big brother®
SOFTWARE

# Big Brother® Professional Edition

## Best Practices Guide

## Getting Started

Big Brother® is a Web-based system and network monitoring solution that makes it easy for your organization to monitor, support and maintain a distributed network of computer resources. This document will help you plan for your Big Brother deployment and leverage the product's features to maximize benefits.

The Big Brother Professional Edition (BBPE) Best Practices Guide contains the following sections:

- Architecture
- Planning
- Deployment
- Installation and Configuration
- Customization

## Technical Resources

Big Brother® includes comprehensive product documentation and other technical resources that help you deploy, configure and use Big Brother®. On-line help can be accessed after the Big Brother® Server has been installed by clicking the "?" icon in the upper left hand corner on the browser interface. Both Server and Client help documentation is provided by clicking the "?" on all UNIX/Linux BBServers. Big Brother® Server help documentation is provided by clicking the "?" icon on all Windows BBServers. Windows BBClient help is accessed from Start (button) -> All Programs -> Quest Software -> Big Brother Professional Edition -> Client -> Help. Every Big Brother® configuration file is replete with comments, instructions and examples for configuring the behavior of each feature.

## Quick Feature Overview

Big Brother® is designed to let anyone see how their network is doing in real-time, from any Web browser, anywhere in the world. An experienced Systems Administrator should be able to

get the core of Big Brother® up in about an hour (less if they read the documentation). Once you've done this, you're a Brother.

## Web-Based Matrix Display – Custom Dashboards

Big Brother® displays status information as Web pages or WML pages for WAP-enabled devices. These Web pages have the systems monitored down the left hand side of the page, the tests for each system across the top of the page. This results in a matrix of color coded dots on screen. Green is good, red is bad. In addition, the background color of the status pages is always the color of the most serious condition of any element being monitored at that time. The display can be tailored to create custom dashboards for each department within your organization (NOC, Data Center, IT, Helpdesk, Support) and you can customize the background skins using CSS.

## Architecture

Big Brother® uses a client-server architecture combined with methods which both push and pull data. Network testing is done by polling all monitored services from a single machine, and reporting these results to a central location (the BBDISPLAY). If you want local system information, you can install a BB client on the local machine, which will send CPU, process, disk space and logfile status reports in periodically. Each report is time stamped with an expiration date. This lets you know when a report is no longer valid, which is usually an indication of a more serious problem.

## Redundancy

Brother supports redundancy through allowing you to run multiple instances of Big Brother in parallel. This means that BB clients can report into multiple Web displays (BBDISPLAYs) and notification servers (BBPAGERs).

## Protocol

Big Brother sends all status reports from client to server over port 1984. What other port would Big Brother use? The IANA has assigned Big Brother this port, and the BB protocol itself is open and can be configured to use any port.

## Platforms

The Big Brother servers run on Window/Unix/Linux. Client software is available for Windows/Unix/Linux, while user contributed clients for Netware, Mac OS 9, VMS, AS/400 and VM/ESA at http://www.bb4.com/community or www.deadcat.net

big brother®
SOFTWARE

## Network tests

Big Brother includes support for testing ftp, http, https, smtp, pop3, dns, telnet, imap, nntp and ssh servers. Support for additional tests are easily added.

## Real-Time Diagnostics

Beyond monitoring for high availability, you will also need to manage your system for optimal performance. Once Big Brother alerts you of a condition, you can then use Quest Software's Spotlight® to gather domain specific information and quickly resolve performance issues. Spotlight is a real-time diagnostic tool designed to diagnose and resolve performance bottlenecks before your users are affected. More information on Spotlight is available here.

## Local Tests

If you choose to install a BB client on a local machine, it will monitor disk space, CPU usage, messages and can check that important processes are up and running.

## Notification & Alerting

Big Brother has a robust notification rule set. You can notify based on time-of-day, machine, status color, or the test that failed. In addition we support an initial delay before paging (useful to cut down on late night false alarms), page-only-every defined amount of time, paging groups, acknowledgement and escalation. Built in support for e-mail paging, SNMP traps, alphanumeric paging via Qpage or Sendpage, or numeric and SMS pages via Kermit for the BB Unix/Linux server platform while the Windows server platform supports e-mail and SMS, and SNMP traps. Under the Unix/Linux server platform, you can even create your own custom notification procedure.

