Stop Worrying

Start Monitoring with

Nagios®

Andrew Libby
xforty technologies
alibby@xforty.com

Agenda

- About Me
- What is Nagios
- Features
- Web Screen Shots
- Nagios System Components
- Installation and Configuration
- Conclusions

About Me

- Work for xforty technologies
- Hybrid software developer and systems administrator
- Passionate Linux/ OSS enthusiast since 1994
- Live and work in Suburban Philadelphia

What is Nagios

Nagios is a powerful monitoring system that enables organizations to identify and resolve IT infrastructure problems before they affect critical business processes.

What is Nagios

Peace of mind.

Except...

when it wakes you up in the middle of the night with false positive notifications.....

How xforty uses Nagios

- Monitoring own IT systems and assets
- Monitoring and management services for customers
- Setup of customer monitoring systems

Features

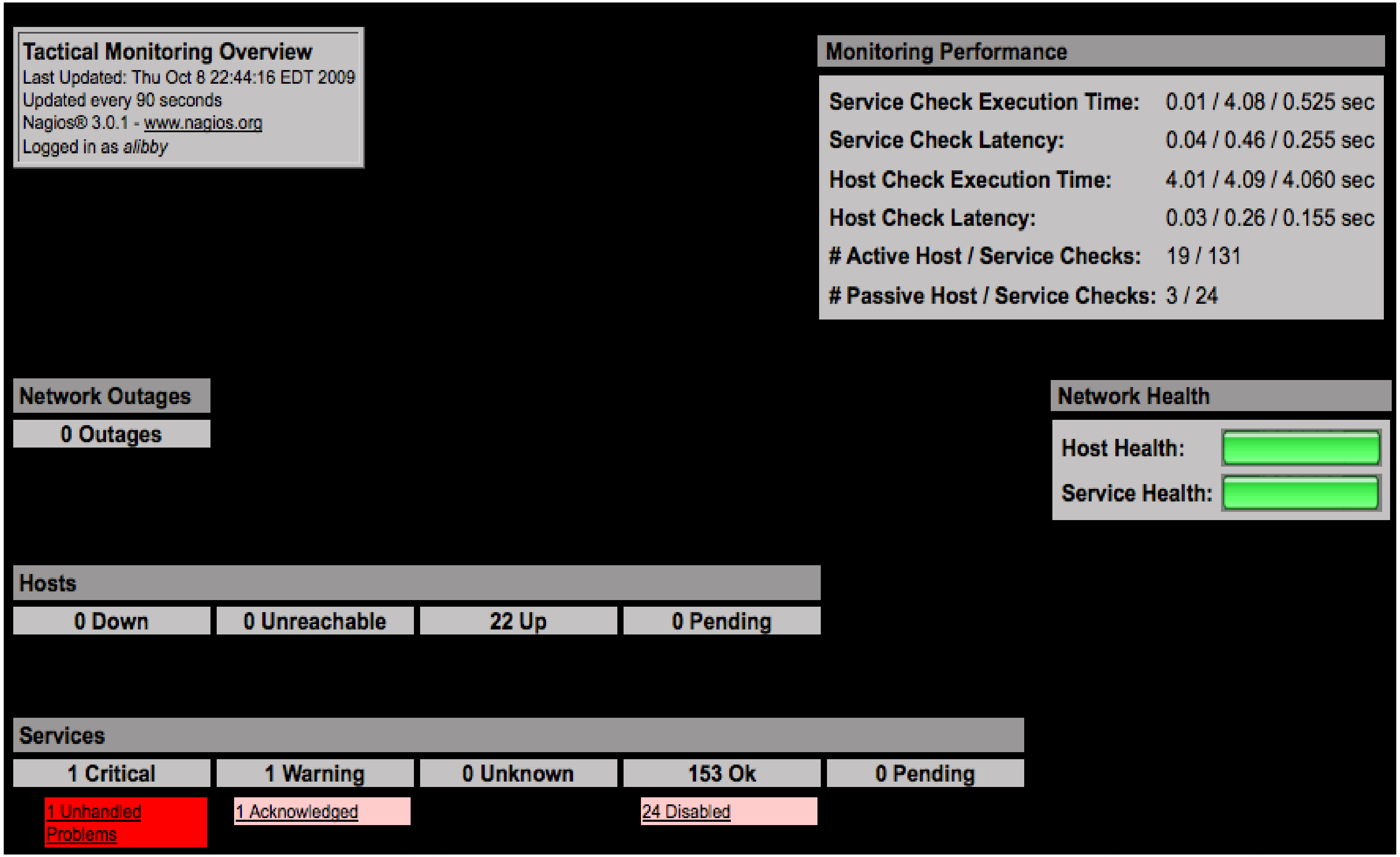
- Crazy Monitoring
- Web Interface
- Cross Platform Monitoring.
- Notifications
- Downtime Scheduling
- Problem acknowledgment
- Event correlation with dependencies

Features

- Distributed Monitoring
- Flap Detection
- Reporting, heh
- Community
- Fuhuhlexible

… Screen Shots

Dashboard



Tactical Monitoring Overview
Last Updated: Thu Oct 8 22:44:16 EDT 2009
Updated every 90 seconds
Nagios® 3.0.1 - www.nagios.org
Logged in as *alibby*

Monitoring Performance

Service Check Execution Time:	0.01 / 4.08 / 0.525 sec
Service Check Latency:	0.04 / 0.46 / 0.255 sec
Host Check Execution Time:	4.01 / 4.09 / 4.060 sec
Host Check Latency:	0.03 / 0.26 / 0.155 sec
# Active Host / Service Checks:	19 / 131
# Passive Host / Service Checks:	3 / 24

