

# Our PLA Install on Fedora 8

## Table of Contents

- PLA Install on Fedora 8 ..... 1
- Yum Update and Installs ..... 2
- MySQL Database Account Setup..... 2
- PLA Database setup ..... 2
- Installing Parsing Scripts ..... 3
- Install Perl ..... 4
- Installing Web-based Front End..... 6
- Configure Web-Based Front End ..... 7
- Configuring PLA Parsing Daemon ..... 8
- Configure rsyslog.conf found in /etc..... 8

After OS install complete the following from the command line:

## Yum Update and Installs

1. Yum update
  - Let it complete and update everything
2. yum install gcc php mysql mysql-server perl perl-DBD-MySQL perl-DBI perl-Net-SNMP php-mysql php-gd cpan rsyslog gd-devel httpd clamav
3. Configure the new services to start automatically from the cli
  - /sbin/chkconfig httpd on
  - /sbin/chkconfig --add mysqld [this is not required with FC4 and above]
  - /sbin/chkconfig mysqld on
  - /sbin/service httpd start
  - /sbin/service mysqld start
4. For the purpose of this document we have created a user on fedora called pla
  - Extract the pla files that you downloaded to /home/pla/Documents/ pla-v2.00
    - i. We will reference this location throughout this document

## MySQL Database Account Setup

1. IMPORTANT! Set up the mysql database root password. Without a password, ANY user on the box can login to mysql as database root. The mysql root account is a separate password from the machine root account.
  - mysqladmin -u root password 'putyourpasswordhere'
2. Make additional security-related changes to mysql.
  - mysql -u root -p
  - mysql> DROP DATABASE test; [removes the test database]
  - mysql> DELETE FROM mysql.user WHERE user = ''; [Removes anonymous access]
  - mysql> FLUSH PRIVILEGES;

## PLA Database setup

PLA makes use of database tables to load the appropriate REGEX strings into memory for log parsing as well as store the parsed log data into tables based on the REGEX strings. These tables include: traffic\_log, info\_log, ids\_log, syslog\_message, and others. The PLA documentation goes into detail on the purpose of each table, the important part is getting the tables loaded so the parser and front-end can function.

- Login to mysql via the command line and process the database build script:
  - mysql -u root -p < '/home/pla/Documents/pla-v2.00/scripts/pla\_database.sql'
    - [after pressing enter, the user will be prompted for the password setup earlier]
2. After successful login, the PLA database (pix) will be created along with all the necessary tables. In order to verify the tables, perform the following tasks and note the output:
  - /usr/bin/mysql -u root -p
    - [after pressing enter, the user will be prompted for the password setup earlier]
3. The prompt at the cursor will change to mysql> at this point and the pix database will be selected as well as the tables displayed. If the output is any different, verify the commands above completed successfully.
  - mysql> use pix;

- Reading table information for completion of table and column names
  - You can turn off this feature to get a quicker startup with -A
  - Database changed
- mysql> show tables;
    - +-----+
    - | Tables\_in\_pix |
    - +-----+
    - | event\_management\_data |
    - | event\_management\_id |
    - | ids\_log |
    - | info\_log |
    - | log\_filter |
    - | parse\_filter |
    - | purge\_config |
    - | syslog\_message |
    - | traffic\_description |
    - traffic\_log |
    - | userdef\_query |
    - +-----+
    - 11 rows in set (0.00 sec)
4. The PLA scripts will need to login as something other than the ROOT or SUPERUSER for access to the PLA database. This is especially important for the web front-end because other databases or system-level commands could be accessed.
    - mysql> GRANT ALL ON pix.\* TO 'plausser'@'localhost' IDENTIFIED BY 'putyourpasswordhere';
      - plausser, localhost, and pladbpassword can be changed as needed. This installation will use the username 'plausser' and the password 'putyourpasswordhere'
      - ' when accessing the 'pix' database and because the installation is on the same server all the connections to the 'pix' database will be done via the localhost address (127.0.0.1). This feature hides the database traffic from the network, which could be advantageous in certain circumstances.
  5. Once the PLA database is configured and access has been setup, the most current syslog\_message format should be loaded to ensure the most current versions of the syslog message formats are used when processing the syslog files. BetterTechInfo contains an update from the original version included with the PLA scripts to handle updated PIX, ASA, and FWSM messages.
    - mysql -u root -p < [http://www.bettertechinfo.com/bti\\_files/syslog\\_message\\_20080215.sql](http://www.bettertechinfo.com/bti_files/syslog_message_20080215.sql)
    - \c
    -

## Installing Parsing Scripts

1. The parsing script is located in the "scripts/parsing/" directory of the PLA Software Package (the "tar.gz" file). This script must be installed on the system which received the system logs (syslog)

and is used to identify which log entries should be pushed to the database, this script requires both Perl and Perl::DBI. Personally, I've put this script in an "/usr/sbin" directory.