## History & Reporting

Big Brother supports trending and reporting, which will allow you to determine whether Service Level Agreements are being met. In addition, we provide access to historical status information so you can see what the problem was at any given time.

## Plug-ins & Extensions

Big Brother supports plug-ins/extensions/customizations. You can write plug-ins in any language, and we include several samples to make it easy. In addition, Brothers from around the world have written thousands of plug-ins to monitor everything from Databases to CPU temperature on machines. You can see the current list at http://www.bb4.com/community.

## Flexibility

Big Brother is very flexible. Warning and alarm levels are all easily definable. The Web display can be easily customized. We have hooks into other products, like LARRD and MRTG for performance and data monitoring and reporting.

## Community

One of the best things about Big Brother is the community that has sprung up around it. 1000's of Brothers on the various mailing lists provide quick and friendly support and commentary. We host over 1000+ scripts in 45+ categories at: http://www.bb4.com/community

# Detailed Technical Architecture

Big Brother is a simple system and network monitor which produces a web page containing a matrix of test results. These test results are shown as red, green, yellow, purple, clear, or blue dots.

A link to a live demo is located at http://www.bb4.com

### 1. Components

Big Brother uses a client/server model, and is comprised of the following parts:

**BBDISPLAY**: The Display Server which processes the status information and creates the BB web pages. Note that a web server such as Apache is needed to view these pages.
**BBPAGER**: The Paging Server which processes alerts and dispatches them to the correct people. Pages can be sent out by e-mail, SMS, SNMP-traps, or alpha/numeric pages.

**BBNET**: The Network Monitor testing routine. Most common network protocols are supported http, ftp, pop3, etc…

**LSM**: Local system monitors (bbclients) which collect local system information and send it to the BBDISPLAY and/or BBPAGER for display and notification, if necessary.

## 2. Communications: TCP/1984 (Configurable port).

BB communicates from client to server over TCP port 1984, which is registered with the IANA. The server accepts incoming client connections, uses them if valid, drops them if not, does not identify itself on connection, or send an ACK of any sort to discourage hackers.

Design: Clients send their local system information to the BB servers (BBDISPLAY and BBPAGER) every 5 minutes (configurable). Redundancy is achieved by having BB clients send status messages to multiple BBDISPLAYs and BBPAGERs with failover configuration.

The BBDISPLAYs themselves can be 'stacked' in such a way that the output from multiple BBDISPLAYs can be fed to a central BBDISPLAY allowing you cover an entire country, for example.

BBNET tests all defined services for all monitored hosts every 5 minutes as well and sends the results to the BB servers. Note that by default BBNET is usually the same machine as the BBDISPLAY.

## 3. Protocol:

BB messages are simple, sent as text, and can be sent to the BBDISPLAY and BBPAGER using the 'bb' command. The format is:

bb 123.123.123.123 "type color machine.test data"

123.123.123.123: IP address of server

| | |
|---|---|
| type: | type of message – status, page, etc |
| machine.test: | machine name, and test column |
| data: | usually the date, plus any output of the test |

Sample:
bb 123.123.213.123 "status red bobo.disk 12:00 pm disk full"

In addition, each message is time stamped with an expiration date 30 minutes into the future; this allows BB to tell if the information on the display is valid; if the current time is later than the expiration date, the status color is changed to purple and this generates an alert.

The format for the time stamp is type+NNN, where NNN is the number of minutes the message is valid. For example, status+1440 would generate a status message valid for 1440 minutes (one day).

## 4. Sizing and Configuration:

We recommend having at most 500 BB clients reporting into a BB server.

In general, BB is quite light and most recent OSs should have no trouble supporting BB out of the box.

Big Brother uses the bb-hosts file to store device configuration, modify the display and define network tests. The bb-hosts file should be the same on all systems.