Network Outages

0 Outages

Network Health

Host Health:	🟩
Service Health:	🟩

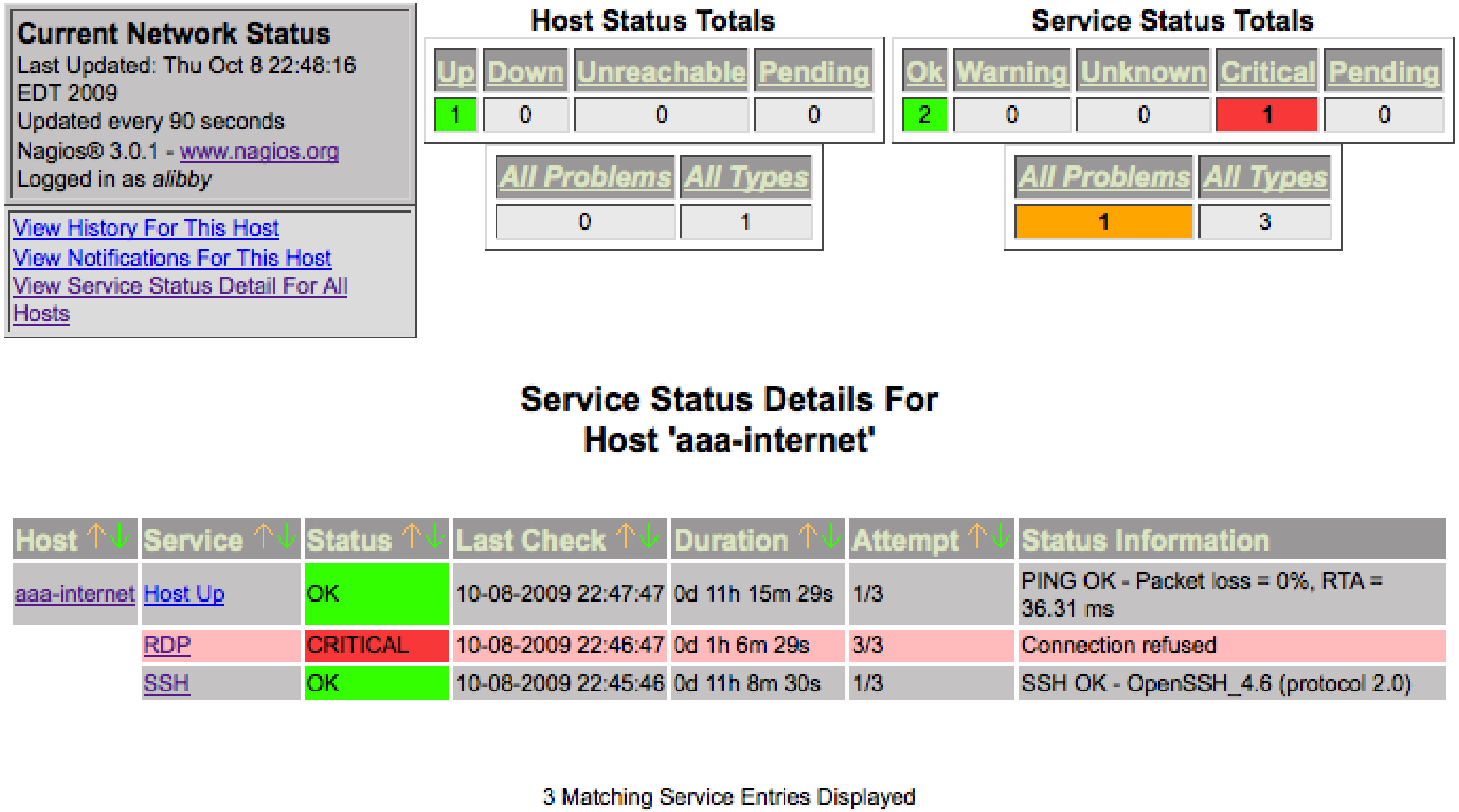
Hosts

0 Down	0 Unreachable	22 Up	0 Pending

Services

1 Critical	1 Warning	0 Unknown	153 Ok	0 Pending
1 Unhandled Problems	1 Acknowledged		24 Disabled	

Fault Detection



Current Network Status
Last Updated: Thu Oct 8 22:48:16 EDT 2009
Updated every 90 seconds
Nagios® 3.0.1 - www.nagios.org
Logged in as *alibby*

View History For This Host
View Notifications For This Host
View Service Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0

