PasTmon

PasTmon.sourceforge.net

PasTmon-0.17.6: Install Guide

Graham Lee Bevan <graham.bevan@ntlworld.com>

May 3, 2015

PasTmon - Install Guide.

Contents

1 Introduction **4**

2 Getting PasTmon **5**

3 Sensor Placement **6**
3.1 Muliple Sensors feeding to Single Database 6

4 Prerequisites **10**
4.1 Supported Platforms 10
4.2 Installing from source 10

5 Installing PasTmon **15**
5.1 Installing from source 15
5.2 Installed directory structure 15
5.3 Installing on Gentoo Linux 16
5.4 The pastmon user 17
5.5 Upgrading PasTmon 17

6 Uninstalling **18**

7 Configuration **19**
7.1 Summary Script Configuration 29

8 Running PasTmon **30**
8.1 Linux Kernel Tuning Recommendations 33

9 Output **34**

10 Creating the PostgreSQL database **35**

11 PasTmon/PHP web based graphics **37**

12 Bug Reporting **38**

13 Becoming a Developer **39**

14 Public Discussion Forum **40**

15 Migrating from previous releases **41**

16 Boot Scripts **44**

17 Open Publication License **46**

1 Introduction

The goal of the PasTmon project is to create the means to passively measure and record network application response times; including network round-trip times and congestion control indicators.

Network packet capture is provided by the libpcap package.

PasTmon originally leveraged code from Marty Roesch's Snort Network Intrusion Detection System for network packet decoding, which is also licensed under the GNU General Public License (GPL).

Regular expression support is provided by the PCRE library package; written by Philip Hazel, and copyright by the University of Cambridge, England — see file README.pcre.

PasTmon implements a multi-threaded plugin architecture with data summarisation / reduction and can feed this into an SQL database for historical reporting, graph generation, and web-based presentation.

PasTmon is available subject to the GNU General Public License (GPL) Version 3 and is available for free. The source is also available for you to peruse/review and even tailor to your own needs.

2 Getting PasTmon

The PasTmon package is available as source tar-ball and Gentoo ebuild from:

http://pastmon.sourceforge.net

Please be sure to verify the package you download against either the provided MD5 checksum file or the respective OpenPGP/GnuPG signature file to ensure that the package has not been tampered with. My public key "graham.bevan@ntlworld.com" is available from http://pastmon.sourceforge.net/glbevan_publickey.txt

The PasTmon project itself is hosted via SourceForge.net at:

http://sourceforge.net/projects/pastmon

3 Sensor Placement

PasTmon , being a passive packet sensor, needs to be strategically placed to ensure optimum data capture and correct measurement of network round-trip-time.

Figure 1 shows all of the PasTmon components installed on the server being monitored. This configuration is only feasible if the server is a Unix/Linux platform and has sufficient spare resources to give to the PasTmon sensor, backend database and web presentation.

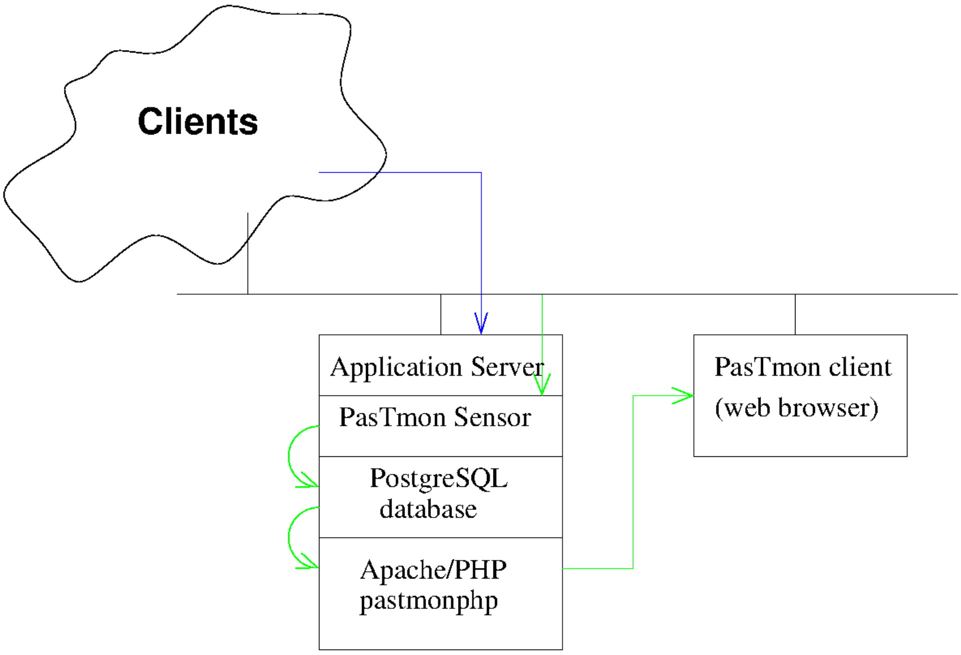

Figure 1: Placing the PasTmon sensor

Figures 2 through 5 show examples of various configurations of PasTmon where the web server(s) being monitored are not touched or affected by the installation.

In these configurations, the PasTmon sensor is run *promiscuously* in order to catch all network traffic to and from the monitored web server(s). If the physical implementation involves switched hubs, then the hub's port attaching to the PasTmon sensor must be configured as *spanning* the hub port(s) of the monitored web server(s).

3.1 Muliple Sensors feeding to Single Database

Since PasTmon -0.13-0 Multiple PasTmon sensors can now be fed to a single central database. Support has also been added into the pastmon-php interface to

