

# Big Brother HowTo

robin 12apr2001

<b>How BB works</b> .....	<b>1</b>
<b>A. Installation</b> .....	<b>1</b>
<b>1. BB Server setup</b> .....	<b>1</b>
<b>BB server configuration</b> .....	<b>2</b>
<b>2. Set up client machines :</b> .....	<b>2</b>
<b>3. On all clients and server , create a startup script</b> .....	<b>3</b>
<b>B. Customisation / Tips etc.</b> .....	<b>3</b>
<b>Disabling alerts:</b> .....	<b>3</b>
<b>Removing old history files to stop purpleness, or spurious alerts:</b> .....	<b>3</b>
<b>BBOUT file</b> .....	<b>4</b>
<b>Add-on scripts</b> .....	<b>4</b>
<b>Adding per-client customisations</b> .....	<b>4</b>
<b>Customisations</b> .....	<b>4</b>
<b>Stonebeat</b> .....	<b>4</b>
<b>HTTP Content monitoring: 'getw'</b> .....	<b>4</b>
<b>Remote Paging from pear : 'bbpage'</b> .....	<b>5</b>
<b>Acknowledging alerts</b> .....	<b>5</b>

## How BB works

Big Brother is used to monitor Unix system services and status (e.g. disks nearly full, processes not running, etc.), and displays this information to the administrators via a web server. It is also fairly easy to write your own BB shell scripts to monitor extra items or services.

N.B. You need to install your own web server to use Big Brother; all BB does is generate HTML pages.

Each item or service you wish to monitor on a machine can be monitored either remotely from the Big Brother server (e.g. services such as smtp, dns, telnet ..) or locally on the machine itself (e.g. disk fullness, cpu business, processes not running). To monitor locally you must install the BB software on that machine, which then becomes a BB client.

Once you have installed a BB client, it checks its local items and services (disk, cpu, processes etc.) regularly (e.g. every 5 minutes) and sends notifications to the BB server.

The BB server runs a daemon (bbd) which listens on port 1984 for status messages from the clients. It then processes those messages into HTML for display.

The BB server also monitors the clients' remote services (e.g. telnet, smtp, dns..) and updates the HTML accordingly. If there is no recent data for a client then the client's colour is marked as purple on the display.

## A. Installation

### 1. BB Server setup

NB You will need gzip and gcc

- create a user bb :  
bb:x:103:10:Big Brother user:/opt/bb:/bin/ksh (or bash if you prefer)

- `su - bb` and extract the distribution tarfile :  
bb source tarfile is : 411062 Apr 11 16:45 bb-1\_7a\_tar.gz
- untar the tarfile in his home dir. This will create a directory bb17a  
`gzip -dc bb-1_7a_tar.gz | tar xf -`  
`ln -s bb17a bb` (not mandatory, but will be useful later)
- Now install a webserver called 'bb' (ie iPlanet server\_name is https-bb) with a cgi-bin pointing to /www/bb/cgi-bin or similar, and a docroot /www/bb/docs which contains a symlink called bb pointing to /opt/bb/bb/www. Make sure the cgi-bin is writeable by user bb.
- Now build BB  
`cd bb/install`  
`../bbconfig solaris`  
`make`  
`make install` (this will also install things in the cgi-bin)

## BB server configuration

Edit `bb/etc/bb-hosts` with your machines, to read something like:

```
group <H3>Unix Servers</H3>
172.31.2.10    jupiter # BBPAGER BBNET BBDISPLAY telnet ftp ssh http://jupiter:8000/
10.161.81.17  europa # telnet http://europa http://10.161.81.19 ssh ftp
10.161.81.12  calisto # telnet ftp ssh dns smtp
172.31.1.10   uranus # telnet ssh ftp
172.31.1.12   pluto # telnet ssh ftp

group-compress <H3>NT Servers</H3>
10.161.81.29  noddy # http://10.161.81.30 http://10.161.81.36 http://10.161.81.37
10.161.81.69  bigears # http://10.161.81.70 http://10.161.81.76 http://10.161.81.77
```

where jupiter is the bb server.

BBPAGER means it will handle alerts via email or pager;

BBNET means it will perform all the remote connectivity tests to check all the other servers (ping, telnet ftp etc)

BBDISPLAY means it will run a Web server for displaying the BB status.

N.B. - the # symbols after the hostname are NOT comments.

- the hostname entries do not need to be real hostnames: BB can use the IP address to check things. However if the hostname does resolve to an IP address, BB will use it. In the example above, europa, noddy and bigears are running several web servers on different IP aliases

Now start BB:

```
cd ~bb/bb
```

```
run 'runbb.sh start' to start it up
```

Make sure it works before installing client machines. When you connect to the web server you should see green dots against all of jupiter's items after a few minutes.

