



Big Brother is still watching

*Web-based Monitoring & Notification
for Systems and Networks*

Sean MacGuire & Robert-André Croteau
The MacLawran Group Inc

Big Brother is Still Watching @SANS99 Sean MacGuire & Robert-André Croteau 1

About the authors

Sean MacGuire, Director, MacLawran Group Inc., Montreal, Canada
sean@maclawran.ca

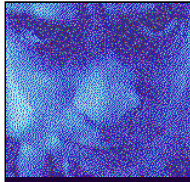
Sean has been working with Unix since 1983 as everything from a programmer, Systems Administrator, Manager of Technical Support, and is currently consulting as a Technical Analyst for Bell Canada.

Robert-André Croteau, Director, SCI MOTU Inc., Montréal, Canada
robert@motu.ca

Robert-André has been doing the same thing, for almost as long. He inhabits the cubicle just south of Sean's. Robert-André is responsible for many of the really useful enhancements to Big Brother, including

Disk space partition monitoring

- Enhanced notification
- Historical statistics graphs



The Ministry of Truth for Big Brother Presents

- ◆ Why Monitor?
- ◆ What is Big Brother?
- ◆ Supported Platforms and Requirements
- ◆ Components and Structure
- ◆ Installation and Configuration
- ◆ NT client specifications
- ◆ Event Notification
- ◆ BB User Contributions
- ◆ BB Benefits
- ◆ BB Availability
- ◆ Conclusion and Questions

Big Brother is Still Watching @SANS99 Sean MacGuire & Robert-André Croteau

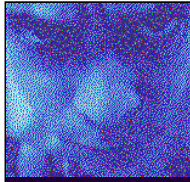
2

Hopefully you'll leave here with an appreciation for the needs and benefits of monitoring, where Big Brother fits in, how it works, some of the cool things it can do, the Community that has sprung up around it, and where it's going.

We'll be covering everything from where to get BB, to how it's put together, to the protocol it uses to get its messages across. We won't be going into a lot of detail about the installation process, since that's better handled by going off and installing it yourself.

It may not be technical enough for some of you, especially if you're already familiar with the product, or just interested in the gory details. For you, the solution is to leave right now and download the source code.

Because, that's the irony. In the time it takes for Robert-André and I to present this talk, you could go the BB web site, download it, compile it, and have it up and running on your network. Not only that, but this Powerpoint presentation is larger than the entire source code to BB.



Why Monitor?

- ◆ Easier to fix something before it explodes
- ◆ Saves lots of time and money
- ◆ Many problems are avoidable given sufficient notice in advance
- ◆ Trends are useful for planning
- ◆ Instant view helpful to everyone
- ◆ Shows bosses that we're doing something

Big Brother is Still Watching @SANS99

Sean MacGuire & Robert-André Croteau

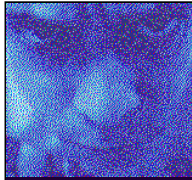
3

It seems like a dumb question; “Why Monitor?”. Then it’s possibly time to ask everyone here for a show of hands: ***How many people here are actively monitoring their systems and networks? How many are using Big Brother?***

It’s easier to fix something before a full blown crash. The best example is disk space monitoring - if a disk fills up on a Unix system, it can often mean a complete crash - and a big mess to clean up. Same with a lot of the messages that show up in the messages file... but it’s really boring going to each system, logging in, and checking everything manually.

I estimate that BB saves me about an hour per month per system it’s installed on - not to mention the savings from not having to reply to help desk queries about the status of elements in the system, or the time and money saved from simple prevention.

Besides, ***BB provides a nice window into the world of a Sys Admin, whose job too often is invisible*** until things go wrong.



What is Big Brother?

