

Perpetual IP Systems GmbH LogBOSS 1.2.1 Installation Guide

This guide assumes the user is familiar with basic UNIX and windows commands. The LogBOSS application is provided as a zip archived file which is password protected (contact your reseller if you are unsure of the password). The archive contains all the files related to LogBOSS with the exception of certain third party components, namely the Java 2 SDK from SUN Microsystems and the MySQL database from MySQL AB. It is beyond the scope of this document to cover the installation of the above two components. Information on the Java 2 SDK can be obtained and downloaded from <http://java.sun.com> and MySQL from <http://www.mysql.com> respectively.

Pre-Requisites:

1. A recent copy of zip (linux/solaris) or winzip (windows – nb windows is not fully supported as of yet).
2. The Java 2 SDK must be installed prior to installation and the JAVA_HOME environment variable must be set.
3. MySQL must be installed and running if the installation script is to automatically create the database.

Installation:

1. Unzip the package into a directory of your choice. The following directory set will be created: collector, bin, etc, rp, jboss-3.2.1, documentation. Also unpacked will be the installation script install.sh. This file is an sh shell script.
2. Run the supplied install.sh script as root, i.e. ./install.sh.

The script will now start the process of installing that application and the user will be required to answer several questions. The first test the scripts does is to check and see if the JAVA_HOME environment variable is set, if not it will exit and ask the user to set this variable. If JAVA_HOME is set, it will prompt the user for a directory to install the applications to, the suggestion provided is /usr/local/perpetual (**NOTE: you must enter the full path and omit trailing slashes**). The script will then prompt the user to enter the location of the Logstore database. The Logstore database will contain all current and archived event data (other than summarized data), the suggestion provided is /var/log/logstore. When choosing the location of the Logstore database take into consideration the possible amount of event data that will be collected. When these two questions are answered, the script will proceed to create a base configuration file (perpetual.conf), create the directories for the applications and logstore and set the proper permissions. The final step is creating the database and populating it with configuration data. The script allows for this to be done automatically or at a later point manually by the user. In order for the script to automatically create the database and populate it, MySQL must be already configured and running.

The installation is now complete and the source files may be deleted as needed to free up space.

Starting LogBOSS:

Two scripts are provided (they are exactly the same) to start the LogBOSS application. The scripts are located in /etc/rc.d/init.d and the bin directory of where the application was installed. To start LogBOSS use one of the scripts with the argument "start".

i.e. "/etc/rc.d/init.d/perpetual start"

i.e. "/usr/local/perpetual/bin/perpetual start"

The startup process takes approximately two minutes to complete. Once complete the user may point a browser at <http://localhost:8080> and will be shown the initial login screen.

Stopping LogBOSS:

The procedure to stop LogBOSS is exactly the same as above, however replacing the start argument with stop.

i.e. "/etc/rc.d/init.d/perpetual stop"

i.e. "/usr/local/perpetual/bin/perpetual stop"

Security:

It is important to note that there are several security issues in running LogBOSS that deal with the third party software it uses. In order to mitigate these Perpetual IP Systems GmbH suggests the following actions be taken to ensure a proper level of security is obtained.

1. The JBOSS Application server opens a number of TCP ports which are not directly used by the application, those ports are 8009, 8083, 8090, 8091, 8092, 8093, 1099 and 1701. It is recommended that the user filter these ports on linux using iptables/ipchains allowing only localhost and the primary ethernet interface access to them.
2. MySQL opens TCP port 3306 to allow network based connections and are used by the application. It is recommended the user allow only localhost and the primary ethernet interface access to this port again using iptables/ipchains.
3. The default password supplied for the MySQL database user is insecure as it is the default for all installations Perpetual IP Systems GmbH gives to customers. Therefore it is recommended that the user set a new password, this will need to be reflected in the both the MySQL database (see the MySQL documentation for changing a users password) and the underlying JDBC connection. The JDBC connection information is stored in the APPLICATION_HOME/jboss-3.2.1/server/default/deploy/mysql-ds.xml file. The file is text based and may be edited with any text editor.