## 2. Set up client machines :

Make sure you have added the client to `bb/etc/bb-hosts` on the server, then :

a. On server :

```
cd bb/install
../bbclient client_name
```

which creates a tar file in /opt/bb called `bb-client_name.tar` which you can copy across to the client machine

b. on the client :

create user bb as above and untar `bb-client-name.tar` in /opt/bb

In -s bb17a bb  
then start bb using bb/runbb.sh start

Wait 5 minutes and you should see the client get some green dots on the BB display

### 3. On all clients and server , create a startup script

Startup script : create /etc/init.d/bb and symlink to it from /etc/rc3.d/S98bb and /etc/rc0.d/K12bb:

```
#!/bin/sh
# start/stop/restart Big Brother
# robin 18apr2001

BBUSER=bb
BBHOME="/opt/bb/bb17a"
BBDISPLAY=jupiter          # BBDISPLAY is bb web server

case $1 in
start|stop|restart)      ACTION=$1
                        su - $BBUSER -c "cd $BBHOME;./runbb.sh $ACTION";;
*) echo "Usage: $0 start|stop|restart";exit;;
esac

# start web server if we are the bb web server
if [ `uname -n` = $BBDISPLAY ]
then
    echo ${ACTION}ing web server
    /opt/netscape/server4/https-bb/$ACTION
fi
```

## B. Customisation / Tips etc.

### Disabling alerts:

If you want to stop getting alerts from a particular machine or about a particular service on a machine, either comment out the machine or service from bb-hosts, or change the bb/etc/bbwarnrules.cfg: e.g. to NOT receive alerts about disk problems on calisto, add a line like  
!calisto;;disk;;\*;\*;bb@yourdomain.com

### Removing old history files to stop purpleness, or spurious alerts:

e.g. if you make a typo in a hostname in bb-hosts, then correct it some time later, you may get purple icons when there is no problem. Purple means 'no report available' and means that it sees some data from the old hostname, but no recent data. So you have to remove the historical data:

```
[bb@jupiter]/opt/bb/bbvar:=> ls
acks/      data/      disabled/  hist/      histlogs/  logs/
[bb@jupiter]/opt/bb/bbvar:=>
[bb@jupiter]/opt/bb/bbvar:=> find . -name "*dzwLar*"
./hist/dzwLarch.conn
./hist/dzwLarch
./hist/dzwLarch.http
./histlogs/dzwLarch
./logs/dzwLarch.conn
./logs/dzwLarch.http
[bb@jupiter]/opt/bb/bbvar:=> find . -name "*dzwLar*" | xargs rm -fr
[bb@jupiter]/opt/bb/bbvar:=> find . -name "*dzwLar*"
[bb@jupiter]/opt/bb/bbvar:=>
```

similarly if you remove a service (e.g. http from bigears), then it sees the old data but no recent data, so it shows purple.  
cd ~bb/bbvar

```
find . -name "*bigears*http*" | xargs rm
rm -r histlogs/bigears/http
```

## **BBOU file**

You can see the output of the runbb.sh script in bb/BBOU . this often helps in working out why things are failing.

## **Add-on scripts**

We have added several scripts to BB, downloaded from the BB web site (bb4.com): bb-oracle.sh and bb-ods.sh. These are called from bbdef.sh locally on each box (in \$BBEXT), so if the client doesn't run oracle or DiskSuite you should remove these entries from bbdef.sh and restart bb on the client.

## **Adding per-client customisations**

e.g. setting rowan to alert when a disk is 99% full instead of 90% -see bb/etc/bb-dftab  
or setting which processes should be running on each client -see bb/etc/bb-proctab

then send the updated bb-\*tab files to all the clients

## **Customisations**

### **Stonebeat**

ext/bb-stoneb : this is a script which runs only on jupiter to check the firewalls' Stonebeat status (Stonebeat is FireWall-1's High Availability module). The script uses ssh to connect to each firewall in turn and run 'sbcontrol status', and stores the result. If the result is different from the previous time the script was run (5 minutes previously) then an alert is raised.

The script is run by being included in the EXT section of etc/bbdef.sh on jupiter.

It logs to jupiter:/opt/bb/stoneb\_logs.

### **HTTP Content monitoring: 'getw'**

ext/bb-getw : this is a script which uses curl (a public-domain URL-retriever program like wget) to retrieve the pages from several websites, then uses grep to make sure the page retrieved contains certain HTML text.