- # chmod +x /usr/sbin/pla\_parsed
2. The parsing script is called "pla\_parsed" and is a Perl script which runs in daemon mode so you just need to start it and it keeps running in the background. I've also included the "rc.pla\_parsed" script which needs to be put into the /etc/init.d to automatically start the PLA Parse Daemon (pla\_parsed) on system startup. If you move the pla\_parsed script to another directory than "/usr/sbin" the "rc.pla\_parsed" script will need to be updated.
  3. The script will need to be linked to the correct runlevel for it to started and stopped automatically.
    - # chmod +x /etc/init.d/rc.pla\_parsed
    - ln -s /etc/init.d/rc.pla\_parsed /etc/rc3.d/S99pla\_parsed
  4. Configure the pla\_parsed file in /usr/sbin/pla\_parsed for RSYSLOG
    - \$regex\_log\_begin = "(.\*):(.\*) (.\*) (.\*) (.\*) ((.\*):(.\*):(.\*)) (.\*)";  
##\$regex\_log\_begin = "(.\*):(.\*) (.\*) (.\*) (.\*) (.\*) (.\*)";  
\$var\_pixhost=7;  
\$var\_pixmonth=3;  
\$var\_pixdate=4;  
\$var\_pixyear=5;  
\$var\_pixtime=6;
    - Then issue a to search for the process id.
      - ps -ef | grep pla\_pa
    - then kill the pid
      - kill (PID)
    - Restart the pla\_parsed
      - Just run pla\_parsed from the command-line

## Install Perl

1. perl -MCPAN -e "shell"
  - a. The first question will ask if it can create a working directory
  - b. /tmp/.cpan and press Enter.
  - c. - Next question: Cache size and build directory - leave the default, so just hit Enter
  - d. - Next question: Perform cache scanning - leave the default (atstart), so just hit Enter
  - e. - Next question: Cache metadata - leave the default (yes), so just hit Enter
  - f. - Next question: Your terminal expects ISO-8859-1 - leave the default(yes), so just hit Enter
  - g. - Next question: File to save your history - leave the default, so just hit Enter
  - h. - Next question: Number of lines to save - leave the default [100], so just hit Enter
  - i. - Next question: Policy on building prerequisites - I prefer to just let it do it without asking, so type follow and press Enter
  - j. - Next question: Where is your gzip program - leave the default, so just hit Enter

- k. - Next question: Where is your tar program - leave the default, so just hit Enter
- l. - Next question: Where is your unzip program - leave the default, so just hit Enter
- m. - Next question: Where is your make program - leave the default, so just hit Enter
- n. - Next question: Where is your links program - leave the default, so just hit Enter (you may not have this installed)
- o. - Next question: Where is your wget program - leave the default, so just hit Enter
- p. - Next question: Where is your ncftpget program - leave the default, so just hit Enter (you may not have this installed)
- q. - Next question: Where is your ncftp program - leave the default, so just hit Enter (you may not have this installed)
- r. - Next question: Where is your ftp program - leave the default, so just hit Enter
- s. - Next question: Where is your gpg program - leave the default, so just hit Enter
- t. - Next question: What is your favorite pager program? - leave the default, so just hit Enter
- u. - Next question: What is your favorite shell? - leave the default, so just hit Enter
- v. - Next question: Big paragraph asking for additional parameters to pass - leave default (leave blank), so just hit Enter
- w. - Next question: Parameters for the 'make' command - leave the default, so just hit Enter
- x. - Next question: Parameters for the 'make install' command - leave the default, so just hit Enter
- y. - Next question: Timeout for inactivity during Makefile.PL - leave the default, so just hit Enter
- z. - Next question: Your ftp\_proxy - If you use a proxy server to get to the Internet, enter it here and then press Enter
- aa. - Next question: Your http\_proxy - If you use a proxy server to get to the Internet, enter it here and then press Enter
- bb. - Next question: Your no\_proxy - If you use a proxy server to get to the Internet, enter it here and then press Enter
- cc. - Next question: Select your continent - Enter the appropriate number and press Enter
- dd. - Next question: Select your country - Enter the appropriate number and press Enter
- ee. - Next question: Select URLs (to download from) - Enter 1 2 , and press Enter
- ff. - Next question: Enter additional URL - press Enter
- gg. Now, let's give CPAN an update for itself.
- hh. At the cpan> enter: `install Bundle::CPAN`
- ii. After the install, you will return to the CPAN prompt.