## 5. Complex network support:

Big Brother can handle segmented and firewalled networks using the BBRELAY directive, which allows you to route BB messages via one internal BBDISPLAY to another, external BBDISPLAY.

In addition Big Brother supports point-to-point encryption through the use of shared keys if required.

## 6. Customization and custom tests

Possibly the greatest strength of Big Brother is its ability to support custom tests in a quick and simple way. These tests can be written in any language.

If you can determine a status of red, yellow, or green, then it can be a BB test. In fact, tests you already have running can probably be easily modified by simply adding the bb command as described above to the end of your scripts.

The BB display automatically shows new tests when they arrive.

The Big Brother community site hosts 1000+ scripts, extensions, plug-ins and documentation to enhance and expand the monitor capabilities of Big Brother. The community site is located at: http://www.bb4.com/community, or, http://www.deadcat.net

# Installation and Deployment of Big Brother

This part of the Big Brother Best Practices Guide explains the tasks that are required to install a fully functional Big Brother Management server and monitored clients.

You can install Big Brother in different configurations, depending on your business and technical needs, resources and constraints. Your satisfaction with this product depends on your understanding of basic concepts.

The Big Brother server installation is directed by a configuration script (UNIX), or an installation wizard (Windows), both of which will guide you through the install processes and help you accomplish common tasks. You complete preliminary software installation and define setup options at this time. You then finish the installation process by manually configuring monitored devices, network tests and alert level notifications.

# Big Brother Server

# UNIX

Begin the BBServer installation process on UNIX by untaring the appropriate tar file in the Big Brother operating system user's home directory. This will create the directory structure for the Big Brother server software.

The install script bbconfig exists in the bb3.20-bbpe/install directory and must be executed by the root user. The install script displays the software license agreement, which you must accept, then asks several questions about the system, software owner, BBDISPLAY and BBPAGER servers, default email address, the location of the DocumentRoot and cgi-bin web server directories and the web server owner and group. When the install script finishes the Big Brother Server is started and connectivity and http tests can be viewed in short time with a

browser pointed to http://localhost/bb. You are now ready to configure devices and network tests and install Big Brother clients.

## Windows

Initiate the BBServer installation process on Windows by double clicking on the bbntdpe-320.exe installer. An installshield wizard pop's up to guide you through; click next to start, you must accept the license agreement, enter customer information, select a destination folder for the server software and database directory then click Install to begin. The installshield wizard stops and you must click Finish to complete the installation. A command prompt launches displaying information on how to obtain your permanent Big Brother license. The Big Brother Professional Edition Server service should be running; connectivity and http tests for the localhost should be visible on the main display from a browser pointed to http://localhost/bb. You must stop the Big Brother Server service and configure the bb-hosts.cfg file before adding Big Brother clients.

# Big Brother Client

## UNIX

Begin the BBClient installation process on UNIX by untaring the appropriate tar file in the Big Brother operating system user's home directory. This will create the directory structure for the Big Brother client software.

The install script bbconfig exists in the bbc3.20-bbpe/install directory and must be executed by the root user. The install script displays the software license agreement, which you must accept, then asks several questions about the system, software owner, BBDISPLAY and BBPAGER servers. When the install script finishes follow the instructions for starting the BBClient software.

## Windows

Initiate the BBClient installation process on Windows by double clicking on the bbntpe-320.exe installer. An installshield wizard pop's up to guide you through; click next to start, you must accept the license agreement, enter customer information, select a destination folder for the

client software, click Next, then click Install to begin. The installshield wizard stops and you must click Finish to complete the installation. The Big Brother Client Configuration Editor pops up after installation. The DISPLAY and PAGER host input fields must be populated with a valid IP address, or, fully qualified domain name of the BBServer and the loopback data should be deleted. Save the configuration and click the Start button to start the Big Brother Professional Edition Client service.

# Server Configuration

There are three primary modules of the Big Brother server, BBDISPLAY which controls the look and feel of the main display, BBNET which performs all network tests and BBPAGER which is responsible for all notifications. These three modules are controlled by three configuration files – bb-hosts, bbwarnsetup and bbwarnrules.