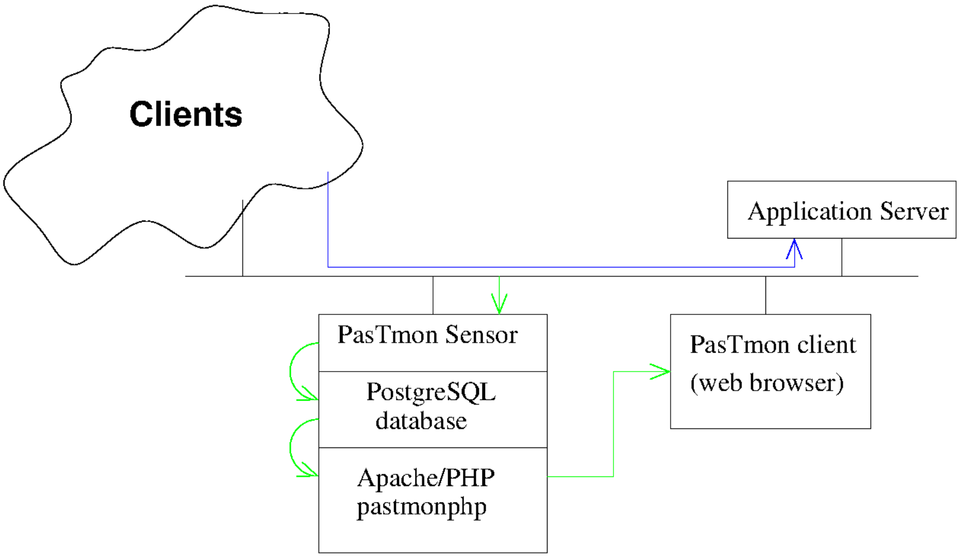

Figure 2: PasTmon sensor on a seperate box

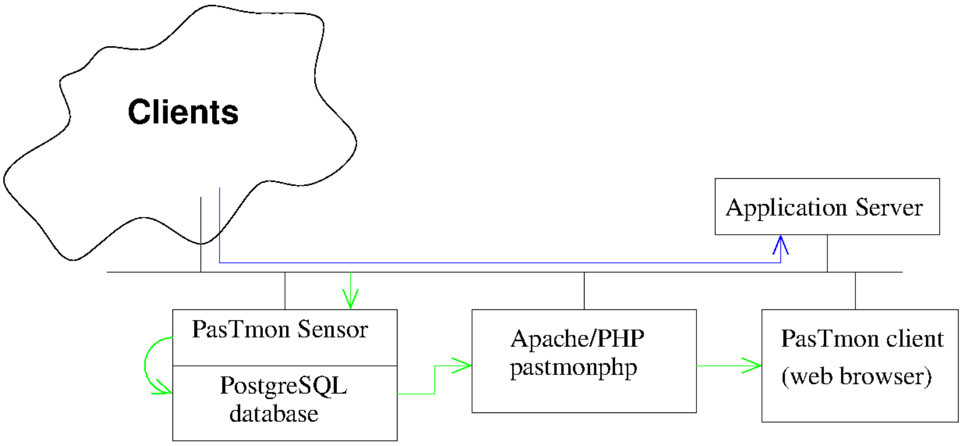

Figure 3: Splitting the PasTmon components up

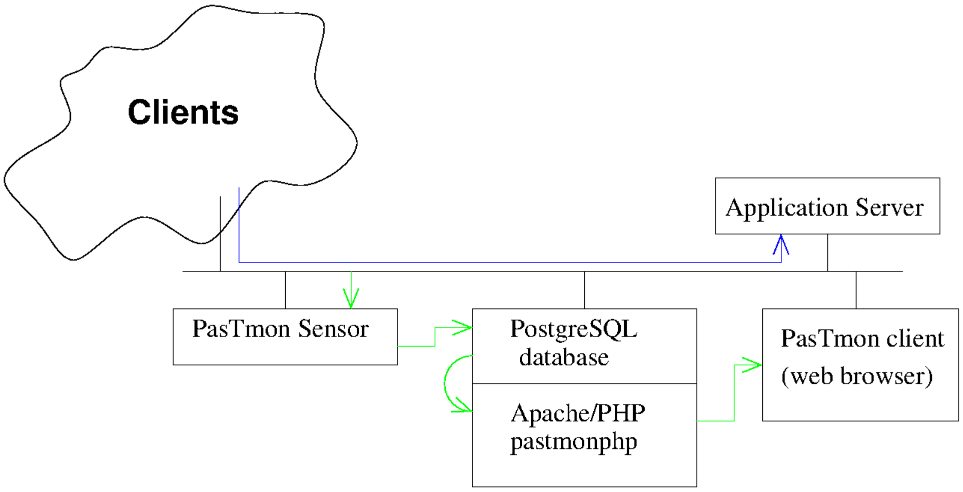

Figure 4: Splitting the PasTmon components up

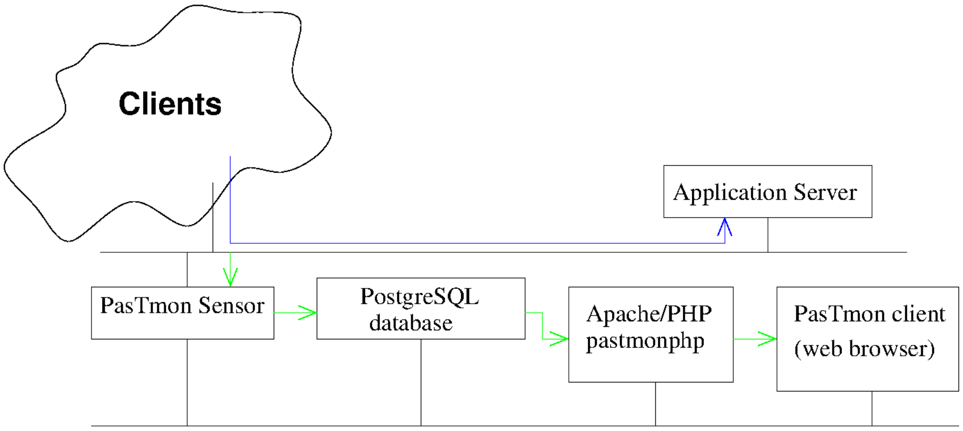

Figure 5: Splitting the PasTmon components up, access via seperate LAN

allow filtering and drill down by sensor name.

The sensor name defaults to the system hostname (plus the network interface name - so each interface is internally tracked as a seperate sensor).

4 Prerequisites

4.1 Supported Platforms

PasTmon is developed on Gentoo Linux, but is known to run on other Linux and Unix operating systems.

Also, see file readme.centos in the PasTmon distribution for detailed instructions for installing on CentOS.

4.2 Installing from source

If you are installing PasTmon from source, you will need the following prerequisite packages.

gcc - ANSI C Compiler	
Gentoo	sys-devel/gcc
RedHat	gcc-*.rpm
Debian/Ubuntu	gcc
Source	gcc from ftp://ftp.gnu.org/pub/gnu/gcc/

bison - grammer parser	
Gentoo	sys-devel/bison
RedHat	bison-*.rpm
Debian/Ubuntu	bison
Source	bison from http://ftp.gnu.org/gnu/bison/

flex - lexical analyser	
Gentoo	sys-devel/flex
RedHat	flex-*.rpm
Debian/Ubuntu	flex
Source	flex from ftp://ftp.gnu.org/pub/non-gnu/flex/

pkgconfig - Package config system that manages compile/link flags for libraries	
Gentoo	dev-util/pkgconfig
RedHat	pkgconfig-*.rpm
Debian/Ubuntu	(unknown)
Source	pkgconfig from http://pkgconfig.freedesktop.org/wiki/
Comments	

glib2 - A general-purpose utility library	
Gentoo	dev-libs/glib
RedHat	glib2-*.rpm
Debian/Ubuntu	(unknown)
Source	glib from http://www.gtk.org/
Comments	

libpcap - packet capture library	
Gentoo	net-libs/libpcap
RedHat	libpcap-*.rpm
Debian/Ubuntu	libpcap-dev
Source	libpcap from http://www.tcpdump.org/release/
Comments	For high packet rate environments, you might also try PF_RING available at http://www.ntop.org/PF_RING.html.

PostgreSQL - database server	
Gentoo	dev-db/postgresql
RedHat	postgresql-*.rpm postgresql-server-*.rpm postgresql-libs-*.rpm
Debian/Ubuntu	postgresql postgresql-client postgresql-dev
Source	postgresql from http://www.postgresql.org/ftpsite/

Comments	To grant trusted access to local accounts, set the following in your *pg_hba.conf*:
	`# TYPE  DATABASE    USER        CIDR-ADDRESS          METHOD`
	`local   all         all                               trust`
	`host    all         all         127.0.0.1/32          trust`
	although the above is the simplest way to get up and running with the database, **it is insecure**. There are options using *ident* or passwords for user authentication. Please refer to the PostgreSQL manual for further details: http://www.postgresql.org/docs/

libdbi - a database-independent abstraction layer in C, similar to the DBI/DBD layer in Perl	
Gentoo	dev-db/libdbi, dev-db/libdbi-drivers
RedHat	libdbi-*.rpm libdbi-dbd-pgsql
Debian/Ubuntu	(unknown)
Source	libdbi from http://libdbi.sourceforge.net/
Comments	Is known to work with libdbi-0.6.5-8.1 on Fedora, also with libdbi-0.7.*. However issues have been reported with 0.6.5-7 on Fedora and 0.8.1. libdbi-0.8.3 or above is now recommended. Also see readme.centos. Tested ok on Ubuntu 14.04 with libdbi 0.9.

DBI, DBD::Pg - PostgreSQL db interface	
Gentoo	dev-perl/DBI, dev-perl/DBD-Pg
RedHat/Fedora	perl-DBI, perl-DBD-Pg
Source	CPAN http://search.cpan.org DBI, DBD::Pg.

