Network Monitoring

Presented by:

Lance Rea

CIO

Davis & Gilbert LLP

lrea@dglaw.com

A Little Background info

- D&G – 100+ Attorney firm in Midtown Manhattan
- Full Service firm specializing in Media and Advertising
- One office location and one DR site
- 40 servers, 225 PCs, 60+ printers & copiers
- 8 people in IT (including me)
- 95% Windows, 5% FOSS

What is a Network Monitoring System?

- Monitors devices and services
- Alerts staff to outages or performance degradation
- Common NMSs:
  - Nagios, OpenNMS, Zenoss, Spiceworks
  - Tivoli, Argent, OpenView
  - WhatsUp Gold, ServersCheck
  - RRDTool, MRTG, PRTG, Cacti
  - SmokePing, NTOP, Ethereal
  - Nessus & Snort

What a NMS can do for you

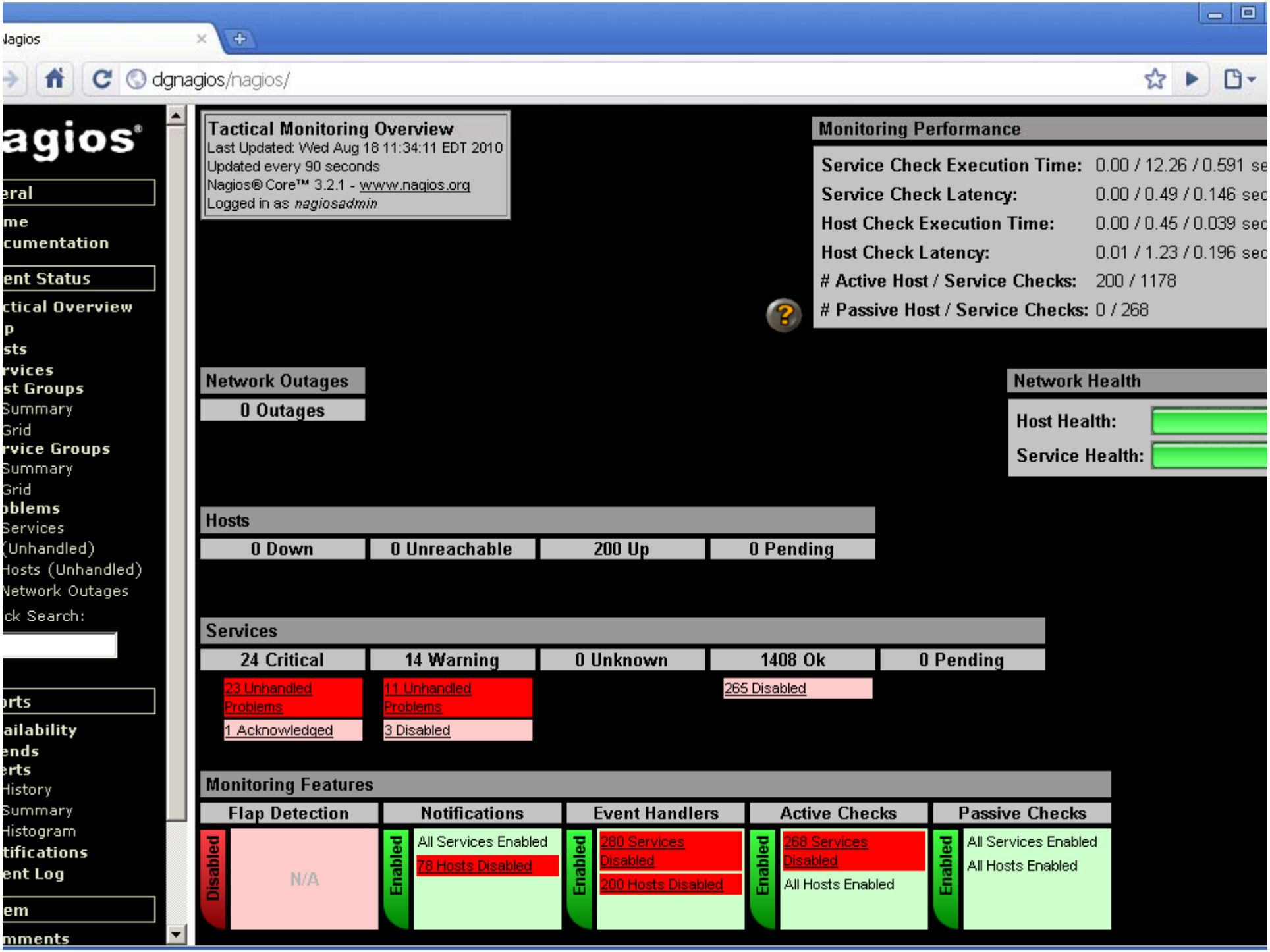
- Event monitoring – Alert us when something breaks
- Trend Analysis – CPU usage on SQL server spikes every Wed. between 2PM & 4PM.
- Bandwidth Analysis – Who is chewing up all the bandwidth?
- Security Monitoring – check for patch levels and detect network threats