The bb-hosts file is used to add monitored devices and network test for those devices and to control the look of the Big Brother main page. The bbwarnsetup.cfg file controls the behavior of the notification mechanism and bbwarnrules.cfg is where you configure the rules under which to notify.

# The bb-hosts Configuration File

When you first open the bb-hosts file, it will contain the following:

# upon install, your Big Brother server is assigned
# a basic configuration. Modify with the proper BBNTD server address and hostname
# then start adding the other client servers you want to test.
#
#127.0.0.1 somehost.quest.com # testip BBPAGER BBNET BBDISPLAY
http://somehost.quest.com/bb/

The format for the host definition lines is:

- <IP-ADDR> <HOSTNAME> # <DIRECTIVES>

The following sections discuss the parts of the host definition and directives.

- IP Address and Hostname

The first entry on the line is the IP address of the host. To get started, change the 127.0.0.1 on the first line to the address of the server on which Big Brother is installed. The second part of the line is the hostname. Enter the fully-qualified domain name for the server where Big Brother is installed, such as mymachine.quest.com instead of simply mymachine.
Stop and start Big Brother after making these changes to your bb-hosts file. You may have to wait up to five minutes for your changes to effect the Big Brother display.

- Directives

Everything after the # sign is a directive (a space should always follow it). For computers with the Big Brother server software installed, directives determine what roles this host fills for Big Brother— BBDISPLAY, BBPAGER, and/or BBNET.
For all hosts, they determine what network tests are performed on the host. In the above example, the directives indicate that the host with this IP is the Big Brother web server (directive BBDISPLAY), the notification server (directive BBPAGER), and runs the IP network services (directive BBNET). It will test IP connectivity regardless of the hostname but using the IP address (directive testip) and check the web page http://somehost.quest.com/bb/.
Many other directives are possible; refer to the Big Brother online help for more information.

# The bbwarnsetup.cfg Configuration File

Big Brother sends a notification request to the BBPAGER server if a test reaches a certain threshold or reports a problem (usually on a red condition). This request is sent to the BBPAGER server as a "page" message. The BBPAGER server processes the request and determines if a notification needs to be sent out. If so, it can notify via e-mail, numeric page (beeper), SMS message (this requires a third-party application such as sms_client or qpage), or SNMP-trap.

**Note**. Big Brother loads the contents of bbwarnsetup.cfg every time a notification request is received by the BBPAGER server. As you make the changes to the configuration, you do not need to stop and restart the BBPAGER server for them to take effect.

Before you create rules to specify who to call and when for which problems, you must first configure the etc/bbwarnsetup.cfg file. This file contains the overall settings and configures the behavior of the notification feature. Detailed explanations of each configuration parameter and the available options are documented in the help files and the bbwarnsetup.cfg file itself.

big brother
SOFTWARE

# The bbwarnrules.cfg Configuration File

Defining notification recipients; once you have configured bbwarnsetup.cfg, you can create notification rules in bbwarnrules.cfg.
Tip. We suggest you get basic e-mail notification working (replace the e-mail recipient in the rule towards the bottom of the bbwarnrules.cfg file) before you try more advanced options.

Rules are written in the following format:

```
hosts;exhosts;services;exservices;color;day;time;recipients
```

Field descriptions are listed in the on line help documentation.

**Note**. The default field delimiter is the semi-colon ( ; ), as shown. You can change this using the cfgdelim setting in bbwarnsetup.cfg. Even though egrep regular expressions are allowed, do not use the .* construct, just use *. It will be replaced with .* in the regexp.

You can use a special hostname, unmatched-, to create a rule for any hosts which are not listed in the server's bb-hosts file:

```
unmatched-*;;*;;*;*;*;bbadmin@localhost.com
```

Here is a more complex sample rule:

```
*;win34 unix12;*;cpu disk;*;0 5 6;*;backupadmin@quest.com 555-9999
```

This rule send notifications for all hosts except win34 and unix12, and all tests except the cpu and disk tests, on Sunday, Friday, and Saturday only, via e-mail to backupadmin@quest.com and to a pager with the number 555-9999.