A Web-based System and Network Monitor

- ◆ Web-based status display
- ◆ Matrix of machines and areas
- ◆ **Green is Good / Red is Bad**
- ◆ Very lightweight and small
- ◆ Written in Bourne shell & C
- ◆ Simple client-server design
- ◆ Ability to set thresholds and notify administrators

| Local Server Group | | | | | | | | | |
|--------------------|------|-----|------|-----|------|------|------|-------|------|
| | comm | cpu | disk | ftp | http | msgs | pop3 | proc3 | smtp |
| iri-s01 | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| ns | ● | - | - | ● | - | - | - | - | ● |

| Third Display Group - same machine... | | | | | | | | | |
|---------------------------------------|------|-----|------|-----|------|------|------|-------|------|
| | comm | cpu | disk | ftp | http | msgs | pop3 | proc3 | smtp |
| iri-s01 | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| ns | ● | - | - | ● | - | - | - | - | ● |

Big Brother is Still Watching @SANS99

Sean MacGuire & Robert-André Croteau

4

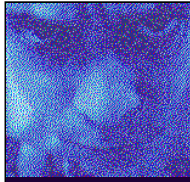
Big Brother is the same stuff that every Sys Admin has been writing since entropy first attacked Unix machines, and things started to fall apart.

Watching over machines isn't Rocket Science. It's like the description of being a pilot: ***Dull and Boring with occasional moments of sheer terror.***

The general task of an admin is to make sure that the machines stay up and running, that everybody else, users and managers, don't bother the admin. Generally, my goal has been to keep my phone from ringing.

So what does BB do differently - what makes it so special and wonderful that you should run out and download it? Two things. It includes a really simple set of client server programs that allow you to send data in a relatively secure fashion, and it displays the information you send on a really pretty web page for everyone to see.

That results in two things. Everyone knows how well the network is doing, and the phone doesn't ring quite as often for stupid questions.



What's New since SANS '98?

- ◆ Welcome Robert-André Croteau
- ◆ 2 major releases / 11 minor releases
- ◆ 35,000 more downloads
- ◆ NT and Netware client availability
- ◆ Enhanced Notification & Acknowledgment (BBWARN)
- ◆ History Logs & Service Availability data
- ◆ HTMLized enhanced status messages
- ◆ Y2K compliant
- ◆ IANA has officially assigned port 1984 to BB

Big Brother is Still Watching @SANS99

Sean MacGuire & Robert-André Croteau

5

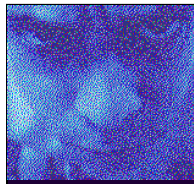
Lots of changes since last time - one of the most fun being my long-time work partner Robert-André Croteau has become my partner is working on Big Brother - some of you may have read his article about BBWARN in Sys Admin. That functionality has been rolled into BB.

We've had 13 releases which have made BB more stable, elegant, and increased the amount of information available on screen, as well as having all reports HTMLized.

The NT client for BB is a thing of beauty, as is Henrik Olsen's Netware client.

BB now can provide rudimentary historical availability information, and includes little graphs of uptime and availability by service.

Not only is BB Y2K compliant, but the IANA has seen fit to assign port 1984 to Big Brother and there's an RFC for the protocol on the way.



Supported Platforms and Requirements

◆ Supported Platforms

- ◆ All flavors of Unix
- ◆ BB Clients on NT4 - Service Pack 3
- ◆ Netware Clients available from Henrik Olsen

◆ Requirements

- ◆ At least one Unix box for BB Servers
- ◆ C compiler for the Unix versions
- ◆ Web server for publishing results
- ◆ Kermit if you want numeric paging
- ◆ Working e-mail for e-mail notification
- ◆ A little time and patience

Big Brother is Still Watching @SANS99

Sean MacGuire & Robert-André Croteau

6

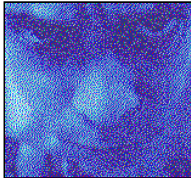
BB runs on just about every version of Unix known to man. The source code is included, and you'll need a C compiler to compile it unless you've gotten one of the precompiled versions that come with FreeBSD and Debian.

BB also has clients for NT 4 (Service Pack 3), and all versions of Netware available in binary format.