Apache - web server	
Gentoo	net-www/apache
RedHat/Fedora	httpd rpm
Debian/Ubuntu	apache, apache-common
Source	apache from http://httpd.apache.org
Comments	If you run apache under a user account other than *nobody* or *apache* then you will need to add that user to PostgreSQL using the creatuser command (as user postgres): `$ createuser -D -A www-data`

PHP4/5 - hypertext preprocessor	
Gentoo	dev-lang/php (now PHP5) add "`APACHE2_OPTS="-D PHP5"`" to /etc/conf.d/apache2.
RedHat/Fedora	php, php-pgsql rpms
Debian/Ubuntu	php5, php5-pgsql
Source	php from http://www.php.net/downloads.php use configure "`--with-pgsql`" when building for PostgreSQL support

Comments	You may need to add the following to your apache configuration file:
	`LoadModule php4_module <install-path>/libphp4.so`
	the above path to libphp4.so will vary depending on your installation
	`AddType application/x-httpd-php .php`
	`AddType application/x-httpd-php-source .phps`
	or on Gentoo, add `-D PHP5` to APACHE2_OPTS in file */etc/conf.d/apache2*.

jpgraph - Object-Oriented Graph creating library for PHP	
Gentoo	dev-php/jpgraph
RedHat/Fedora	see Source below, will also need rpm php-gd
Debian/Ubuntu	install 3.0.7 from jpgraph.net
Source	http://jpgraph.net/download/
Comments	This package produces pie charts and plots in pastmon-php. It is now mandatory. Will probably need to increase `memory_limit` value to 32MB in your `php.ini` file. It is recommended that you also install TrueType fonts "dejavu" (http://dejavu.sourceforge.net/), see jpgraph documentation for details. Edit jpgraph's file jpg-config.inc.php to point to dejavu, e.g.: `define('TTF_DIR','/usr/share/fonts/dejavu/');`

pcre - Perl-compatible regular expression library	
Gentoo	dev-libs/libpcre
RedHat	pcre-*.rpm and pcre-devel-*.rpm
Debian/Ubuntu	libpcre3-dev
Source	pcre from ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

*NB: the pcre library is shipped with many flavours of Linux.

sysstat - System Monitoring Tools	
Gentoo	app-admin/sysstat
RedHat/Fedora	sysstat
Debian/Ubuntu	sysstat
Source	http://sebastien.godard.pagesperso-orange.fr/documentation.html
Comments	

5 Installing PasTmon

5.1 Installing from source

Installation follows the standard procedure for building GNU applications packaged using the GNU Autotools.

1. Download the latest release of PasTmon .
2. Untar the downloaded package:
   ```
   $ tar zxvf pastmon-<version-release>.tar.gz
   ```
   and change directory into the resulting directory:
   ```
   $ cd pastmon-<version-release>
   ```
3. Run the configure script to configure the package for your system and your requirements:
   ```
   $ ./configure --prefix=/usr/local/pastmon
   ```
   The parameter `--prefix=` specifies where you want the built package to be installed into, this defaults to `/usr/local/pastmon`.

   If you have installed *libpcap* into a non-default location (e.g. `/usr/local` or `/opt`) then you will need to tell configure where to find the library, *libpcap.a*, and the include files:
   ```
   $ ./configure --with-pcap-lib=<libpcap-lib-dir> \
                 --with-pcap-include=<libpcap-include-dir>
   ```
   For a list of all configure options:
   ```
   $ ./configure --help
   ```
   Also see readme.centos.
4. Compile the package:
   ```
   $ make
   ```
5. Lastly install the package into the location specified earlier using the `--prefix=` parameter; for this you will need to be root:
   ```
   # make install
   ```

5.2 Installed directory structure

If you wish to use the *pastmonphp* web interface then you will need to create a symbolic-link, in your Apache root directory, to the `share/pastmonphp` subdirectory (your web server must be configured to permit symbolic links, see “`Options FollowSymLinks`” in the Apache documentation).

e.g.:

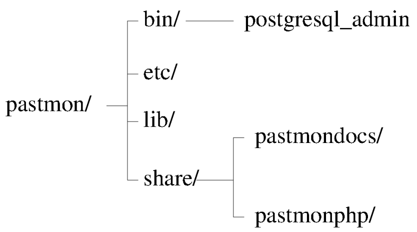

Figure 6: PasTmon installation directory structure

```
lrwxr-xr-x  1 root root   36 Mar 14 20:37 pastmonphp ->
/usr/local/pastmon/share/pastmonphp/
```

5.3 Installing on Gentoo Linux

You can use the provided ebuild to build and install PasTmon on Gentoo Linux. You should use a local portage overlay:

```
# su -
# mkdir -p /usr/local/portage/net-analyzer/pastmon
# cd /usr/local/portage/net-analyzer/pastmon
```

Download the PasTmon ebuild (e.g. `pastmon-0.17.6-r1.ebuild`) and save in the above directory. Then run:

```
# ebuild pastmon-0.17.6-r1.ebuild digest
```

You need to add `/usr/local/portage` to `PORTDIR_OVERLAY` in `/etc/make.conf`.

The finally emerge pastmon:

```
# emerge pastmon
```

The ebuild will install the PasTmon components into `/usr/pastmon/` and `/etc/pastmon/`. It will also create a pastmon script in `/etc/init.d/` which can be set to start PasTmon at reboot by running:

```
# rc-update add pastmon default
```

and you can start PasTmon immediately by running:

```
# /etc/init.d/pastmon start
```

The service script will also be installed for systemd based Gentoo systems.

```
# systemctl enable pastmon
# systemctl start pastmon
```

Note: you should create the database tables for PasTmon before trying to start the dæmon - see section 10.

5.4 The pastmon user

The installation will create a group and user called `pastmon`. This is used by the pastmon dæmon to drop from root privileges and to provide a working directory in case it core dumps - If PasTmon crashes for any reason, you will find crash dumps in `~pastmon/`.

Note: you will also need to enable the `pastmon` user to use cron for the daily level 2 summarisation job.

5.5 Upgrading PasTmon

Section 15 details additional steps required to migrate to specific releases. If this is a first time install then you can skip Section 15; otherwise it is important that you take time and read the section for the release you are upgrading to (including interim releases).

6 Uninstalling

To uninstall PasTmon simply use “`make uninstall`”, as root, from the source directory.