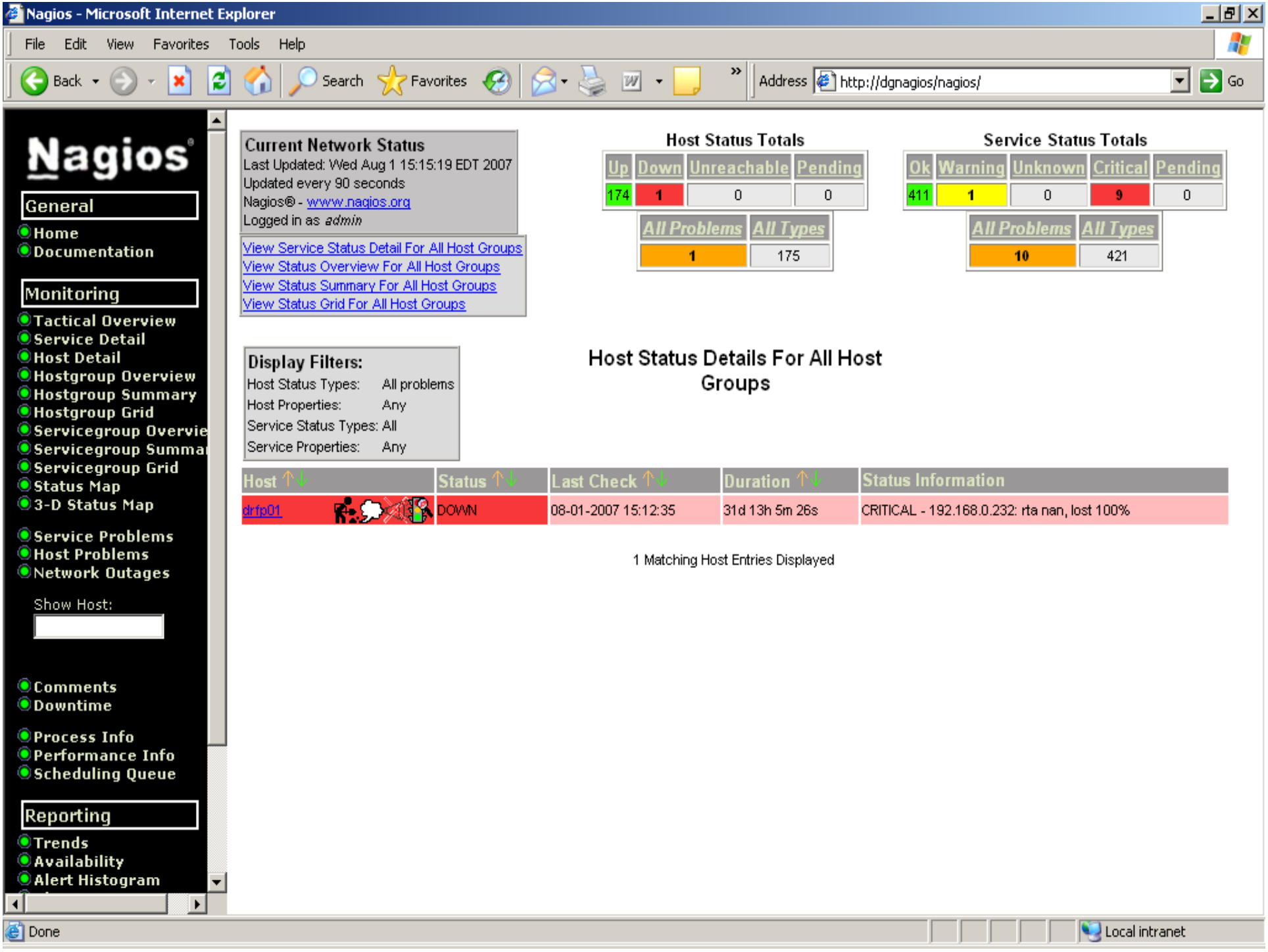
Nagios

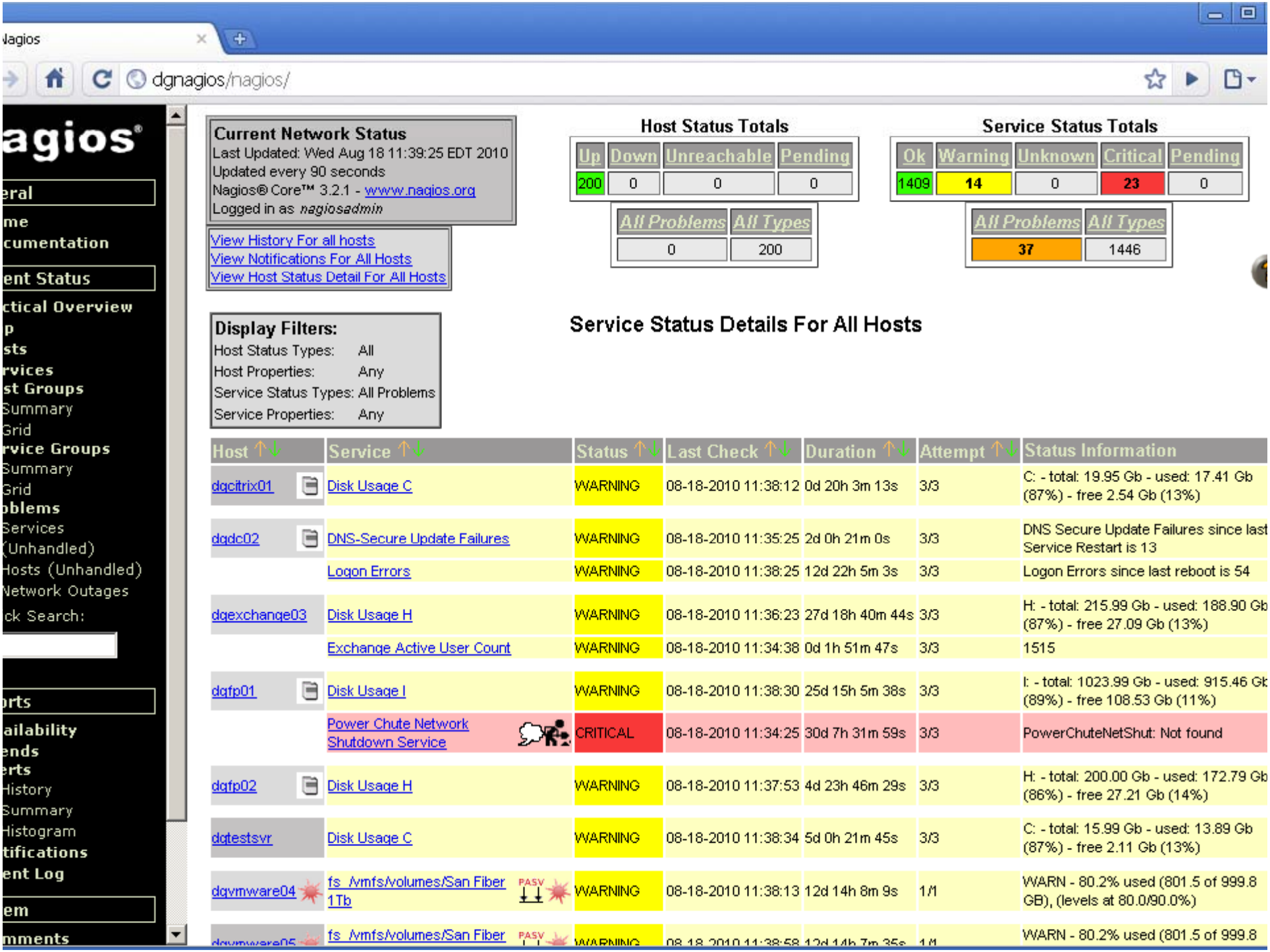
- "NAH-gee-ohs" with a hard 'G' like geese
- Originally called NetSaint, written in C
- (**N**agios **A**in't **G**onna **I**nsist **o**n **S**ainthood)
- GPL v2, runs on Linux and Unix variants
- Extremely stable / reliable
- Configuration is file-based/template ready
- Supports active and passive checks as well as distributed monitoring and failover

