Abstract: Describes the Big Brother System and Network Monitor installation and maintenance process.

<table>
<thead>
<tr>
<th>Abstract:</th>
<th>Describes the Big Brother System and Network Monitor installation and maintenance process.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue:</td>
<td>01</td>
</tr>
<tr>
<td>Date:</td>
<td>07/12/2002</td>
</tr>
</tbody>
</table>
## Document History

<table>
<thead>
<tr>
<th>Issue</th>
<th>Author(s)</th>
<th>Date</th>
<th>Description Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N. Metrowsky</td>
<td>07/12/2002</td>
<td>Document Creation. This document describes the implementation of Big Brother at the Wisconsin Department of Natural Resources. This is a step by step guide which provided the reader the methodology to implement Big Brother at their site.</td>
</tr>
</tbody>
</table>
# Table of Contents

**Big Brother System and Network Monitor** ................................................................. 5
  - Introduction........................................................................................................... 5
  - Obtaining Big Brother ....................................................................................... 5
  - Installation ........................................................................................................ 6
  - Initial Customization .......................................................................................... 11
  - Local Customization and Enhancement .............................................................. 12
  - Local Customization – Detailed Information .................................................... 14
  - Local Customization Extensions – Detailed Information ................................... 17
  - Installation of Extensions .................................................................................. 18
  - More Customization Tasks ............................................................................... 19
  - bb-central Notes ............................................................................................... 21
  - Running Big Brother Extensions ...................................................................... 22
  - Conclusion ........................................................................................................ 22
  - Scripts ............................................................................................................... 23

**Multi Router Traffic Generator Integration with Big Brother** .......................... 25
  - Introduction ...................................................................................................... 25
  - Installing MRTG Prerequisite Software ........................................................... 25
    - Installing libpng ............................................................................................. 25
    - Installing jpeg ............................................................................................... 26
    - Installing gd .................................................................................................. 26
    - Installing MRTG ........................................................................................... 27
  - Making Effective Use of MRTG ........................................................................ 27
  - MRTG, Big Brother and You ............................................................................ 28
  - Integration With Big Brother .......................................................................... 30
  - Conclusion ....................................................................................................... 30

**Setting up the Apache Web Server for Big Brother** ........................................... 31
  - Introduction ...................................................................................................... 31
  - Obtaining Apache ............................................................................................ 31
  - Installing Apache on Tru64 Unix ...................................................................... 31
    - Unpack the Apache Distribution Kit ............................................................... 32
    - Configure the Apache kit ............................................................................. 32
    - Build and install Apache ................................................................................ 32
  - Configuring the Apache Web Server ................................................................ 33
  - Starting Apache for the first time .................................................................... 36
  - Shutting down the webserver ......................................................................... 38
  - Automatic Startup or Shutdown of Apache ...................................................... 38

**Big Brother Implementation Plan** ........................................................................ 40
  - Introduction ...................................................................................................... 40
  - Implementation ............................................................................................... 40
  - Installing Supporting Libraries for MRTG ....................................................... 41
  - Installing Big Brother and MRTG ................................................................... 42
  - Starting and Viewing Big Brother ................................................................... 44

**Big Brother Maintenance** .................................................................................... 45
  - Introduction ...................................................................................................... 45
  - Setting Up New UNIX Servers for Big Brother .............................................. 45
  - Removing a Host from Big Brother Monitoring .............................................. 47
  - Removing a Service from Big Brother Monitoring ........................................ 48
  - Other Big Brother Items .................................................................................. 48
    - Notifications ................................................................................................. 48
    - Documentation .............................................................................................. 48
    - Updates and Patches ..................................................................................... 48
Big Brother System and Network Monitor

Introduction

This chapter addresses the installation, configuration and customization of the Big Brother System and Network Monitor (Big Brother). Big Brother is a tool developed to monitor resources on hosts and network protocols associated with those hosts. It was originally released in 1996 and has been faithfully maintained ever since. While there are various commercial products that provide the functionality of Big Brother and then some, the idea of Big Brother lies within its' simplicity. This, and the fact that Big Brother operates on the "look, but do not touch philosophy".

The authors of Big Brother developed software that can run virtually unchanged on any UNIX or linux platform. The heart of Big Brother is written in C and all the supporting scripts are written in the Bourne shell (/bin/sh). The authors have also developed a client that supports the Windows NT/2000/XP environment. The simplicity, however, has spawned a large following on the Internet. Those who chose to run Big Brother in their enterprise, have helped to make improvements to the base Big Brother software, this, in turn, has spawned over 100 customizations or extensions, which are readily available to Internet community at large.

In the case of the Wisconsin Department of Natural Resources (WDNR), the Big Brother environment consists of the Big Brother software and several customizations and extensions. The customizations and extensions provide WDNR with additional information, which is not available in the distributed Big Brother software.

Obtaining Big Brother

Big Brother is available from [http://bb4.com](http://bb4.com). It is from this site that one can find out a great deal of information about Big Brother, documentation, download the software and view a running Big Brother environment.

Before going on, Big Brother has an open license, at present, as long as the software is just used to monitor an entities' enterprise. If for some reason, Big Brother is being used to monitor external, revenue generating hosts and services, it is bundled with a “turn key” solution and the solution is sold from a vendor to a customer, or it is part of a vendor’s software distribution kit sold to a customer, then there is a cost for the software. Recently, Big Brother was purchased by Quest Software, which plans to continue to provide the Internet community with the Big Brother we know today. Quest Software, will also be providing a feature filled commercial version, as well. According to the authors, and Quest Software, there are no plans to limit, stop developing or discontinue the existing Big Brother software and how it is licensed.

With that said, it is time to download Big Brother. Go to the Big Brother Web Site mentioned above, and click on Download; the download screen will appear. At
this point enter the required information, agree to the licensing terms and
download the software.
You will notice, that besides the Big Brother source code, this page directs you to
various user written clients, user contributed software and the commercial
software available from Quest Software. You may want to explore these areas to
see what is available.

Installation

Upon downloading the Big Brother source kit, you should find the following file:

```
bb-1.9c.tar.gz
```

We will now go through the process of installing the Big Brother software.

Before doing anything more, make sure that a running web server is available on
the UNIX host which Big Brother is going to run on. This will require the
installation of Apache, please refer to the Apache Web Server chapter, to learn
more about installing Apache.

**WDNR NOTE:** There is an Apache Web Server running on
randgpin00.dnr.state.wi.us. Once, WDNR gets comfortable to Big Brother, then it
is probable that the Apache Web Server and Big Brother will reside on
devlgpin00.dnr.state.wi.us. Therefore, any reference to the location of the
aforementioned software will imply the presumed final location of the software.

**NOTICE:** The Apache Web Server chapter is a basic chapter for setting up
Apache. As with all web server software, security considerations should always
be taken into account. By no means should a web server run under the root
account. Also, you may want to set up password access to the Big Brother web
areas. You will notice, that the Apache Web Server is running under the WWW
user id and httpd UNIX Account group, for security purposes.

**SECURITY NOTE:** Big Brother should not run as root, for security reasons.
Though, there may be no harm in doing so, it is possible that a error in the Big
Brother code could lead to a Denial of Service issue. Keep this in mind, as we
begin the Big Brother installation.

First, create a user id, on the target UNIX system, you wish to install Big Brother.
For WNDR, the user name chosen was BBMON; the initial directory should be
/home/bbmon. The BBMON account should be placed in the same UNIX
Account Group (gid) as the web server, for WDNR purposes the group is httpd.
In addition, so Big Brother can read the system message files, the BBMON user
id needs to be added to the adm UNIX Account Group. By doing this, Big Brother
has access to what it needs, without the need of root privileges.

To allow full web server access (read and update) to the Big Brother files, edit
the .profile file in the bbmon directory and add:

```
umask 002
```
Now, copy the Big Brother distribution kit to the bbmon directory.

At this point, you will need to perform the following steps:

```
$ gzip -d bb-1.9c.tar.gz
$ tar -xf bb-1.9c.tar
```

You, should now see the following in the bbmon directory:

- README.FIRST  Information file about the kit
- bb19a.tar  The Big Brother Software
- bbvar  The Big Brother Data Area

At this point, you want to extract the Big Brother software:

```
$ tar -xf bb19c.tar
```

You now should see a new directory called bb19c. For ease of configuration, upgrading, etc., it would be useful to create the following soft link:

```
$ ln -s bb19c bb
```

Even though the following is not required, it is convenient to also create the following links:

```
$ cd bb19a
$ ln -s ../bbvar/disabled
$ cd www
$ rm -r acks data html rep notes
$ mkdir ..../bbvar/acks ..../bbvar/data ..../bbvar/rep
$ mkdir ..../bbvar/notes ..../bbvar/errors
$ mkdir ..../bbvar/statrrd ..../bbvar/statrrd/rrd
$ mkdir ..../bbvar/statrrd/graphs
$ ln -s ..../bbvar/acks
$ ln -s ..../bbvar/data
$ ln -s ..../bbvar/errors
$ ln -s ..../bbvar/hist
$ ln -s ..../bbvar/histlogs
$ ln -s ..../bbvar/html
$ ln -s ..../bbvar/logs
$ ln -s ..../bbvar/notes
$ ln -s ..../bbvar/rep
$ ln -s ..../bbvar/statrrd
```

**NOTICE:** The statrrd directories and softlink are an extension to Big Brother. The statrrd extension creates graphs for CPU Load Average, Swap Space Usage and Disk Space Usage. It will be addressed late in this document.

With the basic preparations made, it is now time to configure and build the Big Brother software. You now want to go to the Big Brother Installation Directory and begin the configuration process. The installation requires you to be root.

```
$ su -
$ cd /home/bbmon/bb/install
```
$ ./bbconfig

THE BIG BROTHER SYSTEM AND NETWORK MONITOR
============================================

This program is Copyright (c) 1997-2002
BB4 Technologies Inc.
All Rights Reserved

The Big Brother System and Network Monitor
is not free software. The terms and conditions
under which you may use the Big Brother System
and Network Monitor at no charge is detailed
in our license below. If you need a commercial license, you
can get one online from http://bb4.com/

We've put thousands of hours into our software, please
take 30 seconds to read our license, it's not long, or
complicated, but it is important,

Thanks.