- jj. Pix If you want to look at all the modules available to install on your system type `m` and press Enter. Be sure to have your scrollback buffer set pretty high
- kk. If you see something you want to install - use `install blah::blah` at the `cpan>` prompt

2. Install from the Cli `cpan>` CASE SENSITIVE BELOW

- `Install Bundle::CPAN`
- `install Test::More`
- `install CPAN`
- `install DBI`
- `install CGI`
- `install Net::Whois::IP`
- `install Date::Manip`
- `install File::Tail`
- `install GD::Graph`
- `force install Socket`
  - `install default`
- `force install POSIX`
  - `install default`

## Installing Web-based Front End

1. `httpd.conf` file should look like this in the Directory Section:
  - `<Directory />`
    - `Options FollowSymLinks`
    - `AllowOverride None`
  - `</Directory>`
2. The web-based frontend is a collection of Perl/CGI scripts located in the "scripts/frontend/" directory of the PLA software package. These scripts query the MySQL database for information and entries pertaining to the Cisco PIX/FWSM logs. These scripts should be copied to a scripts executable directory on your web server. For example the "/cgi-bin/" directory on many web servers. In the configuration section of this document I've explained how to configure a directory to be script executable within Apache. For example, on my web server I've created a "pla2" directory in the main Apache HTML documents directory (DirectoryRoot – '/var/www/pla') and set this to scripts executable.
3. You will have to create the directories first then move the files as ROOT on the CLI
  - Move everything into the folders and make the top a parent folder
    - `mkdir -p /var/www/pla`
    - `cp -R /home/pla/Documents/pla-v2.00/scripts/frontend/* /var/www/pla`
4. Now create the following files
  - `cd /etc/httpd/conf.d`
  - `touch pla.conf`
    - Put the following in the `pla.conf` file using the cli and then typing `vi` then `i` then paste then `esc` then `:x` to save
      1. `Alias "/pla" "/var/www/pla"`
      2. `<Directory/var/www/pla>`

3. Options ExecCGI
  4. SetHandler cgi-script
  - 5.
  6. </Directory>
  7. <Directory /var/www/pla/images>
  8. Options MultiViews -ExecCGI
  9. SetHandler default-handler
  10. </Directory>
- touch php5.conf
    - In the php5.conf file put the following using the cli and then typing vi then i then paste then esc then :x to save
      1. <IfModule mod\_php5.c
      2. AddType application/x-httpd-php .php3
      3. AddType application/x-httpd-php .php4
      4. AddType application/x-httpd-php .php5
      5. AddType application/x-httpd-php .php
      6. AddType application/x-httpd-php-source .php3s
      7. AddType application/x-httpd-php-source .php4s
      8. AddType application/x-httpd-php-source .php5s
      9. AddType application/x-httpd-php-source .phps
      10. DirectoryIndex index.php3
      11. DirectoryIndex index.php4
      12. DirectoryIndex index.php5
      13. DirectoryIndex index.php
      14. </IfModule>
5. Permissions to Files in the pla directory:
    - The perm's need to be set to execute and they need to be owned by apache (can double check who the owner should be by doing `ps -ef | grep httpd` . Whoever is running httpd besides root should own those pla files and directories. Also, make sure the main /pla folder is set correctly too.
    - `ls -l` should spit out x's and owned by apache (unless the `ps -ef | grep httpd` above shows another user account)
      - `chown -R apache /var/www/pla/* *`
        1. will reset all that for you
      - but you also need to verify x is set on the files in the main /var/www/pla folder.
        1. Chown apache /var/www/pla
      - Then you will have to stop and restart the httpd service to make sure things are correct.
        1. `/sbin/service httpd stop`
        2. `/sbin/service httpd start`
    - Then test the webpage by going to localhost. You should get a Internal server error