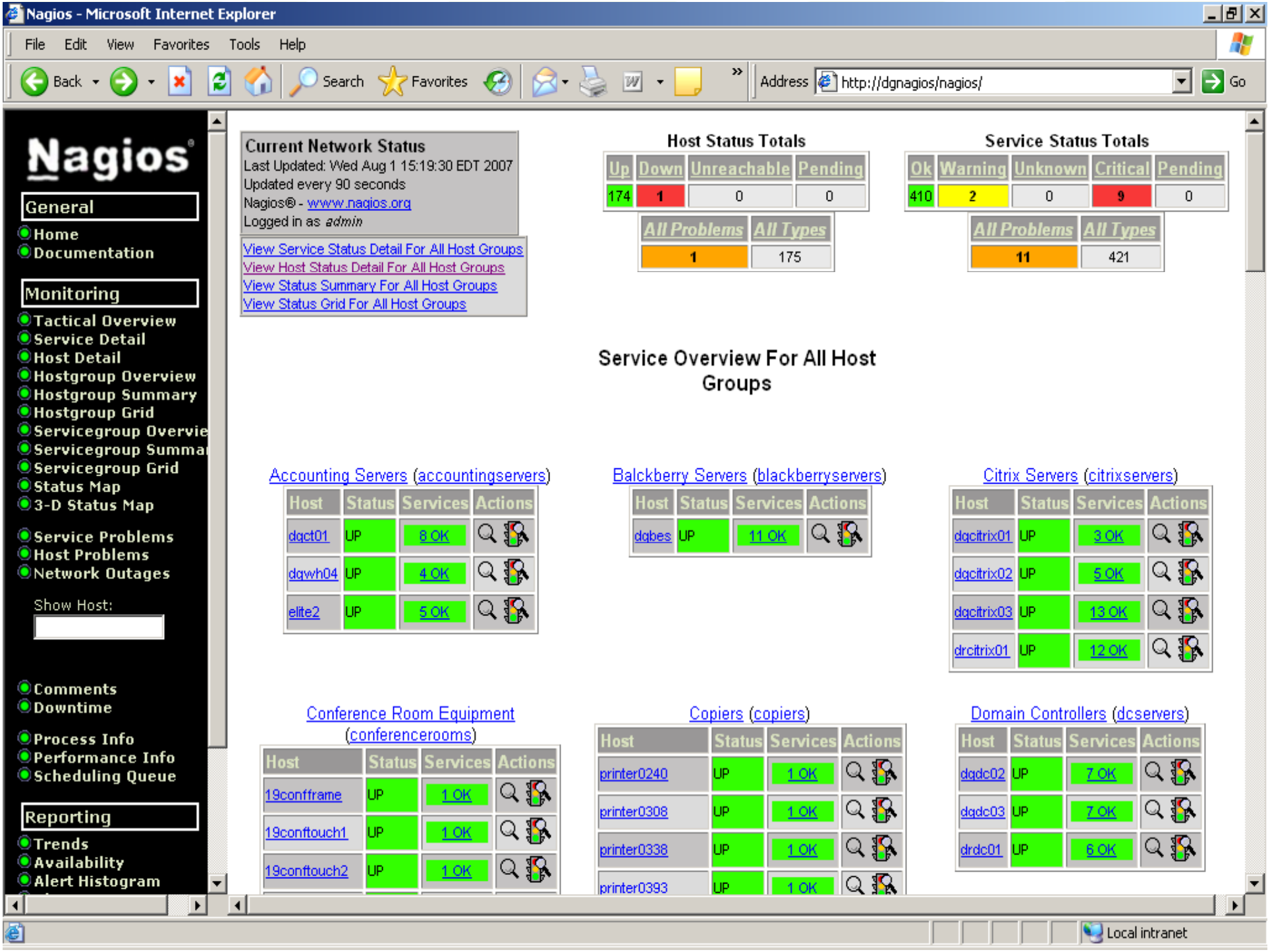
Nagios Architecture

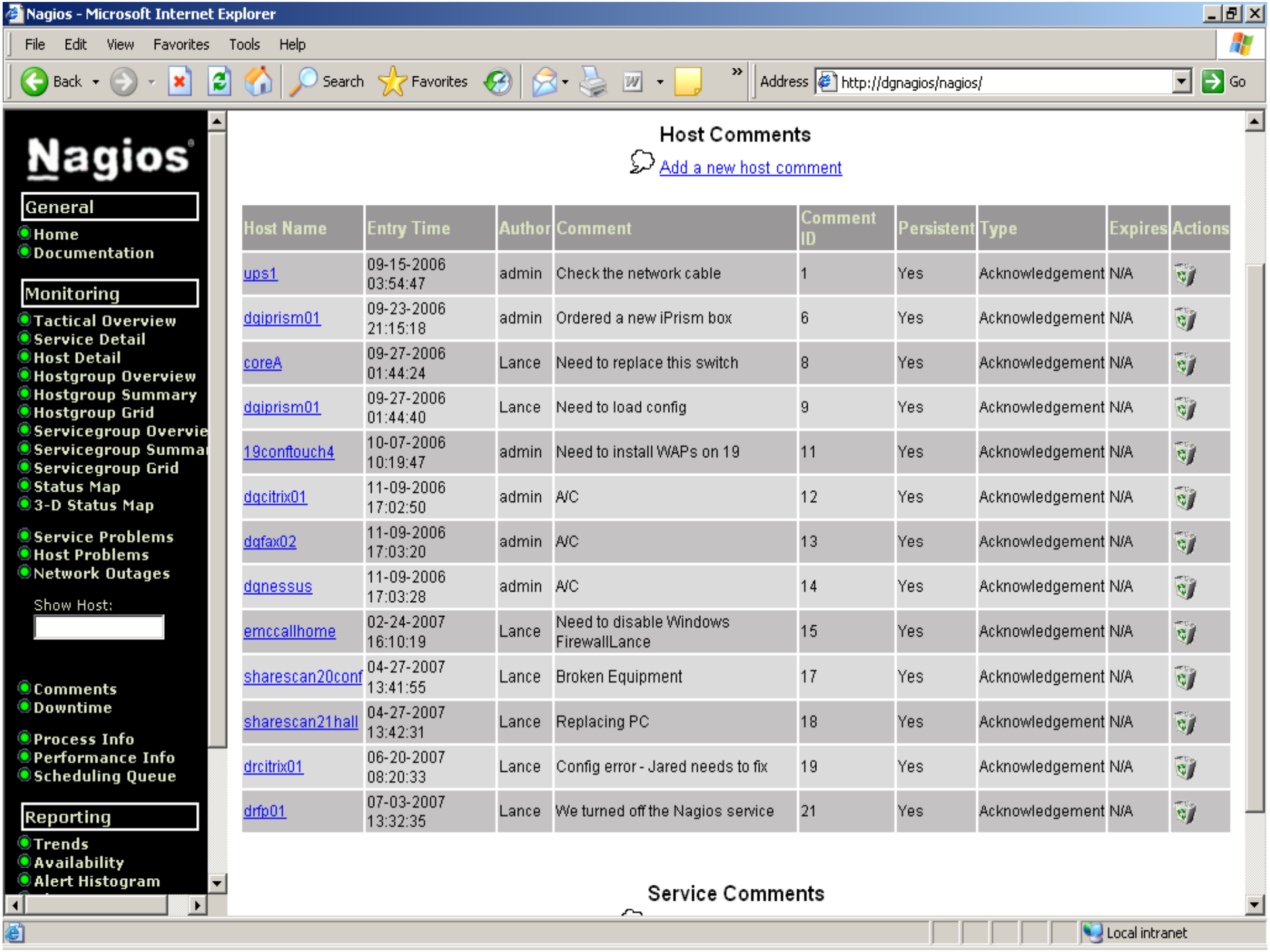
- Simplest setup is one central server that polls clients for information
- Install a service to your Windows and Linux servers (hosts)
- Nagios checks services on a host for one of the following states: OK, Warning, Critical, Unknown
- Status is viewed from a web page served by the Nagios server


Nagios
dgnagios/nagios/
agios
eral
me
cumentation
ent Status
ctical Overview
p
sts
rvices
st Groups
Summary
Grid
rvice Groups
Summary
Grid
oblems
Services
(Unhandled)
Hosts (Unhandled)
Network Outages
ck Search:
orts
ailability
ends
erts
History
Summary
Histogram
tifications
ent Log
em
mments
Tactical Monitoring Overview
Last Updated: Wed Aug 18 11:34:11 EDT 2010
Updated every 90 seconds
Nagios® Core™ 3.2.1 - www.nagios.org
Logged in as nagiosadmin
Monitoring Performance
Service Check Execution Time: 0.00 / 12.26 / 0.591 se
Service Check Latency: 0.00 / 0.49 / 0.146 sec
Host Check Execution Time: 0.00 / 0.45 / 0.039 sec
Host Check Latency: 0.01 / 1.23 / 0.196 sec
Active Host / Service Checks: 200 / 1178
Passive Host / Service Checks: 0 / 268
Network Outages
0 Outages
Network Health
Host Health:
Service Health:
Hosts
0 Down
0 Unreachable
200 Up
0 Pending
Services
24 Critical
14 Warning
0 Unknown
1408 Ok
0 Pending
23 Unhandled Problems
1 Acknowledged
11 Unhandled Problems
3 Disabled
265 Disabled
Monitoring Features
Flap Detection
Disabled
N/A
Notifications
Enabled
All Services Enabled
78 Hosts Disabled
Event Handlers
Enabled
280 Services Disabled
200 Hosts Disabled
Active Checks
Enabled
268 Services Disabled
All Hosts Enabled
Passive Checks
Enabled
All Services Enabled
All Hosts Enabled


Nagios - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://dgnagios/nagios/
Go
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Hostgroup Overview
Hostgroup Summary
Hostgroup Grid
Servicegroup Overvie
Servicegroup Summa
Servicegroup Grid
Status Map
3-D Status Map
Service Problems
Host Problems
Network Outages
Show Host:
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Current Network Status
Last Updated: Wed Aug 1 15:15:19 EDT 2007
Updated every 90 seconds
Nagios® - www.nagios.org
Logged in as admin
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
174 1 0 0
All Problems All Types
1 175
Service Status Totals
Ok Warning Unknown Critical Pending
411 1 0 9 0
All Problems All Types
10 421
Display Filters:
Host Status Types: All problems
Host Properties: Any
Service Status Types: All
Service Properties: Any
Host Status Details For All Host Groups
Host Status Last Check Duration Status Information
drfp01 DOWN 08-01-2007 15:12:35 31d 13h 5m 26s CRITICAL - 192.168.0.232: rta nan, lost 100%
1 Matching Host Entries Displayed
Done
Local intranet