7 Configuration

PasTmon is configured via the *etc/pastmon.conf* file. An example is provided in *etc/pastmon-example.conf*, which is shown below:

```
/*
    PasTmon is a passive application response time monitor based on network
    packet capture (sniffer) technology.

    Copyright (C) 2000-2014  Graham Lee Bevan.

    This file is part of PasTmon.

    PasTmon is free software; you can redistribute it and/or modify
    it under the terms of the GNU General Public License as published by
    the Free Software Foundation; either version 3 of the License, or
    (at your option) any later version.

    PasTmon is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License
    along with this program.  If not, see <http://www.gnu.org/licenses/>.

    You can contact the author at graham.bevan@ntlworld.com, please add
    "[PASTMON]" at the front of the subject line so as to differentiate
    from spam/other projects etc...

*/

/* $Id$ */

/*
 * The "pastmon" section is the root section and provides setup for
 * the PasTmon base code.
 *
 */
pastmon {
        /*
         * The "load" statements define which plugin libraries to load at
         * run time
         */

        /* this must come before the generic plugin */
        load "/usr/local/pastmon/lib/libplugin_tcpsynack.so";
        load "/usr/local/pastmon/lib/libplugin_generic.so";
        load "/usr/local/pastmon/lib/libplugin_icmp.so";
        load "/usr/local/pastmon/lib/libplugin_dns.so";

        /*
         * The "output" statements define which output plugin to load
         * and use
         */

        /* Load DBI */
        output "/usr/local/pastmon/lib/liboutput_DBI.so";

        /*
         * drop root privileges to user/group
         * (can be overridden by command line options -u and -g)
         */
        user = "pastmon";
        group = "pastmon";
        /*
         * When reducing data in pastmon prior to flushing to the database,
             * summarise according to subnet.
         * The value is the CIDR netmask length,such as:  192.168.0.1/24
         * 32/128 means no summary, default is 32
         * 24 means summary by 255.255.255.0
             * (is not applied to ICMP plugin data reduction - yet)
         */
        // netmasklen = 32;     // IPv4
        // netmasklen6 = 128;   // IPv6

        /*
         * collect_internal = 0|1; collect pastmon internal stats.
         * (defaults to 1)
         */
        collect_internal = 1;

        /*
         * enable_p0f = 1 turns on p0f passive finger printing.  Defaults to 0.
         */
        enable_p0f = 0;
}

output_DBI {
        /*
         * define user connection parameters for access to the pastmon
         * PostgreSQL database - this user is not a unix user, but is a
         * database user created in script create_database_summary.
         */
        driver = "pgsql";
        // host = "localhost";   // defaulting to local Unix Domain Socket
        // port = 5432;          // defaults to 5432 (if using TCP/IP)
        username = "pastmon";
        //password = "password";
        dbname = "pastmon2";

        /*
         * retry this many times to connect to the database on startup and
         * on SQL query failure. -1 = try for ever
         */
        connect_max_retries = -1;

        /*
         * incremental delay, in seconds, for retries
         */
        connect_retry_delay = 30;

        /*
         * perform hostname lookups?
         *      0 = no
         *      1 = yes
         */
        // hostname_lookup = 1;         // default = 1, do lookups

        /*
         * hostname lookup "cache" time to live in seconds
         */
        // ip_host_ttl = 86400;         // default = 1 day
        /*
         * IPC Message Queue size, this acts as a buffer between the core
         * of pastmon and the DBI output plugin
         *
         * this is limited by the kernel IPC MSGMNB setting, in fact on
         * linux this defaults to MSGMNB
         */
        // ipc_message_queue_kbytes = 32;

        /*
         * IPC Message Queue and Semaphore Keys - these must be unique on your
         * system - see ipcs -a (as root).
         */
        ipc_msg_key = 0xa0a0a0a0;
        ipc_sem_key = 0xa0a0a0a0;

        /*
         * When save the data to database, whether to summarise according
         * to subnet.
         * The value is the CIDR netmask length,such as:  192.168.0.1/24
         * 32 means no summary, default is 32
         * 24 means summary by 255.255.255.0
         * IPv6 defaults to 128.
         */
        // dbi_netmasklen = 32;
        // dbi_netnasklen6 = 128;
}


/*
 * plugin_name {
 *      [ Cutoff        = transaction cutoff in seconds (defaults to
 *                        summary_interval * 4); ]
 *      [ SessionHashSize
 *                      = Set size of the Session tracker hash array.
 *            Needs to be a prime number.
 *                        Defaults to 7919 (applies to the generic
 *                        and tcpsynack plugins only); ]
 *      [
 *        netmasklen = 32
 *         When save the data to dabase, whether to summary accoring to subnet
 *         The value is the CIDR netmask length,such as:  192.168.0.1/24
 *         32 means no summary, default is 32
 *         24 means summary by 255.255.255.0    ]
 *
 *
 *      rule rule_name {
 *              // Summarise detail by "ip" or by "port" (probably best to
 *              // set to "port" when running in raw mode)
 *              [ Summarise_by  = [ "ip"|"port" ]; ]
 *
 *              // Rule Matching variables
 *              [ Server_ip     = [ any | IP Address | CIDR ]; ]
 *              [ Server_port   = [ any | port number ]; ]
 *              [ Client_ip     = [ any | IP Address | CIDR ]; ]
 *              [ Client_port   = [ any | port number ]; ]
 *
 *              // Wait for TCP SYN packet before starting to track
 *              // session
 *              [ WaitforSYN    = 1 | 0 ] // default = 1
 *
 *              // DelSessionOnCutoff - delete the session tracker if
 *              // Cutoff is exceeded.
 *              [ DelSessionOnCutoff    = 1 | 0 ] // default = 1
 *
 *              // Start of transaction matching variables
 *              transaction transaction_name {
 *                      [ Length        = packet length; ]
 *                      [ Offset        = offset in packet; ]
 *                      [ Depth         = Depth to scan from offset for
 *                                        match; ]
 *                      [ Content       = "string to match maybe
 *                                        including hex strings
 *                                        e.g. |0d0a|"; ]
 *                                      = regex: "Perl-like regular
 *                                        expression" [, regex_options];
 *                                      =~ "Perl-like regular expression"
 *                                        [, regex_options];
 *                      [ ConvMatchVars = "UpperCase" | "LowerCase";
 *                                        Used in conjuction with
 *                                        regular expressions. ]
 *                      [ Ignore        = [ 0 | 1 ];
 *                                        0 = track this transaction
 *                                        1 = ignore this transaction ]
 *              }
 *      }
 * }
 *
 * regex_options are:
 *      i - Ignore case
 *      m - the "start of line" and "end of line" constructs match immediately
 *          following  or  immediately  before  any newline in the subject
 *          string, respectively, as well as at the very start and end.
 *          This is equivalent to Perl's /m option. If there are no "\n"
 *          characters in a subject string, or no occurrences of ^ or $ in a
 *          pattern, setting PCRE_MULTILINE has no effect.
 *      e - If this bit is set, a dollar metacharacter in the pattern matches
 *          only at the end of the subject  string.
 *      s - (PCRE DOTALL) If this bit is set, a dot metacharater in the pat-
 *          tern matches all characters, including newlines. Without it, new-
 *          lines are excluded. This option is equivalent to Perl's /s option.
 *
 * you can also include files using the 'include "";' directive in any
 * part of the configuration file.  Nested includes are also supported.
 * e.g.
 *      include "/usr/local/pastmon/etc/pastmon-http-rules.inc";
 *
 * The ICMP plugin can be configured:
 *      ICMP {
 *              destination_unreachable = 0;    // disabled
 *              source_quench           = 1;    // enabled
 *      }
 */

generic {
        SessionHashSize = 7919;         // a prime number

        include "/usr/local/pastmon/etc/pastmon-http-rules.inc";
        include "/usr/local/pastmon/etc/pastmon-ssl-rules.inc";
        //include "/usr/local/pastmon/etc/pastmon-telnet-rules.inc";
        //include "/usr/local/pastmon/etc/pastmon-ssh-rules.inc";
        //include "/usr/local/pastmon/etc/pastmon-rlogin-rules.inc";
        //include "/usr/local/pastmon/etc/pastmon-rsh-rules.inc";
        include "/usr/local/pastmon/etc/pastmon-ftpcontrol-rules.inc";
        include "/usr/local/pastmon/etc/pastmon-smtp-rules.inc";
        include "/usr/local/pastmon/etc/pastmon-pop3-rules.inc";
        include "/usr/local/pastmon/etc/pastmon-irc-rules.inc";
        include "/usr/local/pastmon/etc/pastmon-postgresql-rules.inc";
        include "/usr/local/pastmon/etc/pastmon-mysql-rules.inc";
        include "/usr/local/pastmon/etc/pastmon-mssql-rules.inc";
        include "/usr/local/pastmon/etc/pastmon-smb-rules.inc";

        include "/usr/local/pastmon/etc/OpenStack/rules.inc";
}

tcpsynack {
        SessionHashSize = 7919;         // a prime number

        include "/usr/local/pastmon/etc/tcpsynack-http-rules.inc";
        include "/usr/local/pastmon/etc/tcpsynack-ftpcontrol-rules.inc";
        include "/usr/local/pastmon/etc/tcpsynack-irc-rules.inc";
        include "/usr/local/pastmon/etc/tcpsynack-pop3-rules.inc";
        include "/usr/local/pastmon/etc/tcpsynack-postgresql-rules.inc";
        include "/usr/local/pastmon/etc/tcpsynack-mysql-rules.inc";
        include "/usr/local/pastmon/etc/tcpsynack-mssql-rules.inc";
        //include "/usr/local/pastmon/etc/tcpsynack-rlogin-rules.inc";
        //include "/usr/local/pastmon/etc/tcpsynack-rsh-rules.inc";
        include "/usr/local/pastmon/etc/tcpsynack-smtp-rules.inc";
        //include "/usr/local/pastmon/etc/tcpsynack-telnet-rules.inc";
        include "/usr/local/pastmon/etc/tcpsynack-ssh-rules.inc";
        include "/usr/local/pastmon/etc/tcpsynack-https-rules.inc";
        include "/usr/local/pastmon/etc/tcpsynack-smb-rules.inc";

        include "/usr/local/pastmon/etc/OpenStack/tcpsynack.inc";
}

ICMP {
        destination_unreachable = 1;
        source_quench           = 1;
        redirect                = 1;
        time_exceeded           = 1;
        parameter_problem       = 1;
        conversion_error        = 1;
        the_rest                = 1;
}

/*
 * Active Agents
 *              activeplugin1 {
 *                      class:  metric1[,metric2,...] = "/path/script_metric1.py|.sh etc..."
 *                  [, every=1m|60s] [, daemon=1] [, skiplines=4] [, columns="(3,4,..|3-8)"];
 *          e.g.:
 *          syscpu: cpuuser,cpunice,cpusystem,cpuiowait,cpusteal,cpuidle = "sar -u 60 300",
 *                  daemon=1, skiplines=3, columns="3-8", nsmatch="^Default";
 *              }
 */
active_agents {
        system {

        syscpu:         cpuuser,cpunice,cpusystem,cpuiowait,cpusteal,cpuidle = "sar␣-u␣60␣300",
                                                daemon=1, skiplines=3, columns="3-8", nsmatch="^Defa

        sysrunq:        runqsz,plistsz,ldavg1,ldavg5,ldavg15,blocked = "sar␣-q␣60␣300",
                                                daemon=1, skiplines=4, columns="2-7", nsmatch="^Defa
        sysmem:         kbmemfree,kbmemused,pctmemused,kbbuffers,kbcached,kbcommit,pctcommit,
                        kbactive,kbinact,kbdirty = "sar␣-r␣60␣300",
                            daemon=1, skiplines=4, columns="2-11", nsmatch="^Default";

        syspg:          pgpgin_per_s,pgpgout_per_s,fault_per_s,majflt_per_s,
                        pgfree_per_s,pgscank_per_s,pgscand_per_s,pgsteal_per_s,pctvmeff = "sar␣-B␣60
                            daemon=1, skiplines=4, columns="2-10", nsmatch="^Default";

        sysprocrt:      proc_per_s,cswch_per_s = "sar␣-w␣60␣300",
                            daemon=1, skiplines=4, columns="2-3", nsmatch="^Default";

        // TODO: sar -n DEV etc...

        //sshstate:     sshd_up = "ps -efl | grep sshd | grep -v grep | wc -l", every=60s, nsmatch="
        }
}
```