====================================
License Agreement & Lack of Warranty
====================================

By installing, copying or otherwise using this software
product, you agree to abide by the following terms and
conditions:

1. NON-COMMERCIAL USE

   No part of the Big Brother System and Network Monitor
   may be used for any commercial purpose after a 30
day evaluation period without obtaining a commercial
license from BB4 Technologies Inc. Commercial purpose
includes any activity engaged for the purpose of directly
generating revenues including the sale of the product,
use of the product to provide a service or in support
of a service for which you charge.

2. TRADEMARKS AND NOTICES

   The software, graphics and documentation which
make up the Big Brother System and Network
Monitor are Copyright (c) 1997-2002
BB4 Technologies Inc. "Big Brother System
and Network Monitor" is a trademark of
BB4 Technologies Inc. You agree to respect
these rights and leave all notices and product
references intact.

3. REDISTRIBUTION

   This software may not be redistributed without prior
   written permission from BB4 Technologies Inc.

4. REQUIRED LINKS

   At least one link to the Big Brother System
and Network Monitor home site at http://bb4.com
must be available from the status pages
generated by the Big Brother System and
Network Monitor so that others may obtain a
copy of this software.

5. LIMITATION OF LIABILITY AND DISCLAIMER OF WARRANTY
You understand that this software is provided as-is. BB4 Technologies Inc. makes no claims towards its suitability for any purpose and accepts absolutely no liability for any damages the software may cause. Use at your own risk.

Questions? Comments?

Contact:
BB4 Technologies Inc.
E-mail: info@bb4.com
Tel: +1 (514) 996-INET
Fax: +1 (514) 996-0326

Do you agree to the terms of this license (y/n): y

Thank you, installation continuing . . .

Welcome to the Big Brother installation procedure...
The first thing we need to know is that OS you're running...

Choose one of the following: bsdi bsdi4 sco3 sco freebsd solaris hpux9 hpux linux sunos netsd osf ulxrix irix unixware unixware7 redhat aix dynix debian dgx openbsd caldera mandrake sinix suse darwin

Please enter your OS: [osfl]: osf
---> OK, we'll try osf...

*** WARNING: Don't run BB as root ! ***
Executing BB as root is not recommended

Prevent the execution of BB as user 'root' (y/n) [y]:
---> OK... BB is NOT ALLOWED to run as root

What will be the user ID of BB [bb]: BBMON

Making sure BBHOME </home/bbmon/bb19c> is writable...

---> OK, /home/bbmon/bb19c is fine...

Do you want to preserve the old style directory structure ?
You may want to do so if you use BB extensions or externals that do not understand the new directory structure. This option is *NOT* recommend as keeping the old directory around represents a security risk.

Old-style directory structure (y/n): [n]

When you set up your machines, you should use Fully Qualified Domain names, this means you use the whole name, like www.bb4.com, instead of just 'www'. This is recommended.

Use FQDN (y/n): [y]

Big Brother creates HTML pages with the status of your network. You'll need a web server to publish this information.
What machine will be the BBDISPLAY [prodsmin01.dnr.state.wi.us]:

Big Brother sends important messages to a pager server. This machine will at a minimum to be able to send mail.

What machine will be the BBPAGER [prodsmin01.dnr.state.wi.us]:

Some questions regarding the current host (prodsmin01.dnr.state.wi.us) will be asked.

Is this host a BBDISPLAY host (y/n): [y]

Is this host a BBPAGER host (y/n): [y]

Enter the default recipient: [root@localhost] root@prodsmin01.dnr.state.wi.us

Since Big Brother produces results to be displayed on web pages, we need to know where to view these results.

Enter the base URL for BB [/bb]:

--- OK... Big Brother will live under http://devlgpin00.dnr.state.wi.us/bb

Big Brother also uses CGI scripts to create dynamic output. What directory do these scripts live in?

Enter CGI directory [/home/www/httpd/cgi-bin]: /usr/local/apache/cgi-bin

--- OK... CGI scripts will live at /usr/local/apache/cgi-bin

Enter the base URL of the CGI scripts [/cgi-bin]:

---------------------------------------------

-- UPDATING Makefile
-- UPDATING runbb.sh
-- UPDATING bbsys.local
-- CHECKING COMMAND PATHNAMES
*** Verifying pathnames to necessary commands...
DIG is unavailable, the directive "dig" cannot be used in bb-hosts

You are missing these commands:
DIG
*** Done.
-- UPDATING bbdef.sh
-- UPDATING URL location
-- INSTALLING CGI scripts

BB needs to set the group name of the www/rep directory to the group name of the web server by using its user name

Enter web server user id [nobody]: www

You may override the group name determined by the previous step.

Enter group name [httpd]:

-- SETTING WRITE PERMISSION FOR OWNER AND GROUP FOR www/rep
-- CHANGING THE GROUP ID OF www/rep
-- UPDATING pager scripts

---------------------------------------------

-- Done. Now do
  cd ..../src
  make
  make install
  cd ..../
  chown -R bbmon bbvar bb<ver>
where bb<ver> is the new version's directory name

su - bbmon
to continue installation using that user ID

You are now ready to build Big Brother. However, if you want the capability of deactivating Big Brother monitoring of a host or service, you need to make a modification to src/Makefile, before executing the commands you see above. With an editor, connect to the src directory and make the following change:

```bash
cd /home/bbmon/bb/src
vi Makefile
```

Change: CFLAGS=-DZOMBIE -DOSF -DREGEXEC -O
To: CFLAGS=-DZOMBIE -DOSF -DENABLE_DISABLE -DREGEXEC -O

After you make the change, then execute the commands noted above. In order that the softlinks are under correct ownership, issue the following commands:

```bash
cd /home/bbmon
chown -h BBMON:httpd *
```

At this point, Big Brother has now been successfully installed.

**Initial Customization**

As mentioned earlier, Big Brother is very simple in structure and concept. Mainly, a set of Bourne shell scripts and several C based executables. This simplicity allows the user to customize Big Brother to a specific sites needs, wants and desires. Because you have the source code, you can add, change or remove anything you want. In this way, Big Brother is immensely powerful. It is also why there is such a large library of user written extensions and enhancements to Big Brother; power in simplicity.

Once Big Brother is installed, it is a matter of making a few changes to various configuration files. Big Brother comes with excellent documentation, which can be read locally or from [http://bb4.com](http://bb4.com). It is a very good idea to read through the documentation and familiarize yourself with Big Brother. Because of the extent of the documentation, it is beyond the scope of this document to replicate this information here.

Initially, you want to do the following:

1. Add hosts and services to be monitored in `/home/bbmon/etc/bb-hosts`
2. Place the subnets that allowed access to the Big Brother daemon in `/home/bbmon/etc/security`. Big Brother runs on tcp port 1984, this change will allow only hosts within particular networks to connect to the Big Brother daemon running on the Big Brother Monitor Server.
3. Set thresholds for alerts by customizing the following configuration files in `/home/bbmon/etc:bbcputab, bbproctab, bbmsgstab, and bbdftab.`
4. Modify `/home/bbmon/etc/bbwarnrules.cfg` to set up who will receive alerts. By default Big Brother uses e-mail to send alerts. It is possible for Big Brother to be set up to send numeric pages, or even alpha-numeric pages. To send numeric pages, Big Brother will need at least Kermit and a modem; the alpha-numeric pages capability requires additional software.

5. Modify `/home/bbmon/etc/bbwarnsetup.cfg` to set up alert subsystem.

6. Install Big Brother clients on each host you want monitored (see `/home/bbmon/install/bbclient`).

7. Create an rc script (see last page for an example) that will start Big Brother at boot time. Until you get comfortable, you may start Big Brother as follows:

   ```
   $ /home/bbmon/bb/runbb.sh
   ```

Big Brother will now collect information. Big Brother, by default, runs on a 5 minute cycle. So after 10 minutes, you may check to see if you are getting data by typing the URL to the web server acting as the Big Brother Display Host, for example:

   ```
   http://prodsmin01.dnr.state.wi.us/bb
   ```

By now, you should have a running Big Brother Monitoring Environment, it is now time to go on to the next step; local customization and enhancement.

**Local Customization and Enhancement**

Up until this point, you were able to get a Web Server up and running and succeeded in a basic Big Brother installation. It is now time to discuss the various changes and enhancements to Big Brother that have been performed for WDNR. It may look on paper to be a great deal, but in actuality it was a matter of changing a few lines of perl code, downloading and building one software package and creating a few parameter files. Upon completion of this discussion, you will not only see how powerful Big Brother is, but also the power of the feature enhancements.

The best approach, is to go directory by directory in the Big Brother directory structure and discuss the changes or additions made within. One of the customizations, concerning setting up links from the Big Brother www directory to various directories in the Big Brother bbvar directory should have been completed earlier. If not, please do so.

In directory `bb`:

`runbb.sh` Set up BBHOME to `/home/bbmon/bb`
Turned off bb-local.sh, as it has been replaced by bb-central.
Added line to run locally written bb-check.sh
enable.ksh/disable.ksh  Scripts to start and stop Big Brother monitoring on a particular hosts. These scripts frontend the Big Brother scripts that perform this function.

bb-check.sh  Checks to see if all the Big Brother processes are running, 5 minutes after runbb.sh is executed.

In directory bb/etc:

bb-bbexttab  External Script Execution
bbdef.sh  Page and mail settings
bbsys.local  OSF Support (Big Brother creates this)
bbinc.sh  Changed font and color settings
bb-hosts  Local hosts and services to be monitored
bbwarnrules.cfg  Local Notification definitions
bbwarnsetup.cfg  Local Notification setup
security  Local subnets only

In directory bb/ext:

statrrd  BB Extension to display CPU, disk space and swap utilization using RRDTOOL.
mkbb/eventlog.sh  Increased event count from 20 to 100. Changed title bar color from "teal" to "cyan".
bb-local-ext.sh  Script to run all local extensions.
bb-central  BB Extension that eliminates the need for Big Brother clients. Using the SSH protocol, bb-central can gather information from a remote system and process the data on a central host. The only requirement, a bbmon user account with trusted ssh access to the Big Brother central host, is required.

In directory bb/install

bbsys.osf  Changed df command (-tnoautofs,nfsv3,nfs...) Ignores autofs mounted mount points

In directory bb/src:

Makefile  Set up for Digital UNIX and added the flag "-DENABLE_DISABLE" to the compile to allow the capability of stopping and starting monitoring of a host and its' services.