All Problems	*All Types*
0	1

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
2	0	0	1	0

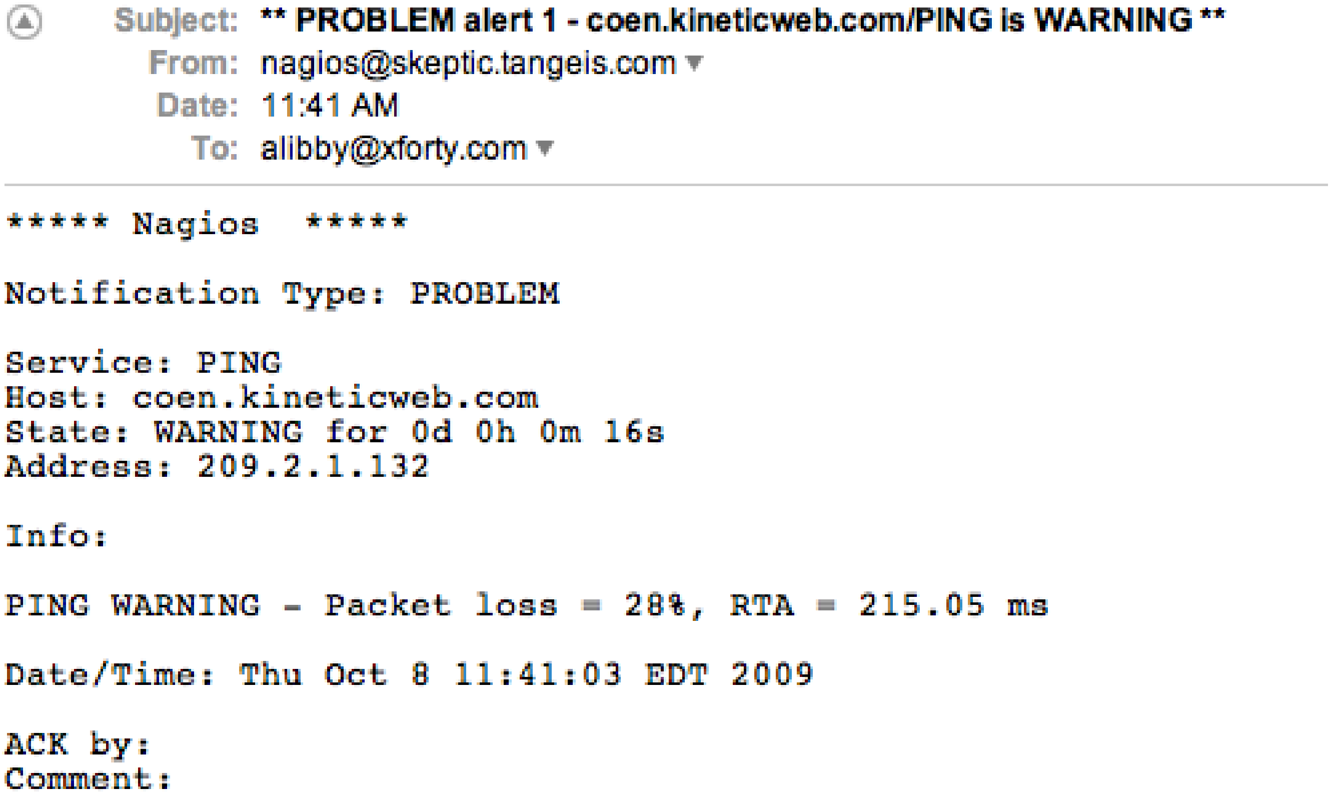
All Problems	*All Types*
1	3

Service Status Details For Host 'aaa-internet'

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
aaa-internet	Host Up	OK	10-08-2009 22:47:47	0d 11h 15m 29s	1/3	PING OK - Packet loss = 0%, RTA = 36.31 ms
	RDP	CRITICAL	10-08-2009 22:46:47	0d 1h 6m 29s	3/3	Connection refused
	SSH	OK	10-08-2009 22:45:46	0d 11h 8m 30s	1/3	SSH OK - OpenSSH_4.6 (protocol 2.0)

3 Matching Service Entries Displayed

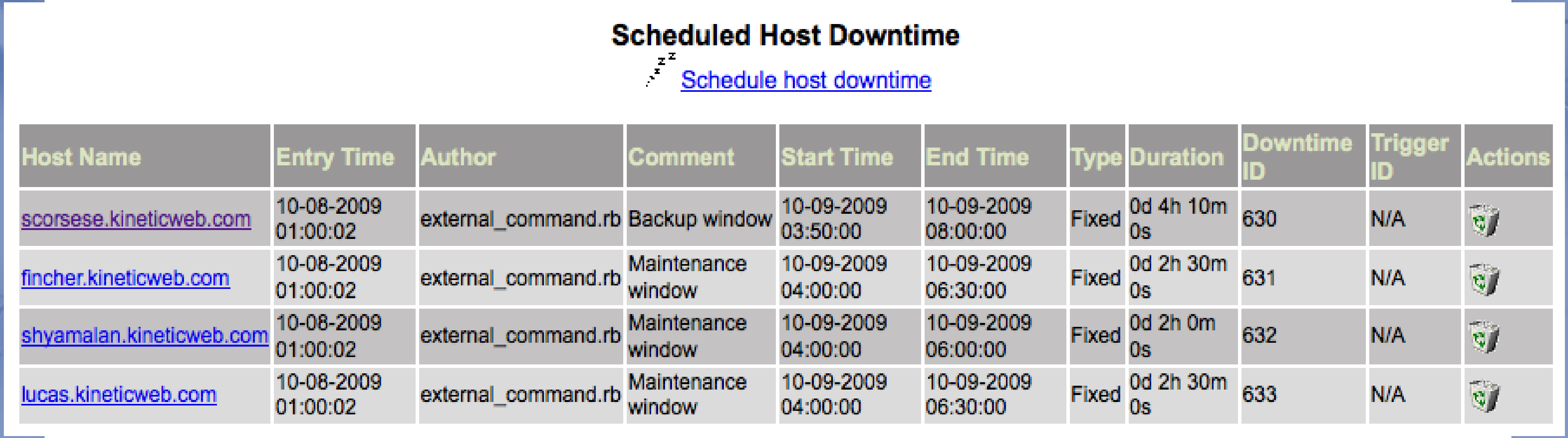
Notifications



Subject: ** PROBLEM alert 1 - coen.kineticweb.com/PING is WARNING **
From: nagios@skeptic.tangeis.com ▾
Date: 11:41 AM
To: alibby@xforty.com ▾

```
***** Nagios  *****

Notification Type: PROBLEM

Service: PING
Host: coen.kineticweb.com
State: WARNING for 0d 0h 0m 16s
Address: 209.2.1.132

Info:

PING WARNING - Packet loss = 28%, RTA = 215.05 ms

Date/Time: Thu Oct 8 11:41:03 EDT 2009

ACK by:
Comment:
```