The included *etc/pastmon-http-rules.inc* file:

```
/*
    PasTmon is a passive application response time monitor based on network
    packet capture (sniffer) technology.

    Copyright (C) 2000-2013  Graham Lee Bevan.

    This file is part of PasTmon.

    PasTmon is free software; you can redistribute it and/or modify
    it under the terms of the GNU General Public License as published by
    the Free Software Foundation; either version 3 of the License, or
    (at your option) any later version.

    PasTmon is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License
    along with this program.  If not, see <http://www.gnu.org/licenses/>.

    You can contact the author at graham.bevan@ntlworld.com, please add
    "[PASTMON]" at the front of the subject line so as to differentiate
    from spam/other projects etc...
*/

// Submitted by: Graham Lee Bevan.

// standard http on port 80
rule http_80 {
        // Summarise detail by "ip" or by "port"
        // Summarise_by = "ip"|"port";
        Summarise_by    = "ip";

        // Treat a client RESET packet as a FIN.  This to support
        // the broken http implementation in MS IE.
        // 0 = no, 1 = yes
        ClientRSTasFIN  = 1;

    // Rule Matching variables
    Server_ip       = any;
    Server_ip6      = any;
    Server_port     = 80;
    Client_ip       = any;
    Client_ip6      = any;
    Client_port     = any;

        include "/usr/local/pastmon/etc/pastmon-http-sigs.inc";
}

// http to proxy port 8080
rule http_8080 {
        // Summarise detail by "ip" or by "port"
        // Summarise_by = "ip"|"port";
        Summarise_by    = "ip";

        // Treat a client RESET packet as a FIN.  This to support
        // the broken http implementation in MS IE.
        // 0 = no, 1 = yes
        ClientRSTasFIN  = 1;

    // Rule Matching variables
    Server_ip       = any;
    Server_ip6      = any;
    Server_port     = 8080;

    Client_ip       = any;
    Client_ip6      = any;
    Client_port     = any;

        include "/usr/local/pastmon/etc/pastmon-http-sigs.inc";
}

// http to Squid proxy port 3128
rule http_3128 {
        // Summarise detail by "ip" or by "port"
        // Summarise_by = "ip"|"port";
        Summarise_by    = "ip";

        // Treat a client RESET packet as a FIN.  This to support
        // the broken http implementation in MS IE.
        // 0 = no, 1 = yes
        ClientRSTasFIN  = 1;

    // Rule Matching variables
    Server_ip       = any;
    Server_ip6      = any;
    Server_port     = 3128;

    Client_ip       = any;
    Client_ip6      = any;
    Client_port     = any;

        include "/usr/local/pastmon/etc/pastmon-http-sigs.inc";
}

// monitor for adzapper proxy on port 51966
rule http_51966 {
        // Summarise detail by "ip" or by "port"
        // Summarise_by = "ip"|"port";
        Summarise_by    = "ip";

        // Treat a client RESET packet as a FIN.  This to support
        // the broken http implementation in MS IE.
        // 0 = no, 1 = yes
        ClientRSTasFIN  = 1;

    // Rule Matching variables
    Server_ip       = any;
    Server_ip6      = any;
    Server_port     = 51966;

    Client_ip       = any;
    Client_ip6      = any;
    Client_port     = any;

        include "/usr/local/pastmon/etc/pastmon-http-sigs.inc";
}
```

The nested included *etc/pastmon-http-sigs.inc* file:

```
/*
    PasTmon is a passive application response time monitor based on network
    packet capture (sniffer) technology.

    Copyright (C) 2000-2014  Graham Lee Bevan.

    This file is part of PasTmon.

    PasTmon is free software; you can redistribute it and/or modify
    it under the terms of the GNU General Public License as published by
    the Free Software Foundation; either version 3 of the License, or
    (at your option) any later version.

    PasTmon is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License
    along with this program.  If not, see <http://www.gnu.org/licenses/>.

    You can contact the author at graham.bevan@ntlworld.com, please add
    "[PASTMON]" at the front of the subject line so as to differentiate
    from spam/other projects etc...
*/

// $Id$
//
// Submitted by: Graham Lee Bevan.

                transaction GET {
                        Offset = 0;
                        Depth = 20;
                        Content = "GET␣";
                }

                                transaction PUT {
                        Offset = 0;
                        Depth = 20;
                        Content = "PUT␣";

                        merge Content-Type {
                           Offset = 0;
                           Depth = 20;
                           Content =~ "^Content-Type:␣",i;
```

```
        }

        merge Content-Length {
           Offset = 0;
           Depth = 30;
           Content =~ "^Content-Length:␣(\d+)",i;
           Expect_data_bytes = $1;
        }
}


transaction POST {
        Offset = 0;
        Depth = 20;
        Content = "POST␣";

        merge Content-Type {
           Offset = 0;
           Depth = 20;
           Content =~ "^Content-Type:␣",i;
        }

        merge Content-Length {
           Offset = 0;
           Depth = 30;
           Content =~ "^Content-Length:␣(\d+)",i;
           Expect_data_bytes = $1;
        }
}

transaction DELETE {
        Offset = 0;
        Depth = 20;
        Content = "DELETE␣";
}
```

The "pastmon {...}" section specifies which packet processor plugins to load using the "load" statement and the output plugins using the "output" statement. The "output_PostgreSQL {...}" section provides configuration for the PostgreSQL output plugin via the connectdb setting. The format of the connectdb string is dictated by the requirements for connecting to the PostgreSQL database. Next we have sections specific to the packet processor plugins. Shown above, PasTmon will load the "generic" plugin and the "generic {...}" section provides the configuration specific to that plugin.

The "SessionHashSize =" specifies the size of the hash array for the session tracker linked-lists. The default of 100 is probably suitable for most environments, but if PasTmon is consuming a lot of CPU under heavy network traffic it may be possible to tune this by increasing this value.

The "ClientRSTasFIN = 1;" enables support for Microsoft Internet Explorer which implements an http protocol that appears to deviate from the standard.

Within the plugin section we define rules in the "rules {...}" subsections which are included from files using the "include" directive. Within the rule subsection we define the server IP address, server port, client IP address and port for the rule to match on and further define individual signatures for start of transactions within the rule (via the “transaction {...}” rule-subsections).