In directory web server’s cgi-bin:

bb-hist.sh  Converted bb-hist.sh to perl. It also displays graphs and summaries for 24 hours, 1 week, 4 weeks and 52 weeks.
bb-rep.sh  Service Availability Reporting. Replaces the distributed bb-rep.sh with a more featured perl script.
bb-servmaint.sh  Service Maintenance. This perl script will enable the user to turn monitoring on or off on a particular service.

In directory bb/web:

* _header  Increased web page refresh from 60 seconds to 300 seconds, in order to reduce system resource usage. Added bbnav4.gif (report) icon to be used to access bb-local.html. bb normally used the report icon to access the distributed bb-rep.sh.

In directory bb/www:

help/bb-local.html  Links to bb-rep and bb-servamint (see above).

**Local Customization – Detailed Information**

In this section, this chapter will now document each change noted on the previous two pages. For directories, `/home/bbmon/bb` is implied, so only the Big Brother Level Directory and file will be listed, e.g. `/etc/bbdef.sh`

```
/runbb.sh
```

Line 18: Check to make sure `BBHOME` is set to `/home/bbmon/bb`. Lines 178, 196, 209, 317: If you desire to play around with the Big Brother run time Interval, then you may change it here. Also, you will need to do so in `/etc/bbdef.sh` at line 370. The default, in all cases, is 300 seconds. These lines were left alone. Line 319: If you are going to run bb-central, comment out the lines related to bb-local.sh. Line 325: Added execution of bb-check.sh

```
/enable.ksh
```

The file is as follows:

```
#!/bin/ksh
BBHOME="/home/bbmon/bb"
export BBHOME

$BBHOME/bin/bb prodsmin01.dnr.state.wi.us "enable $1"
```

If Big Brother moves to a new host, this file needs to be changed.

```
/disable.ksh
```

The file is as follows:

```
#!/bin/ksh
BBHOME="/home/bbmon/bb"
```
export BBHOME

$BBHOME/bin/bb prodsmin01.dnr.state.wi.us "disable $1"

If Big Brother moves to a new host, this file needs to be changed.

/etc/bb-bbexttab

All lines were commented out, the only active line should be:

localhost : : bb-local-ext.sh

/etc/bbdef.sh

Much of this file is automatically generated by Big Brother and usually does not require much customization. There were some changes made and they are noted here. Also, any references to web servers and directories are noted, as well:

Line 14: Big Brother Operating System Host is set to osf: BBOSTYPE="osf"
Line 18: Big Brother User is set to BBMON: BBUSER="BBMON"
Line 27: Fully Qualified Domain Name is TRUE: FQDN="TRUE"
Line 32: Big Brother Allows as root: FALSE: STOPROOT="TRUE"
Lines 33 and Line 162 inclusive: There are various thresholds for Big Brother. NOTICE: The thresholds should be modified using the bb-params file in the bb-central extension or the various *tab files located in the /etc directory.
Line 163: Big Brother Web Page root is set to /bb: BBWEB="/bb"
Line 164: Big Brother Web Server is set to prodsmin01.dnr.state.wi.us

BBWEBHOST=http://prodsmin01.dnr.state.wi.us

NOTICE: There is no "/" after the hostname!
Line 204: Big Brother cgi-bin directory is /cgi-bin: CGIBINURL="/cgi-bin"

This should not be changed, as it ties into the system-wide web server definition of the location for the cgi-bin files.
Line 216: Receive Notification on colors set to red: PAGELEVELS="red"

The default is "red purple". E-mail will be sent on red alerts.
Line 255: Generate Big Brother Status Page on demand:

BBLOGSTATUS="DYNAMIC"

The default is to generate them all the time. This can really slow down the Big Brother server and generate a great deal of html files, changing the default STATIC to DYNAMIC is a great performance enhancement.

/etc/bbsys.local

Line 11: If autofs is desired, then change this line so it looks like:

DF="/bin/df -k -tnoautofs,nfsv3,nfs,procfs,ffm,fdfs"

/etc/bb-hosts

List of monitored hosts and services go in this file.
/etc/bbinc.sh

You may change the following lines to the desired colors, or leave as is. Currently this file has not been changed to what is shown below.

Line 59: # BBVAR=/home/bbmon/bbvar
Line 80: MKBBLOCAL="<B>WDNR Overview</B>"
Line 86: MKBBTITLE="COLOR=silver SIZE=+1 FACE="Tahoma, Arial, Helvetica"
Line 89: MKBBROWFONT="SIZE=+1 COLOR=silver FACE="Tahoma, Arial, Helvetica"
Line 92: MKBBCOLFONT="COLOR=cyan SIZE=-1"

/etc/security

The file contains the following subnets:

```
168.236.0.0
192.189.183.0
```

/etc/bbwarnrules.cfg

This file needs to be configured. All messages are now being sent to user BBMON.

/etc/bbwarnsetup.cfg

This file needs to be configured.

/install/bbsys.osf

Line 11: If autofs is desired, then change this line so it looks like:
```
DF="/bin/df -k -tnoautofs,nfsv3,nfs,procfs,ffm,fdfs"
```

/src/Makefile

As noted earlier, in the Big Brother Installation section of this document, this file was changed to support the enabling and disabling of Big Brother monitoring for a host or service.

/ext/mkbb/eventlog.sh

Line 28: Changed Number of Events to Display from 20 to 300:
```
NUMEVENTS="300"
```
Line 29: Changed time for events to be displayed from 1 day to 3 days:
```
LASTMINUTES=4320
```
Lines 72, 192 & 196: Changed color from teal to cyan.
Local Customization Extensions – Detailed Information

This section is the continuation of local customizations; however, this area involves the installation and configuration of software external to the Big Brother base installation kit. All the products, plus may others, are available for download at http://www.deadcat.net.

**NOTICE:** For all those cat fanciers out there, there must be some Aussie humor in regards to the selection of the aforementioned host name.

For WDNR, the following software kits were obtained from the Big Brother Contribution ftp Site:

- **bb-hist-2.6.tar.gz** Perl replacement for Big Brother bb-hist.sh
- **bb-rep-1.7.tar.gz** Perl replacement for Big Brother bb-rep.sh
- **bb-central-1.4.tar.gz** Perl and sh replacement for Big Brother clients; Centralized data gathering and reporting via ssh.
- **bb-swap-1.10.tar.gz** Extension to monitor swap space. Installed **bb-swap-cfg.sh** only

In addition, the following were obtained from JILA – University of Colorado:

- **bb-servmaint.sh** Perl web based interface to stop and start monitoring of services.
- **statrrd** Set of tools to generate graphs for CPU Load Average, Disk Space Usage and Swap Space Usage. Part of the bb-central-1.4 kit.
- **bb-local.html** HTML page to allow access to bb-servmaint.sh and bb-rep.sh.

**DISCLAIMER:** The author, which is also the author of this document, give full usage rights, of the above named software extensions, to the Wisconsin Department of Natural Resources to use these extensions in their enterprise. The software conforms to the licensing and distribution policy of Big Brother and shall be treated as one in the same, in regards to licensing issues. While every effort has been made to eliminate programming flaws, there may be a possibility that a problem may occur. This software is provided “as is” and no warranty is implied. The author, however, is willing to make corrections and will make those corrections available to the Big Brother community at large.

Finally, the following software was obtained to support graph generation for **statrrd**.

- **rrdtool-1.0.38** Database and graph generation tool. Information about this tool can be obtained from [www.rrdtool.org](http://www.rrdtool.org).
Installation of Extensions

Fortunately, the installation of everything mentioned is a very simple process. In all cases, it requires unpacking the kits and following the instructions included with the kit.

So here are some general notes and common mistakes:

1. In all cases, every perl script should be checked at the first line to make sure it can find the perl interpreter. For WNDR, the first line should read `#!/usr/bin/perl`. This is by far the biggest error anyone can make when installing these scripts.

2. Make sure `BBHOME` is set correctly in the scripts.

3. Make sure the web server name is set correctly in the scripts.

4. Make sure when the scripts are installed, they have an `sh` extension, the second biggest error everyone makes.

5. Make sure the permissions are set to `755` on any script installed.

6. Make sure the scripts are own by the web server user and group. For WDNR that is user name `WWW` and group `httpd`.

7. In the case of bb-central, check permissions and ownership. Also, make sure that you create the following directories, as follows:

   ```bash
   $ cd /home/bbmon/bb/etc/bb-central
   $ mkdir tmp
   $ mkdir tmp/cpu
   $ mkdir tmp/cpumode
   $ mkdir tmp/disk
   $ mkdir tmp/mem
   $ mkdir tmp/mq
   $ mkdir tmp/procs
   $ chown -R BBMON:httpd tmp
   $ chmod -R 775 tmp
   ```

   This is another common error that is made.

8. In the `bb-params` file, required for bb-central, please use `TABS` between each field. The perl code can handle multiple spaces, but you will find that `TABS` are much easier to deal with for entering parameters and for readability.

9. After downloading the rrdtool code from [www.rrdtool.org](http://www.rrdtool.org), the installation is as simple as:

   ```bash
   $ gzip -d rrdtool-1.0.38.tar.gz
   $ tar -xf rrdtool-1.0.38.tar
   $ cd rrdtool-1.0.38
   $ ./configure --prefix=/usr/local
   $ gnumake
   $ gnumake install
   ```

   In the case of WDNR, all the work has already been done for you. Please refer to the documentation provided with each kit for more information. The modules being provided are very mature and have not required any maintenance for a
while. In the case of bb-central, a couple minor bugs have been repaired and a new bb-central kit will be released to the Big Brother Contribution ftp Site; WDNR need not do anything, as the changes have already been applied to the code.

More Customization Tasks

At this time, you should have all the kits installed, and looked at the list of issues that befall someone working with perl, Big Brother and a Web Server. In this section, is discussed the software that was locally written for JILA – University of Colorado, but I found it useful for here. The software in question is: statrrd, bb-servmaint.sh and bb-local.html.

The statrrd software has already been installed and set up in the /home/bbmon/bb/ext/statrrd. The only time anyone would need to change the statrrd software, is if the Web Server changes or the location of Big Brother changes. This really is “as is” software, it works and it does the job.

