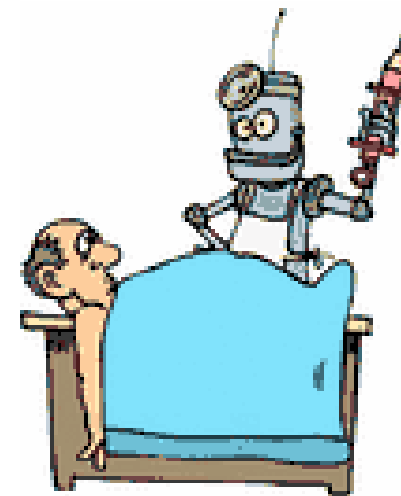


Professional Network Monitoring Made Easy w/ Nagios (TAFKAN)

William Emmanuel S. Yu

SVI Technologies Inc.

March 29, 2005



What makes a good network monitor?



Network Monitoring

- Ability to track resources within a network from a **centralized monitoring system**

- Ability to monitor various resources such as:

- **Network Links**
- **Systems and Hosts**
- **Services**



- The ultimate goal of any network monitoring system is ***“To inform administrators of faults before the customer knows about them”***.

Important Characteristics



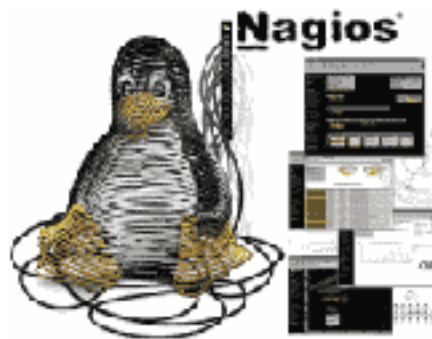
- **Transparency**
 - No changes to any client or server are required
- **Security**
 - No one has access to data except owner of monitor machine (such as auditor)
 - Monitored machine cannot change data once it is collected
- **Performance**
 - Checks are designed to take limited resource in the monitored host or service
 - Monitor never writes packets
- **Accessibility**
 - Necessary hosts and services are available

Other Characteristics



- **Notification**
 - Electronic mail, SMS, Pagers
- **Reports**
 - Ability to generate necessary reports
 - Enable monitoring of statistics and trends
- **Service Level Availability**
 - Most important of possible reports
 - Determine service or host performance with SLAs
 - Key metric use to measure system performance

What is Nagios?



Nagios



- **TAFKAN**
 - The Application Formerly Known as Netsaint
- **Open**
 - Open Source Network Monitoring Software
- **Complete**
 - Host and service based network monitor
- **Modular**
 - Uses Plug-in to provide testing functionality
- **Portable**
 - Designed to run under Linux, works under most UNIX variants

Why Use Nagios?



- Urgent need for a network monitoring solution
 - Easy to obtain (**Open Source**)
 - Just a download away!
- **Cost**
 - Commercial monitoring solutions (Tivoli, CA, HP) are expensive
 - Commercial solutions charge on a per monitored host
- **Configuration, maintenance**
 - Relatively tedious but straight forward to configure
- Monitor many **disparate servers** and network rather than a few central servers

Capabilities



- Pro-active monitoring the following **systems**:
 - **Network Interfaces** and Links
 - **Edge-of-Network** Services (Proxies, DNS and others) Staff servers
 - Core Application and **Production Servers**
- Pro-active monitoring the following **subsystems**:
 - **Connectivity**
 - **Storage**
 - **Counters** - Temperature, CPU, memory, MS Performance counters, SNMP
 - **Network Services** - SNMP, POP, IMAP, Exchange, SQL, Oracle, HTTP

Capabilities



- **Generates reports** on host/service
 - Trends
 - Availability
 - Alert Histogram
 - Alert History
 - Alert Summary
- Virtually **unlimited expandability** with plug-ins
 - Open source software. Can write ones own plug-ins!
- Comprehensive **Web-based interface**
- Configurable **notification system**

Limitations



- Restricted by your **network structure**
 - Does not have automatic scanning functionality of commercial tools
 - You must know your network to use this!
- Cannot store **performance data** only states
 - However, some people have written plug-ins to store actual performance counter data (<http://apan.sourceforge.net/>)
- Standard interface **not very user friendly**
 - Must add links to hosts and services that a person or people are responsible for
 - Configuration files are tedious (*A test to you copy-and-paste skills*)

What Next?



