

Four Star Network Management

Jeff Allen (jra@corp.webtv.net)

WebTV Networks

David Williamson (davidw@gnac.com)

Global Networking and Computing





Where this is going

- # Who we think you are
 - # Who we know we are
 - # Tools as a philosophy
 - # A menu of tools to choose from
 - # Choosing from the menu
 - # A sampling of tools we like
 - # Connecting your tools
 - # Marching Orders
-



Our Audience

- # System/network administrators
 - # People who don't think they need Network Management
 - # Managers – you know who you are!
-



Who we are

- # Corporate and Service background
 - # We're sick of monolithic tools that don't do what we want them to do!
 - # A toolsmith and a network admin
 - # David: "MRTG has paid me money"
-



A tale of two philosophies...

The Vendor Approach:

- Deploy a monolithic application/framework.
- Solve all problems directly, or with add-ons.
- Lots of risk that some part won't address your needs.

Our approach:

- Select small tools the do precisely what you need from a menu of choices.
 - Work to interconnect into a web of tools – or not.
 - Incremental improvement reduces risk of failure.
-



The Menu, Part I

- # Alert management
 - # Change management
 - # Trending and thresholding
 - # Intrusion Detection
 - # Project Management
 - # Workflow automation
 - # Document control
-



The Menu, Part II

- # Time Management
 - # Inventory control
 - # Software distribution
 - # A la carte: Miscellaneous Tools
 - Console, dashboard, third-party diagnosis tools
 - # Public relations
 - # Monolithic Systems
-



Choosing from the Menu

Scale:

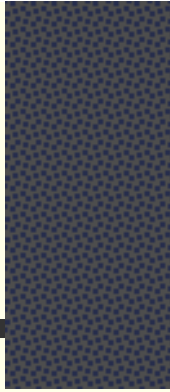
- Big and medium shops
- Small shops too!

Priority

Think BIG!

- This is **not** a closed list

Network Management isn't just for networks anymore!



WebTV's 4-Star System

- ☆ Trending and Thresholding
 - Cricket
 - ☆ Alert Management
 - Netcool
 - ☆ Workflow Management
 - Remedy
 - ☆ Dashboard Approach to problem solving
 - To be solved, if ever...
-



Why Watch Trends?

- # Short-term issues make us act reactively
 - # Need data that we often don't have to make good long-term decisions

 - # Common Questions:
 - Is the link to Europe up?
 - Do we need more bandwidth to Europe?
-

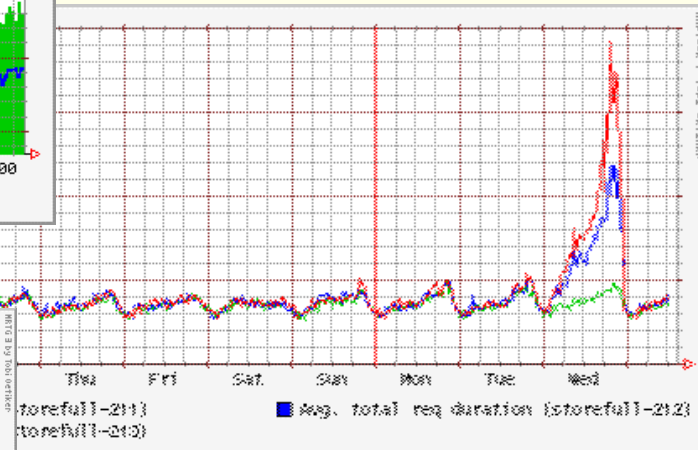
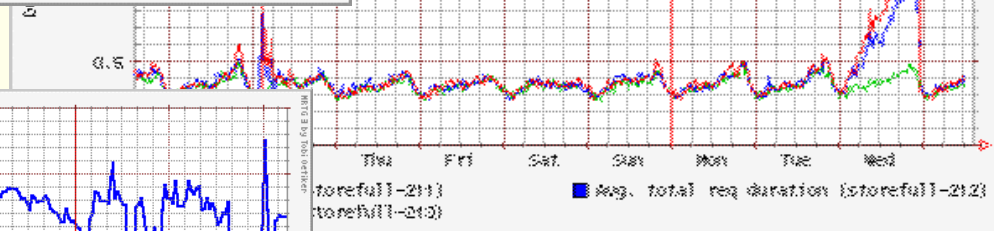
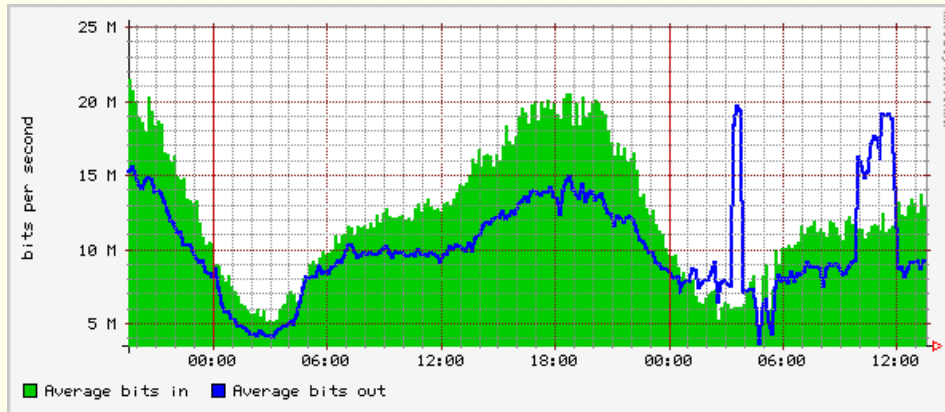