The script uses a configuration file (/opt/bb/etc/getw.cfg) to determine what URLs it should retrieve and what HTML text should be contained in the retrieved pages:

```
jupiter 1 jupiter:8000          Big Brother
dzwbigears 1 10.161.81.91      HTML
dzwbigears 1 http://10.161.81.92  HTML
reseller_proxy 2 www.mac.de/po.asp  McMillen
reseller_proxy 2 https://www.mac.de/po.asp  McMillen
dzsaspen 1 10.161.81.114/cgi-bin/monitor/monitor.jsp France Platinum|Latest News
```

The fields in the configuration file are as follows:

- The first field is the hostname which BB should log to
- the second field is the severity of the error generated if the content check fails (1=most severe; will generate a red alert, 2 will generate a yellow alert)
- third field is the URL to retrieve.
- all other fields are passed to `grep -i` as the search pattern which should be found in the HTML page retrieved

The script is run by being included in the EXT section of etc/bbdef.sh on jupiter.

bb-getw produces several log files each time it runs: these logs are stored under `jupiter:/opt/bb/getw_logs` in a path which reflects the URL being checked, e.g. `/opt/bb/getw_logs/http://10.161.81.92`

there should be two files created in there each time the URL is checked :

`TIMESTAMP` (e.g. `TIMESTAMP` is 200105311257 for 12:57 on 31May2001) which contains the HTML text retrieved from the server

and `TIMESTAMP.head` which contains the HTTP headers and result status (e.g. 500 Server Error) retrieved from the server and `TIMESTAMP.log` which shows the conversation which curl has with the server.

Also under `jupiter:/opt/bb/getw_logs` is a *TIMESTAMP*.status summary file for each server (i.e. the first field in the `getw.cfg` file) which shows a summary of all the URLs associated with that server ,e.g: the .status file for noddy at 15:07 on 31May2001 :

```
[bb@jupiter]/:=> more /opt/bb/getw_logs/noddy/200105311507.status
noddy 10.161.81.110 OK : contents CSG/csg_national_entry_page found OK.
noddy https://10.161.81.110 OK : contents /csg_national_entry_page found OK.
noddy 10.161.81.111 OK : contents CSG/csg_national_entry_page found OK.
noddy https://10.161.81.111 OK : contents /csg_national_entry_page found OK.
noddy 10.161.81.112 OK : contents CSG/csg_national_entry_page found OK.
noddy https://10.161.81.112 OK : contents /csg_national_entry_page found OK.
noddy 10.161.81.113 OK : contents CSG/csg_national_entry_page found OK.
noddy https://10.161.81.113 OK : contents /csg_national_entry_page found OK.
```

## **Remote Paging from pear : 'bbpage'**

In order to avoid spurious pager alerts from Big Brother (there are intermittent errors on the site which do not re-occur) , there is a shell script called **bbpage** running on pear, from bb's crontab :

```
6,21,36,51 7-21 * * * /opt/bb/bin/bbpage 2>&1 | /usr/local/scripts/smailx -s "Persistent BigBrother alert
`date|awk '{print $1 $3 "-" $4}'`" -r bb@rope.com bb@starsky 03419163345@paging.vodafone.net
```

This script will get the BB home page from jupiter , compare any red alerts it finds with the same page retrieved the previous time (normally 15 minutes before) , and only raise an alert if there are persistent red http or conn errors.

The script will also raise an alert if BB appears to have died (i.e. the BB home page has not been updated for 20 minutes) , or if the BB home page cannot be retrieved (e.g. because jupiter is down, or the BB web server has died) , so it functions as a monitor of BB.

The script can be set (via crontab) to send mail to bb@starsky, this will deliver mail via the leased line (or ISDN connection (via starsky and exchange), rather than using hazel and delivering mail over the internet. This should allow us to receive alerts from bbpage even if the Internet connection at Redbus goes down.

N.B. the bbpage script could be moved to another machine if desired; it just needs /usr/local/bin/wget to be already installed

## **Acknowledging alerts**

When you receive an e-mail alert from BB, it contains an acknowledgement code number in the subject :

e.g. Subject : !BB - 9614010! dzwnoddy.conn - 50010161081029

In this case 9614010 is the acknowledgement code

You can paste this number into the Security Code field of the BB "Contact" page (which you get to by clicking on the lightning-bolt icon at the top left of the main BB display), and type a message (e.g your name and what you are doing about the problem) into the "Optional message" field, then click on the "I'm working on it" button.

Once you have done this , the red icon for that alert should turn to a red tick, and you should not receive any alerts for 60 minutes. The message you typed will appear at the bottom of the status page for that item.

The bbpage script will also ignore alerts which have been acknowledged, and not page you about them.