Nagios
dgnagios/nagios/
agios
eral
me
cumentation
ent Status
ctical Overview
p
sts
rvices
st Groups
Summary
Grid
rvice Groups
Summary
Grid
oblems
Services
(Unhandled)
Hosts (Unhandled)
Network Outages
ck Search:
orts
ailability
ends
erts
History
Summary
Histogram
tifications
ent Log
em
mments
Current Network Status
Last Updated: Wed Aug 18 11:39:25 EDT 2010
Updated every 90 seconds
Nagios® Core™ 3.2.1 - www.nagios.org
Logged in as nagiosadmin
View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts
Host Status Totals
Up Down Unreachable Pending
200 0 0 0
All Problems All Types
0 200
Service Status Totals
Ok Warning Unknown Critical Pending
1409 14 0 23 0
All Problems All Types
37 1446
Display Filters:
Host Status Types: All
Host Properties: Any
Service Status Types: All Problems
Service Properties: Any
Service Status Details For All Hosts
Host Service Status Last Check Duration Attempt Status Information
dqcitrix01 Disk Usage C WARNING 08-18-2010 11:38:12 0d 20h 3m 13s 3/3 C: - total: 19.95 Gb - used: 17.41 Gb (87%) - free 2.54 Gb (13%)
dqdc02 DNS-Secure Update Failures WARNING 08-18-2010 11:35:25 2d 0h 21m 0s 3/3 DNS Secure Update Failures since last Service Restart is 13
Logon Errors WARNING 08-18-2010 11:38:25 12d 22h 5m 3s 3/3 Logon Errors since last reboot is 54
dqexchange03 Disk Usage H WARNING 08-18-2010 11:36:23 27d 18h 40m 44s 3/3 H: - total: 215.99 Gb - used: 188.90 Gb (87%) - free 27.09 Gb (13%)
Exchange Active User Count WARNING 08-18-2010 11:34:38 0d 1h 51m 47s 3/3 1515
dqfp01 Disk Usage I WARNING 08-18-2010 11:38:30 25d 15h 5m 38s 3/3 I: - total: 1023.99 Gb - used: 915.46 Gb (89%) - free 108.53 Gb (11%)
Power Chute Network Shutdown Service CRITICAL 08-18-2010 11:34:25 30d 7h 31m 59s 3/3 PowerChuteNetShut: Not found
dqfp02 Disk Usage H WARNING 08-18-2010 11:37:53 4d 23h 46m 29s 3/3 H: - total: 200.00 Gb - used: 172.79 Gb (86%) - free 27.21 Gb (14%)
dqtestsvr Disk Usage C WARNING 08-18-2010 11:38:34 5d 0h 21m 45s 3/3 C: - total: 15.99 Gb - used: 13.89 Gb (87%) - free 2.11 Gb (13%)
dqvmware04 fs /vmfs/volumes/San Fiber 1Tb PASV WARNING 08-18-2010 11:38:13 12d 14h 8m 9s 1/1 WARN - 80.2% used (801.5 of 999.8 GB), (levels at 80.0/90.0%)
fs /vmfs/volumes/San Fiber PASV WARNING 08-18-2010 11:38:58 12d 14h 7m 35s 1/1 WARN - 80.2% used (801.5 of 999.8


Nagios - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://dgnagios/nagios/
Go
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Hostgroup Overview
Hostgroup Summary
Hostgroup Grid
Servicegroup Overvie
Servicegroup Summa
Servicegroup Grid
Status Map
3-D Status Map
Service Problems
Host Problems
Network Outages
Show Host:
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Current Network Status
Last Updated: Wed Aug 1 15:19:30 EDT 2007
Updated every 90 seconds
Nagios® - www.nagios.org
Logged in as admin
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
174 1 0 0
All Problems All Types
1 175
Service Status Totals
Ok Warning Unknown Critical Pending
410 2 0 9 0
All Problems All Types
11 421
Service Overview For All Host Groups
Accounting Servers (accountingservers)
Host Status Services Actions
dgct01 UP 8 OK
dgwh04 UP 4 OK
elite2 UP 5 OK
Balckberry Servers (blackberryservers)
Host Status Services Actions
dgbes UP 11 OK
Citrix Servers (citrixservers)
Host Status Services Actions
dgcitrix01 UP 3 OK
dgcitrix02 UP 5 OK
dgcitrix03 UP 13 OK
drcitrix01 UP 12 OK
Conference Room Equipment (conferencerooms)
Host Status Services Actions
19conftrame UP 1 OK
19conftouch1 UP 1 OK
19conftouch2 UP 1 OK
Copiers (copiers)
Host Status Services Actions
printer0240 UP 1 OK
printer0308 UP 1 OK
printer0338 UP 1 OK
printer0393 UP 1 OK
Domain Controllers (dcservers)
Host Status Services Actions
dgdc02 UP 7 OK
dgdc03 UP 7 OK
drdc01 UP 6 OK
Local intranet