Better Questions:

- # What is the current state of the link?
- # What has it been recently?
- # Is it what we expect it to be? Is it different from other links that should be the same?
- # What long-term trends can we discern?

Answering questions like these requires a good data collection and graphing system.

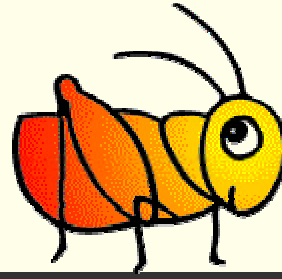
Examples



storefull-211
storefull-212

■ Avg. total req duration (storefull-211)
■ Avg. total req duration (storefull-212)

The System:



Cricket!

- # Cricket is a tool for storing and viewing time-series data
 - Very flexible
 - Extremely Legible Graphs
 - Space and Time efficient
 - Platform Independent



How it works

- # Cricket's collector runs from cron every 5 minutes and stores the data.
 - # Cricket's grapher CGI script is used interactively to browse the data.
 - # The system uses a hierarchical configuration system called a Config Tree.
-

Too many graphs

- # The capacity to draw 5000 graphs hardly qualifies as a proactive monitoring tool.
 - # Humans must check the graphs now.
 - # Wouldn't be nice if Cricket could check the graphs itself? How would a computer know if a graph "looks right"?
 - # Cricket could send traps to an Alert Manager...
-



Too Many Pages?

Ever had this happen to you?

- Step 1: Fetch nifty monitoring package off the net.
- Step 2: Compile, install, point it at your pager.
- Step 3: Fall asleep.
- Step 4: Wake up to a pager with a useless message.
- Step 5: Go to Step 3.

Congratulations! You have just discovered the need for Alert Management!



Alert Management

Alerts are:

- Any message about the state of the system
- Can be good, bad, or neither

Management is:

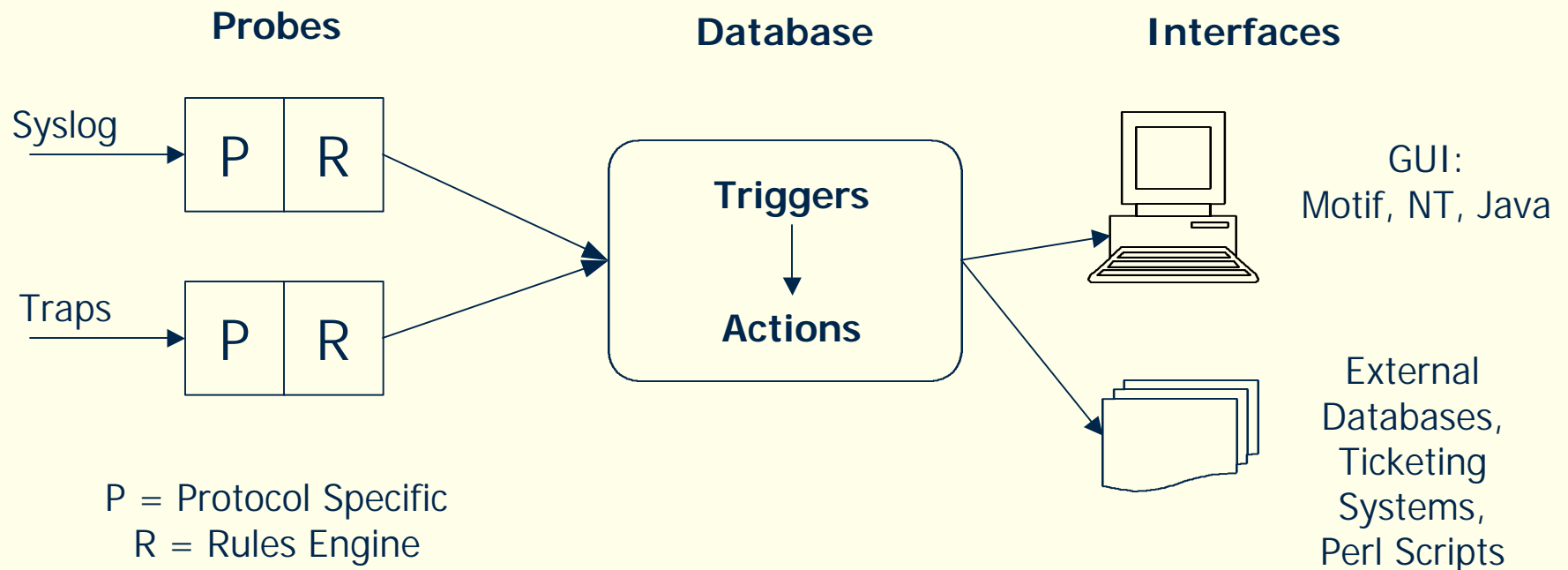
- Prioritizing
 - Filtering
 - Escalation and de-escalation
 - Destruction
-

