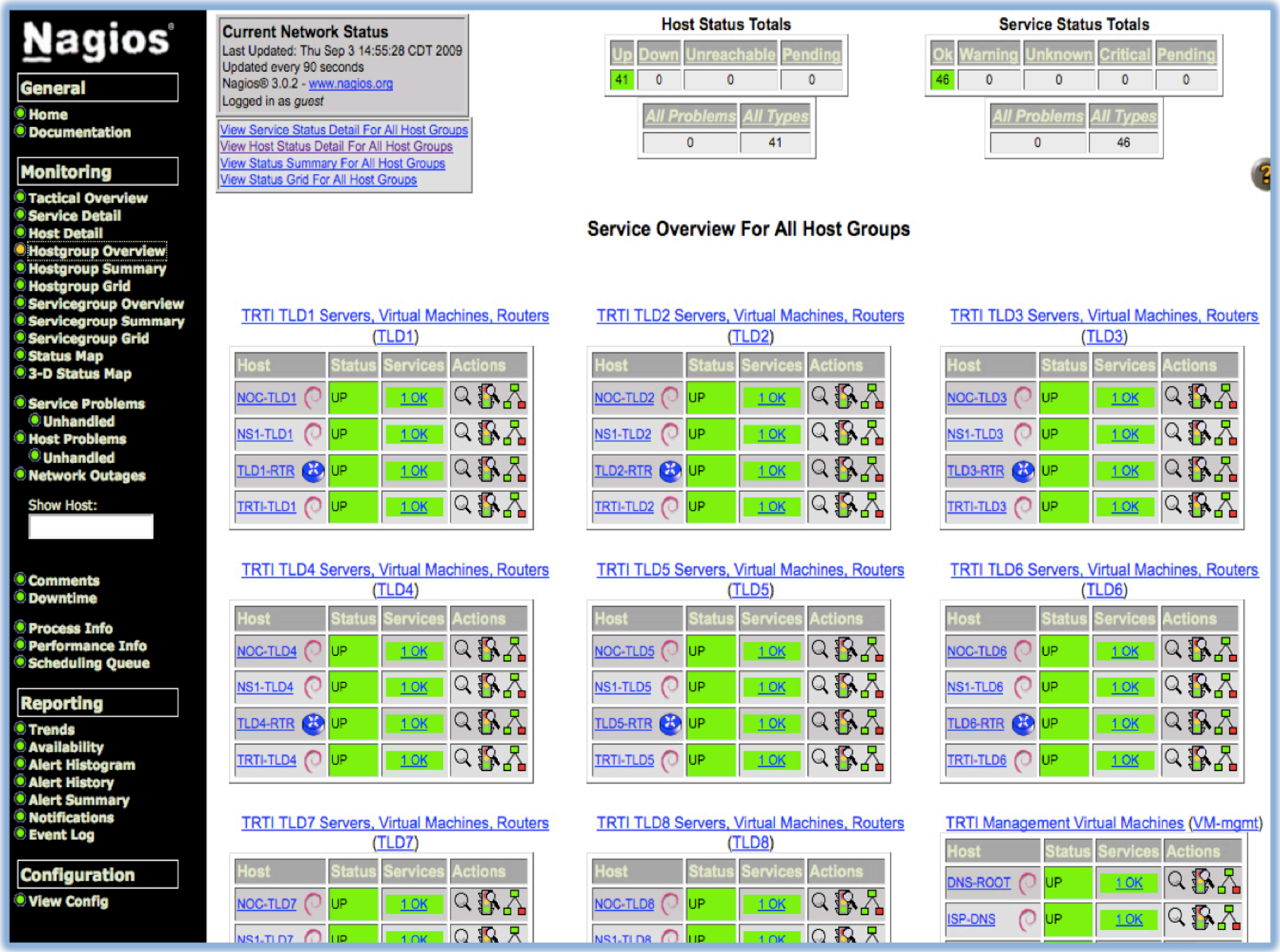
gammu: http://wammu.eu/
gnokii: http://www.gnokii.org/
sms-tools: http://smstools3.kekekasvi.com/