The Server still only runs on Unix, so you'll need at least one Unix box to act as the Display Server, Network Tester, and Pager Server. You'll also need a Web Server running if you want to publish the monitoring results, although you don't have to.

Out of the box, BB supports numeric paging using Kermit, and notification via e-mail - provided your e-mail server is working. Support for other paging methods like sendpage and qpage are available in the BB archives.

And like everything else, a little time and patience goes a long way.



Big Brother Components

- ◆ **Display Server: **BBDISPLAY****
 - ◆ Unix-based Server that collects the local and network information and creates the web pages
- ◆ **Notification Server: **BBPAGER****
 - ◆ Unix-based Server that receives events and dispatches notifications to the proper recipient
- ◆ **Network Testing: **BBNET****
 - ◆ Unix-based host which performs TCP network daemon testing
- ◆ **BB local clients**
 - ◆ Collect local system information like cpu/disk/processes/messages
- ◆ **Custom monitors**
 - ◆ Anything that can be rated as red/yellow/green can be tested

Big Brother is Still Watching @SANS99 Sean MacGuire & Robert-André Croteau 7

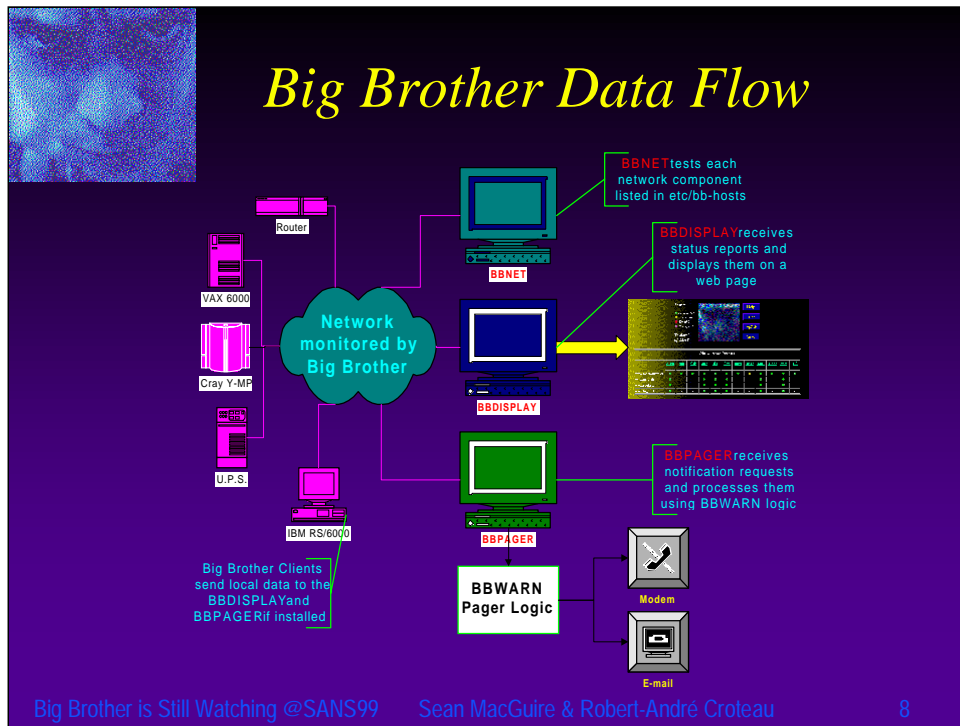
Big Brother consists of three major components. The Display Server generally known as **BBDISPLAY**, the Notification Server known as **BBPAGER** and the Network Testing host known as **BBNET**.

BBDISPLAY accepts incoming status reports. It also creates the display web pages every five minutes.

BBPAGER accepts notification requests from anywhere on the network and notifies whomever has been designated as the contact for whatever host or element has reported trouble.

BBNET is the host that tests every network service listed for every host. If any trouble is found it sends a message to the **BBPAGER** machine, and sends all normal status information to the **BBDISPLAY** server every 5 minutes.