Downtime Scheduling

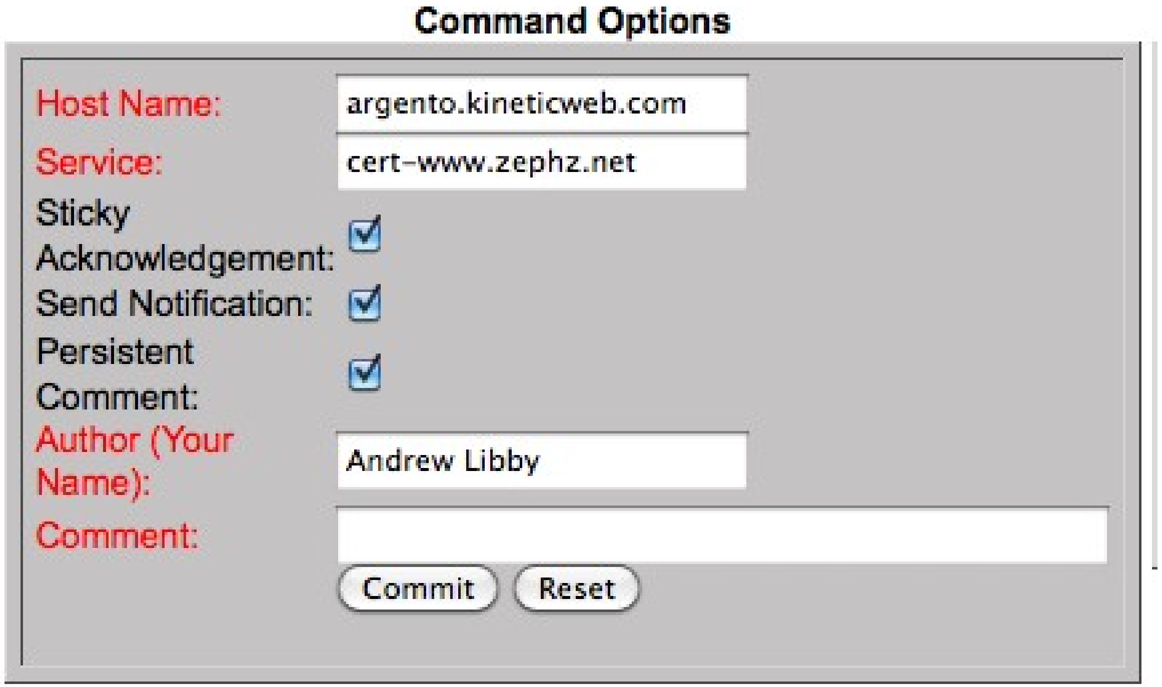


Scheduled Host Downtime

Schedule host downtime

Host Name	Entry Time	Author	Comment	Start Time	End Time	Type	Duration	Downtime ID	Trigger ID	Actions
scorsese.kineticweb.com	10-08-2009 01:00:02	external_command.rb	Backup window	10-09-2009 03:50:00	10-09-2009 08:00:00	Fixed	0d 4h 10m 0s	630	N/A	🗑
fincher.kineticweb.com	10-08-2009 01:00:02	external_command.rb	Maintenance window	10-09-2009 04:00:00	10-09-2009 06:30:00	Fixed	0d 2h 30m 0s	631	N/A	🗑
shyamalan.kineticweb.com	10-08-2009 01:00:02	external_command.rb	Maintenance window	10-09-2009 04:00:00	10-09-2009 06:00:00	Fixed	0d 2h 0m 0s	632	N/A	🗑
lucas.kineticweb.com	10-08-2009 01:00:02	external_command.rb	Maintenance window	10-09-2009 04:00:00	10-09-2009 06:30:00	Fixed	0d 2h 30m 0s	633	N/A	🗑