There's also a special format of the rule line:

```
!hosts;exhosts;services;exservices;colors:day;time;recipients
```

If a rule line starts with !, the event that matches the rule line will disable notification to any recipient defined on that rule line. If the recipients field is * then no notification will occur for that event. Here's an example:

```
!*;;*;;*;*;*;*
```

This will in effect disable all notifications and render useless any other rule that you have defined. Here's another example:

## Escalation

To escalate a notification, use the following format for the recipient:

```
recipient:^XX[-YY]
```

- XX is the initial wait before sending the notification
- YY is the delay for each subsequent call. If it is not specified then the pagedelay value from bbwarnsetup.cfg is used.

An escalation can only be acknowledged by the recipient, not by someone else using a global acknowledgement.

## Initial delay

You can override the page delay default (from bbwarnsetup.cfg) for any recipient. The format is:

```
recipient:~XX[-YY]
```

- XX is the initial delay before sending the notification
- YY is the delay for each subsequent call. If it is not specified then the pagedelay value from bbwarnsetup.cfg is used.
-

An initial delay can be reset if a recipient acknowledges a notification for all recipients of that notification.

### Manual Page Recipient

If you want to use Big Brother's manual paging feature, you must define the recipient for the manual notification. You do this by creating a recipient definition for the host notify-admin, like this:

```
notify-admin;;pagehelp;;*;*;bbadmin@localhost
```

The line must start with notify-admin and must include pagehelp as the service. You can include one or more recipients who will receive manual pages sent from the display Web page.

## User defined tests (custom tests)

You can create your own external script to perform a test and report status to the Big Brother BBDISPLAY server. In general, these tests are run by the client software, which then sends the results to the BBDISPLAY and BBPAGER servers.

There is one change you must make on the server to enable notification for an external test. You must define a numeric code for the test name in the svcerrlist variable in etc/bbwarnsetup.cfg. For example, if your test name is ORA, you could update svcerrlist to include ORA:150. By default, this will cause a notification whenever the status color is red.

Note. There are many community-produced scripts at www.bb4.com/community. In most cases these scripts contain a readme file that tells you how to install and configure them. These scripts are not supported by Quest Software.

## Custom tests on UNIX

External scripts run on either the Big Brother server or client and send information back to the server. To be usable by Big Brother, a script must have two characteristics:

It must be executable by the Big Brother user and it must send a status message to the Big Brother server in the proper format.

To add your own tests, first create the script itself. It may be easiest to start with the template available in the ext/ext-proto file and add your code. When writing the script, remember:

All temporary files should be created in $BBTMP and removed after use.

The script does not have to send notification requests (page messages) to the BBPAGER server. The bb command will create these automatically when the status color in the status message is found in the PAGELEVELS token in etc/bbwarnsetup.cfg.

Once the script is complete, we recommend you place it in $BBHOME/ext and test it before adding it to Big Brother. To test the script:

```
cd /home/bb
BBHOME=/home/bb
export BBHOME
. ./etc/bbdef.sh
cd ext
./yourexternaltest
```

Look for errors, fix them, and rerun your test until you are satisfied.

To have Big Brother run the script, you need to add it to the etc/bb-bbexttab file. This file defines all scripts to run for each host. Copy the etc/bb-bbexttab.DIST file to etc/bb-bbexttab and make your changes. The format of each line is:

```
host : options : scripts
```

Host is the name of the host where the scripts will run. You must copy bb-bbexttab to each host where you want to run external scripts.

Options is not yet implemented; be sure to enter two colons (: :) after the host and before the script names.

Scripts are the scripts to run on this host, separated by spaces. Each script must exist in the $BBHOME/ext directory on the host.

Tip. Since the script names are separated by spaces, there cannot be any spaces in the command you use to start the script. If you need to include arguments for this script, have Big Brother run a script without arguments which in turn runs the script with arguments.