Finally local BB clients send their information in every 5 minutes as well.

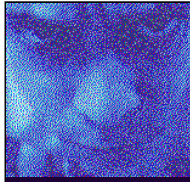


The BB data flow is very simple. Each system with a local BB client tests itself. If it sees trouble, it sends a message to that effect to the **BBPAGER** machine to notify the admin, and sends a status report to the **BBDISPLAY**. This process generally happens every five minutes.

The **BBNET** machine tests every service for every machine listed in the bb-hosts file. If a service doesn't reply, or an error is detected, a message is sent to the **BBPAGER** to notify the admin, and a status report is sent to the **BBDISPLAY**. Again, this process happens every five minutes.

The **BBDISPLAY** Display Server formats these incoming messages into pretty web pages and makes sure no message files are over 30 minutes old. If an old message file is found, it's status is turned purple to indicate a possible loss of service - since we haven't heard anything in a while.

The **BBPAGER** server takes incoming pages and routes them according to preset rules for who, what, where and when and which admin to contact.



Big Brother Protocol

- ◆ **BB clients** send data to **BBDISPLAY/BBPAGER** over port 1984
- ◆ The message format is:
 - ◆ **action** machine.area color data
- ◆ On **BBDISPLAY/BBPAGER** the bbd daemon listens on port 1984 for incoming messages. A valid request has an **action** of:
 - ◆ **status** writes a file in the log directory with the name **machine.area** containing the rest of the line sent
 - ◆ **page** calls the **bb-page.sh** script to page the admin with the error message to send to the pager
 - ◆ **summary** inserts a summary file into the log file directory
 - ◆ **ack** starts the **do-ack.sh** script to process an acknowledgment
- ◆ The protocol only sends data - no acknowledgment is required or sent.

Big Brother is Still Watching @SANS99 Sean MacGuire & Robert-André Croteau

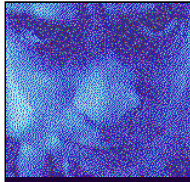
9

The daemon has very little to do: the severity levels and data are pre-formatted. All **bbd** has to do is take very simple actions:

- it writes file in the log with current status information
- it creates a corresponding html page in the html directory
- it appends a line to the history file on status change in the hist directory
- it can run the paging routines or ack a page

Because the status information is pre-formatted and encoded by color in the data sent to **bbd**, different machines can have different thresholds for red, and yellow. Also since the status is in the file, page creation is trivial and just involves creating a matrix of machines and areas, and putting the correct colors in the boxes. The colors of course, are the first word in the status files.

Extending BB to test for other functions is easy; just have **bb** send the new data to **bbd** with a new function name. So to add a function called **bobo**, do the test and have bb send this data to “**machine.bobo**” and the display will be updated automatically the next time the page is created.



What Big Brother tests

- ◆ **local client program** runs on the local machine to
 - ◆ Available disk space
 - ◆ 5 minute CPU load
 - ◆ notices and warnings
 - ◆ processes running
- ◆ **BBNET** tests all the daemons for each host listed in `bb-hosts`
 - ◆ http, pop3, smtp
 - ◆ ftp, nntp, dns
 - ◆ connectivity via ping
- ◆ All scripts run every 5 minutes - they
 - ◆ send data back to the display server `BBDISPLAY`
 - ◆ send data to pager `BBPAGER` if required

Big Brother is Still Watching @SANS99

Sean MacGuire & Robert-André Croteau

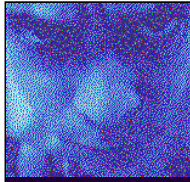
10

On unix systems, *bb-local.sh* runs on every system Big Brother is installed on, checking that the local machine is sane, that the disk hasn't exploded, the CPU isn't too overloaded, or that important processes haven't dropped dead.

bb-network.sh uses the program *bbnet* to test all the daemons listed for each machine in the *etc/bb-hosts* file in addition to pinging each of them.