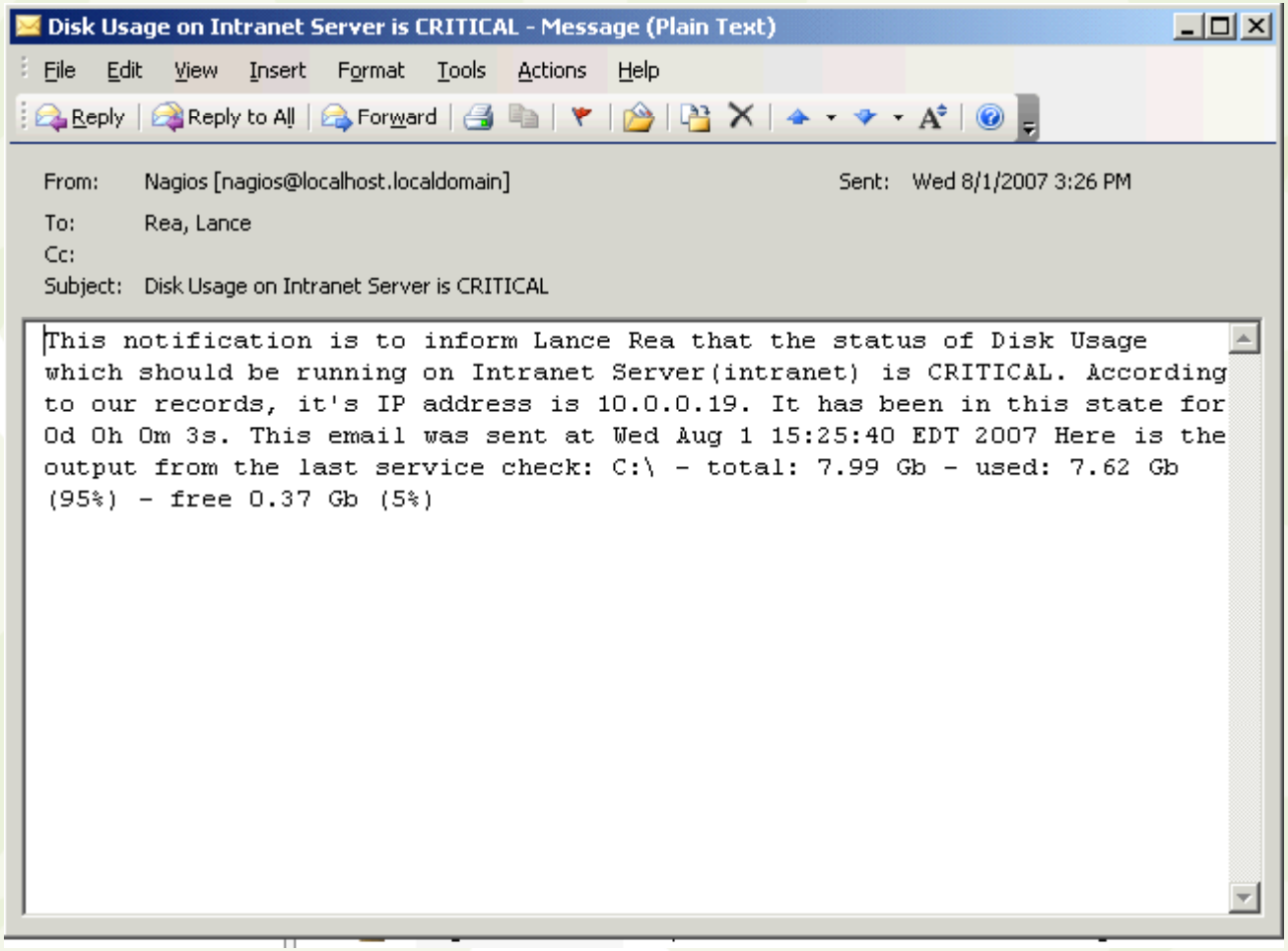
Host Comments

Add a new host comment

Host Name	Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
ups1	09-15-2006 03:54:47	admin	Check the network cable	1	Yes	Acknowledgement	N/A	
dqiprism01	09-23-2006 21:15:18	admin	Ordered a new iPrism box	6	Yes	Acknowledgement	N/A	
coreA	09-27-2006 01:44:24	Lance	Need to replace this switch	8	Yes	Acknowledgement	N/A	
dqiprism01	09-27-2006 01:44:40	Lance	Need to load config	9	Yes	Acknowledgement	N/A	
19conftouch4	10-07-2006 10:19:47	admin	Need to install WAPs on 19	11	Yes	Acknowledgement	N/A	
dqcitrix01	11-09-2006 17:02:50	admin	A/C	12	Yes	Acknowledgement	N/A	
dqfax02	11-09-2006 17:03:20	admin	A/C	13	Yes	Acknowledgement	N/A	
dqnessus	11-09-2006 17:03:28	admin	A/C	14	Yes	Acknowledgement	N/A	
emccallhome	02-24-2007 16:10:19	Lance	Need to disable Windows FirewallLance	15	Yes	Acknowledgement	N/A	
sharescan20conf	04-27-2007 13:41:55	Lance	Broken Equipment	17	Yes	Acknowledgement	N/A	
sharescan21hall	04-27-2007 13:42:31	Lance	Replacing PC	18	Yes	Acknowledgement	N/A	
drcitrix01	06-20-2007 08:20:33	Lance	Config error - Jared needs to fix	19	Yes	Acknowledgement	N/A	
drfp01	07-03-2007 13:32:35	Lance	We turned off the Nagios service	21	Yes	Acknowledgement	N/A	

Service Comments

Email Alerts



You can monitor lots of stuff

- CPU Usage
- Memory Usage
- Disk Usage
- Service States
- SQL, AD, Exchange
- File versions
- Printer states
- Routers / switches
- Temp / humidity
- SANs
- VOiP
- UPSs via SNMP
- Websites (external & internal)
- VMWare hosts & guests
- Citrix
- ANY Windows Service

Extending Nagios

- Add visualization with NagVis
- Use check_mk plugin
- Search the Exchanges & Internet for Plugins

For the impatient…

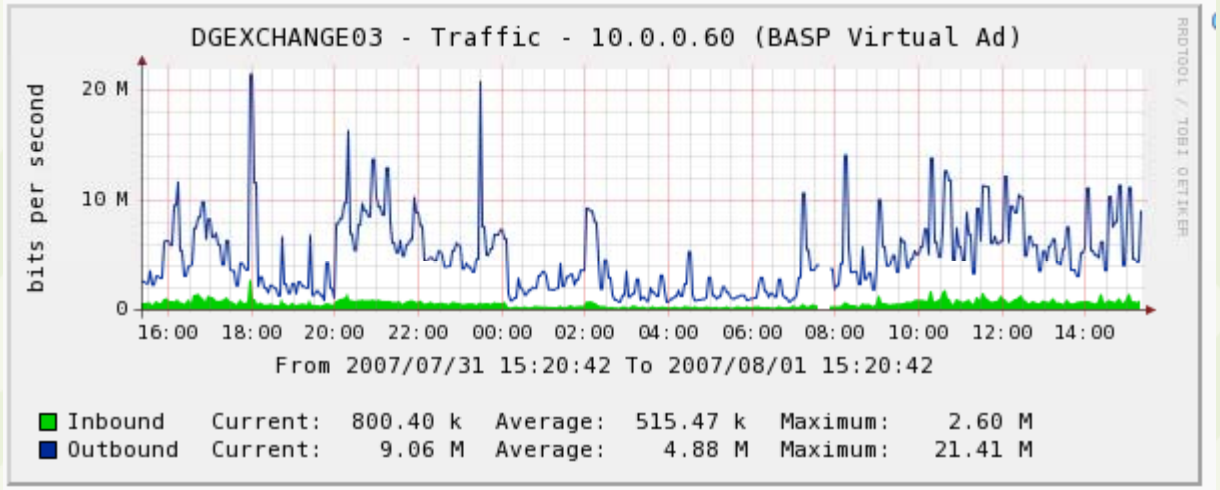
- Nagios is tough up front:
  - CLI and text file editing can be intimidating
  - Upgrades mean using a package manager or running make…
  - Some scripting helps get the most out of the system
- Groundworks (gwos.com) $59 / 100 devices
  - Gwos.com/resources: groundwork in an hour
- Zabbix / Mikoomi – silly names, good monitoring
  - Pre-built VM appliances
- OpsView Community Edition – pre-built VM
- Turnkeylinux.org – hasn't released a Nagios VM yet

Configuration – Don't be GUI

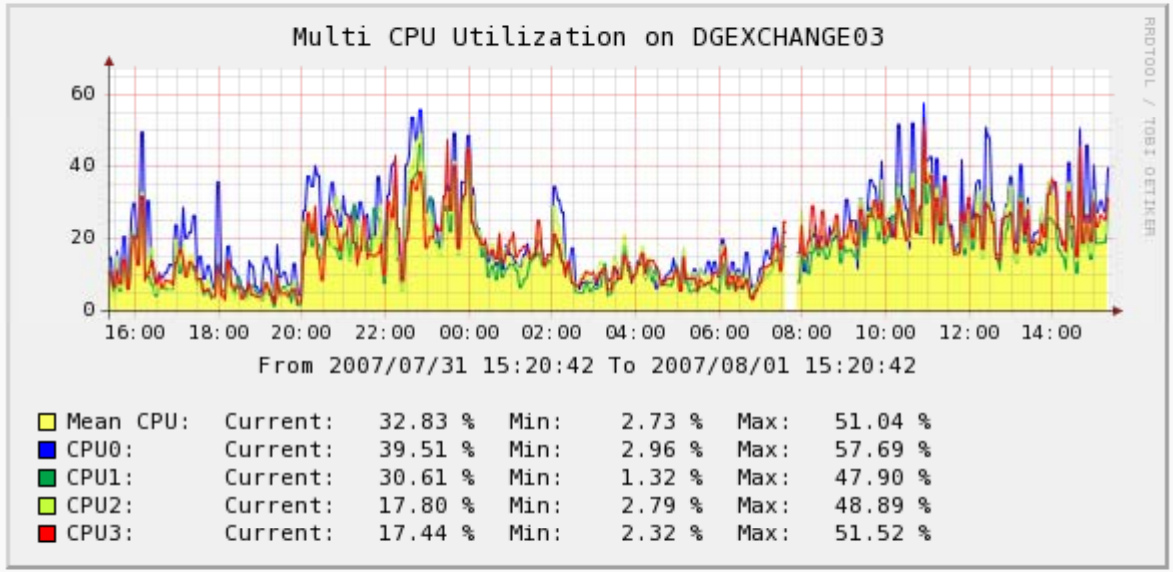
- GUI interfaces to configure Nagios stink
- Once setup, there are only a few config files you'll need to maintain
- WinSCP works great for this
- Nagios was made for lazy editing
- After using a GUI config for a couple years, we're back to hand-editing.
- GUI Options – NINJA, Lilac