Installation



- Binaries and sources can be downloaded from:
 - *<http://www.nagios.org/>*
- Install **Nagios** using the default package installer of your operating system
 - RedHat, Fedora, SuSE users use RPM
 - Debian, Ubuntu users use DEB
 - Other people build from source
- **Minimum packages** to install to be useful:
 - Base Nagios Package
 - Base Nagios Plug-ins Package
 - Nagios Icons (Extras)

Configuration



- What **key items** to be configured?
 - Hosts/Host Groups
 - Services
 - Contacts
 - Notifications

- Other **optional items** that can be configured?
 - Dependencies
 - Extended Definitions
 - CGI Definitions

Host Configuration



- Types of devices **Nagios** can monitor
 - Servers, Switches, Routers
- Most kind of network devices
- Hosts can be grouped together (**Hostgroup**)
- Can hold a '**parent**' **directive** for common configuration items
- Gives a relational view of hosts
- Creates the logic that then distinguishes between **DOWN** and **UNREACHABLE** hosts

Service Configuration



- The core of the **Nagios** process
- Does the work by running **plug-ins** via command definitions
- **Nagios** Agents
 - Unix/Linux - **NRPE**
 - Windows NT/2K/XP - **NSClient**
- Can be configured - **Active** vs. **Passive**
- Can hold a '**parent**' **directive** for common configuration items

Contract Configuration



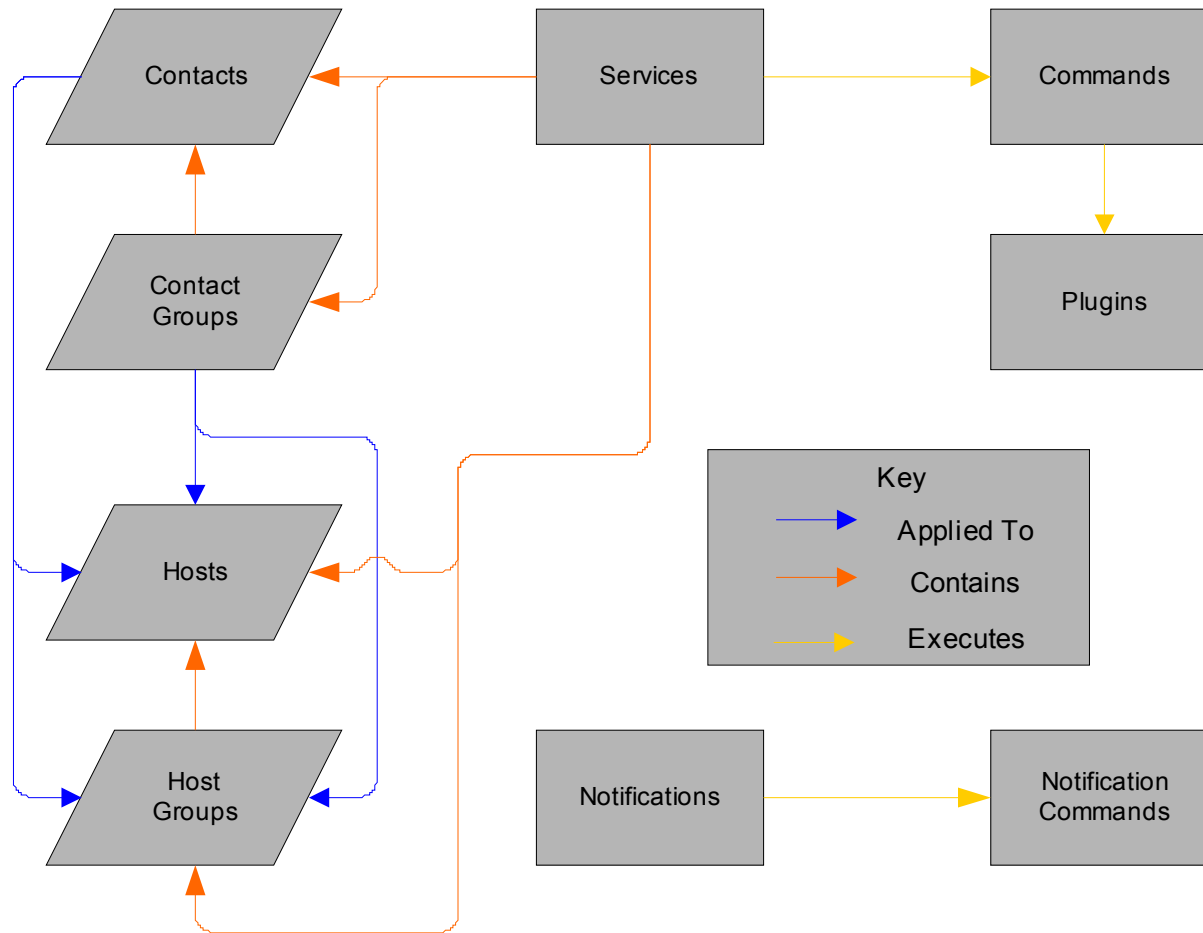
- Define notification conditions and cases
- Contains **contact** addresses
 - Pager/SMS
 - Electronic mail
 - Instant Messaging
- Contains **notification methods**
- Can define **shifts** and other parameters
- **Virtual contacts** (groups of contacts)