The transaction start signature is specified with the “Offset =”, “Depth =” and “Content =” assignment statements. A content match filter can also be specified as a Perl-like Regular Expression using either

```
Content = regex: "regular-expression" [, flags]
```

or

```
Content =~ "regular-expression" [, flags]
```

Where *flags* can be any or none of:

e (PCRE_DOLLAR_ENDONLY) If this bit is set, a dollar metacharacter in the pattern matches only at the end of the subject string.

i (PCRE_CASELESS) Ignore case

m (PCRE_MULTILINE) The ”start of line” and ”end of line” constructs match immediately following or immediately before any newline in the subject string, respectively, as well as at the very start and end. This is equivalent to Perl’s /m option. If there are no ”\n” characters in a subject string, or no occurrences of ˆ or $ in a pattern, setting PCRE_MULTILINE has no effect.

s (PCRE_DOTALL) If this bit is set, a dot metacharater in the pattern matches all char- acters, including newlines. Without it, newlines are excluded. This option is equivalent to Perl’s /s option.

When using Regular Expression signatures, it is possible to have dynamicaly generated transaction names by embedding match ’$n’ variables, e.g.:

```
rule PostgreSQL_5432 {
        Summarise_by    = "ip";
        Server_port     = 5432;
        transaction Q_$1-$2 {
                Offset = 0;
                Depth = 255;
                Content = regex:"Q(SELECT)␣.*␣from␣(\w+)",i;
        }
}
```

In this example the first matched parenthesized sub expression maps into the transaction name's $1 variable and the second expression in parentheses maps into the $2 variable.

The "`Ignore =`" assignment allows this transaction to be flagged as ignored.

The example configuration files provided configures PasTmon to track http traffic, splitting the transactions into "`GET`" and "`POST`" requests and a number of other open standard protocols. Note the use of the `merge {}` sections to add subtransactions to be consumed within the overall `POST` transaction.

7.1 Summary Script Configuration

The level 2 summary script, "`pastmon_summarise_level_2.pl`", uses file

```
etc/pastmon_summary.conf
```

to specify parameters for connecting to the database. Check that these are correct for your installation.

```
# Database connection parameters for pastmon summary
user:                   pastmon
password:
hostname:
dbname:                 pastmon2
intsumm_keepfor:        182     # days
```

The parameter `intsumm_keepfor` specifies how many days to keep the internal summary records for.

8 Running PasTmon

To start PasTmon as a dæmon with default out-of-the-box settings (best-practice), simply run *bin/pastmon* from the installation root folder.

The PasTmon executable *bin/pastmon* can also be executed with the following parameters:

```
pastmon [-v] [-d level] [-i iface[,...]] [-N renice_value] [-p] [-P]
        [-s snaplen] [-f trace_file] [-o ofile] [-u user] [-g group]
        [-r summary_interval] [-C config_file] [-K] [-M] [-D] [-O]
        [-S] [-w] [-l i|w|c] [bpf filter expression]
```

-v Set verbose mode

-d level Set the debugging level
0 - Debugging turned off (default)
1 - Plugin packet breakout
2 - Packet decoder
4 - Function entry/exit trace
8 - Parsed tokens from pastmon.conf
16 - Posix Mutex lock trace
32 - Misc message trace
64 - Unacknowledged packet dump
128 - SQL trace (output plugins)
256 - IPC queue trace (output plugins)
512 - Internal stats thread debugs
These can be added together to enable multiple debug options.

-i iface[,...] Set network interface(s) to monitor. To listen on all network interfaces at once use the name "any"[1]. Multiple network interfaces can be specified, as a comma seperated list, so transaction analysis can occur across multiple NICs.

-N renice_value Set process renice value (defaults to -10)

-p Set network interface to promiscuous mode

-P Set process memory as pinned (ie not pageable)

-s snaplen Packet capture size (default 256 bytes)

-f trace_file Input raw trace data from a file created by tcpdump. This allows for offline response time analysis of tcpdump traces taken on systems where PasTmon is not installed. This option forces `-r 0`, `-D` and `-O` options.

[1] "any" does not support Promiscuous mode.

-o ofile	Output file for raw transaction mode ("-" sets stdout)
-u user	User id to setuid to (dropping root privileges)
-g group	Group id to setgid to (dropping root privileges)
-r summary_interval	Set data reduction/summarisation interval in seconds (0 sets raw transaction mode). Output in summary mode is written to stdout (or via an output plugin, if specified).
-C config_file	Use alternate configuration file (defaults to */usr/local/pastmon/etc/pastmon.conf*).
-K	Save the process id of the running pastmon instance for automated shutdown from system "rc" scripts.
-M	Set memory allocation trace (Linux only).
-O	Don't load any output plugins, even if specified in pastmon.conf. This effectively forces output to stdout.
-D	Do not dæmonise at startup.
-S	Write messages to syslog instead of stdout/stderr.
-F	Disable p0f Operating System Fingerprinting (experimental feature).
-w	Pcap raw data save file suffix (nic name is appended to for each nic).

-l i|w|c	Display GPL copyright,
	i = GPL copyright/disclaimer,
	w = GPL warranty statement,
	c = GPL Conditions

expression	An optional BPF filter expression - see manual page for tcpdump for syntax.

To startup PasTmon in raw transaction mode (you would not normally do this - raw mode generates a record for every transaction!) use (as root):

```
# ./pastmon -i eth0 -u pastmon -g pastmon -o - -r 0 -D -O
```

This starts PasTmon on interface eth0, will switch uid/gid to pastmon/pastmon (this is recommended for security reasons!), output raw transactions to stdout and -r 0 sets raw mode (ie no summary interval).

To startup PasTmon in summary mode (averages transaction data into summary intervals) use (as root):

```
# ./pastmon -i eth0 -u pastmon -g pastmon -r 300
```

Here the summary interval is set to 300 seconds (5 minutes). You can use the example script `pastmon_startpastmon`, simply passing it the network interface name:

```
# ./pastmon_startpastmon eth0
```

To populate the postgresql database with the raw summary data you can use the script `pastmon_startpastmonsql`, again passing it the network interface name:

```
# ./pastmon_startpastmonsql eth0
```

To start PasTmon listening on all network interfaces at once, use:

```
# ./pastmon_startpastmonsql any
```

There is also a script that will run sitting in the background, detecting what network interfaces are active and start a copy of pastmon to monitor each one. If pastmon exits for any reason, it will restart it.

```
# ./pastmon_starter.sh
```

Also see Section 16 for an example RedHat Linux RC Boot script to auto start PasTmon on reboot.

Data held at 5 minute intervals is going to build up over time, so there is a level 2 summary script which reduces the data to any larger summary interval (I recommend 1 hour) and deletes the old level 1 summary data. I recommend running this once a day (over night).

```
# /usr/local/pastmon/bin/pastmon_summarise_level_2.pl --age=32  \
--interval=3600 --delete
```

--age=days specifies the age in days overwhich the level 1 data will be summarised to level 2 and deleted.

--interval=seconds specifies the new summary interval for level 2 (typ. 3600 seconds which is 1 hour).

--delete enables deletion of the summarised level 1 data.

A typical user `pastmon` crontab entry for this might look like:

```
0 1 * * * /usr/local/pastmon/bin/pastmon_summarise_level_2.pl \
              --age=32 --interval=3600 --delete 2>&1 \
      | logger -t pastmon_summarise_level_2.pl
```

8.1 Linux Kernel Tuning Recommendations

The following kernel tunings are recommended (especially to resolve pcap dropping packets):

```
echo 33554432 > /proc/sys/net/core/rmem_default
echo 33554432 > /proc/sys/net/core/rmem_max
echo 10000 > /proc/sys/net/core/netdev_max_backlog
```

These are from the following link:

High Performance Packet Capture

http://www.net.t-labs.tu-berlin.de/research/bpcs/

The script `pastmon_starter.sh` will do the above automatically on Linux systems.

9 Output

Normally, you would run PasTmon with the DBI output plugin to feed the data directly into a PostgreSQL database. You can, however, run PasTmon on it's own; feeding its data to stdout.

10 Creating the PostgreSQL database

For this, of course, you will need to have PostgreSQL installed.

Within the PasTmon **bin/** directory you will find a sub-directory called **postgresql_admin/**. The script to create the PasTmon database called *create_database_summary*. This must be run as root (it su's to user postgres).