This structure results in a certain amount of built-in redundancy. If a machine is down, *bb-network.sh* will catch it and report. If the *bb-network* machine itself is down, the *BBDISPLAY* machine notices that the log files haven't been updated and changes the screen color.

The Big Brother Web pages will always have a background color corresponding to the most severe condition on the network at that time. Remember you can click on any dot on the Big Brother Web page to get more details about the results of any particular test.

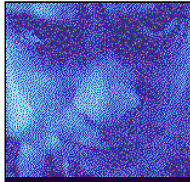


Big Brother Output

- ◆ **Static pages**
 - ◆ Main HTML page
 - ◆ Summary HTML page
 - ◆ HTML Status reports
 - ◆ Text Status reports
 - ◆ History text file
 - ◆ Acknowledgment history file
- ◆ **Dynamic pages**
 - ◆ Acknowledgment
 - ◆ Admin notification
 - ◆ History graphs

Big Brother produces the following output:

- The main **BBDISPLAY** page: **bb.html** containing the current status of all machines and areas being monitored. The background color will always correspond to the most severe condition of any element being monitored at any given time.
- The **brief display**: **bb2.html** accessed by hitting the **VIEW** button on the main screen. This screen shows only hosts and elements with a non-green status.
- The **status reports** themselves are accessed by clicking on any button. They contain the current full status information, an indication of how long that status has been there, and a history button.
- The **history status reports** provide a graphic look at how the service has been doing over the last 24 hours, along with a percentage color breakdown of availability.
- The **history log file** text is available and can be downloaded into a spreadsheet for more complete analysis.
- Pages are also produced for Admin notification and Acknowledgments.



bb-hosts file keywords

- ◆ Keywords control everything:
 - ◆ **BBDISPLAY** defines the machine to send the results to
 - ◆ **BBNET** is the machine responsible for network testing
 - ◆ **BBPAGER** is the machine that will handle pager requests
 - ◆ Daemons as defined in /etc/services
 - ◆ **pop3, smtp, ftp, telnet, http, nntp, dns, imap, ssh**
 - ◆ **group** is used for display groupings
 - ◆ **group-compress** is used to not display unused columns
 - ◆ **summary** sends summary info to another BBDISPLAY
 - ◆ **dialup** doesn't make BB upset if it can't be reached
 - ◆ **noping** to disable the default ping test for connectivity

Big Brother is Still Watching @SANS99

Sean MacGuire & Robert-André Croteau

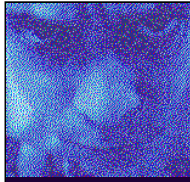
12

The *etc/bb-hosts* file controls the execution of Big Brother. This file should be the same on all machines running BB. If you're having trouble with Big Brother, this is the first place to look.

The *bb-hosts* file is based on the */etc/hosts* file format, in fact, they used to be the same. However, as BB expanded, and for security purposes (not everyone is allowed to edit */etc/hosts*), BB got it's own file.

The first thing any BB client does upon startup is looks for its own name (as returned by a **uname -n** call) in the file. Once it finds itself, it can determine whether it's a **BBDISPLAY**, **BBPAGER** or **BBNET**, and where it has to send reports.

- **BBDISPLAY** is the Web Server where the Big Brother Display will live and where the BB web pages will be created.
- **BBNET** is the machine that will do the network testing. This can be the same as **BBDISPLAY**, and often is.
- **BBPAGER** is the machine which will handle pager requests.