Notification Configuration



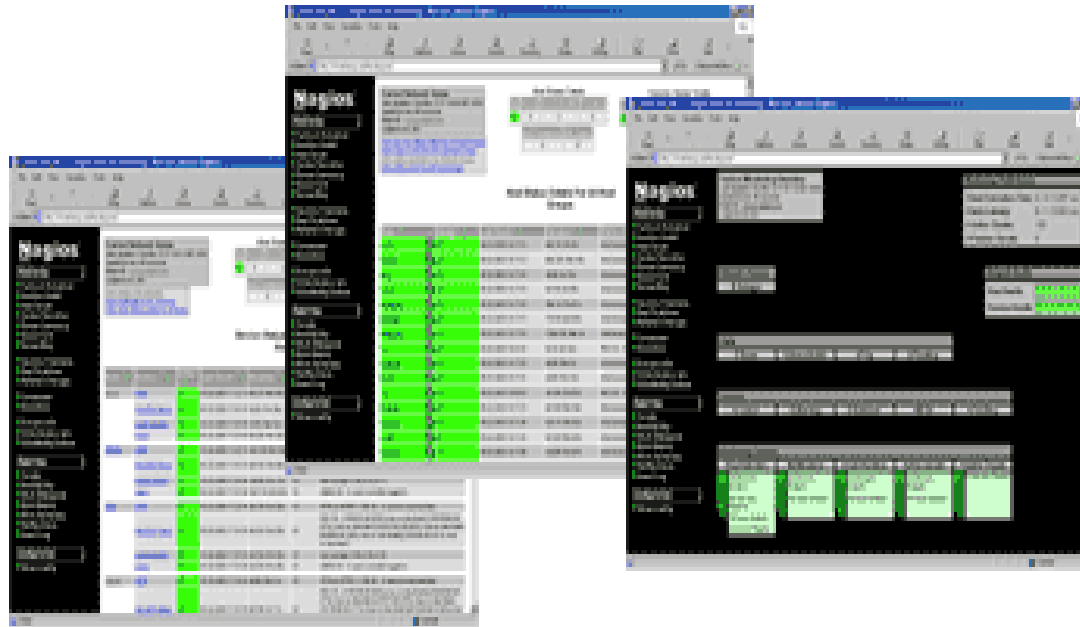
- Sent on a state change occurring
 - **Host change:** CRITICAL, UNREACHABLE, WARNING, OK, RECOVERY
 - **Service change:** CRITICAL, WARNING, OK, RECOVERY
- Can be escalated to **alternative** and **inclusive contacts**
- **Date** and **Time** can be specified

Configuration Relationships



Screenshots

Nagios[®]



Exception Tracking Screen



Nagios

- General
- Home
- Home screen
- Monitoring
 - Hosts Overview
 - Service Overview
 - Service Summary
 - Service Map
 - IT Service Map
- Network Problems
- Network Utilization
- Triggers
- Availability
- Configuration
- Log Files
- Comments
- Queries
- Performance Data
- Configuration
 - Configuration
 - View Config