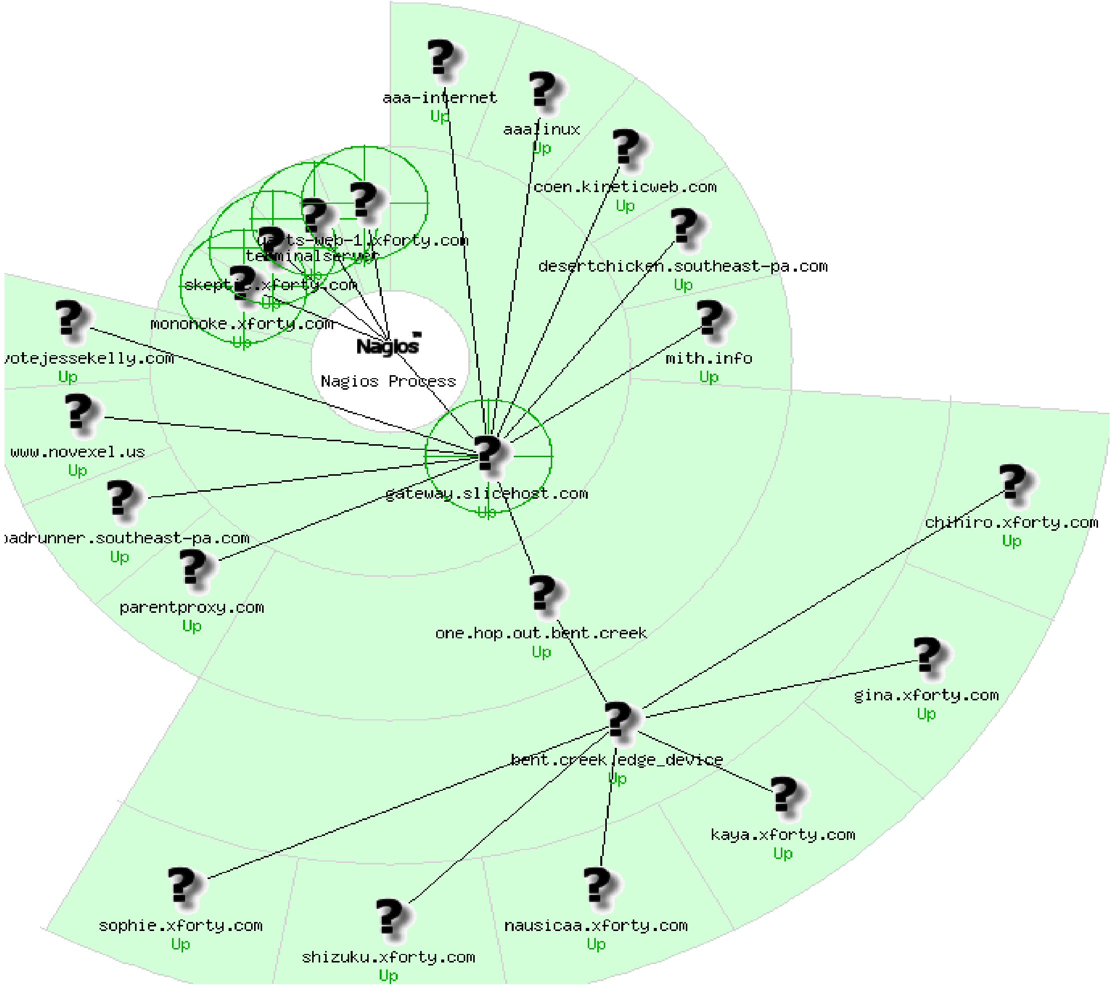
Problem Acknowledgment



Command Options

Host Name:	argento.kineticweb.com
Service:	cert-www.zephz.net
Sticky Acknowledgement:	☑
Send Notification:	☑
Persistent Comment:	☑
Author (Your Name):	Andrew Libby
Comment:	

Event Correlation with Deps



Reporting

- Reports provide a historical record of outages, events, notifications, and alert response for later review. Availability reports help ensure your SLAs are being met.

“My boss told me I had to do comprehensive reporting using only Nagios reports – FML.”

Nagios
System Components

High Level

- Web Interface/ CGI Programs
- Core Nagios Engine (/usr/bin/nagios)
- Plugins (/usr/lib/nagios/plugins)
- Add Ons (nrpe/ nsca/ netc)

Web / CGI

- A series of C language CGI programs
- Read Nagios data files to present and report status
- Invoke actions by writing to a file that's monitored by nagios
- Typically runs under apache, but likely to work under any CGI capable web server.

Nagios Core

- Runs as daemon
- Invokes active checks by according to configuration
- Reads commands from external command file
- Carries out notifications

Plugins

- The secret sauce of Nagios extensibility
- Small simple programs
- Conform to a basic protocol for communicating status back to Nagios core

Developing Plugins

```
#!/bin/bash
. /usr/lib/nagios/plugins/utils.sh

STATE=$[$RANDOM % 4]

case $STATE in
  $STATE_OK )
        echo "OK: Karma good";;
  $STATE_WARNING )
        echo "WARN: Karma so so";;
  $STATE_CRITICAL )
        echo "CRIT: You're a bad person";;
  * )
        STATE=3
        echo "UNKNOWN: The universe knows not of you";;
esac

exit $STATE
```

Plugins

apt

- breeze
- clamd
- cluster
- dhcp
- disk
- disk_smb
- file_age
- flexlm
- ftp
- http
- icmp
- ide_smart
- ifoperstatus
- ifstatus
- imap
- ircd
- load
- log
- mailq
- mrtg
- mysql
- nagios
- nntp
- nrpe
- ntp
- Oracle
- pgsql
- ping
- pop
- procs
- smtp
- ssh
- swap
- tcp
- time
- udp
- ups
- users

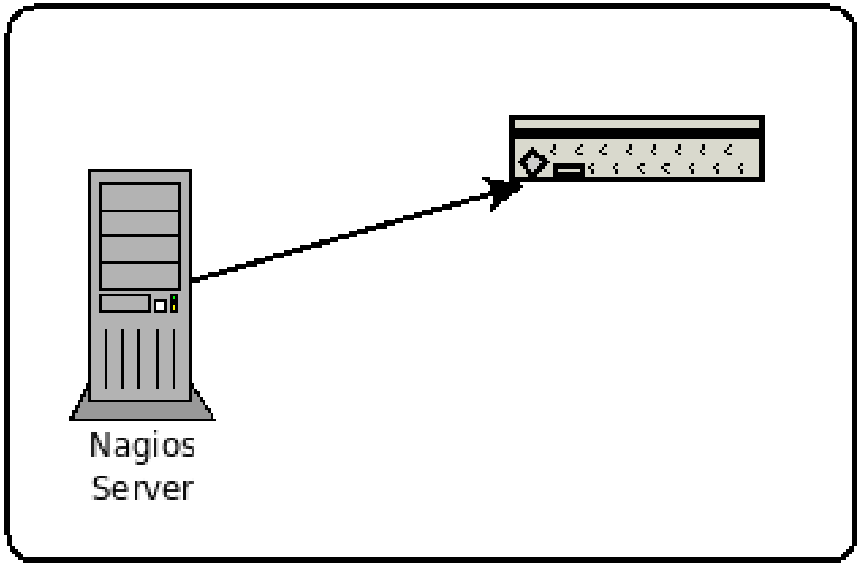
Add Ons

- NRPE – Remote agent for running active checks
- NCSA – Remote agent for running passive checks. Distributed Nagios...
- NagVis – Visualization add on. Makes maps of nagios hosts.
- Nagios Grapher – Nagios RRD tool integration.
- NDO

