Adventures in Monitoring
or
All about Big Brother

Sean MacGuire
Robert-André Croteau
BB4 Technologies Inc
Introduction

Big Brother is a framework for systems & network monitoring and notification written by Systems Administrators for Systems Administrators. This is important - because until Big Brother, similar products were written only for Network health by strange Network people.

It’s also a great means to provide Management with some sort of idea of how their network is doing (and what they’re paying us for) in a way that even they can understand (red is bad)

Becoming a Brother is not automatic - you need to get BB running, first...
What does Big Brother do

- Monitors client systems for disk space, messages, processes, load average, etc
- Monitors Network services like web servers, ftp, mail, nntp, telnet, etc.
- Custom monitors for Oracle databases, bandwidth via MRTG, SNMP2BB
- Notification via e-mail, alphanumeric pager, SMS
- Reporting - useful for SLA management
- Can display the results of any custom tests provided you can determine red/yellow/green
- All tests are done every 5 minutes (configurable)
Guiding Development Principles

- Monitor and Notify but don’t act
- Keep it simple
- Make it easily understandable
- Make it easily extensible
- Make it portable
- Make it work, make it right, make it fast
Architecture

• Client/Server architecture
  - Written in Bourne Shell and C
  - Big Brother servers listen on port TCP/1984

• Big Brother has 4 major parts
  - BBDISPLAY receives all incoming messages and displays them on the web page
  - BBPAGER processes all pager requests
  - BBNET tests all network services
  - And the client software sends local system information like cpu/mgs/procs/disk
Architecture

BBNET tests each network component listed in etc/bb-hosts

BBDISPLAY receives status reports and displays them on a web page

BBPAGER receives notification requests and processes them using BBWARN logic

Network monitored by Big Brother

Big Brother Clients send local data to the BBDISPLAY and BBPAGER if installed
What you’ll need

- A machine with network connectivity and a little disk space
- A working C compiler and include files
- Web Server up and running
- About 2 hours
- The Big Brother archive itself, available from bb4.com
- A little patience...
Installation

- Unpack the archive
- `cd bb<ver>`
- `cd install`
- `./bbconfig` (preferably as root)
- `cd ..../src`
- `make`
- `make install`
- Also link APACHEDIR/htdocs/bb to BBHOME/www
  - add Options FollowSymLinks to httpd.conf
Configuration

• etc/bb-hosts format similar to /etc/hosts should be the same on all machines

• etc/bbdef.sh Tunable parameters

• etc/bbsys.local Local pathnames

• etc/bbwarnsetup.cfg Paging setup

• etc/bbwarnrules.cfg Paging rules

• etc/security Who can connect to bbd

• etc/bb-dftab Disk space by partition

• etc/bb-proctab Process monitoring
etc/ bb-hosts

• Keywords control everything:
  - **BBDI SPLAY** 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
  - **group-only** is used to display only specific columns
  - **summary** sends summary info to another BBDI SPLAY
  - **dialup** doesn’t make BB upset if it can’t be reached
  - **noping** to disable the default ping test for connectivity
  - **noconn** to remove the default ping test for connectivity
etc/bb-hosts

# Sample bb-hosts file
#
0.0.0.0  www.bb4.com  # BBDISPLAY BBPAGER BBNET
group-compress <H3><I>Zoo net</I></H3>
216.191.117.55 tower.bordercontrol.com  # http://www.bordercontrol.com/
216.191.20.20 ns1.zoo.net  # dns
216.191.20.21 ns2.zoo.net  # dns
216.191.20.36 cougar.zoo.net #
0.0.0.0  somehost.bb4.com  # noconn
216.191.20.205 pm3a.zoo.net  #
216.191.20.135 hippo.zoo.net  #
#204.101.218.10 aardvark.zoo.net #
The Smoke Test

- `cd BBHOME`
- `./runbb.sh start`
- Check BBOUT log file for errors
- After 2 mins: BBHOME/bb/bb.html is generated (so is bb2.html)
- If you’re lucky, your display will resemble this...
<table>
<thead>
<tr>
<th>Zoo net</th>
<th>conn</th>
<th>cont</th>
<th>cpu</th>
<th>disk</th>
<th>dns</th>
<th>fping</th>
<th>http</th>
<th>msgs</th>
<th>procs</th>
</tr>
</thead>
<tbody>
<tr>
<td>tower.bordercontrol.com</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><a href="http://www.zoo.net">www.zoo.net</a></td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ns1.zoo.net</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ns2.zoo.net</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>cougar.zoo.net</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>somehost.bb4.com</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>pm3a.zoo.net</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>hippo.zoo.net</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Getting help...

- The documentation… READMEs and the web help
- The search engine: http://support.bb4.com
- The BB mailing lists: bb / bbd / bbntd
  - To subscribe mailto: MajorDomo@bb4.com
  - In the *body* of message: subscribe bb|bbd|bbntd]
- Commercial support is available from us
Adding Network Services

• Well-behaved TCP services are supported out of the box, like ftp, http, telnet, nntp, etc.

• Add the TCP service name in bb-hosts file

• Add the same service name in bb-network.sh with the other TCP tests

• The TCP service directive can have qualifiers:
  – ! Make sure service is not responding (!ftp)
  – ? If service does not respond, display clear (?ftp), it’s assumed to be a dialup link
Adding Clients

- If the OS/architecture is the same as your
  BBDISPLAY:
    - cd BBHOME/etc
    - edit bb-hosts with the new client host line
    - cd ../install
    - ./bbclient <hostname>

- reload the BB archive on the client and recompile if it’s not the same OS/architecture

- Make sure the client hostname matches the contents of the etc/bb-hosts file exactly!
Getting notification to work

- Sacrifice a chicken to the pager gods
- If that doesn’t work, try e-mail first
- In etc/bbwarnrules.cfg, try a catch-all rule:
  - *;*;*;*;*;*;mymail@somemailhost.com
  - If that fails, join the mailing list
- For modem based notifications, install:
  - qpage / sendpage / kermit
- Support for custom notifications
- Test notifications by adding a dummy line to etc/bbdftab (warn at 1% page at 2%):
  
  ./:1:2
Custom tests and other cool stuff

- BB Supports multiple BBDI SPLAYs and BBPAGERS
- Failover support in ext/
- BBMRTG - BB-based thresholds/notifications for MRTG
- Fping support to replace standard connectivity test (ping)
- SNMP2BB - Pass SNMP info to BB, especially useful with Netapps and Cisco routers
- LARRD - Trending
- http://www.deadcat.net (over 150 contributions)
Conclusion

• Not complicated
• Great community with an excellent mailing list
• Very easy to extend and add your own tests
• Any questions?