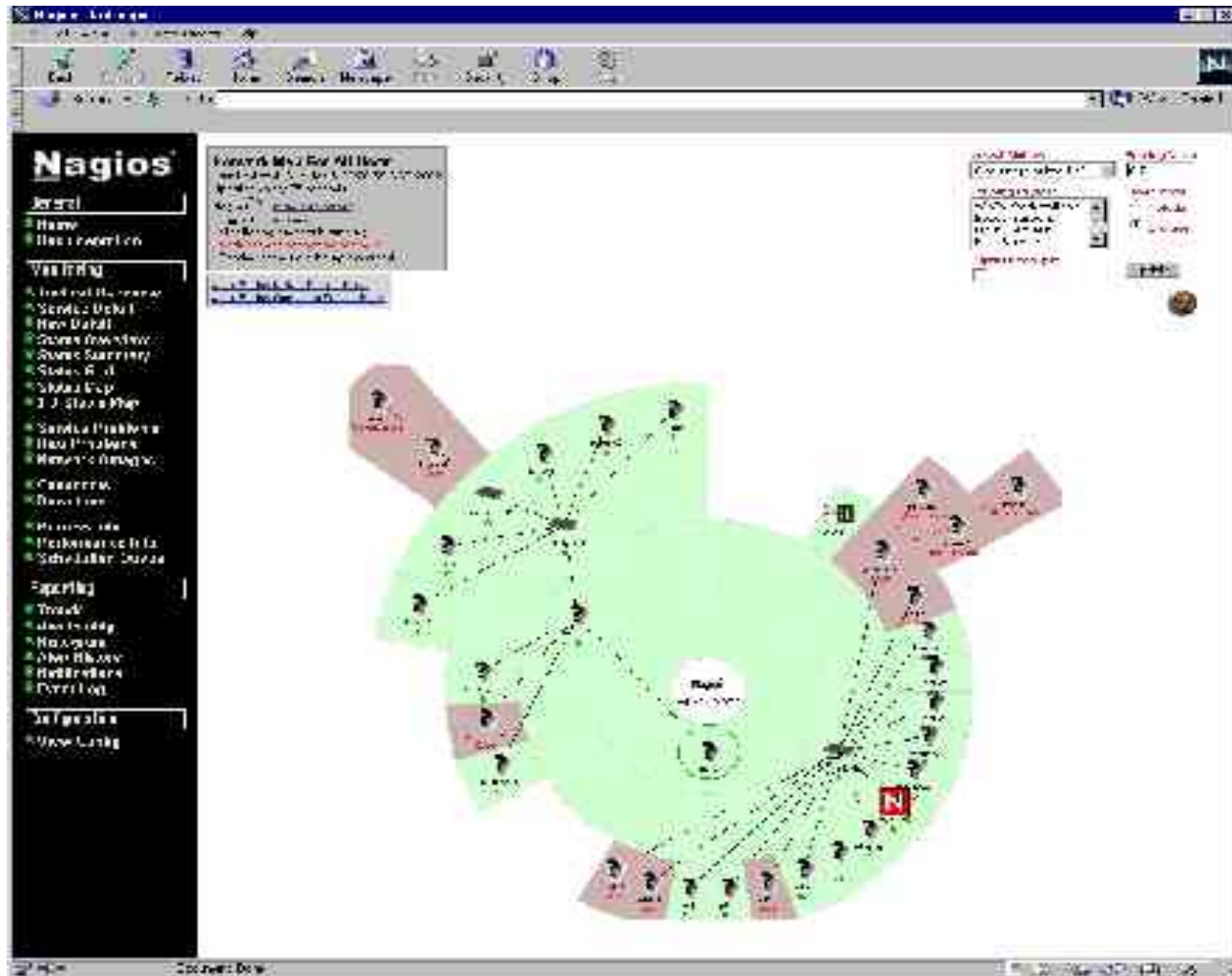
Host Status Table

Service Status Table

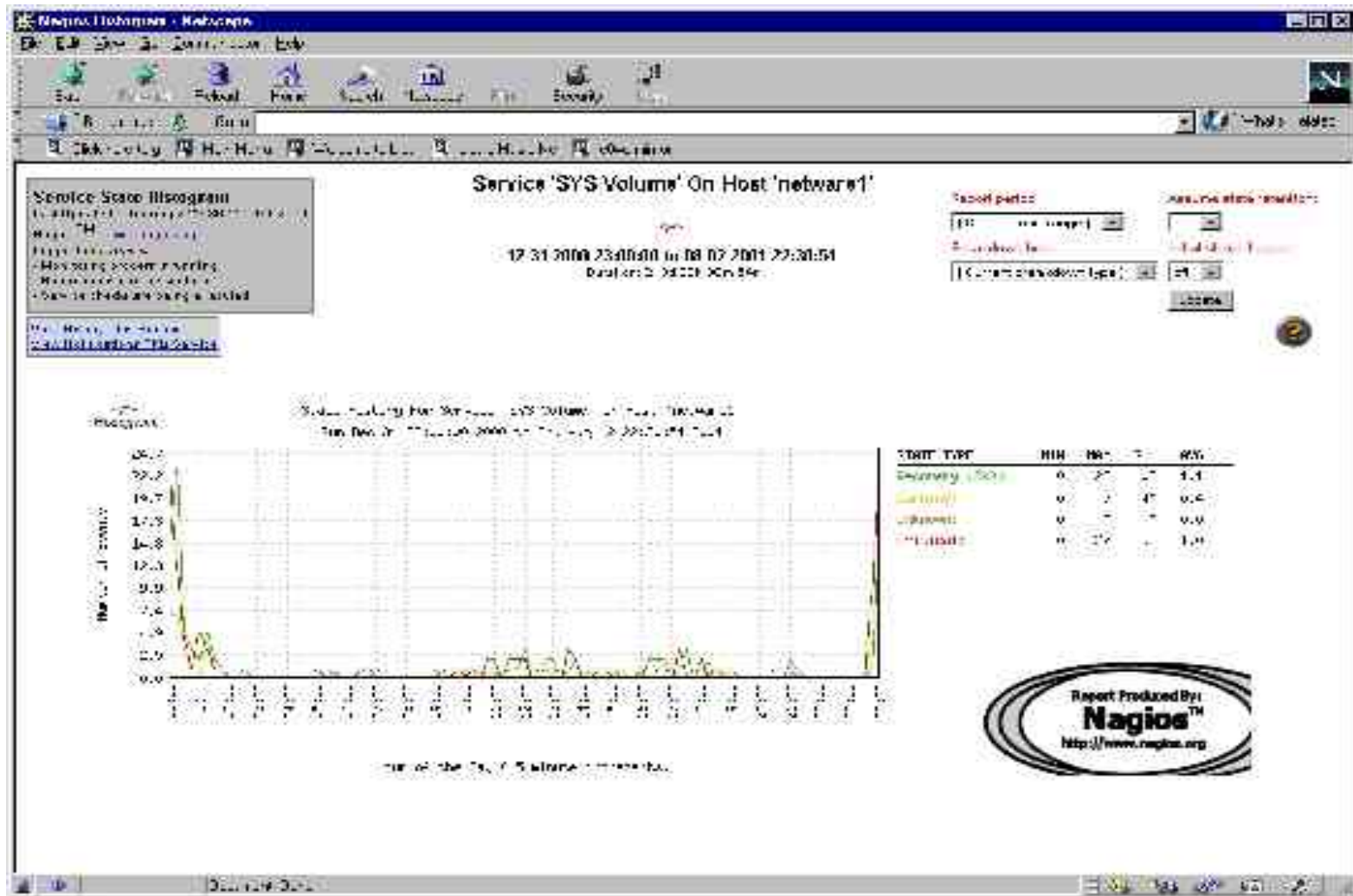
Service Details For All-Hosts

Host	Service	Status	Host Group	Duration	Service ID	Service Description
Host1	Service1	Down	Host Group 1	10:00:00 - 10:00:01	1000000000	Service 1 Description
Host2	Service2	Down	Host Group 2	10:00:00 - 10:00:01	1000000001	Service 2 Description
Host3	Service3	Down	Host Group 3	10:00:00 - 10:00:01	1000000002	Service 3 Description
Host4	Service4	Down	Host Group 4	10:00:00 - 10:00:01	1000000003	Service 4 Description
Host5	Service5	Down	Host Group 5	10:00:00 - 10:00:01	1000000004	Service 5 Description
Host6	Service6	Down	Host Group 6	10:00:00 - 10:00:01	1000000005	Service 6 Description
Host7	Service7	Down	Host Group 7	10:00:00 - 10:00:01	1000000006	Service 7 Description
Host8	Service8	Down	Host Group 8	10:00:00 - 10:00:01	1000000007	Service 8 Description
Host9	Service9	Down	Host Group 9	10:00:00 - 10:00:01	1000000008	Service 9 Description
Host10	Service10	Down	Host Group 10	10:00:00 - 10:00:01	1000000009	Service 10 Description

