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”.

Copyright 2005 SVI Corporation - Confidential
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 one's 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/](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
Host Configuration
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

Contacts → Services → Commands
Contacts → Contact Groups → Services
Contacts → Hosts → Services
Contacts → Host Groups → Services

Contacts → Plugins

Services → Commands
Services → Plugins
Services → Notifications
Services → Notification Commands

Contact Groups → Services
Contact Groups → Plugins
Contact Groups → Notifications
Contact Groups → Notification Commands

Hosts → Services
Hosts → Plugins
Hosts → Notifications
Hosts → Notification Commands

Host Groups → Services
Host Groups → Plugins
Host Groups → Notifications
Host Groups → Notification Commands

Key:
- Applied To
- Contains
- Executes

Copyright 2005 SVI Corporation - Confidential
Exception Tracking Screen
System Map
Histogram Screen
Tactical Overview Screen
# Host Details Screen

## Host State Breakdowns

<table>
<thead>
<tr>
<th>Service</th>
<th>Type</th>
<th>Reason</th>
<th>Time</th>
<th>% Total Time</th>
<th>% Known Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>UP</td>
<td>Unscheduled</td>
<td>12:34 PM</td>
<td>123.45%</td>
<td>0.00%</td>
<td>123.45%</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td>123.45%</td>
<td>0.00%</td>
<td>123.45%</td>
</tr>
<tr>
<td>UOMA</td>
<td>Unscheduled</td>
<td>6:54 PM</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>IMPOSSIBLE</td>
<td>Unscheduled</td>
<td>7:12 PM</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
</tbody>
</table>

## Service Breakdowns For Host Services:

<table>
<thead>
<tr>
<th>Service</th>
<th>% Time OK</th>
<th>% Time Running</th>
<th>% Time Unknown</th>
<th>% Time Critical</th>
<th>% Time Undetermined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>98.7%</td>
<td>5.3%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>User</td>
<td>99.0%</td>
<td>1.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>User2</td>
<td>99.5%</td>
<td>0.5%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>User3</td>
<td>99.8%</td>
<td>0.2%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>User4</td>
<td>99.9%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

## Hosting Log Entries:

<table>
<thead>
<tr>
<th>Event Start Time</th>
<th>Event End Time</th>
<th>Event Duration</th>
<th>Event State Type</th>
<th>Event State Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/12/2000 10:00</td>
<td>02/12/2000 10:01</td>
<td>1 min</td>
<td>UP</td>
<td>First host state transition (from Down to Up)</td>
</tr>
<tr>
<td>02/12/2000 08:00</td>
<td>02/12/2000 08:01</td>
<td>1 min</td>
<td>DOWN</td>
<td>CRITICAL</td>
</tr>
<tr>
<td>02/12/2000 08:00</td>
<td>02/12/2000 08:01</td>
<td>1 min</td>
<td>UP</td>
<td>PINGCHECK 1 failed, 20% up, 70% down</td>
</tr>
</tbody>
</table>

Copyright 2005 SVI Corporation - Confidential
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!