Where do Alerts come from?

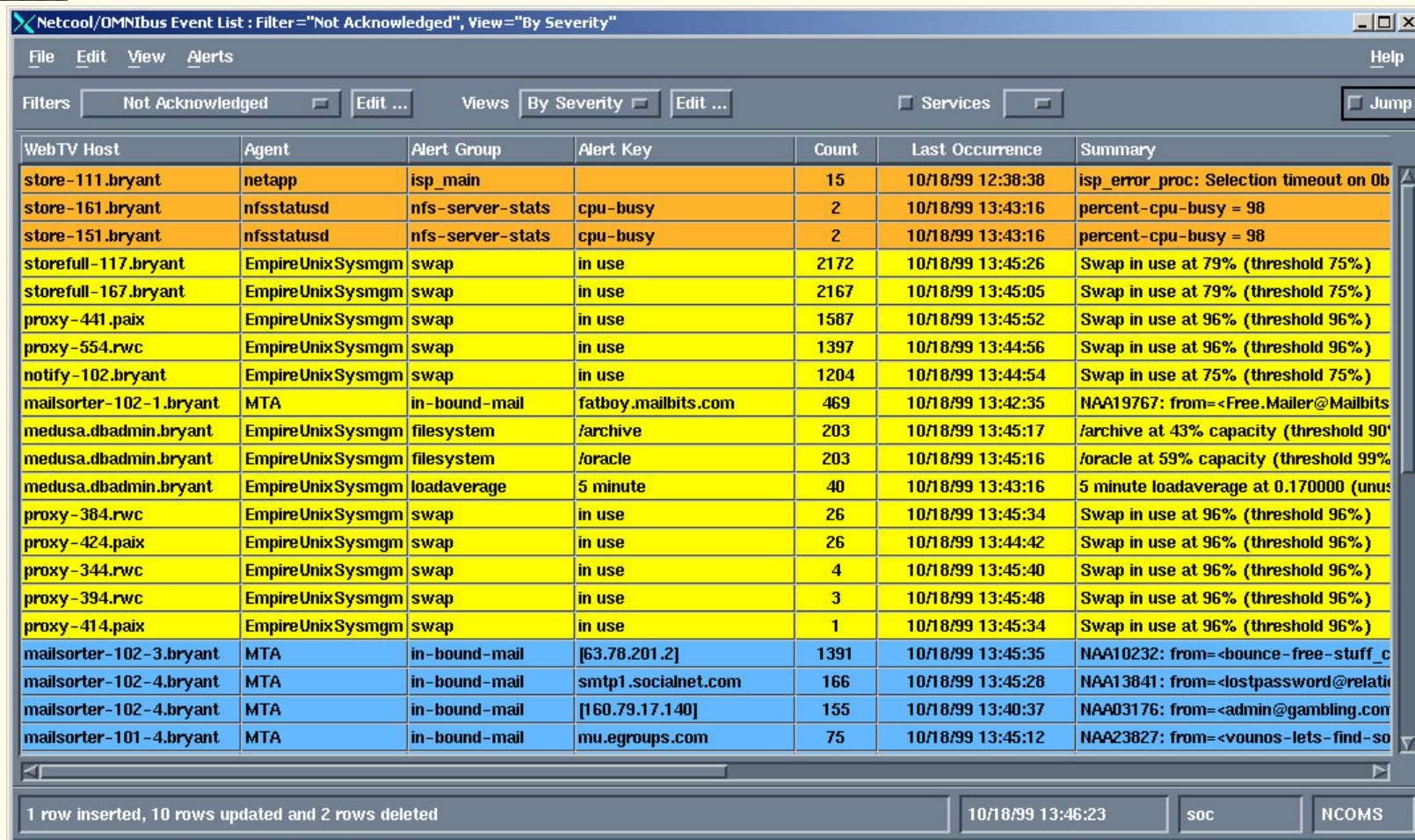
- # Network Devices (syslog, SNMP traps)
 - # Operating Systems (syslog, SNMP traps)
 - # Applications
 - # Cricket (threshold violations and recoveries)
 - # Miscellaneous monitoring scripts
 - # Intrusion Detection system
-