Typical Configurations

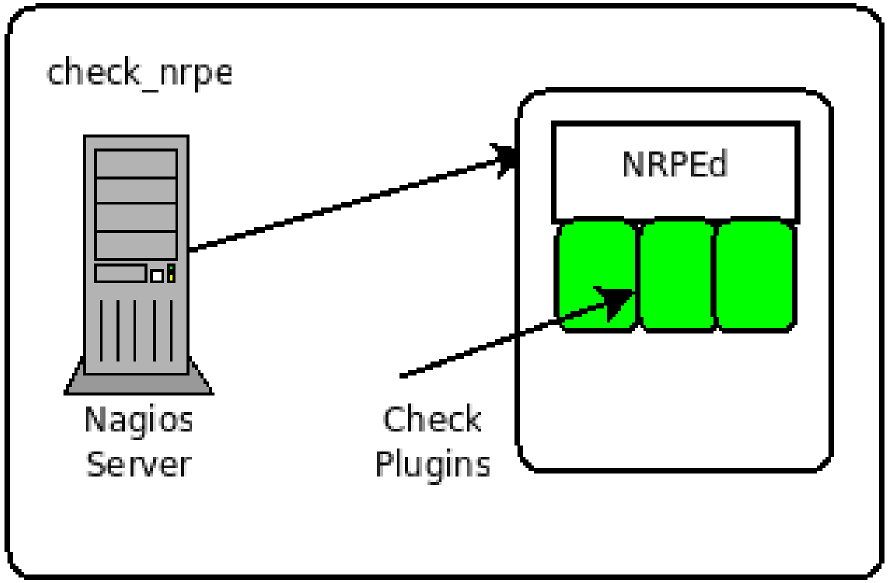
Simple Active Monitor

- Monitors services directly accessible by the Nagios server.
- Handy for public network services, little else.



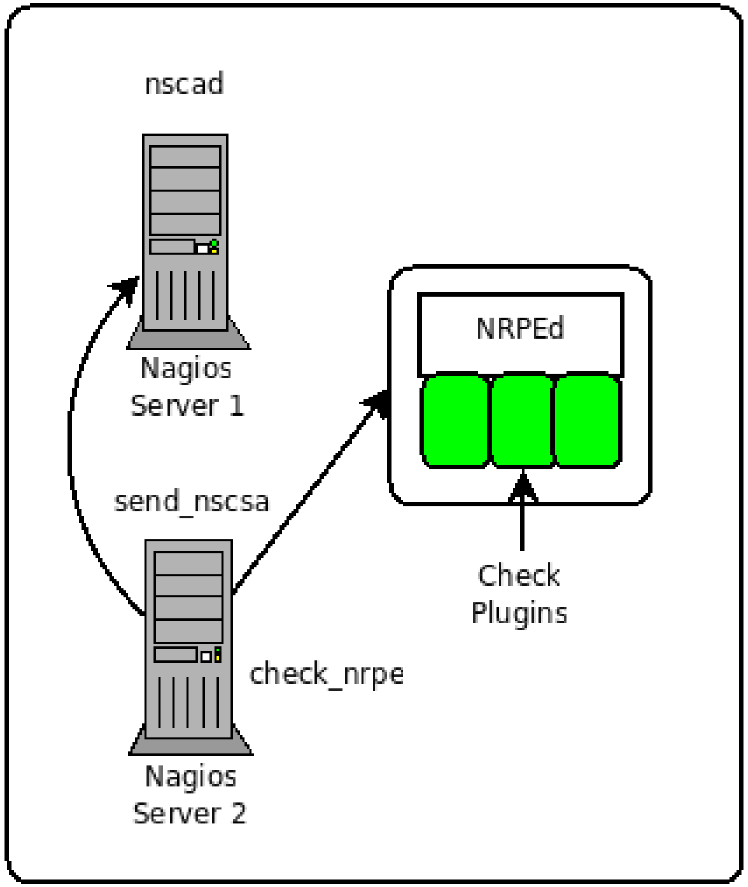
NRPE Monitoring

- NRPE is an agent/ plugin combination
- Can run standard plugins on monitored host.
- Expands montoring greatly.
- check_nrpe! remote_plugin