The same goes for bb-servmaint.sh, the software has already been configured and installed in the Web Server cgi-directory. The only time this software would need maintenance, is changing the name of the Web Server or the location where Big Brother is installed.

I saved the more complex change for last. It is not complex, as it just requires creating one HTML file and modifying a couple lines in 8 others (One of the files, statrrd_header was already modified and would not be affected with a Big Brother upgrade). Fortunately, the change is very simple and has already been performed. I put this here, in the event that the Big Brother software is upgraded and bb-servamint.sh is no longer be accessed via the web interface and the bb-rep.sh script looks and acts “different”, you will know why.

First, you will need to create a bb-local.html in /home/bbmon/www/help/bb-local.html.

A copy looks like:

```html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">

<!-- BEGIN HEADER -->

19
```
Big Brother Local Scripts

Big Brother Availability Report

Big Brother Service Maintenance

<!-- The license agreement requires a link back to the BB main site -->
Once the file is created, make sure the permission and the mode are correct.

Now, for the following files, you are going to make the same change (they are all in the Big Brother web directory or /home/bbmon/bb/web):

- bb2_header
- bbrep_header
- histlog_header
- replog_header
- bb_header
- hist_header
- hostsvc_header

You want to change any line that looks similar to this:

```html
<META HTTP-EQUIV="REFRESH" CONTENT="60">
```

TO:

```html
<META HTTP-EQUIV="REFRESH" CONTENT="300">
```

You want to change any line that looks similar to this:

```html
ALT<A HREF="&BBWEB/help/bb-rep.html"><IMG SRC="&BBSKIN/bbnav4.gif" ="Report"
```

TO:

```html
<A HREF="&BBWEB/help/bb-local.html"><IMG SRC="&BBSKIN/bbnav4.gif" ALT="Local"
```

The first change changes the time between Big Brother displays from 1 minute to 5 minutes, it cuts down on Web server traffic. It is up to the site to determine the best setting. The second change activates the `bb-local.html` module, by clicking the Big Brother report icon in the upper left corner of the Big Brother Display.

**bb-central Notes**

In the event that WDNR wants to take advantage of bb-central, there is very little required for its’ setup. The only requirements are:

1. All monitored hosts and services need to be placed in `bb-param` file. You must group all host entries together for a particular host.
2. A BBMON user account needs to be set up on every UNIX host you plan to monitor.
3. The ssh software must be installed on every host you wish to be monitored.
4. An authorized_keys file must be installed in the BBMON account .ssh directory of each monitored host. The file must contain the public key file from the host to which bb-central will be executed from.
5. To speed up processing, it would be a good idea to have each monitored host send syslog data to the host running bb-central. In this way, bb-central only has to look at 6 message files, as opposed to (6*number of
hosts) being monitored. We found that this was a great time saver at JILA. We determined each ssh connection takes 1.5 seconds, and unfortunately, the way the message file routine works, it has to make a connection for each message file. In the end, we were able to monitor over 30 hosts, several switches, routers, etc. for about 70 components and it took about 60 seconds to accomplish this on a XP1000 EV6 500mhz processor using a 10/100 ethernet card.

6. Of course check permissions and ownership, if things are not working the way they should be.

**Running Big Brother Extensions**

Ordinarily when running an extension is required, one would place the desired extension in the Big Brother `etc/bb-bbexttab` file. For WDNR, this standard was used for running various extension software products and to gather specific information for the Big Brother Server (prodsmin01).

The local `etc/bb-bbexttab` file contains this entry:

```
localhost : : bb-central.sh bb-mrtg.sh bb-statrrd.sh
```

**Conclusion**

This chapter has presented the Big Brother software, how to install and configure Big Brother, and how to customize Big Brother. Big Brother is a very good tool for System and Network Monitoring, again its’ simplicity lets it take care of some complex tasks. You should review the Big Brother Contribution ftp Site for various additions you may desire. In the case of WDNR, if you go ahead with bb-central, you will only need one copy of Big Brother that will have to be maintained. I will always be available to answer queries about the installation, even after I leave, but hopefully this chapter will answer the many questions that may come up.
The following is an example of a Big Brother rc script that can be used:

```bash
#!/bin/ksh
#
# initbb     This shell script takes care of starting and stopping
#            big brother monitoring.
#
BBHOME=/home/bbmon/bb
BBUSER=BBMON

# See how we were called.
case "$1" in
  start)
    # Start daemons.
    echo -n "Starting big brother: "
    echo "bb"
    su - $BBUSER -c "$BBHOME/runbb.sh start > /dev/null 2>&1"
    echo "done"
  ;;
  stop)
    # Stop daemons.
    echo -n "Shutting down big brother: "
    /bin/ps waux | grep $BBUSER | grep -v grep | cut -b 10-15 | xargs kill -9
    echo "done"
  ;;
  restart)
    # Stop daemons.
    echo -n "Shutting down big brother: "
    /bin/ps waux | grep $BBUSER | grep -v grep | cut -b 10-15 | xargs kill -9
    echo "done"
    # Start daemons.
    echo -n "Starting big brother: "
    echo "bb"
    su - $BBUSER -c "$BBHOME/runbb.sh start > /dev/null 2>&1"
    echo "done"
  ;;
  *)
    echo "Usage: initbb {start|stop|restart}"
    exit 1
esac
exit 0
```

The following is a copy of `bb-check.sh`:

```bash
#!/bin/sh
# bb-check.sh
# BIG BROTHER STARTUP CHECK SCRIPT
# Nick Metrowsky
# Version 1.0
# June 6th, 2002
# (c) Copyright Quest Software, Inc. 1997-2002 All rights reserved.
#
# This script will check to make sure that bb-network.sh and bb-display.sh are
# running. There are times upon system reboot, that the aforementioned scripts
# do not start up properly. This script, which will run 15 minutes after the
# the Big Brother host reboots, will make sure that these scripts are started.
# This script is run 15 minutes after runbb.sh starts via the unix at command.
# BBHOME IS THE ROOT DIRECTORY OF BIG BROTHER!!!
# YOU MUST SET THE NEXT LINE TO WHERE BB LIVES

BBHOME="/home/bbmon/bb"
export BBHOME

if [ "$BBHOME" = "" -o ! -d "$BBHOME" ]
then
echo "BBHOME IS INVALID IN runbb.sh"
echo "Please edit runbb.sh to correct this problem!"
exit 1
fi

cd $BBHOME      # AVOID ANOTHER REDHAT BUG - CAN'T WRITE IN cwd
# IF NOT STARTED IN BBHOME
.

BBHOME/etc/bbdef.sh   # GET STANDARD INCLUDES

BBNETRUN="FALSE"
BBDISPLAYRUN="FALSE"

network_test=`$PS | $GREP -v grep | $GREP bbrun | $GREP bb-network.sh`
display_test=`$PS | $GREP -v grep | $GREP bbrun | $GREP bb-display.sh`
statrrd_test=`$PS | $GREP -v grep | $GREP bbrun | $GREP bb-statrrd.sh`

if test "$network_test" = "" then
  BBNETRUN="TRUE"
  echo "bb-network.sh not running"
fi
if test "$display_test" = "" then
  BBDISPLAYRUN="TRUE"
  echo "bb-display.sh not running"
fi
if test "$statrrd_test" = "" then
  BBSTATRRDRUN="TRUE"
  echo "bb-statrrd.sh not running"
fi

# start of bb-network block

if test "$BBNETRUN" = "TRUE" then
  BBSLEEP=600; export BBSLEEP             # NETWORK TESTING FREQUENCY
  { sleep 30; nohup $BBHOME/bin/bbrun -a $BBHOME/bin/bb-network.sh ;} >> $BBOUT
fi

# end of bb-network block

# start of bbdisplay block

if test "$BBDISPLAYRUN" = "TRUE" then
  BBSLEEP=300; export BBSLEEP             # HOW OFTEN TO UPDATE DISPLAY (IN SECONDS)
  { sleep 90; nohup $BBHOME/bin/bbrun -a $BBHOME/bin/bb-display.sh ;} >> $BBOUT
fi

# end of bb-display block

# start of statrrd block

if test "$BBSTATRRDRUN" = "TRUE" then
  BBSLEEP=300; export BBSLEEP             # HOW OFTEN TO UPDATE DATABASE (IN SECONDS)
  { sleep 90; nohup $BBHOME/bin/bbrun -a $BBHOME/ext/bb-statrrd.sh ;} >> $BBOUT
fi

# end of bb-statrrd block
Multi Router Traffic Generator Integration with Big Brother

Introduction

This chapter introduces the Multi Router Traffic Generator (MRTG) software. The purpose of this software is to monitor network traffic on network ports. The network ports can be a switch, router, or a network card in a host or printer. The MRTG software uses Simple Network Management Protocol (SNMP) to obtain the data required and the data is subsequently moved to a database for analysis. MRTG is designed to analyze the data, upon acquisition, and produce a graph based upon the data received.

In the scope of this chapter, we are going to discuss the integration of MRTG with the Big Brother System and Network Monitor (Big Brother). It is assumed that Big Brother has already been installed in the enterprise and is now functional. Please refer to the chapter Big Brother System and Network Monitor for more information. If Big Brother has not been installed, then please follow the instructions in the aforementioned chapter.

Installing MRTG Prerequisite Software

MRTG requires additional software so it can be built and compiled. Fortunately, some components, zlib and gnumake, should have already been installed on the target host, as those two software products are required. MRTG also requires the following components:

1. libpng – png image format library - Available from www.libpng.org
2. gd – Graphic Display Tool - Available from www.boutell.com/gd
3. libjpeg – jpeg image format library - Available from www.jpeg.org

Installing libpng

The following is the step by step process for building and installing libpng:

1. Using Netscape or Explorer connect to www.libpng.org
2. Download the latest version: e. g. libpng-1.2.2.tar.gz
3. Copy the libpng kit to the target UNIX host.
4. Using gzip, uncompress the kit: gzip –d libpng-1.2.2.tar.gz
5. Using tar, extract the kit: tar –xf libpng-1.2.2.tar
6. Connect to the kit directory: cd libpng-1.2.2
7. Copy the correct makefile from the scripts directory: cp scripts/makefile.dec Makefile
8. Using an editor, change the Makefile, as follows:
   Change lines 12 - 15:
   From:
   ```
   ZLIBLIB=/usr/local/lib
   ZLIBINC=/usr/local/include
   ```
To:

ZLIBLIB=/usr/local/lib
ZLIBINC=/usr/local/include

#ZLIBLIB=../zlib
#ZLIBINC=../zlib

9 Compile the kit: gnumake
10 Install the kit: gnumake install
11 Make sure all *.h files are copied to /usr/local/include: cp *.h /usr/local/include/.

Installing jpeg

The following is the step by step process for installing jpeg:

1. Using Netscape or Explorer connect to ftp://ftp.uu.net/graphics/jpeg/
2. Download the latest version: e.g. jpegsrc.v6b.tar.gz
3. Copy the jpeg kit to the target UNIX host.
4. Using gzip, uncompress the kit: gzip –d jpegsrc.v6b.tar.gz
5. Using tar, extract the kit: tar –xf jpegsrc.v6b.tar
6. Connect to the kit directory: cd jpeg-6b
7. Configure the kit: ./configure –prefix=/usr/local
8. Compile the kit: gnumake
9. Install the kit: gnumake install
10. Make sure all *.h files are copied to /usr/local/include: cp *.h /usr/local/include/.

Installing gd

The following is the step by step process for installing gd:

1. Using Netscape or Explorer connect to www.boutell.com/gd
2. Download the kit: e.g. gd-1.8.4.tar.gz Note: The latest kit does not work with MRTG.
3. Copy the gd kit to the target UNIX host.
4. Using gzip, uncompress the kit: gzip –d gd-1.8.4.tar.gz
5. Using tar, extract the kit: tar –xf gd-1.8.4.tar
6. Edit the Makefile and change Line 6 to read: COMPILER=cc
7. Compile the kit: gnumake
8. Install the kit: gnumake install

At this point, all the prerequisite software should be installed for MRTG.
**Installing MRTG**

At this point, we are ready to install the MRTG software. The following is a step by step process for building and installing MRTG:

1. Using Netscape or Explorer connect to [www.mrtg.org](http://www.mrtg.org)
2. Download the latest version: e.g. `mrtg-latest.tar.gz`
3. Copy the mrtg kit to the target UNIX host.
4. Using gzip, uncompress the kit: `gzip –d mrtg-latest.tar.gz`
5. Using tar, extract the kit: `tar –xf mrtg-latest.tar.gz`
6. Using tar again, extract the kit: `tar –xf mrtg-2.9.18.tar`
7. Connect to the kit directory: `cd mrtg-2.9.18`
8. Configure mrtg as follows:
   
   ```bash
   ./configure --prefix=/home/bbmon/mrtg-2.9.18
   --with-gd=/usr/local --with-gd-lib=/usr/local/lib --with-gd-inc=/usr/local/include
   --with-z=/usr/local --with-z-lib=/usr/local/lib --with-z-inc=/usr/local/include
   --with-png=/usr/local --with-png-lib=/usr/local/lib --with-png-inc=/usr/local/include
   ```
9. Compile the kit: `gnumake`
10. Install the kit: `gnumake install`

The MRTG software has now been installed in the same directory tree as the Big Brother software. For WDNR purposes, that would be `/home/bbmon`. The next thing to do is to connect to the `/home/bbmon` directory and create a softlink for mrtg:

```bash
# cd /home/bbmon
# ln –s mrtg-2.9.18
```

Next, make sure the files are owner by Big Brother:

```bash
# chown –R BBMON:httpd mrtg-2.9.18
# chown –h BBMON:httpd mrtg
```

At this point, MRTG is installed and ready for site configuration.

**Making Effective Use of MRTG**

As mentioned earlier, MRTG requires Simple Network Management Protocol (SNMP) to gather information about network interfaces. Before we can continue, the MRTG monitored UNIX hosts need to be setup for SNMP. You will need to modify the `/etc/snmpd.conf` file to set up to identify the host to SNMP and to set up a community name. It is a good idea to use a community name other than `public`, the default.

The following are suggested changes:

On Lines 47 – 49:

```
SysName dnrutest.dnr.state.wi.us
SysLocation WDNR Data Center 030
SysContact root@dnrutest.dnr.state.wi.us
```
In the previous example, the host is defined to the snmpd protocol and the
snmpd "password" is **wdnrnet**. The combination of the community name and
host name grants snmpd access to the information on a given host, thus using a
fully qualified domain name is a good security measure, for SNMP V2. The
SNMP V3 protocol will actually use a more stronger security method for
passwords and security.

You may now start the snmpd daemon by issuing the command:

```
# /sbin/init.d/snmpd start
```

**NOTICE:** As of the writing of this chapter, SNMP is inactive on WDNR servers.
The appropriate rc0.d, rd2.d and rc3.d entries need to be changed to activate
SNMP at boot time.

**MRTG, Big Brother and You**

At this point, everything that MRTG requires has been installed and the snmpd
daemon should now be running to accept queries from MRTG. The main purpose
of having MRTG is to integrate it with Big Brother. It would be nice to have a
single point to view Big Brother status information and network traffic. Though,
we are addressing UNIX host monitoring, it is possible to add network equipment
to Big Brother, so it can report on various items. Basically, MRTG can obtain any
item that is defined in SNMP. For the scope of this document and installation,
MRTG will be set up to track the number of incoming and outgoing bytes of
network traffic. It will also track the number of input and output errors per network
interface.

Before going on, a couple scripts were written by the author and installed with the
MRTG software, to facilitate integration with Big Brother. The tools help “clean
up” the MRTG configuration files to make them easier to read and maintain. The
provided scripts are:

- **mrtg.sh** Shell script to run MRTG data gathering
- **fix_cfg.pl** Script that cleans up the `cfgmaker` generated mrtg config file
- **error_cfg.pl** Script that takes uses the `mrtg.cfg` file to create `mrtg-error.cfg`

The process to set up a host in MRTG is as follows:

```
# cd /home/bbmon/mrtg
# ./bin/cfgmaker wdnrnet@dnrutest.dnr.state.wi.us > x.pl
# ./fix_cfg.pl
```

The output from **fix_cfg.pl** is sent to **new_mrtg.cfg**. The **fix_cfg.pl** script is
designed to eliminate a great deal of comments and other information not
required for MRTG monitoring. However, you should review the **new_mrtg.cfg**
file and make a few changes to "clean things up". The following is a sample new_mrtg.cfg file:

```
WorkDir: /home/bbmon/bb/www/notes
Refresh: 900
Interval: 15
WithPeak[\[\]]: ymwd

Target[dnrutest.dnr.state.wi.us]: 1:wdnrnet@dnrutest.dnr.state.wi.us:
MaxBytes[dnrutest.dnr.state.wi.us]: 12500000
Title[dnrutest.dnr.state.wi.us]: Traffic Analysis for 1 -- dnrutest@dnr.state.wi.us
PageTop[dnrutest.dnr.state.wi.us]: <H1>dnrutest.dnr.state.wi.us Input and Output
Counters</H1>

---

There are a few things you need to do, as follows:

1. The lines before the pound signs are only needed once in mrtg.cfg. If you are adding a second or later entry, then remove these lines.
2. Check the comments to see if they are to your liking.
3. If you do not want to interface with Big Brother, please remove the following line, before the Target Line:

```
bb*host[dnrutest.dnr.state.wi.us]: dnrutest.dnr.state.wi.us
```

Once you have inspected the new_mrtg.cfg file, then create or append to the mrtg.cfg file and create the mrtg_error.cfg file:

```
# cat new_mrtg.cfg >> mrtg.cfg
# ./error_cfg.pl
```

To test to see if MRTG works, do the following:

```
# ./mrtg.sh
```

If MRTG ran ok, you should see several files created in /home/bbmon/bbvar/notes and /home/bbmon/bbvar/errors:
You will notice several file types. The **log** is the MRTG database for the network device being monitored, the **png** files are histograms of the collected data, and the **html** file is a page containing the graphs and network device (in this case the host network interface) information.

**Integration With Big Brother**

MRTG was designed to run as its’ own standalone product; however, integrating with Big Brother combines both products into a nice cohesive unit. In other words, a single point to obtain information about monitored hosts and components, combined with reviewing network traffic for the same hosts and components.

In order for Big Brother to provide status information collected by MRTG, it requires an extension script to be installed, **bbmrtg.pl**. The **bbmrtg.pl** script can be downloaded from [ftp.deadcat.net](ftp.deadcat.net). This has already been done for WDNR purposes.

Next, review `/home/bbmon/bb/ext/bbmrtg.pl` to make sure that the script is correctly configured. For our purposes, it has already been set up for WDNR. Once the changes are made, restart Big Brother:

```
# /sbin/init.d/initbb restart
```

Big Brother will now include MRTG monitoring and data gathering in its’ normal run cycle.

**Conclusion**

This chapter has presented the Multi Router Traffic Generator (MRTG) software, how to install and configure MRTG, how to customize MRTG and how to integrate MRTG with Big Brother. The MRTG too is an excellent extension to the Big Brother System and Network Monitor, as it provides a single point for system and network monitoring. As long as the MRTG and Big Brother configurations are maintained, WDNR has a very powerful set of tools that can be used for system, network and performance monitoring.
Setting up the Apache Web Server for Big Brother

Introduction

This chapter will cover setting up the Apache Web Server on Tru64 Unix. There is significant documentation that is available covering Apache, thus this chapter will supplement the existing documentation.

The Apache Web Server is software that allows a site to serve out web pages on the Internet. Apache is a widely used web server on various UNIX and Linux environments, and it is supported in Windows environments, as well. Obtaining, installing and configuring Apache is relatively straightforward, and in the case of UNIX, the configuration files can easily be maintained with any text editor.

Obtaining Apache

Apache is available from http://www.apache.org/dist/httpd. The kit comes with the complete documentation set in HTML format. The documentation can also be viewed at http://httpd.apache.org/docs. It is a good idea to review the documentation and installation notes, before going any further. The documentation is very extensive and can be downloaded in pdf format, available in the same directory as the distribution kit; the pdf document contains 576 pages of information for the current Apache release.