Sample bb-hosts file

```
group <H3><I>MacLawran Servers</I></H3>
#
# This is a comment - next line is for BBPAGER BBNET and BBDISPLAY
#
192.168.117.80 www.maclawran.ca # BBPAGER BBNET BBDISPLAY ftp dns smtp pop3 http://www.maclawran.ca/ ssh
192.168.117.80 www.unix.sh # ftp smtp pop3 http://www.unix.sh/ dns telnet imap
group <H3><I>ITI Servers</I></H3>
192.168.117.6 www.iti.qc.ca # ftp pop3 http://www.iti.qc.ca/
192.168.117.7 ns.iti.qc.ca # ftp pop3 http://www.iti.qc.ca/ dns smtp
192.168.116.250 cisco-116.iti.qc.ca cisco-116 # dialup
group-compress <H3><I>Andrew's Monitoring Stuff</I></H3>
192.168.213.185 www.istar.ca # noping http://www.istar.ca
192.168.136.2 dns.istar.ca # dns noping
192.168.136.6 home.istar.ca # ftp http://home.istar.ca/
dialup modem-bank 192.168.116.20 4
summary bigbrother.dev1 192.168.117.80 http://www.maclawran.ca/bb/bb.html
```

Big Brother is Still Watching @SANS99

Sean MacGuire & Robert-André Croteau

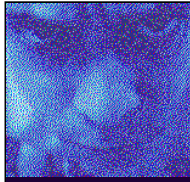
13

The **group** keyword tells BB to create a new display table. Groups are in effect until the next **group** line is reached. This will give the display a pleasant table structure. The **group-compress** keyword works the same way except columns without data are not displayed. HTML codes are permitted only on the **group** and **group-compress** lines.

- **noping** tells the **BBNET** machine not to perform ping testing on the host in question. This is useful where firewalls are blocking ping.
- **dialup** lines are used to test banks of modems for connectivity. It's nothing special, it just pings banks of IP addresses to see which are active.
- **summary** lines allow you to send the cumulative results of a **BBDISPLAY** to another machine defined as a **BBDISPLAY**. You can stack BBs.

The `/etc/services` file is used to map the service names to be checked against the TCP port numbers to open. Common error are things like misspellings of **pop3** as **pop-3** or even just **pop**. Spelling counts.

Only well-behaved TCP services can be checked natively by BB, other services (like ldap and dns) require custom built tests.



Security Considerations

- ◆ *etc/security* allows you to define which hosts and networks can connect
- ◆ Big Brother doesn't have to run as root
- ◆ Big Brother daemons can only write in the BB directories
- ◆ All commands are executed using their full pathname to avoid Trojan horses
- ◆ Big Brother has it's own tmp directory
- ◆ You have the source code!

Big Brother is Still Watching @SANS99

Sean MacGuire & Robert-André Croteau

14

The *etc/security* file just contains lines with IP or network addresses of clients permitted to connect to the BB server running on that machine. If the file exists, then only those hosts and networks listed will be allowed to connect. All others will be silently dropped. For example:

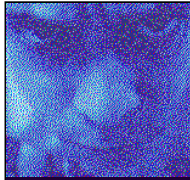
```
204.101.110.101           Allow client to connect  
204.101.112.0 Allow subnet to connect
```

If Big Brother is not running as root, it could have trouble reading log files on certain machines depending on permissions.

The BB Server checks to see if the *bb* client is trying to do funny things with the pathnames or is attempting to overflow buffers. All communications happen over port 1984.

All BB commands are stored in environment variables, and are executed using their full pathnames to avoid possible Trojan horses.

The best security is that you have the source code!



Event Notification

- ◆ Any color level can generate an event
- ◆ Notification of the event can be sent via e-mail, numeric page or SMS message
- ◆ Notification can be sent to users based on originating host, service, day & time
- ◆ Acknowledgment of a notification can delay the repeated notification of the event

Big Brother is Still Watching @SANS99

Sean MacGuire & Robert-André Croteau

15

By default Red and Purple colors generate an event

e-mail message has subject

!BB - 4480010! www.maclawran.ca.http - 600192168001001

4480010 - Acknowledgement code

www.maclawran.ca.http - host and service code

600192168001001 - 600 http service code

192168001001 IP address

The e-mail body is text of the status message

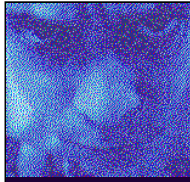
numeric message: **600192168001001480010**