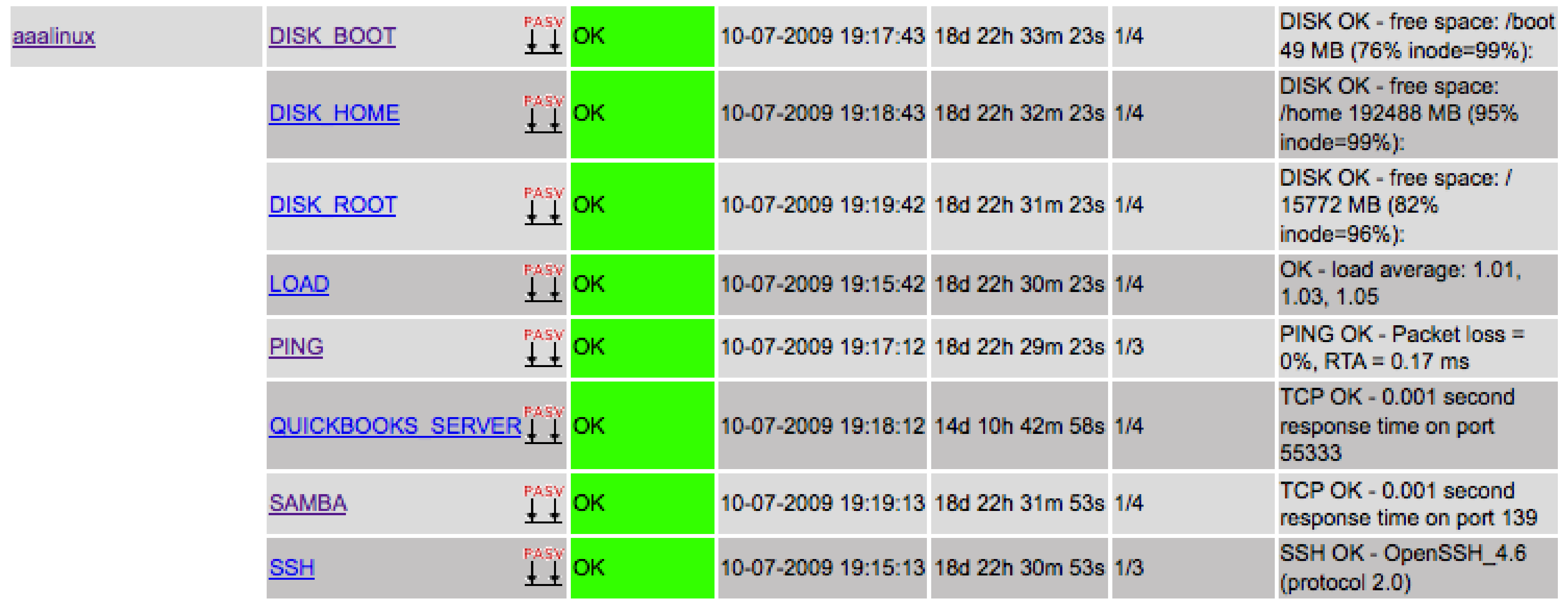


NSCA Setup

- Multiple Nagios servers
- srv2 monitors and sends events to srv1
- Srv1 and Srv2 can monitor like normal.
- Forwarded events are 'passive'



Passive vs Active



aaalinux	DISK_BOOT	PASV	OK	10-07-2009 19:17:43	18d 22h 33m 23s	1/4	DISK OK - free space: /boot 49 MB (76% inode=99%):
	DISK_HOME	PASV	OK	10-07-2009 19:18:43	18d 22h 32m 23s	1/4	DISK OK - free space: /home 192488 MB (95% inode=99%):
	DISK_ROOT	PASV	OK	10-07-2009 19:19:42	18d 22h 31m 23s	1/4	DISK OK - free space: / 15772 MB (82% inode=96%):
	LOAD	PASV	OK	10-07-2009 19:15:42	18d 22h 30m 23s	1/4	OK - load average: 1.01, 1.03, 1.05
	PING	PASV	OK	10-07-2009 19:17:12	18d 22h 29m 23s	1/3	PING OK - Packet loss = 0%, RTA = 0.17 ms
	QUICKBOOKS_SERVER	PASV	OK	10-07-2009 19:18:12	14d 10h 42m 58s	1/4	TCP OK - 0.001 second response time on port 55333
	SAMBA	PASV	OK	10-07-2009 19:19:13	18d 22h 31m 53s	1/4	TCP OK - 0.001 second response time on port 139
	SSH	PASV	OK	10-07-2009 19:15:13	18d 22h 30m 53s	1/3	SSH OK - OpenSSH_4.6 (protocol 2.0)

Monitoring Windows

- Typically nsclient++
- Like nrpe (actually can be nrpe)
- Can monitor any windows performance monitor counter
- Not as common as Linux/ Unix but still done.