Installing Apache on Tru64 Unix

Before installing the actual code, a decision needs to be made concerning the desired location for installing the software, a user account and group account for the Apache server and various configuration options. The Apache server should run from an unprivileged account, the author suggests the user name of WWW and the group httpd. The installer should choose a gid and uid that will only run the web server; a very good security procedure. This becomes especially true if there is a desire to use cgi scripts, as they can also be stored and run under the selected user name and group name. The same goes for served out web pages. Next, decide the location of the web server, it is suggested that /usr/local/apache_current_version is a good location.

Once the installer has reviewed the documentation, set up the WWW user, the httpd group and decided on an install location, then they can begin the installation process.
**Unpack the Apache Distribution Kit**

Once Apache has been downloaded, see *Obtaining Apache* above, using the following commands, please unpack the downloaded Apache kit in the desired build directory:

```
$ gzip -d httpd_2.0.39.tar.gz
$ tar -xf httpd_2.0.39.tar
```

**Configure the Apache kit**

With the Apache kit now in its' own directory, connect to the directory and configure the Apache kit, as follows:

```
$ cd httpd_2.0.39
$ ./configure --prefix=/usr/local/apache_2.0.39
Configuring for Apache, Version 2.0.39
 + using installation path layout: Apache (config.layout)
Creating Makefile
Creating Configuration.apaci in src
Creating Makefile in src
 + configured for DEC OSF/1 platform
 + setting C compiler to cc
 + setting C pre-processor to cc -E
 + checking for system header files
 + adding selected modules
 + using builtin Expat
 + checking sizeof various data types
 + doing sanity check on compiler and options
Creating Makefile in src/support
Creating Makefile in src/regex
Creating Makefile in src/os/unix
Creating Makefile in src/ap
Creating Makefile in src/main
Creating Makefile in src/lib/expat-lite
Creating Makefile in src/modules/
```

As you can see in the above example, the Apache configure script is intelligent enough to build on Tru64 Unix or any other operating system.

**Build and install Apache**

Using gnumake, issue the `gnumake` command to build and install the Apache software.

```
$ gnumake
```

Once the compile is complete, and there should not be any errors, a command prompt is returned. The following shows the Apache installation into the target directory, in this case `/usr/local/apache_2.0.39`:

```
$ gnumake install
    100 lines of messages removed
```
You now have successfully built and installed the Apache 2.0 HTTP server. To verify that Apache actually works correctly you now should first check the (initially created or preserved) configuration files

/usr/local/apache-2.0.39/conf/httpd.conf

and then you should be able to immediately fire up Apache the first time by running:

/usr/local/apache_2.0.39/bin/apachectl start

Thanks for using Apache. The Apache Group
http://www.apache.org/

You should see the previous messages, if everything went okay.

With Apache installed in the correct location, please do the following to facilitate easy access:

$ cd /usr/local
$ ln –s apache_2.0.39 apache

In the future, when a new version of Apache is installed, the configuration files can be copied from the old Apache configuration directory to the new Apache configuration directory. As you will see in Configuring the Apache Web Server, all the directory information in the configuration files are changed to generic /usr/local/apache.

Next, change the ownership to the Apache files to the user and group created earlier. In this example, the user name is WWW and group name is httpd:

$ chown –R WWW:httpd /usr/local/apache_2.0.39

Configuring the Apache Web Server

At this point, Apache is now installed on the host; however, in order for Apache to run as a webserver, several changes need to be made to the Apache configuration files. The files can be found in /usr/local/apache/conf. Before starting, it would be a good idea to review the Apache documentation, mentioned earlier, as it is very extensive in regards to setting up a webserver.

CAUTION: The following can be done just to get a basic web server up and running and to see if one can connect to the webserver. By no means is the following a true representation of how a web server should be set up.

The main configuration file is httpd.conf, this file contains several directives about location of Apache files, default web server user name, default web server group, activation of cgi files, root directory of the web server and other important configuration parameters. In the following example, the changes to httpd.conf
are reflected after the “>”. The following changes were made to /usr/local/apache/conf/httpd.conf:

The first changes seen here are to make the Apache directory generic:

```
18c18
< # /usr/local/apache_2.0.39/conf/srm.conf and then \
/usr/local/apache_2.0.39/conf/access.conf
---
> # /usr/local/apache/conf/srm.conf and then
/usr/local/apache/conf/access.conf
63c63
< ServerRoot "/usr/local/apache_2.0.39"
---
> ServerRoot "/usr/local/apache"
74c74
< #LockFile /usr/local/apache_2.0.39/logs/httpd.lock
---
> #LockFile /usr/local/apache/logs/httpd.lock
80c80
< PidFile /usr/local/apache_2.0.39/logs/httpd.pid
---
> PidFile /usr/local/apache/logs/httpd.pid
88c88
< ScoreBoardFile /usr/local/apache_2.0.39/logs/httpd.scoreboard
---
> ScoreBoardFile /usr/local/apache/logs/httpd.scoreboard
```

Normally web servers run on tcp port 80. By default, Apache is configured to run on port 8080 for testing purposes. So you do not have to provide the port number when requesting a web page on this server, change the port number to 80.

```
236c236
< Port 8080
---
> Port 80
```

By default, Apache runs with user name nobody and group name nobody. This is a known security issue, thus a locally unprivileged user name and group should be used instead. In the following, the user name used is WWW and group name used is httpd.

```
250,251c250,251
< User nobody
< Group nobody
---
> User WWW
> Group httpd
```

The following sets up an e-mail address for the webmaster.

```
258c258
< ServerAdmin metron@randgpin00.dnr.state.wi.us
---
> ServerAdmin root@randgpin00.dnr.state.wi.us
```

The following sets up the name of the webserver. It is here that you can set up an alias name for your web server, e.g. www.xyz.com for example. If you choose
an alias, make sure that it is already active in the Domain Name Service database:

```
< #ServerName randgpin00.dnr.state.wi.us
---
> ServerName randgpin00.dnr.state.wi.us
```

The following sets up the base document root for the web server. This is where your web site starts. Because Apache can follow links, you can have the index.html file on another physical disk location than the htdocs directory (another good security move): For example, at JILA we did the following:

```
$ cd /usr/local/apache/htdocs
$ ln -s /data/jila/index.html index.html
```

Also, all the files in /data/jila were owned by user name www and group name httpd.

```
< DocumentRoot "/usr/local/apache_2.0.39/htdocs"
---
> DocumentRoot "/usr/local/apache/htdocs"
```

The following are more generic directory setups:

```
< Directory "/usr/local/apache_2.0.39/htdocs"
---
> Directory "/usr/local/apache/htdocs"
```

```
< TypesConfig /usr/local/apache_2.0.39/conf/mime.types
---
> TypesConfig /usr/local/apache/conf/mime.types
```

```
< MIMEMagicFile /usr/local/apache_2.0.39/conf/magic
---
> MIMEMagicFile /usr/local/apache/conf/magic
```

```
< ErrorLog /usr/local/apache_2.0.39/logs/error_log
---
> ErrorLog /usr/local/apache/logs/error_log
```

```
< CustomLog /usr/local/apache_2.0.39/logs/access_log common
---
> CustomLog /usr/local/apache/logs/access_log common
```

```
< #CustomLog /usr/local/apache_2.0.39/logs/referer_log referer
< #CustomLog /usr/local/apache_2.0.39/logs/agent_log agent
---
> #CustomLog /usr/local/apache/logs/referer_log referer
> #CustomLog /usr/local/apache/logs/agent_log agent
```

```
< #CustomLog /usr/local/apache_2.0.39/logs/access_log combined
---
> #CustomLog /usr/local/apache/logs/access_log combined
```

```
< Alias /icons/ "/usr/local/apache_2.0.39/icons/"
---
```
The following is where you decide about the location and running of CGI scripts. CGI scripts can be very useful, but also can cause serious security issues. It is a good idea to set up the webserver so only user name WWW and group name httpd can run CGI scripts. The CGI scripts should be centralized and maintained in a single directory structure and maintained by the webmaster. That is, no individual user should be allowed to run CGI scripts from their personal areas.

More generic directory changes:

Starting Apache for the first time

With the above changes made, you may now start up the Apache server for the first time, as follows:

```
$ cd /usr/local/apache/bin
$ ./apachectl start
./apachectl start: httpd started
```

You may now check to see if the web server started successfully, as follows:
Connect to the web server, in this example using a web browser type in the following URL: http://randgpin00.dnr.state.wi.us. You should get something that looks like the following:

If you can see this, it means that the installation of the Apache web server software on this system was successful. You may now add content to this directory and replace this page.

**Seeing this instead of the website you expected?**

This page is here because the site administrator has changed the configuration of this web server. Please contact the person responsible for maintaining this server with questions. The Apache Software Foundation, which wrote the web server software this site administrator is using, has nothing to do with maintaining this site and cannot help resolve configuration issues.

The Apache documentation has been included with this distribution.

You are free to use the image below on an Apache-powered web server. Thanks for using Apache!

---

To make sure the web server started up under the correct user name and group, please issue the following command:

```
$ ps -ef | grep httpd
```

You should see the following:

```
root     31053   1  0.0 11:44:56 ??    0:00.29
/usr/local/apache_2.0.39/bin/httpd -k start
www 31056  31053  0.0 11:44:56 ??  0:01.79
/usr/local/apache_2.0.39/bin/httpd -k start
www 31059  31053  0.0 11:44:56 ??  0:01.63
/usr/local/apache_2.0.39/bin/httpd -k start
www 31060  31053  0.0 11:45:05 ??  0:01.44
/usr/local/apache_2.0.39/bin/httpd -k start
www 31063  31053  0.0 11:44:56 ??  0:01.82
/usr/local/apache_2.0.39/bin/httpd -k start
www 31066  31053  0.0 11:44:56 ??  0:01.53
/usr/local/apache_2.0.39/bin/httpd -k start
www 31067  31053  0.0 11:44:56 ??  0:01.71
/usr/local/apache_2.0.39/bin/httpd -k start
www 31081  31053  0.0 11:47:59 ??  0:01.60
```
There should only be one httpd process running under the root account, the others should be running under the site specific user name, in this example WWW.

**Shutting down the webserver**

To shutdown the web server, issue the following commands:

```
$ cd /usr/local/apache/bin
$ ./apachectl stop
./apachectl stop: httpd stopped
```

At this point, the web server is shutdown.