To create the summary database you should first review the *create_database_summary* script, changing any user privileges as required (the default is to allow access using user `pastmon` without a password). Be carefull as this script will completely delete the database called **pastmon2** and re-create it from scratch. When happy with the script you can run the *create_database_summary* script.

The following tables are created:

Name	Type	Owner
control	table	postgres
dns_summary	table	postgres
dns_summary2	table	postgres
favorites	table	postgres
generic_summary	table	postgres
generic_summary2	table	postgres
hostip	table	postgres
icmp_summary	table	postgres
icmp_summary2	table	postgres
internal_summary	table	postgres
iptable	table	postgres
psession	table	postgres
puser	table	postgres
signature	table	postgres
tcpsynack_summary	table	postgres
tcpsynack_summary2	table	postgres

Views are also created for the summary data:

Name	Type	Owner
dns_summary2_view	view	postgres
dns_summary_all_view	view	postgres
dns_summary_view	view	postgres
generic_summary2_view_mss	view	postgres
generic_summary2_view_thruput	view	postgres
generic_summary2_view_time	view	postgres
generic_summary2_view_win	view	postgres
generic_summary_all_view_mss	view	postgres
generic_summary_all_view_thruput	view	postgres

generic_summary_all_view_time	view	postgres
generic_summary_all_view_win	view	postgres
generic_summary_view_mss	view	postgres
generic_summary_view_thruput	view	postgres
generic_summary_view_time	view	postgres
generic_summary_view_win	view	postgres
icmp_summary2_view	view	postgres
icmp_summary_all_view	view	postgres
icmp_summary_view	view	postgres
tcpsynack_summary2_view	view	postgres
tcpsynack_summary_all_view	view	postgres
tcpsynack_summary_view	view	postgres

11 PasTmon/PHP web based graphics

The PasTmon PHP interface allows drill-down to the required collected metric and to view these graphicaly. The graphs are produced using the PHP library jpgraph.

If you experience the problem where all the graphs are showing as broken images then you need to make sure jpgraph is locatable via the php `include_path` (see your site's php.ini and refer to jpgraph's installation documentation for further details).

On installing (or upgrading to PasTmon 0.14) default the default accounts created are:

User	**Password**
admin	admin
guest	guest

The `admin` user is a superuser and via the Admin link provides access to the User Maintenance utility.

12 Bug Reporting

This is very important for the success of this project. Please report any faults that you find with this package - in any part of it, no matter how small. You can submit any bugs you have found to the project at

http://sourceforge.net/tracker/?group_id=21894

13 Becoming a Developer

The PasTmon project needs more developers! The kind of skills wanted (though, not all at once of course) are:

1. C programming,
2. Perl programming,
3. PostgreSQL database design/performance,
4. HTML, PHP, Javascript with Dojo Toolkit and artistic web design,
5. TCP/IP including congestion control mechanisms (there is still much work to do in this area),
6. Application protocols and transaction signature analysis
7. Documentation,
8. Support and problem diagnosis,
9. Porting to other operating systems.

To become a developer on the PasTmon project simply become a member at

http://sourceforge.net

and email me (graham.bevan@ntlworld.com) your account, details / skills and interests in the project.

Or you can simply send me patches.

14 Public Discussion Forum

An open discussion forum is provided to allow anyone to ask questions, put forward ideas etc at the PasTmon user forum:

http://sourceforge.net/forum/?group_id=21894

15 Migrating from previous releases

Migrating to pastmon-0.8-0:

Run script *pg_migrate_to_0_8* to update the database schema.

The PostgreSQL Output plugin is now replaced with the DBI (database independent interface) plugin. Please see the Prerequisites section 4 of this manual for details of the libdbi package.

The PasTmon dæmon now accepts multiple network interfaces to the `-i` option. The parameters are provided as a comma separated list. The `pastmon_starter.sh` script now starts PasTmon as a single process, monitoring all discovered NICs. You can reset this script to the previous behaviour of running each NIC sensor as a seperate process instance by setting variable `SEPERATE_PROCS` to 1.

The PasTmon pid file has now been moved from `/usr/local/pastmon/` to `/var/run/`. The example `etc/rc_*` scripts have been modified accordingly. Likewise you must update your `/etc/init.d/pastmon` script.

A new thread has been implemented in PasTmon to capture internal statistics for memory usage and NIC and plugin throughput. A new database table has been introduced:

```
              Table "public.internal_summary"
      Column      |          Type          | Modifiers
------------------+------------------------+-----------
 date             | date                   |
 time             | time without time zone |
 summary_interval | integer                |
 class            | text                   | not null
 metric           | text                   | not null
 value            | double precision       |
Indexes:
    "internal_summary_entry" UNIQUE, btree (date, "time", "class", metric)
```

A new data reduction option has been added to the pastmon.conf file (`pastmon {...}` section), called ”`netmasklen=`”, which allows data to be reduced further by a netmask applied to the client ip address. This option is intended to reduce the load on the output plugin inserting records into the database in environments where there are a large number of clients.

Migrating to pastmon-0.8-1:

The crontab script, `pastmon_summaris_level_1.pl` is now deprecated as the level 1 summarisation now takes place in the DBI output plugin.

Migrating to pastmon-0.9-0:

Run script `pg_migrate_to_0_9` to update the database schema.

Although not mandatory, installing jpgraph (see prereqs) will provide some summary pie charts in pastmon-php.

Migrating to pastmon-0.10-0:

Run script `pg_migrate_to_0_10` to update the database schema.

The package jpgraph is now mandatory for the pastmon-php views.

The section std.reports is now deprecated in favour of the pastmon-php favorites facility. The std.reports crontabs (under user root) can now be removed.

The R and Ghostscript packages are now no longer required (unless you wish to continue to run the now deprecated std.reports).

Migrating to pastmon-0.11-0:

Run script `pg_migrate_to_0_11` to update the database schema.

User `pastmon` is now granted update access to the relevant database tables.

The `pastmon_summarise_level_2.pl` script can now be run under user `pastmon` crontab, instead of root.

It is recommended that you update your pastmon.conf file's `output_DBI` section to connect to the database using the `pastmon` user (this isn't actually mandatory, but helps avoid confusion).

Migrating to pastmon-0.11-1:

The pastmon-php plots now use TrueType fonts, please refer to the jpgraph manual for details on how to acquire "corefonts" and how to comfigure jpgraph to use them.

Migrating to pastmon-0.12-0:

Recommend upgrade to libdbi-0.8.3 and libdbi-drivers-0.8.3 or higher to fix memory leaks in DBI Output Plugin.

Migrating to pastmon-0.13-0:

Run script `pg_migrate_to_0_13` to update the database schema.

Migrating to pastmon-0.14-0:

Run script `pg_migrate_to_0_14` to update the database schema.

You may encounter the following error when running this script:

```
ERROR: column "syn_synack_stddev_acc" of relation "tcpsynack_summary2"
already exists
```

You can safely ignore this.

This creates the new `puser` table to hold user account details. It creates two default accounts admin and guest with passwords matching the account names.

When logged in as the `admin` user, you have the new link ”Admin” to enter user administration.

Migrating to pastmon-0.15-0:

Run script `pg_migrate_to_0_15` to update the database schema.

Migrating to pastmon-0.16.0:

PasTmon now uses Dejavu Truetype Fonts, see prereqs for jpgraph.