600 - http service code

192168001001 - IP address

480010 - Acknowledgement code

Using "Page/Ack" button on the main BB page you can acknowledge an event by entering the ack code and a time delay



Notification Setup

- ◆ etc/bbwarnsetup.cfg
- ◆ tokens:
 - ◆ bbwarn
 - ◆ svcerrlist
 - ◆ ignforall
 - ◆ pagehelpcode
 - ◆ ttyline
 - ◆ prefix
 - ◆ suffix
 - ◆ pagedelay
 - ◆ pagelevels
 - ◆ pagelevelsmail
 - ◆ pagetype
 - ◆ pagemaster
 - ◆ pageaddhtmlpath
 - ◆ cfgdelim

Big Brother is Still Watching @SANS99

Sean MacGuire & Robert-André Croteau

16

bbwarn: TRUE - enable notification

svcerrlist: 600:HTTP - code equivalence for service displayed in numeric paging

ignforall: egrep expression to exclude host.service pairs - nyc*|mtl*|*cpu

pagehelpcode: Numeric code used in notification from "Page/Ack" web page - 911

ttyline: devices to use for numeric paging - /dev/cua0

prefix:init codes for calling modem string (T9,,,...)

suffix: codes to send modem after numeric page code

pagedelay: How long to wait before next page - 15 minutes

pagelevels: color on which to notify - red purple

pagelevelsmail: color level on which only e-mail recipients are notified

pagetype: Specifies which type of notification to use

(specifies how pagedelay is applied, how long)

EVENT - you get notified for all problems . Each is sent at pagerdelay interval

HOST - notification is sent only if no events within pagerdelay has been received
for a host

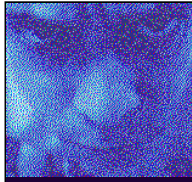
GROUP - recipients get a notification if no other event that belongs to a group
directive in the bb-hosts file within pagerdelay

RCPT - recipients receive only 1 notification per pagerdelay

pagemaster: e-mail recipient for notification processing errors

pageaddhtmlpath: URL path where BB is found. The event status file name is added to this path
in the e-mail notification

cfgdelim: Delimiter to use in bbwarnrules.cfg



Notification rules

- ◆ etc/bbwarnrules.cfg
 - ◆ hosts
 - ◆ excluded hosts
 - ◆ services
 - ◆ excluded services
 - ◆ day
 - ◆ time
 - ◆ recipients

The Notification rules specify who gets notified for what and when, and who gets woken up in the middle of the night. It is based on rules with the following format:

hosts;excluded hosts;services;excluded services;day;time;recipients

***;*;*;*;root@localhost**

All events are sent to root@localhost

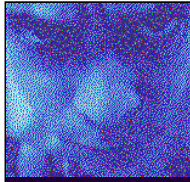
***;buf*;*;1-5;0800-1800;robert@localhost**

all events excepts the hosts matching buf* are sent to robert@localhost from monday-friday during business hours

special rules lines

notify-admin*;*;*;*;root@localhost - when user uses **Page/Ack** page

unmatch*;*;*;*;root@localhost - if host is not found in **bb-hosts** file



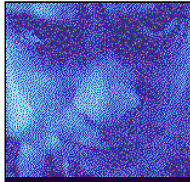
User Contributions

- ◆ Mailing list Technical Support
- ◆ Oracle
- ◆ MRTG integration
- ◆ LDAP
- ◆ Alpha pager support
- ◆ Alternate images
- ◆ fping
- ◆ multidisplay
- ◆

Support via the BB mailing list is the number one user contribution.

Without the BB community, there's no doubt that BB wouldn't have propagated as far as it has.

- The **MRTG integration** can notify if the bandwidth of an interface is saturated - it also adds an mrtg column in the display
- The **alternate images** were created to help people who are color-blind.
- The **fping** contribution is useful for those who have a large site and need a quick connectivity test. The regular connectivity test uses ping and it can stall for a few seconds if a host doesn't respond.
- You can make your own contributions by just uploading your archive to the FTP site and then hit the mailing list telling them of your great enhancement. Sometimes they are even included in the BB archive !