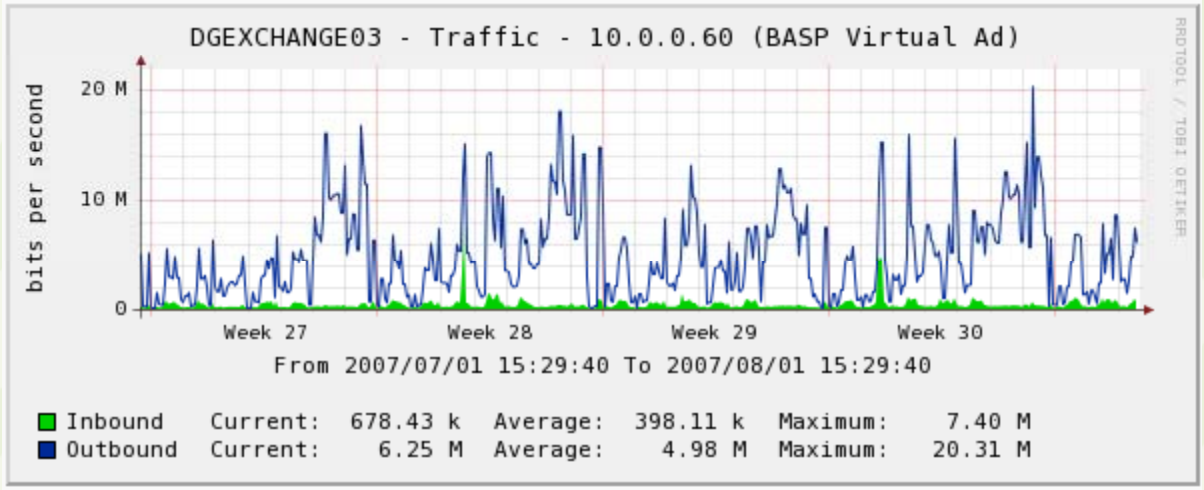
Trend Analysis with Cacti

- Cacti is a web front-end for RRDTool
- Uses SNMP to gather metrics
- Produces clean, easy-to-read graphs
- Monitors Network Traffic, Memory, and CPU usage “out of the box”
- You can create your own data sources to monitor
- Can be installed in Windows or Linux. (Both will monitor Windows & Linux hosts)

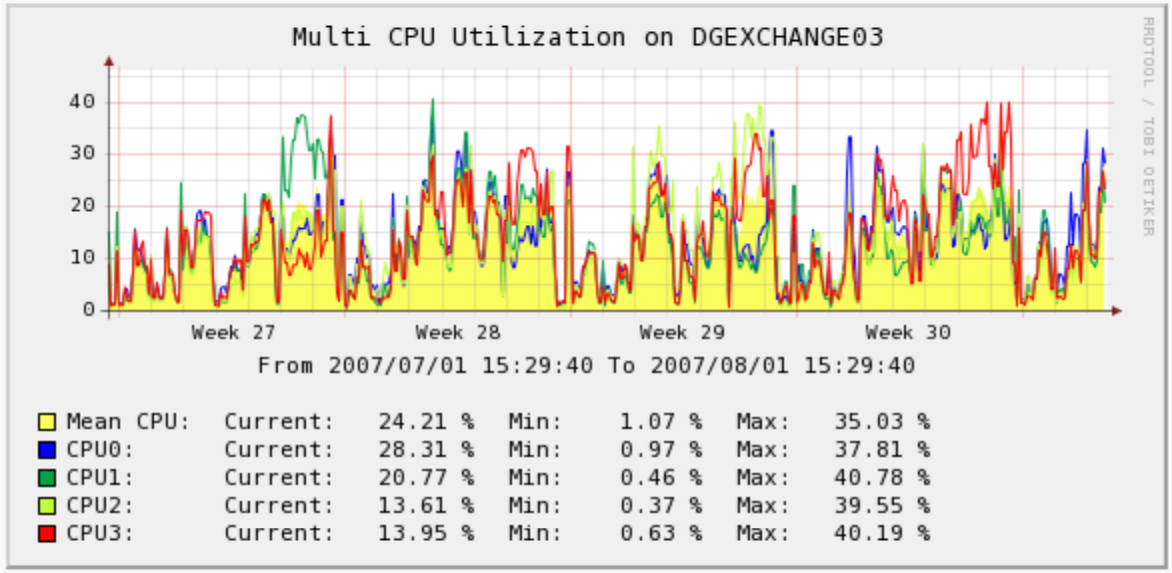


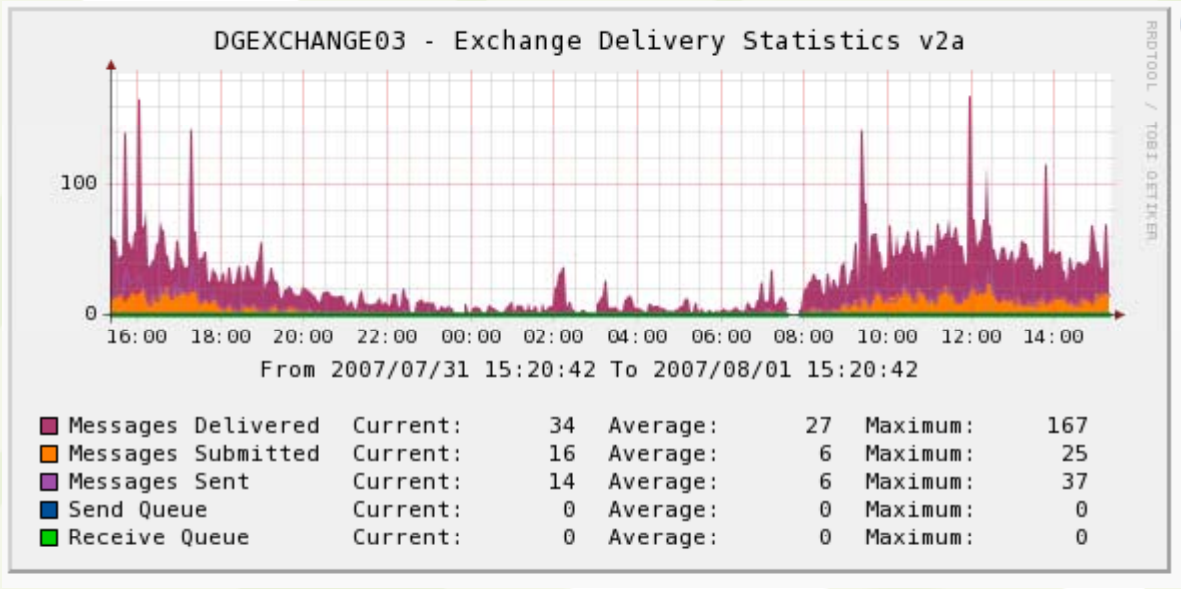
CPU Utilization on 4 Processor Box (v2)