You can set the frequency of any script by specifying the interval it should run at, in seconds, after the script name, separated by a semi-colon (;).

Here are two sample etc/bb-bbexttab entries:

www.bobo.com : : script1 script2;3600 script3;900 script4
www.baba.com : : script2 script5

On www.bobo.com, script1 and script4 will run every five minutes (the default), while script2 and script3 will run every 60 and 15 minutes respectively. On www.baba.com, script2 and script5 will run every five minutes. Both bb-bbexttab and the appropriate scripts must exist on www.bobo.com and www.baba.com.

After updating bb-bbexttab, you must restart Big Brother to start running the scripts.

Finally, you must add the test name and a numeric code for it in the svcerrlist token in the etc/bbwarnsetup.cfg file on the BBPAGER host. If you do not, any notifications for the external script will show the code 999.

# Custom tests on Windows

Using external scripts requires setup on both the client where the script is run and the Big Brother server(s) the client reports the results to.

## On the Client

You need to:

Create an external script which, when run, creates a file containing a properly formatted Big Brother status message in the designated directory.

Use the Configuration Editor to set the directory where the Big Brother client will look for the status message files to send to the server.

Use the Configuration Editor to tell the client what external scripts to run, and how often to run each one.

Note. Besides having the client send the results of external scripts to the server, you can use the bb.exe program to send messages directly to the BBDISPLAY and BBPAGER servers.

## On the Server

You must assign an error ID number to the external script by adding a column name:ID entry to the svcerrlist token in the bbwarnsetup.cfg file. The column name is determined by the name of the file containing the status message sent to the server. See the server help file for information about changing the svcerrlist token.

## Creating External Scripts

An external script can be any type of executable file, such as a Perl script or a .exe file. To be usable by the Big Brother client, it must create a status log file in the directory named in the Saved Logs Location field of the Configuration Editor. The file must be named and have its contents formatted as described below.

The name of the file containing the status log for the external script determines the column name used for the results on the Big Brother display, so give the file a name you want to see on the display. The file must not have an extension; the client only sends files without an extension to the server. This means you have two ways to make sure the file isn't sent prematurely (after it's created but before the contents are complete): either create the file with an extension, then rename it after you've written the contents, or create it in a different directory, then move it to the Saved Logs Location when it is ready.

After the client sends the file to the server, it deletes it. If you do not want this to happen, start the file name with a dash (-). This can be useful if you do not want the external script to return a purple status if it isn't performed; since the file remains in the directory, there is always a status to send to the server, even if the test has not executed again.

The file must be a plain text file. It should contain only the results of the test.

The first line must begin with the status color for the test (generally green, yellow, or red). The rest of the file may contain anything; you will see the contents of the file if you click the colored dot on the Big Brother display.  Generally, we suggest you include the date, time, and host name on the first line, with subsequent lines describing the test results, like this:

color Day date [hostname]
results message
results message
...

For example:

red Thu 08 21:10:24 1998 [xxx.domain.com]
blah blah
blah blah

We strongly recommend you include the hostname on the first line, especially if the client computer uses DHCP.

You can change the amount of time before the test results expire (and the test status shows purple), overriding the default value on the display server(s). Place a plus sign (+) and the amount of time before expiration immediately after the color in the log file. You can express the time in minutes (m), hours (h), or days (d). For example, to have this test not turn purple for 26 hours:

green+26h Thu 08 21:10:24 1998 [xxx.domain.com]
blah blah
blah blah

Changing the expiration time can be useful for scripts you execute only once a day: backup checks, daily system checks, and so on.

Also, you can send the status for a test performed on a different host by including the host name before the color, separated by a colon (:). This is useful if you are running tests for multiple hosts from the same Big Brother client. For example:

some.host.anywhere:red Thu 08 21:10:24 1998 [xxx.domain.com]
blah blah
blah blah

This tells the server that this status is for some.host.anywhere, not for the current client host.

Note. There are 1000+ community-produced plug-ins/scripts available on www.deadcat.net. In most cases, these scripts contain a readme file that tells you how to install and configure them. These scripts are not supported by Quest Software.