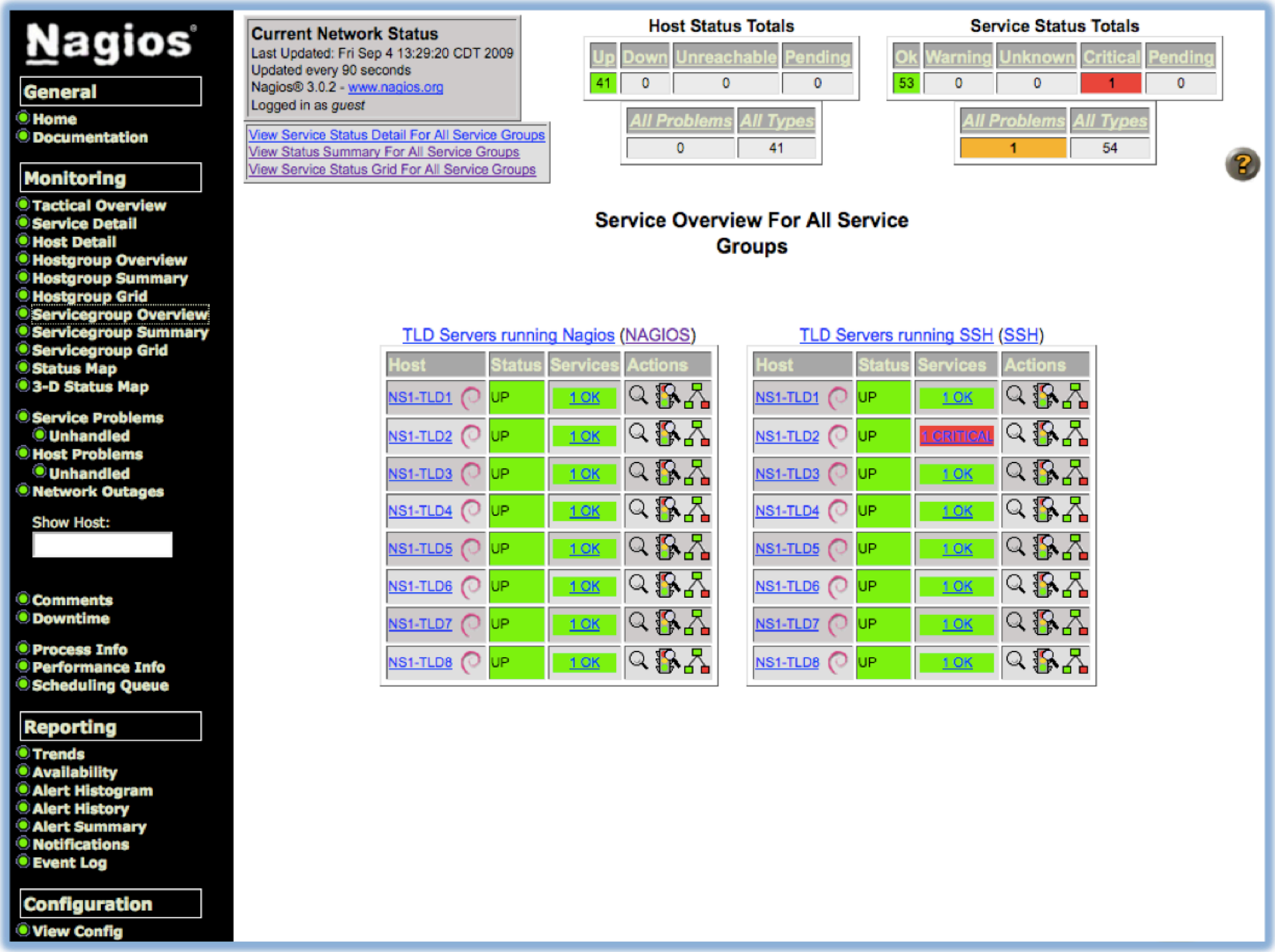
References

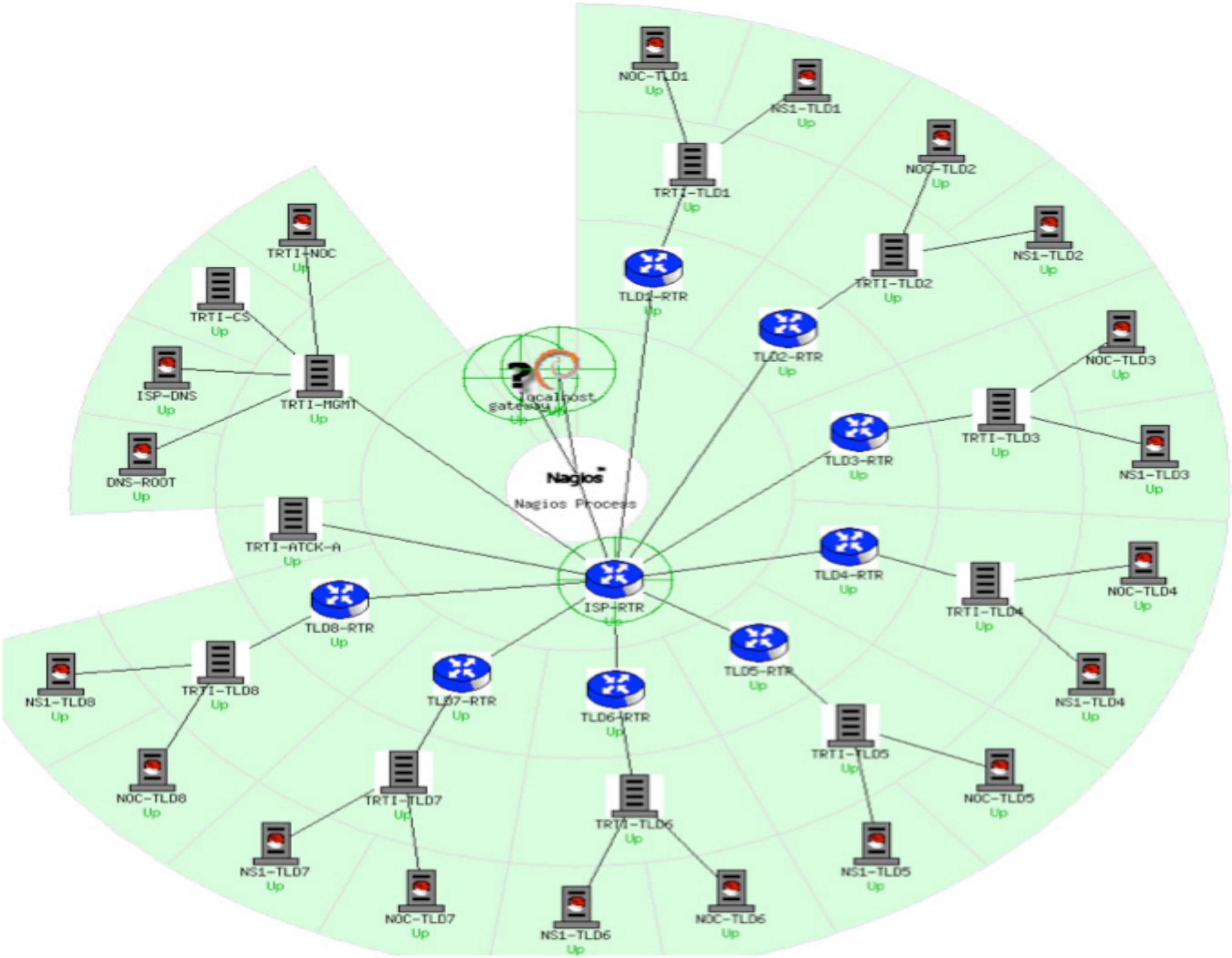
- **Nagios web site**
  http://www.nagios.org/
- **Nagios plugins site**
  http://www.nagiosplugins.org/
- *Nagios System and Network Monitoring*, by Wolfgang Barth. Good book about Nagios.
- **Unofficial Nagios plugin site**
  http://nagios.exchange.org/
- **A Debian tutorial on Nagios**
  http://www.debianhelp.co.uk/nagios.htm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