Netcool

A picture is worth 1000 words:



What it looks like:



Netcool/OMNIBus Event List : Filter="Not Acknowledged", View="By Severity"

File Edit View Alerts Help

Filters Not Acknowledged Edit ... Views By Severity Edit ... Services Jump

WebTV Host	Agent	Alert Group	Alert Key	Count	Last Occurrence	Summary
store-111.bryant	netapp	isp_main		15	10/18/99 12:38:38	isp_error_proc: Selection timeout on Ob
store-161.bryant	nfsstatusd	nfs-server-stats	cpu-busy	2	10/18/99 13:43:16	percent-cpu-busy = 98
store-151.bryant	nfsstatusd	nfs-server-stats	cpu-busy	2	10/18/99 13:43:16	percent-cpu-busy = 98
storefull-117.bryant	EmpireUnixSysmgm	swap	in use	2172	10/18/99 13:45:26	Swap in use at 79% (threshold 75%)
storefull-167.bryant	EmpireUnixSysmgm	swap	in use	2167	10/18/99 13:45:05	Swap in use at 79% (threshold 75%)
proxy-441.paix	EmpireUnixSysmgm	swap	in use	1587	10/18/99 13:45:52	Swap in use at 96% (threshold 96%)
proxy-554.rwc	EmpireUnixSysmgm	swap	in use	1397	10/18/99 13:44:56	Swap in use at 96% (threshold 96%)
notify-102.bryant	EmpireUnixSysmgm	swap	in use	1204	10/18/99 13:44:54	Swap in use at 75% (threshold 75%)
mailsorter-102-1.bryant	MTA	in-bound-mail	fatboy.mailbits.com	469	10/18/99 13:42:35	NAA19767: from=<Free.Mailer@Mailbits
medusa.dbadmin.bryant	EmpireUnixSysmgm	filesystem	/archive	203	10/18/99 13:45:17	/archive at 43% capacity (threshold 90
medusa.dbadmin.bryant	EmpireUnixSysmgm	filesystem	/oracle	203	10/18/99 13:45:16	/oracle at 59% capacity (threshold 99%
medusa.dbadmin.bryant	EmpireUnixSysmgm	loadaverage	5 minute	40	10/18/99 13:43:16	5 minute loadaverage at 0.170000 (unus
proxy-384.rwc	EmpireUnixSysmgm	swap	in use	26	10/18/99 13:45:34	Swap in use at 96% (threshold 96%)
proxy-424.paix	EmpireUnixSysmgm	swap	in use	26	10/18/99 13:44:42	Swap in use at 96% (threshold 96%)
proxy-344.rwc	EmpireUnixSysmgm	swap	in use	4	10/18/99 13:45:40	Swap in use at 96% (threshold 96%)
proxy-394.rwc	EmpireUnixSysmgm	swap	in use	3	10/18/99 13:45:48	Swap in use at 96% (threshold 96%)
proxy-414.paix	EmpireUnixSysmgm	swap	in use	1	10/18/99 13:45:34	Swap in use at 96% (threshold 96%)
mailsorter-102-3.bryant	MTA	in-bound-mail	[63.78.201.2]	1391	10/18/99 13:45:35	NAA10232: from=<bounce-free-stuff_c
mailsorter-102-4.bryant	MTA	in-bound-mail	smtp1.socialnet.com	166	10/18/99 13:45:28	NAA13841: from=<lostpassword@relati
mailsorter-102-4.bryant	MTA	in-bound-mail	[160.79.17.140]	155	10/18/99 13:40:37	NAA03176: from=<admin@gambling.com
mailsorter-101-4.bryant	MTA	in-bound-mail	mu.egroups.com	75	10/18/99 13:45:12	NAA23827: from=<vounos-lets-find-so