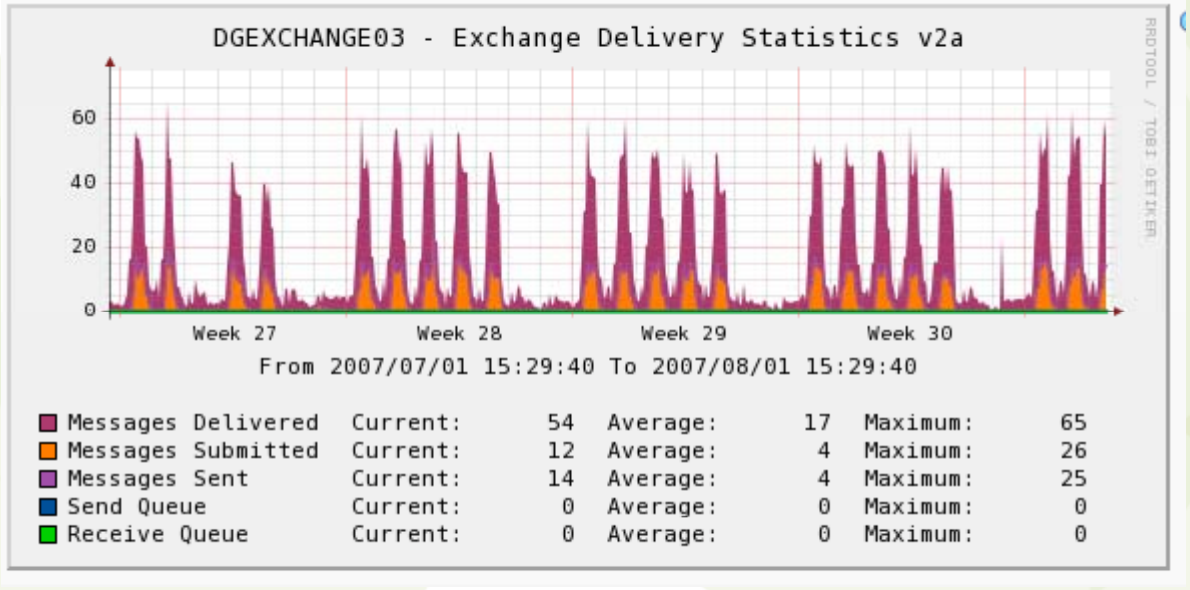


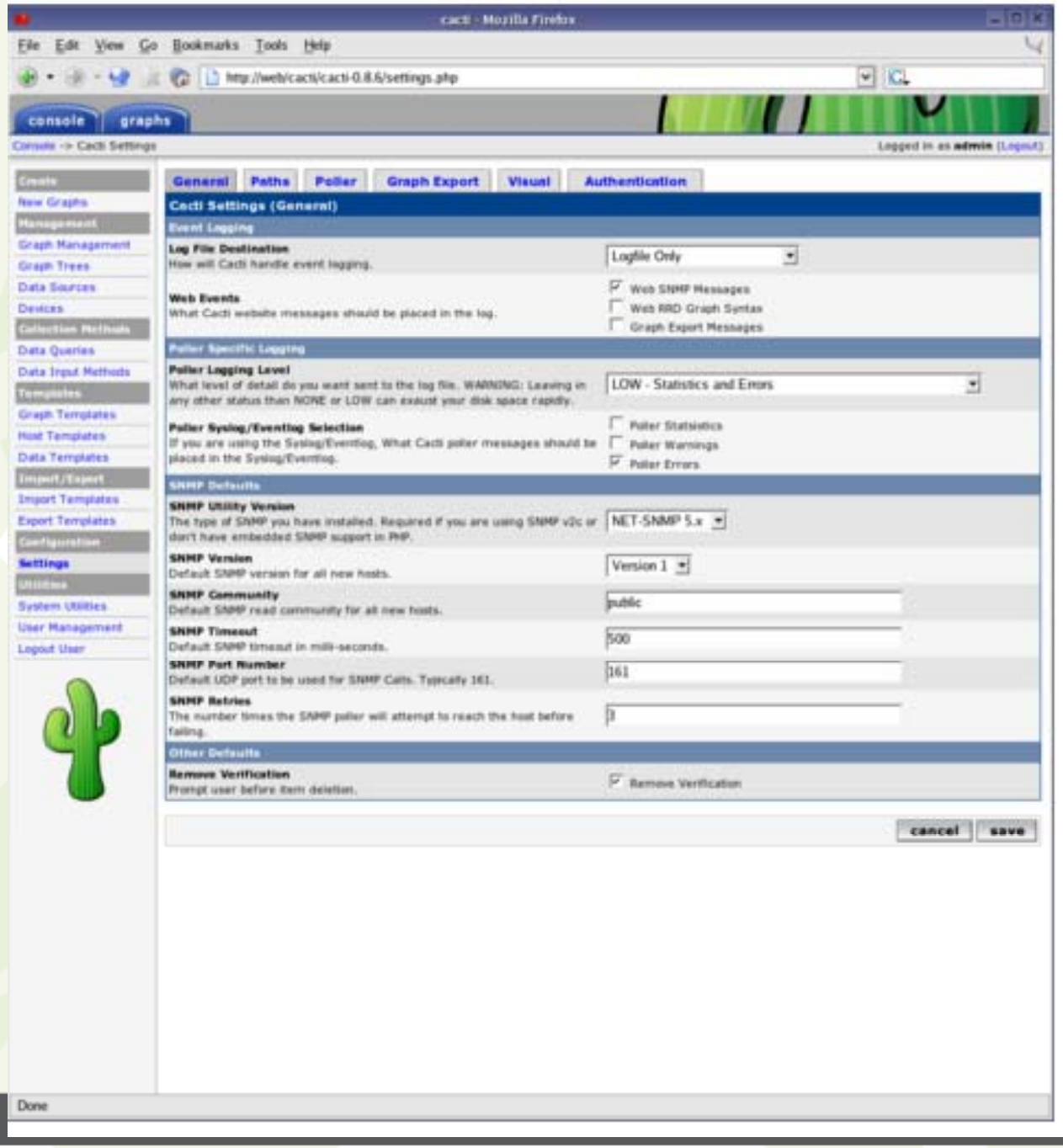


CPU Utilization on 4 Processor Box (v2)




DGEXCHANGE03 - Exchange Delivery Statistics v2a
100
0
16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00
From 2007/07/31 15:20:42 To 2007/08/01 15:20:42
Messages Delivered Current: 34 Average: 27 Maximum: 167
Messages Submitted Current: 16 Average: 6 Maximum: 25
Messages Sent Current: 14 Average: 6 Maximum: 37
Send Queue Current: 0 Average: 0 Maximum: 0
Receive Queue Current: 0 Average: 0 Maximum: 0
RRDTOOL / TOBI OETIKER


DGEXCHANGE03 - Exchange Delivery Statistics v2a
60
40
20
0
Week 27 Week 28 Week 29 Week 30
From 2007/07/01 15:29:40 To 2007/08/01 15:29:40
Messages Delivered Current: 54 Average: 17 Maximum: 65
Messages Submitted Current: 12 Average: 4 Maximum: 26
Messages Sent Current: 14 Average: 4 Maximum: 25
Send Queue Current: 0 Average: 0 Maximum: 0
Receive Queue Current: 0 Average: 0 Maximum: 0
RRDTOOL / TOBI OETIKER


cacti - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://web/cacti/cacti-0.8.6/settings.php
console
graphs
Console -> Cacti Settings
Logged in as admin (Logout)
Create
New Graphs
Management
Graph Management
Graph Trees
Data Sources
Devices
Collection Methods
Data Queries
Data Input Methods
Templates
Graph Templates
Host Templates
Data Templates
Import/Export
Import Templates
Export Templates
Configuration
Settings
Utilities
System Utilities
User Management
Logout User
General
Paths
Poller
Graph Export
Visual
Authentication
Cacti Settings (General)
Event Logging
Log File Destination
How will Cacti handle event logging.
Logfile Only
Web Events
What Cacti website messages should be placed in the log.
Web SNMP Messages
Web RRD Graph Syntax
Graph Export Messages
Poller Specific Logging
Poller Logging Level
What level of detail do you want sent to the log file. WARNING: Leaving in any other status than NONE or LOW can exaust your disk space rapidly.
LOW - Statistics and Errors
Poller Syslog/Eventlog Selection
If you are using the Syslog/Eventlog, What Cacti poller messages should be placed in the Syslog/Eventlog.
Poller Statistics
Poller Warnings
Poller Errors
SNMP Defaults
SNMP Utility Version
The type of SNMP you have installed. Required if you are using SNMP v2c or don't have embedded SNMP support in PHP.
NET-SNMP 5.x
SNMP Version
Default SNMP version for all new hosts.
Version 1
SNMP Community
Default SNMP read community for all new hosts.
public
SNMP Timeout
Default SNMP timeout in milli-seconds.
500
SNMP Port Number
Default UDP port to be used for SNMP Calls. Typically 161.
161
SNMP Retries
The number times the SNMP poller will attempt to reach the host before failing.
3
Other Defaults
Remove Verification
Prompt user before item deletion.
Remove Verification
cancel
save
Done