Screen Shots

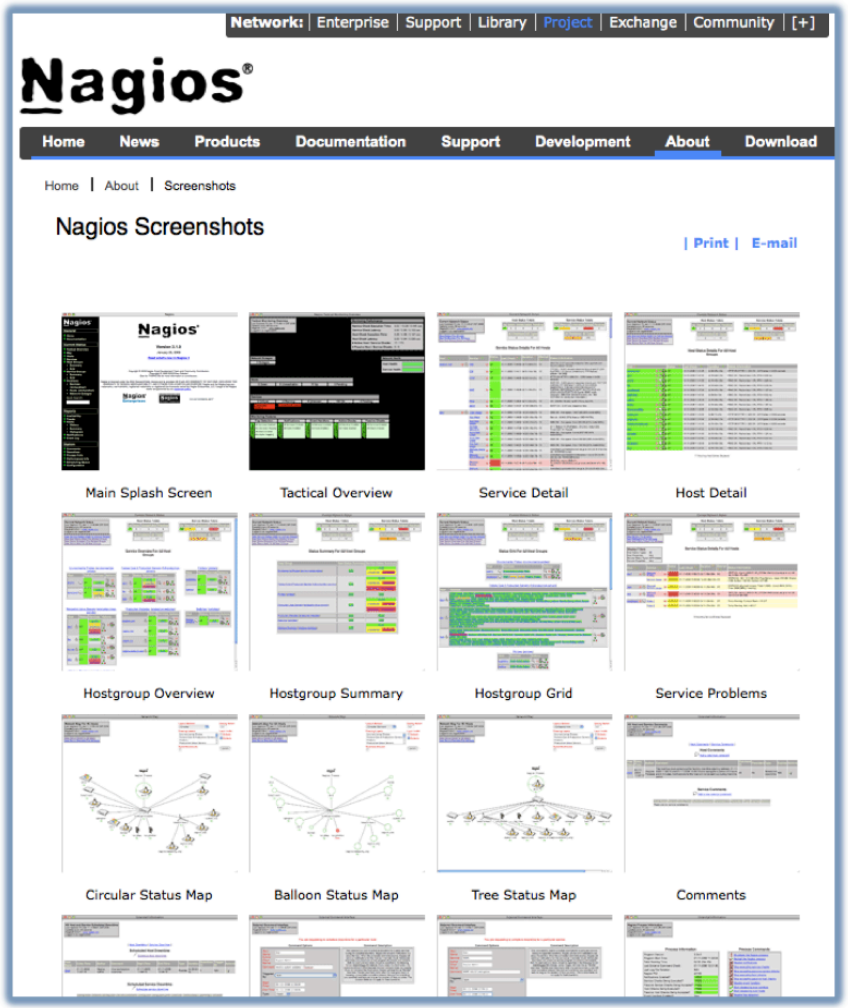
A few sample screen shots from a Nagios install.


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
TRTI TLD8 Servers, Virtual Machines, Routers (TLD8)
Host Status Services Actions
NOC-TLD8 UP 1 OK
TRTI Management Virtual Machines (VM-mgmt)
Host Status Services Actions
DNS-ROOT UP 1 OK
ISP-DNS UP 1 OK


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


NOC-TLD1
Up
NS1-TLD1
Up
TRTI-TLD1
Up
NOC-TLD2
Up
TRTI-TLD2
Up
NS1-TLD2
Up
TRTI-NOC
Up
TRTI-CS
Up
TLD1-RTR
Up
TLD2-RTR
Up
NOC-TLD3
Up
ISP-DNS
Up
TRTI-MGMT
Up
localhost
gateway
Up
TRTI-TLD3
Up
TLD3-RTR
Up
NS1-TLD3
Up
DNS-ROOT
Up
Nagios
Nagios Process
TRTI-ATCK-A
Up
TLD4-RTR
Up
NOC-TLD4
Up
TRTI-TLD4
Up
ISP-RTR
Up
TLD8-RTR
Up
TLD5-RTR
Up
NS1-TLD8
Up
TRTI-TLD8
Up
TLD7-RTR
Up
TLD6-RTR
Up
NS1-TLD4
Up
TRTI-TLD5
Up
NOC-TLD8
Up
TRTI-TLD7
Up
NOC-TLD5
Up
TRTI-TLD6
Up
NS1-TLD7
Up
NS1-TLD5
Up
NOC-TLD7
Up
NS1-TLD6
Up
NOC-TLD6
Up

More Sample Screenshots



Many more sample Nagios screenshots available here:

http://www.nagios.org/about/screenshots