Big Brother Benefits

- ◆ System information is available to anyone who needs it, anytime from anywhere
 - ◆ Systems Administrators
 - ◆ Help Desk personnel
 - ◆ Even Management can understand it
- ◆ Simple, portable, and highly configurable
- ◆ Enhanced Notification makes sure the right person is notified of a problem

Big Brother is Still Watching @SANS99

Sean MacGuire & Robert-André Croteau

20

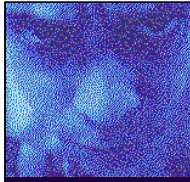
Probably the greatest benefit is the ability to publish system status information in a format that is understandable by all. No more calls about whether or not a service is available.

There's enough information on the Web Pages to finally let managers know how well their complex network and even more complex administrators are doing. Green screens are good.

Even when there is trouble, management and the help desks can be confident that the admin has already been notified by Big Brother and that they are working on the problem.

Since installing BB, I've never been caught by surprise by a user. It also allowed me to go for coffee in peace knowing I'll get paged if need be. Being proactive, that's what they call it.

Conservatively I figure it saves me about an hour per system per month.



BB availability

- ◆ Big Brother lives at <http://www.bb4.com>
- ◆ Distributed as source code
- ◆ Shipped with with FreeBSD and Debian
- ◆ License is free for non-commercial use
- ◆ Support via the BB mailing list & archives
- ◆ Contributions live at <ftp://ftp.deadcat.net/pub/BB/>
- ◆ Mailing list archives live at <http://www.tpdinc.com/~bb/bb.htm>

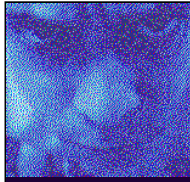
The best way to understand Big Brother is to download it and try it out. It's pretty simple and does a lot of what admins need to do. The code has been ported to just about every Unix box around, from the very old, to Crays... there's even an OpenVMS port out there somewhere.

The install is simple. You may have to adjust some paths in *etc/bbdef.sh* in case there is some screaming, but that should be the extent of the mods required.

Commercial use is restricted. ***You can't charge others for the services BB provides or include it in a product for sale without first obtaining a Commercial License.***

The mailing list is run by Paul Sittler from Texas A&M and lives at taex001.tamu.edu - send a message with "**subscribe bb your-email-addr**" in the body of the message.

- Archives of the list are kept by Nick Silberstein, another long time brother. The archives live at: <http://www.tpdinc.com/~bb/>
- Adam Goryachev runs the **BB User Contributions** FTP site at [ftp.deadcat.net/pub/BB](ftp://ftp.deadcat.net/pub/BB)



In Conclusion

- ◆ Big Brother is simple
 - ◆ Shell scripts and C programs
 - ◆ Polls and Collects data from your network
 - ◆ Displays this information on a Web page
- ◆ Big Brother isn't
 - ◆ bloatware
 - ◆ costly, complicated or cumbersome
- ◆ Any Questions?

Big Brother is Still Watching @SANS99

Sean MacGuire & Robert-André Croteau

22

Big Brother is a combination of monitoring methods. Unlike SNMP where information is just collected and devices polled, Big Brother is designed in such a way that each local system broadcasts it's own information to a central location. Simultaneously, Big Brother also polls all networked systems from a central location. This creates a highly efficient and redundant method for proactive network monitoring.

The entire network status is displayed on an incredibly intuitive web page. Red is bad, and green is good. Click on the dot and get more information. You get paged if things get really bad.

Since BB is so lightweight, free, and simple, there's no reason not to install it on your network. Even if only to make sure that the expensive monitoring system is up and running, or as a panacea to upper management.

Thanks for listening, and at this point we'd be happy to answer any questions you might have about BB.