## Configure Web-Based Front End

1. Copy New PLA Parsing Daemon
  - Copy the PLA Parsing Daemon (pla\_parsed) v2.00 to the /usr/sbin directory as follows:
  - `# cp <PLA_PACKAGE_DIRECTORY>/scripts/parsing/pla_parsed /usr/sbin`
  - *Put rc.pla\_parsed* script which needs to be put into the /etc/init.d from the same directory

2. vi /var/www/pla/conf.pl
  - \$mysql\_db\_host = "localhost"; # Host running MySQL DB
  - \$mysql\_db\_port = "3306"; # Port running MySQL DB
  - \$mysql\_db\_user = "plouser"; # MySQL DB Username
  - \$mysql\_db\_pass = "putyourpasswordhere"; # MySQL DB Password

## Configuring PLA Parsing Daemon

1. vi usr/sbin/pla\_parsed
  - \$mysql\_db\_host = "localhost"; # Host running MySQL Database
  - \$mysql\_db\_port = "3306"; # Port on which MySQL is running (usually: 3306)
  - \$mysql\_db\_user = "plouser"; # Username you configured in the MySQL database
  - \$mysql\_db\_pass = "putyourpasswordhere"; # Password you configured in the MySQL database
  - \$mysql\_db\_name = "pix"; # MySQL PIX Logging Architecture Database Name (default: pix)
  - \$pix\_log\_file = "/var/log/pixlog.log"; # PIX Logging file you configured in /etc/rsyslog.conf

## Configure rsyslog.conf found in /etc

1. Add the following lines above local7.\*
  - #Redirect system log messages received from the Pix
    - local6.\* /var/log/pixlog.log
2. Turn on rsyslog listening from command line
  - Also check the /etc/sysconfig/rsyslog
    - Add the following to the SYSLOGD\_OPTIONS=" -m 0 -r514"
  - Add the following if the firewall is on
  - iptables -I INPUT -p udp -i eth0 -s 172.16.1.1 -d 172.16.1.51 --dport 514 -j ACCEPT
  - /sbin/iptables-save > /etc/sysconfig/iptables

## Steps to disable SELINUX in Fedora 8

vi /etc/selinux/config

# This file controls the state of SELinux on the system.

# SELINUX= can take one of these three values:

# enforcing - SELinux security policy is enforced.

# permissive - SELinux prints warnings instead of enforcing.

# disabled - SELinux is fully disabled.

SELINUX=disabled

# SELINUXTYPE= type of policy in use. Possible values are:

# targeted - Only targeted network daemons are protected.

# strict - Full SELinux protection.

```
SELINUXTYPE=targeted
```

```
# SETLOCALDEFS= Check local definition changes
```

```
SETLOCALDEFS=0
```

### 5.3.1 Configuring PIX System Logging

The following commands should be used to set up system logging on the Cisco PIX Firewall:

```
pix(config)# logging on
```

```
pix(config)# logging timestamp
```

```
pix(config)# logging buffered informational
```

```
pix(config)# logging trap informational
```

```
pix(config)# logging facility 22
```

```
pix(config)# logging host inside PUTHOSTIPHERE
```

```
pix(config)# logging device-id hostname
```

### 5.3.2 Configuring IDS Logging

The following commands should be used to set up IDS logging on the Cisco PIX Firewall:

```
LynnPIX(config)# ip audit name info info action alarm
```

```
LynnPIX(config)# ip audit name attack attack action alarm drop reset
```

```
LynnPIX(config)# ip audit interface outside info
```

```
LynnPIX(config)# ip audit interface out
```

```
LynnPIX(config)# ip audit interface outside attack
```

```
LynnPIX(config)# ip audit info action alarm
```

```
LynnPIX(config)# ip audit attack action drop
```

### How to restart things

```
/sbin/service httpd restart
```

`/sbin/service rsyslog restart`

`Service network restart`

`Service network reload`

`System-config-securitylevel`

`/sbin/chkconfig --list`

`/sbin/runlevel`

`system-config-services`

`service mysqld status`

`rpm -q php-gd` this will check the version of gd installed