**Automatic Startup or Shutdown of Apache**

It would be a good idea to create an rc script that would automatically startup and shutdown the web server at system boot time and system shutdown respectively. A sample /sbin/init.d/httpd is as follows:

```
#!/bin/sh
# start or stop httpd daemon
#
if [ -f /usr/local/apache/logs/httpd.pid ]; then
    Pid=`cat /usr/local/apache/logs/httpd.pid`
fi

case $1 in
    'start')
        if [ -f /usr/local/apache/bin/apachectl ]; then
            if [ "X$Pid" = "X" ]; then
                /usr/local/apache/bin/apachectl start
            fi
        else
            echo "$0: /usr/local/apache/bin/apachectl does not exist"
            exit 1
         fi
    ;;
    'stop')
        if [ -f /usr/local/apache/bin/apachectl ]; then
            if [ "X$Pid" != "X" ]; then
                /usr/local/apache/bin/apachectl stop
                rm -f /usr/local/apache/logs/httpd.pid
            fi
        fi
    ;;
    *)
        echo "usage: $0 {start|stop}"
        exit 1
    ;;
esac
exit 0
```
Please create the **httpd** file in `/sbin/init.d`. Make sure that the **httpd** file is set to mode **750** and is owned by **bin:bin**. Also, a links need to be set up in the rc directory structure:

```
# cd /sbin/init.d
# chmod 750 httpd
# chown bin:bin httpd
# cd /sbin/rc3.d
# ln -s ..../init.d/httpd S992httpd
# cd ../rc2.d
# ln -s ..../init.d/httpd K001httpd
# cd ../rc0.d
# ln -s ..../init.d/httpd K001httpd
```
Big Brother Implementation Plan

Introduction

This chapter will highlight implementation of Big Brother on the Wisconsin Department of Natural Resources (WDNR) UNIX servers. This chapter references the Apache Web Server, Big Brother System and Network Monitor, and Multi Router Traffic Generator chapters, which describe in detail the installation of Big Brother and associated software. It is a very good idea to read the aforementioned chapters, before proceeding.

Implementation

On prodsmin01.dnr.state.wisc.us, in /src/Big_Brother, are the kits required for installing Big Brother. It is up to WDNR to decide a location for Big Brother, but it would be best to be installed in an environment with a great deal of resources. It is not the fact that Big Brother takes a lot of resources, it does not; however, its performance can be greatly affected by other applications, if running on a slower processor. Based upon the author’s experience, it would be best to install the Big Brother environment on prodsmin01.dnr.state.wi.us or on its own dedicated server. For the purpose of this chapter, it is assumed that Big Brother will be installed on prodsmin01.dnr.state.wi.us.

Before installing the software packages, you will need to do the following:

1. Create the httpd group for Apache and Big Brother.
2. Create the WWW user id for Apache, directory /usr/local/apache.
3. Create the BBMON user id for Big Brother, directory /home/bbmon.
4. Decide on the target for installation, as noted above.

Decompress the contents of the kits:

```
# gzip -d apache.prod.tar.gz
# gzip -d gd-1.8.4.build.tar.gz
# gzip -d jpeg-6b.build.tar.gz
# gzip -d libpng-1.2.2.build.tar.gz
# gzip -d rrdtool-1.0.38.build.tar.gz
# gzip -d bb.prod.tar.gz
```

Now that the kits are downloaded and decompressed, it is a matter of extracting the kits contents and configuring the software. In order to keep this document to a minimum, you will be referred to Apache Web Server, Big Brother System and Network Monitor, and Multi Router Traffic Generator chapters. Once the above kits are installed, they can be removed. The original source code is also stored in /src/Big_Brother, if the need arises to rebuild the software.

Also, to save some time, the Apache and Big Brother kits have been saved from the installed software on randgpin00.dnr.state.wi.us. The Big Brother kit also
includes the MRTG software, as well. All you have to do is extract the files and change all references from `randgpin00` to `prodsmin01` in the configuration files.

The following is a step by step process for installing Apache:

1. Extract the apache software: `tar -xf apache.prod.tar`
2. The apache software is now installed in `/usr/local/apache`. Please check the ownership of the files so they are owned by user `WWW` and group `httpd`. If not, issue the command: `# chown -R WWW:httpd /usr/local/apache-2.0.39`
3. Create a link to Apache in `/usr/local`, as follows:

   ```
   # cd /usr/local
   # ln -s apache-2.0.39 apache
   # chown -h www:httpd apache
   ```
4. See Page 4 of the *Apache Web Server* chapter, change the Web Master (`ServerAdmin`) e-mail address and Web Server Name (`ServerName`), to the desired setting.
5. Set up Apache so it will startup at boot time:

   ```
   # cp /src/httpd /sbin/init.d/.
   # cd /sbin/init.d
   # chmod 750 httpd
   # chown bin:bin httpd
   # cd ../rc3.d
   # ln -s ../httpd S992httpd
   # cd ../rc2.d
   # ln -s ../httpd K001httpd
   # cd ../rc0.d
   # ln -s ../httpd K001httpd
   ```
6. Now start up the Apache server: `# /sbin/init.d/httpd start`
7. Using a Netscape or Explorer connect to the Apache Web Server, e.g. `http://prodsmin01.dnr.state.wi.us`

You should see something similar to the sample page shown the *Apache Web Server* chapter.

**Installing Supporting Libraries for MRTG**

As mentioned earlier, all software has been pre-built, all that is required is to extract the pre-built kits from tar archives and follow some simple instructions:

```
# cd /src
# tar -xf gd-1.8.4.build.tar
# cd gd-1.8.4
# gnumake install
# cd /src
# tar -xf jpeg-6b.build.tar
# cd jpeg-6b
# gnumake install
# cp *.h /usr/local/include/.
# cp libjpeg.a /usr/local/lib/.
```
At this point, all the software that Big Brother and MRTG depends on, is now installed

## Installing Big Brother and MRTG

Before installing Big Brother, you must decide if you will be using the `bb-central` extension for centralized gathering of host information via `ssh`. Using `bb-central` will be a great time saver, as you will only have to maintain one copy of Big Brother in the enterprise. This chapter assumes that WDNR will be using `bb-central` and does not address installing Big Brother clients on each monitored UNIX host.

If you plan to use `bb-central`, then install `ssh` on each of the UNIX hosts to be monitored. Next, please set up a `BBMON` on each UNIX host you want to monitor. Make sure `BBMON` is added to the `adm` group, so it can read the system log files in `/var/adm/syslog.dated`. Now, set up trusted `ssh` for `BBMON`, please do the following on the Big Brother host:

```bash
# su - BBMON
$ cd .ssh
$ ssh_keygen -t dsa
$ copy id_dsa.pub authorized_keys
$ scp authorized_keys bbmon@host/.ssh/.
```

On each host you want to monitor, copy the `authorized_keys` file to the `.ssh` directory of the `BBMON` account (last command above).

To test trusted `ssh` access, please issue the following command for each host:

```bash
# ssh BBMON@host
```

If `ssh` is set up correctly, you will not be asked for a password.

Now, we can install Big Brother on the desired host. As with Apache, the Big Brother and MRTG tar archive, `bb-prod.tar`, is a copy of the installation from `randgp00.dnr.state.wi.us`. All that needs to be done is the following:

```bash
# cd /src
# tar -xf bb-prod.tar
```

The Big Brother software should now be in `/home/bbmon`. It is a good idea to make sure ownership and permissions are correct; that is the files are owned by
user **BBMON** and group **httpd**. The permission should be set that both the **httpd** group has full permissions to access the files in the Big Brother file structure.

The following are a list of changes required to change to host to the location where Big Brother, MRTG and Apache are located:

1. Connect to `/usr/local/apache/cgi-bin` and change the following files:
   - **bb-hist.sh** – The **BBWEB** and **BBWEBCGI** variables.
   - **bb-servmaint.sh** – The **BBMAINHOST** variable.
   - **statrrd-graph.sh** – The **BBWEB** and **BBWEBCGI** variables.

2. Connect to `/home/bbmon/bbvar` and issue the following commands:
   ```bash
   # cd logs
   # rm *
   # cd ../hist
   # rm -r *
   # cd ../notes
   # rm *
   # cd ../errors
   # rm *
   # cd ../histlogs
   # rm *
   # cd ../statrrd/rrd
   # rm *
   # cd ../graphs
   # rm *
   ```
   This clean out the test data created on randgpin00.

3. Connect to `/home/bbmon/bb` and change the following files:
   - **bb-enable.ksh** – Host Name of Big Brother Server
   - **bb-disable.ksh** – Host Name of Big Brother Server

4. Connect to `/home/bbmon/bb/etc` and change the following files:
   - **bbdef.sh** – **BBWEBHOST** variable
   - **bb-hosts** – Insert hosts you want to monitor
   - **bbwarnrules.cfg** – To whom you want to send alerts to
   - **bbwarnsetup.cfg** – To whom you want to send alerts to.

5. Connect to `/home/bbmon/bb/ext` and change the following files:
   - **bb-mrtg.pl** – the `$baseUrl` variable

6. Connect to `/home/bbmon/bb/ext/statrrd`
   - **statrrd.sh** – The **BBWEB** and **BBWEBCGI** variables

7. Connect to `/home/bbmon/bb/etc/bb-central` and change the following files:
8. Set up Big Brother so it will startup at boot time:

```
# cp /src/initbb /sbin/init.d/
# cd /sbin/init.d
# chmod 750 initbb
# chown bin:bin initbb
# cd ../rc3.d
# ln -s ../initbb S993initbb
# cd ../rc2.d
# ln -s ../initbb K003initbb
# cd ../rc0.d
# ln -s ../initbb K001initbb
```

At this point, we are done with the Big Brother portion of the installation. Now, we turn our attention to MRTG. Before going on, MRTG requires Simple Network Management Protocol (SNMP) to be turned on for any system being monitored with MRTG. Please see the section Making Effective Use of MRTG in the *Multi Router Traffic Generator* chapter, for setting up SNMP.

Once, you have SNMP running where you want it, the next step is to create the MRTG configuration files. Please see the section MRTG, Big Brother and You in the *Multi Router Traffic Generator* chapter for detailed instructions.