Installation and Configuration

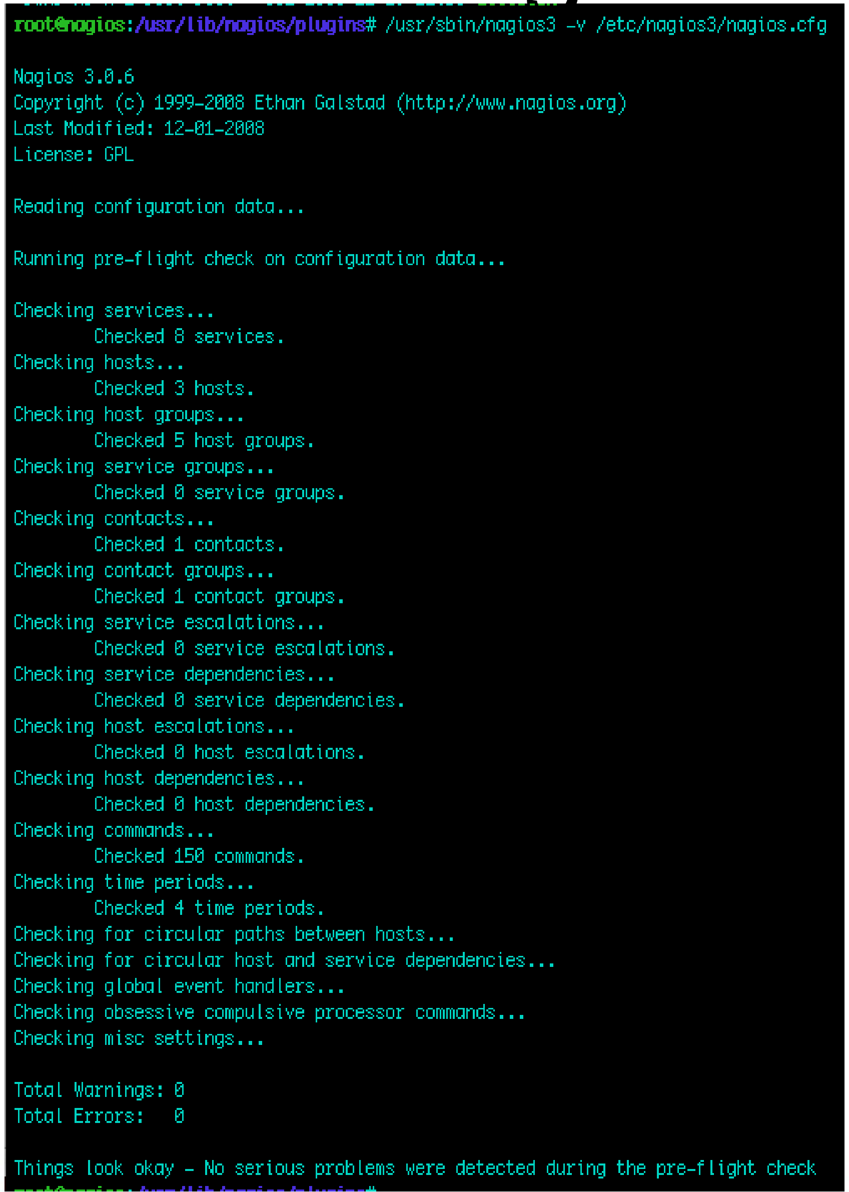
Installing

- Installation is pretty simple
- Ubuntu: apt-get install nagios3 nagios-plugins
- RedHat equally simple, but it's been a while.
- Once it's installed, the configuration begins.

Configuring

- Initially it blows.
- Zillions of options.
- Docs can be difficult to navigate.
- Be patient.
- Make use of -v configuration testing.

Configuration Testing



```
root@nagios:/usr/lib/nagios/plugins# /usr/sbin/nagios3 -v /etc/nagios3/nagios.cfg

Nagios 3.0.6
Copyright (c) 1999-2008 Ethan Galstad (http://www.nagios.org)
Last Modified: 12-01-2008
License: GPL

Reading configuration data...

Running pre-flight check on configuration data...

Checking services...
        Checked 8 services.
Checking hosts...
        Checked 3 hosts.
Checking host groups...
        Checked 5 host groups.
Checking service groups...
        Checked 0 service groups.
Checking contacts...
        Checked 1 contacts.
Checking contact groups...
        Checked 1 contact groups.
Checking service escalations...
        Checked 0 service escalations.
Checking service dependencies...
        Checked 0 service dependencies.
Checking host escalations...
        Checked 0 host escalations.
Checking host dependencies...
        Checked 0 host dependencies.
Checking commands...
        Checked 150 commands.
Checking time periods...
        Checked 4 time periods.
Checking for circular paths between hosts...
Checking for circular host and service dependencies...
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
root@nagios:/usr/lib/nagios/plugins#
```

Common File Locations

- /etc/nagios3 – Main configuration files
- /etc/nagios3/objects – Host/ Service/ Contact coniguratіons
- /etc/nagios-plugins/config – Plugin check command definitions

nagios.cfg

- Global configuration
- References to other configuration files
- Logging configuration
- User Nagios runs under, etc

nagios.cfg

```
log_file=/var/log/nagios3/nagios.log

# Commands definitions
cfg_file=/etc/nagios3/commands.cfg

# nagios-plugins package
cfg_dir=/etc/nagios-plugins/config

cfg_dir=/etc/nagios3/conf.d
```

cgi.cfg

- CGI Interface configuration
- Specifies locations of CGI assets
- Authentication and Authorization policy
- Either need to edit for each user, or specify * for all appropriate permissions.

Configuration Concepts

- Hosts
- Services
- Host Groups
- Service Groups
- Contacts
- Contact Groups
- Check Commands
- Templates

Hosts/ Services

```
define host {
     use                 generic-host
     host_name           moejoe.local
     alias               moejoe
     address             10.211.55.2
     }

define service {
     use                 generic-service
     host_name           moejoe.local
     service_description SSH
     check_command       check_ssh
     }
```

Templates

```
define host{
  name                            generic-host
  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
  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
  }
```

Host/ Service Groups

```
define hostgroup {
     hostgroup_name  leenux-servers
     alias           Servers running Leenux
     members         localhost
     }

define hostgroup {
     hostgroup_name  http-servers
     alias           HTTP servers
     members         localhost
     contact_groups  web_group
     }
```

Contacts/ Contact Groups

```
define contactgroup{
     contactgroup_name  admins
     alias                   admins
     members                 alibby
     }

define contactgroup{
     contactgroup_name  web_group
     alias                   web_group
     members              pearcec, sshivell
     }
```

Check Commands

```
define command{
        command_name    check_disk_root
        command_line    /pth/to/check_disk \
                -p / -c 10G -w 20G
     }
```

Getting Value from Monitoring

- Disciplined Maintenance. Managing the signal to noise ratio.
- Notification Policies. Does it make sense to get update warnings at night?
- Use host and service deps to keep notifications useful.

Conclusion

- Nagios is a very respectable monitoring system.
- Initial setup is somewhat involved.
- Can perform basic to advanced monitoring
- With a little work sophisticated needs can be met including trending, data visualization, and reporting
- *(Free Vinyl)

Contacting Me

- alibby@xforty.com
- twitter.com/alibby
- xforty.com and riderx.net