CactiEZ

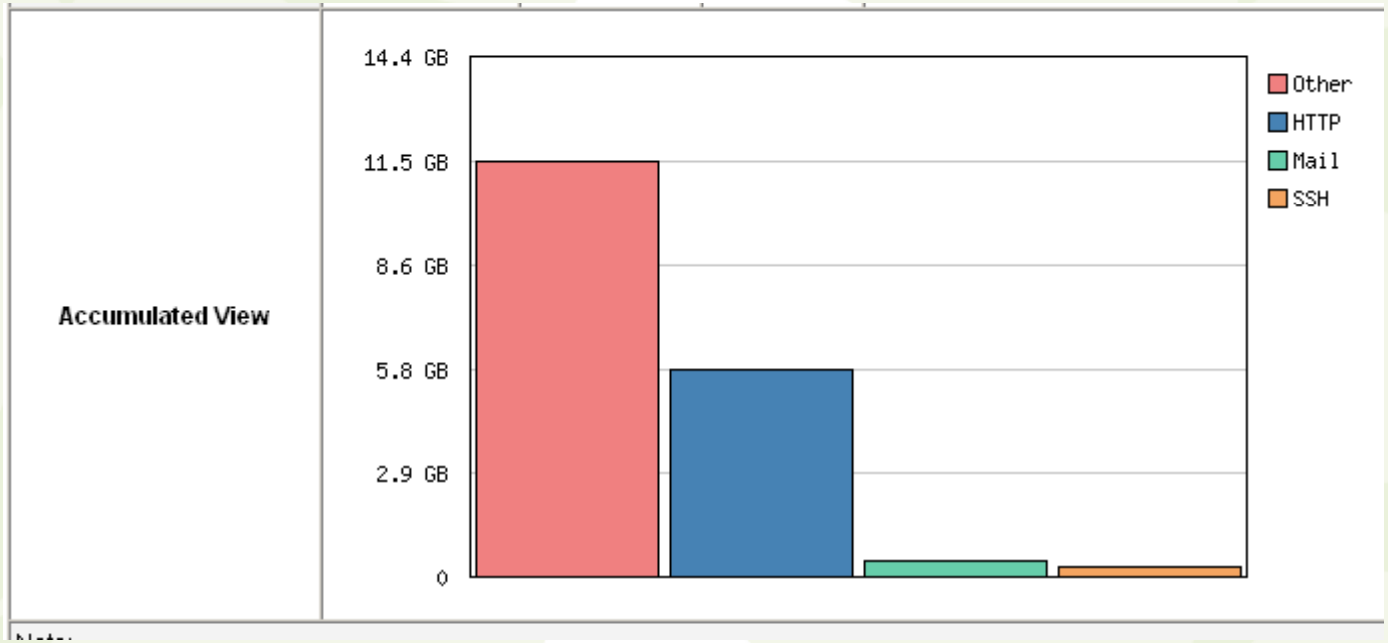
- CactiEZ is a pre-built distribution of Cacti with other utilities
- Built on CentOS
- Works well in VMWare
- Features a plug-in architecture
- Don't let the 0.6 version scare you away

Network Monitoring with NTOP

- Gives a real-time look at network traffic
- Extremely easy installation
- Web interface
- Modest hardware requirements
- Drill-down interface
- Spot bandwidth hogs, network anomalies, and networking errors (flags)
- Ntop data is NOT persistent*

NTOP – Accumulated Network Traffic

- View of network traffic after 6 hours of monitoring



Streaming Radio anyone?

Statistics for all Domains

Name	Domain	TCP/IP								ICMP			
		Total				TCP		UDP		IPv4		IPv6	
		Sent		Rcvd		Sent	Rcvd	Sent	Rcvd	Sent	Rcvd	Sent	Rcvd
com		11.7 GB	93.4%	14.5 GB	98.9%	11.7 GB	14.5 GB	7.2 MB	21.0 MB	1.5 MB	650.6 KB	0	0
213.stw.streamtheworld.com		199.9 MB	1.6%	2.3 KB	0.0%	199.9 MB	2.3 KB	0	0	0	0	0	0
213.streamtheworld.com		133.3 MB	1.0%	2.8 MB	0.0%	133.3 MB	2.8 MB	0	0	0	0	0	0
stream.aol.com		130.0 MB	1.0%	306.0 KB	0.0%	130.0 MB	306.0 KB	0	0	0	0	0	0
lexsolutio.com		75.6 MB	0.6%	2.1 MB	0.0%	75.6 MB	2.1 MB	0	0	0	0	0	0
ix.sitestream.net		61.0 MB	0.5%	37.3 KB	0.0%	61.0 MB	37.3 KB	0	0	0	0	0	0
nwrk.east.verizon.net		31.1 MB	0.2%	19.2 MB	0.1%	31.1 MB	19.2 MB	0	0	0	0	0	0
lexis.com		25.8 MB	0.2%	6.0 MB	0.0%	25.8 MB	6.0 MB	0	0	0	0	0	0
dyn.optonline.net		25.6 MB	0.2%	16.9 MB	0.1%	25.6 MB	16.9 MB	0	0	0	0	0	0
akamai.com		24.2 MB	0.2%	34.8 KB	0.0%	24.2 MB	34.8 KB	0	0	0	0	0	0
google.com		22.0 MB	0.2%	4.7 MB	0.0%	22.0 MB	4.7 MB	0	0	0	0	0	0
ord.scnet.net		20.6 MB	0.2%	2.0 KB	0.0%	20.6 MB	2.0 KB	0	0	0	0	0	0
webex.com		14.6 MB	0.1%	129.9 KB	0.0%	14.6 MB	129.9 KB	0	0	0	0	0	0
dns.cogentco.com		10.8 MB	0.1%	3.0 MB	0.0%	15.0 KB	1.4 KB	10.8 MB	3.0 MB	0	0	0	0
ycs.vip.a2s.yahoo.com		9.6 MB	0.1%	500.0 KB	0.0%	9.6 MB	500.0 KB	0	0	0	0	0	0
doubleclick.net		6.1 MB	0.0%	3.9 MB	0.0%	6.1 MB	3.9 MB	0	0	0	0	0	0
everestbroadband.com		5.7 MB	0.0%	884.8 KB	0.0%	0	0	5.7 MB	884.8 KB	0	0	0	0
ttn.xpc-mii.net		4.8 MB	0.0%	567.0 KB	0.0%	4.8 MB	567.0 KB	0	0	0	0	0	0
broadbandinstruments.com		4.0 MB	0.0%	626.7 KB	0.0%	4.0 MB	626.7 KB	0	0	0	0	0	0
proxy.aol.com		3.5 MB	0.0%	2.2 MB	0.0%	3.5 MB	2.2 MB	0	0	0	0	0	0

Vulnerability Scanning

- Nessus was the standard app – no longer free.
- OpenVAS is the GNU GPL fork of Nessus
- MBSA is an option (can be scripted)

SpiceWorks

- SpiceWorks (www.spiceworks.com)
- Free (ad-supported) Inventory and asset program
- Does basic monitoring
- "5-minute install"
- No clients required on hosts
- Support for larger networks has improved
- Things SpiceWorks does: http://www.spiceworks.com/spicelist/

LanSweeper

- Strength is Hardware & Software Inventory
- Free version is nice, Premium is worth the $299 (Adds AD-integration & custom reports)
- Custom actions are really cool
- Event log reporting
- OS & Software license compliance reports
- Just added support for non-windows devices (premium version only)
- rolfsa.blogspot.com/2010/06/lansweeper.html

Splunk

- Index your IT data
- Point syslog traffic at Splunk server
- Getting data from Windows servers is now easier
- Nice drill-down web 2.0 interface
- Free version has a limitation on data (500Mb / day)
- Watch the Splunk Ninja: splunkninja.com
- http://www.Splunk.org

Monitor External Websites

- Montastic is a free service
- Let's you monitor up to 3 sites
- Checks every 30 minutes
- Price plans check every 5 minutes and allow more accounts

Driftnet

- Displays images pulled from TCP stream
- Your NTOP server is a nice place for it
- Careful what you wish for…
- “if you are possessed of Victorian sensibilities, and share an unswitched network with others who are not, you should probably not use it.”
- http://www.ex-parrot.com/~chris/driftnet/

Nagios Links

- Official Nagios Website: nagios.org
- Nagios Plugins Website: nagiosplugins.org
- Nagios Exchange: monitoringexchange.org
- Monitoring Forge: monitoringforge.org
- Socbox: http://gforge.ingby.com/gf/project/socbox/
- Your local on-line documentation
  http://yournagioshost/docs/index.html
- Building a Monitoring Infrastructure with NAGIOS – David Josephson (book)

Cacti Links

- Main Cacti Site: http://cacti.net
- CactiEZ: http://cactiez.cactiusers.org
- CactiEZ Forums: http://cactiusers.org/forums/

NTOP Links

- Home Site: http://www.ntop.org
- Basic Setup Tips: http://bobcares.com/article60.html
- Video on setup: Search for “install ntop”
- NTOP Usage: http://www.ntop.org/UsageNotes.html
- NTOP Guide: http://techowto.files.wordpress.com/2008/09/ntop-guide.pdf

Other Links

- Snort: http://www.snort.org
- OpenNMS looks promising: www.openNMS.org
- Checkout: NMap, SmokePing, & WireShark
- Nagios Fork Icinga: www.icinga.org
- Observium: www.observium.org