16 Boot Scripts

Example RC startup scripts for PasTmon are available for RedHat/Fedora, Tru64/Solaris and Gentoo (including systemd based init startup). These are located in:

/usr/local/pastmon/etc/

The listing below is an example RedHat RC script for auto-starting PasTmon on reboot. This would typically be placed in **/etc/rc.d/init.d/** and be called simply “pastmon”. This file is available in the distribution as *etc/rc_pastmon.redhat* and can be copied to */etc/rc.d/init.d/pastmon*, then, as root, run:

```
# /sbin/chkconfig --add pastmon
```

```
# chkconfig: 2345 99 02
# description: pastmon - Start/stop the pastmon daemon
#
# Copy this script to /etc/init.d/pastmon then execute the following command:
#
#       /sbin/chkconfig --add pastmon
#
#
# $Id$

# Source function library.
. /etc/rc.d/init.d/functions


# this is to fix segfaults in the DBI plugin when calling libdbi functions.
# believe the issue is due to nptl, this reverts to linuxthreads.
# If you encounter similar segfaults with this set, try unsetting.
# please report any issues to project maintainer.
#export LD_ASSUME_KERNEL=2.4.1  removed LinuxThreads deprecated


RETVAL=0

case "$1" in
  start)
        echo -n "Starting␣PasTmon:␣"
        nohup /usr/local/pastmon/bin/pastmon_starter.sh </dev/null >/dev/null 2>&1 &
        RETVAL=$?
        echo
        touch /var/lock/subsys/pastmon
        exit $RETVAL
        ;;
  stop)
        echo -n "Stopping␣PasTmon:␣"
        killall pastmon_starter.sh
        cat /var/run/pastmon_*.pid | xargs -i@ kill @
        rm -f /var/run/pastmon_*.pid
        RETVAL=0
        echo
        rm -f /var/lock/subsys/pastmon
        exit $RETVAL
        ;;
  status)
        exit 0
        ;;
  restart)
        $0 stop
        sleep 5
        $0 start
        ;;
  reload)
        ;;
  *)
        echo "Usage:␣pastmon␣{start|stop|restart}"
        exit 1
esac

exit $RETVAL
```

17 Open Publication License

Open Publication License Draft v1.0, 8 June 1999

I. REQUIREMENTS ON BOTH UNMODIFIED AND MODIFIED VERSIONS

The Open Publication works may be reproduced and distributed in whole or in part, in any medium physical or electronic, provided that the terms of this license are adhered to, and that this license or an incorporation of it by reference (with any options elected by the author(s) and/or publisher) is displayed in the reproduction.

Proper form for an incorporation by reference is as follows:

> Copyright (c) <year> by <author's name or designee>. This material may be distributed only subject to the terms and conditions set forth in the Open Publication License, vX.Y or later (the latest version is presently available at http://www.opencontent.org/openpub/).

The reference must be immediately followed with any options elected by the author(s) and/or publisher of the document (see section VI).

Commercial redistribution of Open Publication-licensed material is permitted.

Any publication in standard (paper) book form shall require the citation of the original publisher and author. The publisher and author's names shall appear on all outer surfaces of the book. On all outer surfaces of the book the original publisher's name shall be as large as the title of the work and cited as possessive with respect to the title.

II. COPYRIGHT

The copyright to each Open Publication is owned by its author(s) or designee.

III. SCOPE OF LICENSE

The following license terms apply to all Open Publication works, unless otherwise explicitly stated in the document.

Mere aggregation of Open Publication works or a portion of an Open Publication work with other works or programs on the same media shall not cause this license to apply to those other works. The aggregate work shall contain a notice specifying the inclusion of the Open Publication material and appropriate copyright notice.

SEVERABILITY. If any part of this license is found to be unenforceable in any jurisdiction, the remaining portions of the license remain in force.

NO WARRANTY. Open Publication works are licensed and provided ”as is” without warranty of any kind, express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose or a warranty of non-infringement.

IV. REQUIREMENTS ON MODIFIED WORKS

All modified versions of documents covered by this license, including translations, anthologies, compilations and partial documents, must meet the following requirements:

1. The modified version must be labeled as such.
2. The person making the modifications must be identified and the modifications dated.
3. Acknowledgement of the original author and publisher if applicable must be retained according to normal academic citation practices.
4. The location of the original unmodified document must be identified.
5. The original author’s (or authors’) name(s) may not be used to assert or imply endorsement of the resulting document without the original author’s (or authors’) permission.

V. GOOD-PRACTICE RECOMMENDATIONS

In addition to the requirements of this license, it is requested from and strongly recommended of redistributors that:

1. If you are distributing Open Publication works on hardcopy or CD-ROM, you provide email notification to the authors of your intent to redistribute at least thirty days before your manuscript or media freeze, to give the authors time to provide updated documents. This notification should describe modifications, if any, made to the document.
2. All substantive modifications (including deletions) be either clearly marked up in the document or else described in an attachment to the document.
3. Finally, while it is not mandatory under this license, it is considered good form to offer a free copy of any hardcopy and CD-ROM expression of an Open Publication-licensed work to its author(s).

VI. LICENSE OPTIONS

The author(s) and/or publisher of an Open Publication-licensed document may elect certain options by appending language to the reference to or copy of the license. These options are considered part of the license instance and must be included with the license (or its incorporation by reference) in derived works.

> A. To prohibit distribution of substantively modified versions without the explicit permission of the author(s). ”Substantive modification” is defined as a change to the semantic content of the document, and excludes mere changes in format or typographical corrections. To accomplish this, add the phrase ‘Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.’ to the license reference or copy.
>
> B. To prohibit any publication of this work or derivative works in whole or in part in standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

To accomplish this, add the phrase ’Distribution of the work or derivative of the work in any standard (paper) book form is prohibited unless prior permission is obtained from the copyright holder.’ to the license reference or copy.

OPEN PUBLICATION POLICY APPENDIX:

(This is not considered part of the license.)

Open Publication works are available in source format via the Open Publication home page at http://works.opencontent.org/.

Open Publication authors who want to include their own license on Open Publication works may do so, as long as their terms are not more restrictive than the Open Publication license.

If you have questions about the Open Publication License, please contact David Wiley, and/or the Open Publication Authors’ List at opal@opencontent.org, via email.

To subscribe to the Open Publication Authors’ List: Send E-mail to opal-request@-opencontent.org with the word ”subscribe” in the body.

To post to the Open Publication Authors’ List: Send E-mail to opal@opencontent.org or simply reply to a previous post.

To unsubscribe from the Open Publication Authors’ List: Send E-mail to opal-request@opencontent.org with the word ”unsubscribe” in the body.

Index

- ANSI C Compiler
  - gcc, 10
- Apache, 12
- Autotools, 15

- bison, 10
- Boot Scripts, 44–45
- Bug Reporting, 38

- configuration, 19
- Copyright, 2

- DBI, 12
- Developer, 39
- directories, 15

- flex, 10
- Forum, 40

- gcc, 10
- Gentoo, 16
- glib2, 11
- GNU
  - Autotools, 15
- GnuPG, 5
- GPL, 2, 4

- Installing, 15–17
- Introduction, 4

- jpgraph, 13

- libdbi, 12
- libpcap, 4, 11
- Linux
  - Kernel Tuning, 33

- Marty Roesch
  - Snort, 4
- md5, 5
- migrating, 17, 41–43
- Multiple Sensors, 6

- Open Publication License, 2, 46–48
- OpenPGP, 5
- output, 34

- PasTmon
  - Boot Scripts, 44–45
  - Bug Reporting, 38
  - configuration, 19
  - Copyright, 2
  - Developer, 39
  - directories, 15
  - Forum, 40
  - Gentoo, 16
  - Getting, 5
  - Installing, 15–17
  - License
    - GPL, 2
  - migrating, 17, 41–43
  - Multiple Sensors, 6
  - output, 34
  - pastmonphp, 37
  - PostgreSQL, 35–36
    - creating db, 35–36
  - Prerequisites, 10
  - Project goal, 4
  - running, 30–33
  - Sensor Placement, 6–9
  - Source, 10
  - summary configuration, 29
  - supported platforms, 10
  - uninstalling, 18
  - upgrading, 17
  - user, 17
- pastmonphp, 37
- pcre, 13
- PHP4/5, 13
- pkgconfig, 10
- Platforms
  - Supported, 10
- PostgreSQL, 11, 35–36
  - creating db, 35–36
- Prerequisites, 10–14

Apache, 12
bison, 10
DBI, 12
flex, 10
gcc, 10
glib2, 11
jpgraph, 13
libdbi, 12
libpcap, 11
pcre, 13
PHP4/5, 13
pkgconfig, 10
PostgreSQL, 11
sysstat, 14
Public Key, 5

Regular Expressions, 28
round-trip-time, 6
running, 30–33

Sensor Placement, 6–9
Snort, 4
Marty Roesch, 4
Source, 10
SourceForge, 5
Supported Platforms, 10
sysstat
sar, 14
systemd, 17, 44

uninstalling, 18
upgrading, 17