1 row inserted, 10 rows updated and 2 rows deleted

10/18/99 13:46:23 soc NCOMS



Implementing policy

Rules engine:

- Selects alerts
- Sets initial priority

Triggers and actions:

- Calculate rates
 - Adjust priority
 - Automatic resolution
 - Trim and maintain database
-

How we implemented policy

- # Configure the system to send everything in as “uncategorized”. See what you get.
- # Codify policies for what gets attention:
 - Edit rules files to prioritize alerts
- # Implement other policies:
 - Triggers and actions for escalation, resolution, and destruction.



Workflow Systems

- # A system to help operations folks “accomplish their mission” by:
 - Keeping things from falling through the cracks
 - Maintaining an audit trail
 - Making it possible to measure things:
 - quality of service
 - where all the time goes
 - which systems (or users) are unreliable
-



A Good Workflow System

- # Helps move tasks through the organization smoothly
 - Handoffs happen reliably
 - Helps operators implement established processes
 - # Lets management understand the value of the operations staff, and where to make improvements.
 - # Is Really Hard To Make!
-

Why is it so difficult?

- # It's a software solution to an essentially social problem.
 - Requires commitment at a management level
 - Requires buy-in at an operator level
 - # To facilitate this buy-in, the software needs to be:
 - Lightweight, unobtrusive, accurate, quickly extensible, and completely reliable.
 - Ha! This is *software* we are talking about!
-

What WebTV uses...

- # We have created several schemas in Remedy's Action Request system.
 - # Three departments use a common Remedy server:
 - Development (bug tracking, configuration tracking)
 - Operations (trouble tracking)
 - Customer Care (call/e-mail tracking)
 - # Operations tickets can be linked to customer tickets.
-



Remedy Pros and Cons

Pros

- Very customizable: can solve any problem
- Scalable and reliable

Cons

- Very customizable: need consulting help to set it up, and internal expertise to manage it going forward
 - No referential integrity
 - Clunky UI
 - The good news is that it's not too hard to replace its UI for simple tasks, using ARSPerl and web interface.
-

Where we are going...

- # We are implementing a change management system, using Remedy.
 - Codifies existing best practices.
 - Will add new procedures to avoid known mistakes.
 - A fundamental design consideration: must be easy to use, or it will be abused or ignored.
 - It will be “advisory”, not “supervisory”.
-



The Dashboard

- # The genesis of the idea was Spectrum's "device view".
 - # The vision: A dynamic web page you can go to and see everything there is to know about a host:
 - Embedded graphs of recent network and OS trends.
 - Output from `top`, `vmstat`, `iostat`, etc.
 - Application status (via app-specific test scripts)
 - A button that pops up an `ssh` session
 - Links to recent tickets related to this kind of machine
 - Links to troubleshooting tips for this kind of machine
-



Why isn't it done?

- # Is it a bad idea? No, it just always falls off the bottom of the priority list.
 - # This is OK! It means you know the limits of your appetite for tools.
 - # It also leaves an interesting project for junior toolsmiths to cut their teeth on.
-



The Rest of the Constellation

Change Management

- Multiple version control systems in use.

Project Management

Software Distribution

Monoliths

- Spectrum: OK at mapping and displaying network topology.

Public Relations

- For us, this is a solved problem: it's nice to work in a group with good executive support!
-



Connections

- # Once you have small tools doing useful work for you, start making connections between them.
 - # Monolithic systems fail in part because they have too many connections.
 - # Add connections **only** where they add value to your system or simplify it.
-

Examples of Connections

- # We have a system that puts POP Health data into Remedy tickets.
 - One less tool for operations folks to monitor.
 - # We'd like to have Cricket generate alerts in Netcool.
 - The ability to make 5000 graphs is not a proactive tool!
 - # The mythical Dashboard is one too!
-



Go forth and Think!

- # Take control of your environment by rolling out small tools that do what you need, a little at a time.
 - # As you add new tools, work to integrate them with what you already have.
 - # Use our website to find the tools you need and the tools we've demonstrated.
-

About that web site...

- # GNAC hosts a site with material related to this presentation:

<http://www.gnac.com/four-star>

- # This is a work in progress! We're depending on you to help us fill out a larger menu.
-