System Map



Histogram Screen



Tactical Overview Screen



The screenshot displays the Nagios Tactical Overview screen. On the left is a navigation menu with the following items:

- General
- Home
- Home/Configuration
- Home/Overview
- Tactical Overview
- Status Detail
- System Overview
- Status Summary
- Status Grid
- Status Map
- Full Status Map
- Service Production
- Network Diagrams
- Home
- Config/Modify
- Config/History
- Config/Features
- Log On
- Configure
- Describe
- Program Info
- Performance Info
- Configure Help
- View/Logout

The main content area includes several panels:

- Latest Monitoring Overview:** A summary of the current monitoring status.
- Monitoring Parameters:** A table showing various monitoring parameters and their values.
- Network Diagram:** A visual representation of the network topology.
- Hosts:** A table listing monitored hosts and their status.
- Services:** A table listing monitored services and their status.
- Monitored Services:** A detailed view of specific monitored services.

Host Details Screen



Host State Breakdowns:



State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	16:23h 51m 21s	96.43%	99.70%
	Scheduled	16:23h 51m 21s	100.00%	100.00%
	Total	16:23h 51m 21s	96.43%	99.70%
DOWN	Unscheduled	00:00h 0m 0s	0.00%	0.00%
	Scheduled	00:00h 0m 0s	0.00%	0.00%
	Total	00:00h 0m 0s	0.00%	0.00%
UNREACHABLE	Unscheduled	16:23h 51m 21s	100.00%	100.00%
	Scheduled	16:23h 51m 21s	100.00%	100.00%
	Total	16:23h 51m 21s	100.00%	100.00%
un-determined	Scheduled - Warning	00:00h 0m 0s	0.00%	
	un-determined	16:23h 51m 21s	100.00%	
	Total	16:23h 51m 21s	100.00%	
All	Total	16:23h 51m 21s	100.00%	100.00%

State Breakdowns For Host Services:

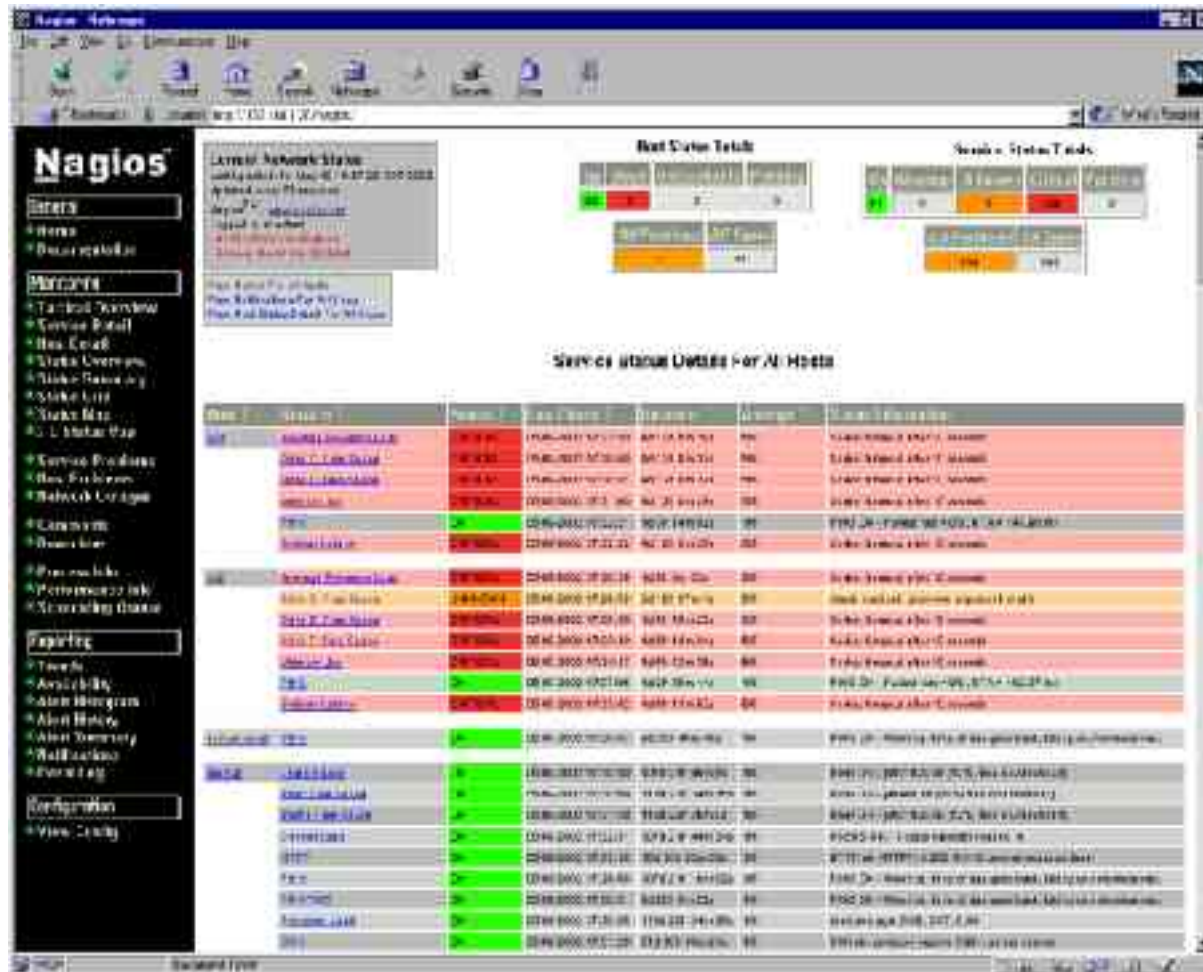
Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
HTTP	99.752% (99.752%)	0.000% (0.000%)	0.000% (0.000%)	1.248% (1.248%)	0.000%
SNMP	99.711% (99.711%)	0.000% (0.000%)	0.000% (0.000%)	0.600% (0.600%)	0.000%
SSH	97.000% (97.000%)	0.000% (0.000%)	16.362% (16.362%)	1.238% (1.238%)	0.000%
POP	96.414% (96.414%)	0.000% (0.000%)	0.000% (0.000%)	3.586% (3.586%)	0.000%
SMTP	96.045% (96.045%)	0.000% (0.000%)	0.000% (0.000%)	1.955% (1.955%)	0.000%

Host Log Entries:

[View All Log Entries](#)

Event Start Time	Event End Time	Event Duration	Event State	Event Type	Event State Information
02/17/2000 11:00:00	02/17/2000 11:00:10	00:00:10	UP	Host	First time state assumed (7... L... B...)
02/21/2000 08:10:11	02/21/2000 08:10:20	00:00:09	DOWN	CRITICAL	CRITICAL: Ping failed over a 10 second...
02/21/2000 08:18:20	02/21/2000 08:22:00	00:03:40	UP	Host	PING OK: 3... 3% 57% 0.21...

System Status Screen

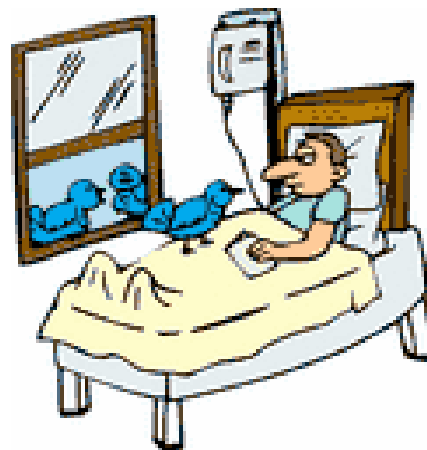


Advanced Configuration



- **Dependencies**
 - Host and service
 - Enable smart notification
- **External Definitions**
 - Icons, graphics and etc.
- **Event Handlers**
 - Specify events and triggers for automatic execution
- **Redundant and Distributed Set-up**
 - Multiple **Nagios** monitoring systems
- **Flap detection**

What are you waiting for?



Conclusion



- If you are in need of a **cost effective, scalable** and **extendable** network monitoring solution
 - **Nagios** is the answer!
- If you can bear the brunt of doing **manual configuration**
 - **Nagios** is the answer!
- If you want to monitoring multiple hosts and services **without paying a single cent**
 - **Nagios** is the answer!
- If you need something **Nagios** does not support
 - Use the SOURCE Luke! and write it yourself!