**Starting and Viewing Big Brother**

If you did everything right, you will now be able to start up Big Brother and it will start gathering information. Issue the following command:

```
# /sbin/init.d/initbb start
```

Wait about 5 minutes and using Netscape or Explorer connect to the Big Brother host’s webserver:

```
http://prodsmin01.dnr.state.wi.us/bb
```

You should see the Big Brother display in action.
Big Brother Maintenance

Introduction

This chapter contains notes about maintaining Big Brother at the Wisconsin Department of Natural Resources (WDNR). You should review the following chapters to become familiar with Big Brother and its associated products:

- Big Brother System and Network Monitor
- Big Brother Implementation Plan
- Apache Web Server
- Multi Router Traffic Generator

The above chapters provide detailed information about the Big Brother implementation at WDNR.

Setting Up New UNIX Servers for Big Brother

After a new UNIX server is installed, you need to do the following so Big Brother can monitor the new host:

On the new host:

1. Add group httpd, gid 59999 to /etc/group.
2. Add user id BBMON to the adm group in /etc/group. This is required so Big Brother can examine the system log files.
3. Add user id BBMON, uid 370, gid 59999 as a local user account. Make sure the Big Brother directory is set to /home/bbmon and shell is set to /bin/ksh.
4. Add ssh service to /etc/services, required for Big Brother to monitor the ssh port.

```
ssh         22/tcp
```

5. In dxaccounts, modify the BBMON account so the password or account does not expire.
6. Log into the new BBMON account, and change the password.
7. Create an ssh public and private key: ssh-keygen -t dsa (Take the defaults for the prompts). The above command will create the .ssh directory as a subdirectory to /home/bbmon and create the files id_dsa and id_dsa.pub.
8. Modify /etc/snmpd.conf, as follows:

```
sysName    newhost.dnr.state.wi.us
sysLocation WDNR Data Center 030
sysContact root@devlgpin00.dnr.state.wi.us
```
Also, change the community string to look like the following:

```
community  wdnrnet       0.0.0.0    read
```

Restart snmpd:

```
# /sbin/init.d/snmpd stop
# /sbin/init.d/snmpd start
```

9 Insert the following in `/etc/syslog.conf` (required for centralized system log monitoring):

```
*.err;kern.debug;daemon,auth.info;mail.debug;user.none  @prodsmin01
```

**NOTICE:** There is a <TAB> between `user.none` and `@prodsmin01`

Restart syslog:

```
# /sbin/init.d/syslog stop
# /sbin/init.d/syslog start
```

On the Big Brother Server (`prodsmin01.dnr.state.wi.us`):

- Append the `id_dsa.pub` file (created on the new host in `/home/bbmon/.ssh`) to the `authorized_keys` file you will find in the `/home/bbmon/.ssh` directory on the Big Brother server. The following commands are done on the Big Brother Server:

  ```
  $ cd /home/bbmon/.ssh
  $ scp newhost:/home/bbmon/.ssh/id_dsa.pub x
  $ cat x >> authorized_keys
  $ rm x
  ```

- Copy the new `authorized_keys` file to all UNIX servers being monitored.

  ```
  $ scp authorized_keys host:/home/bbmon/.ssh/.
  ```

- Test connecting to the new host from the BBMON account on the Big Brother hosts:

  ```
  $ ssh newhost
  ```

  You should now be able to connect to the new host, via the BBMON account, with no password.

- Modify `/etc/hosts` and insert the new server name and IP address. This is needed for the consolidated message files check. Because WNDR does not use DNS reverse lookup, syslog does not translate IP addresses from other hosts writing to the syslog files.

- Please connect to `/home/bbmon/bb/etc/bb-central` and now insert the new host information in `bb-hosts`.

- Please connect to `/home/bbmon/bb/ext/bb-central` and add the new host information to `bb-param` and `bb-param-local`. 

46
To get Big Brother to display Network Traffic information, lease connect to `/home/bbmon/mrtg` and do the following:

```
$ cd /home/bbmon/mrtg
$ ./bin/cfgmaker wdnrnet@newhost.dnr.state.wi.us > x.cfg
$ ./fix_cfg.pl
```

With an editor review the contents of `new_mrtg.cfg` and make changes. Also, please remove all the lines before the series of pound signs.

```
$ cat new_mrtg.cfg >> mrtg.cfg
$ ./error_cfg.pl
```

Because Big Brother is set at a 10 minute cycle, it will take about 10 to 20 minutes to start seeing the new host in the Big Brother display.

**Removing a Host from Big Brother Monitoring**

Up to now we concentrated on adding a Big Brother host, the following is the procedure for removing a UNIX host. The following procedure is performed on the Big Brother server. It is best to do this procedure when there are no Big Brother processes are active:

1. Please connect to `/home/bbmon/bb/etc` and remove the host information from `bb-hosts`.
2. Please connect to `/home/bbmon/bb/ext/bb-central` and remove the host information from `bb-param` and `bb-local-param`.
3. Please connect `/home/bbmon/mrtg` and remove the host information from `mrtg.cfg` and `mrtg-error.cfg`.
4. Please connect to `/home/bbmon/bbvar/logs` and remove all files associated with the host.
5. Please connect to `/home/bbmon/bbvar/hist` and remove all files associated with the host.
6. Please connect to `/home/bbmon/bbvar/histlogs` and remove all files associated with the host.
7. Please connect to `/home/bbmon/bbvar/notes` and remove all files associated with the host.
8. Please connect to `/home/bbmon/bbvar/errors` and remove all files associated with the host.
9. Please connect to `/home/bbmon/bbvar/statrrd` and remove all files associated with the host.
10. Please connect to `/home/bbmon/.ssh` and remove the desired host from `authorized_keys`.

Upon completion of the above procedure, the host information will be removed. It is possible that some remnants of the removed host may remain in Big Brother. You can easily tell this, because the host may be showing up in the **purple** Big Brother state. If this happens, just remove the unwanted files as described in steps 4–6 above.
Removing a Service from Big Brother Monitoring

If you decided that you no longer want to monitor a particular service, you would follow the above procedure (except for step 3 above, unless you are discontinuing network traffic monitoring), except you would just remove files associate with the particular host and service.

Other Big Brother Items

Notifications

If you desire to use e-mail paging, the files that control this are in the directory /home/bbmon/bb/etc and are bbwarnrules.cfg and bbwarnseup.cfg. If you desire to use numeric paging, in addition to e-mail paging, then you will need to install Kermit and a modem on the Big Brother Server.

At the present time, e-mail paging notification is inactive, but can be reactivated by uncommenting the various lines in the aforementioned configuration files. Just look for the user id metron, as the author had the notifications going to him self.

Documentation

All documentation provided with Big Brother can be accessed via the “circle I” logo on the Big Brother Display.

Updates and Patches

The author tried to provide a “turn key” solution for Big Brother. However, it is a good idea to subscribe to the Big Brother Mailing Lists to get information about the product releases and possible security patches. The mailing lists also provide a great deal of information and help, if you need it. The Big Brother Community is very helpful and supportive, so it can be a great resource.

Based upon the author’s experience, I have only had to apply one security patch over the last 4 years. The mailing lists are identified and described at the main Big Brother Website: http://www.bb4.com

New Operating Systems and Big Brother Modules

A portion of the Big Brother environment installed at WDNR, was written by the author or by other Big Brother users. The author has provided monitoring for Host Memory, Disk I/O and CPU States; these scripts were written for Tru64 UNIX only. If another UNIX operating system is introduced, then the aforementioned scripts will need to be modified to add support. The author is hopeful that other users of Big Brother will provide the needed information. In any case, releases of external Big Brother modules can be found at http://www.deadcat.net.
Recompiling

A portion of Big Brother is written in C. In the rare case that an operating system upgrade causes problem for Big Brother, just do the following:

```bash
# cd /home/bbmon/bb/src
# gnumake install
# chown –R BBMON:httpd /home/bbmon/bb/bin
```

Conclusion

This chapter has provided information about the maintenance of the Big Brother Monitoring environment. It is very rare that you will have to do anything to the existing environment, except add and remove hosts from the various parameter files and file cleanup, as noted earlier. I hope the information provided herein will provide enough information keep your Big Brother environment running for the foreseeable future.
Introduction to Trusted ssh

Introduction

In order to use ssh in a batch system management environment or interactively to connect to hosts in a rapid manner, it is possible to set up a “trusted” ssh environment. A trusted ssh environment allows the user to connect to various hosts, using the ssh protocol, without the need of a password authentication to go between various hosts.

The protocols rsh and rlogin also can perform this function, but the session would be unencrypted and is subject to various security issues. ssh uses encrypted keys to accomplish the connection between various hosts, and in turn, the ssh protocol already encrypts the session; therefore, the ssh protocol is far more secure, then the aforementioned protocols.

This chapter will now describe the procedure for setting up trusted ssh.

Trusted ssh Setup

On each host that is going to participate in the trusted environment, perform the following series of commands, for the desired user account. That is, you must log into each host, under the desired user account, which you want to have trusted access.

NOTICE: You do not need to enter a passphrase, just hit the RETURN key when prompted. Also, use the default filename for the key file, it is hard coded that way in the ssh code.

```
# cd .ssh
# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (//.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in //.ssh/id_dsa.
Your public key has been saved in //.ssh/id_dsa.pub.
The key fingerprint is:
\root@randgpin00.dnr.state.wi.us
# cp id_dsa.pub authorized_keys
# chmod 600 authorized_keys
```

Once you have completed this for each host, then you need to perform the next step.

On each host you desire to participate in the trusted environment, you will need to append the .ssh/id_dsa.pub, created on each host for the desired user account, to the each other host’s .ssh/authorized_keys file, in the desired user account’s .ssh directory.
The easiest way to accomplish this, is on one of the participating hosts, copy all the other participating host’s `.ssh/id_dsa.pub` files, to the desired user’s account `.ssh/authorized_keys` file; then, copy the resulting `.ssh/authorized_keys` files to each participating host.

Once all hosts are completed, then you should be able to connect to any host, without the need of password authentication, from one host to another. For interactive logins, you will need to enter a password, to login to the target host and desired user account, for the first initial login. For cron jobs, because the cron job is executed under the desired user account, no password will be required for the initial login.

**Maintenance of Keys**

Fortunately, the `ssh` software can be upgraded, without the need of generating new keys. The only time that the `.ssh/authorized_keys` file needs to be changed, is when a host is added or removed.