Perpetual IP Systems GmbH
LogBOSS 1.2.1 Administration Guide

This guide is intended for administrators of the LogBOSS Application. It assumes the user is familiar with UNIX, UNIX commands, processes, editing and other aspects of UNIX System Administration.

The guide covers the following components of the LogBOSS Application; the Collector, the Record Processor, the Viewer and there associated configuration files. Each of these components have associated configuration files and or command line options which may be used to modify the behavior of the component at startup.

## Collector:

The Collector receives incoming event messages and processes them into the Logstore database. By default the Collector runs on UDP port 514 of the system. Certain older versions of syslogd (the UNIX syslog daemon) bind to this port as well as using sockets on the host, in the even that this is the case you may have to tell the Collector to run on a different port or configure the UNIX syslogd to not listen for network events (the Collector will do this).

## Collector usage:

The collector is a java jar file and requires the Java 2 binary (java) to start. It is outside the scope of this document to discuss command line arguments to the java binary itself. ***It is important to note that many of these options can be set in the Collector's configuration file itself (later discussed).***

Example command line:
/usr/java/j2sdk/bin/java -server -jar sherlock-collector.jar &

Any and all command line arguments to the collector jar file must come at the end (i.e. After sherlock-collector.jar). Below are the following options that may be used on the command line;

***-p*** <port number> The UDP port on which the collector will listen.

***-l*** <logstore directory> If the logstore directory is other than the default / var/log/logstore then the -l argument must be used to tell the collector where the logstore resides.

***-b*** <bind address> By default, the Collector binds to all available interfaces on the machine. Should this not be the desired case, or if you wish to run an additional Collector on another port, the -b option allows binding to a specific IP address/interface.

***-r*** <roll-over time in milliseconds> The Collector rolls over its collected event logs by default every hour. This behaviour can be changed using the -r switch.

***-f*** <config file> The Collector supports the ability to selectively forward messages on to other hosts. In order to do so, a config file must be created (format of this file is later discussed). The filename is independent and can be user selected. The config file however must reside in the APPLICATION_HOME/collector/res/properties directory.

**Collector configuration file:**

The configuration file for the collector contains a number of user editable options that govern how the Collector operates after starting. Many of these options are exactly the same as the command line arguments above. The Collector configuration file is located in APPLICATION_HOME/collector/res/properpties and is called sherlock-collector.properties.

***Port=514*** By default the Collector listens on UDP port 514. An administrator selectable port is available by changing the listed port number to a value the administrator requires.

***EnableForwarding="0" or "1"*** The Collector is able to forward event messages on to other hosts, Collectors and NMS Systems. The 0 value turns off forwarding, the 1 value turns forwarding of messages on. Should forwarding be turned on a configuration file is required to tell the Collector which messages should be sent to which hosts (file format discussed later).

***ForwardingConfigFile="example.conf"*** This is the name of the configuration file which the administrator has selected. It is required if forwarding is turned (see above, ***EnableForwarding***).

***collector.listener.NumberOfListenerThreads=*** This is the number of UDP listening threads to use at startup, the default setting is 10. The threads should be incremented in values of 5 to a maximum of 100. Performance and system stability beyond 100 threads is not currently supported.

***collector.listener.ThreadPriority=*** This is the java based priority of the threads in use at startup, the default is MAX_PRIORITY. This means that above all other processes on the Collector, the receiving threads have maximum priority on system resources. Availabe settings are NORM_PRIORITY and MIN_PRIORITY.

The Collector should never be set to a value of MIN_PRIORITY except in rare instances (please consult your reseller support representative for more information).

***collector.message.queue.InitialCapacity=*** This represents the default amount of messages that will be stored on the message queue after reception. The default is value is 10000 messages and should only be increased based on the EPS rating of the system to a maximum currently of 30000.

***collector.message.queue.CapacityIncrement=*** his represents the increment value of the message queue should the default value (10000) receive more messages than currently available to queue. Incrementation is automatic. The default value is 500 messages. The value should never be increased beyond the actual setting of collector.message.queue.InitialCapacity.

***collector.message.queue.GarbargeCollectionInterval=*** The time in miliseconds when the Collector removes entries from the current message queue that have been written to disk. The default value is 1000 miliseconds (1 second). Note that changing this option to a value of less than 500 miliseconds or greater than 1000 miliseconds may cause unexpected results.

***collector.message.queue.ProcessorIdleTime=*** The length of time the queue processor will remain idle before looking for new messages on the queue. This value should never be greater than the GarbageCollectionInterval.

***collector.log.WriterThreadPriority=*** This value represents the priority of the message writing thread. The default value is MIN_PRIORITY. The writing thread takes messages that are currently on the queue and writes them to disk. The value should not be greater than the collector.listener.ThreadPriority value. The available values are NORM_PRIORITY and MAX_PRIORITY.

**Collector Forwarding:**

The Collector supports the ability to selectively forward messages to additional hosts, Collectors and NMS Systems. The following describes the format of the forwarding file configuration (see ***EnableForwarding and ForwardingConfigFile***).

The format of this file is very similar to that of the standard UNIX syslogd syslog.conf file with a few notable exceptions. The format is as follows;

facility.severity<tab><tab>@<ip address>:<port>@<eps rate>

i.e. (note, no quotations marks are required in the configuration file).
“kernel.emergency @10.1.1.1:514@10”
“security.alert @10.1.1.2:514@50”

The above two examples would describe the following, forward all messages of facility “kernel” and severity “emergency” to host 10.1.1.1 on UDP port 514 at a maximum of 10 messages a second, forward all messages of facility “security” and severity “alert” to host 10.1.1.2 on UDP port 514 at a maximum of 50 messages per second. The eps value governs the maximum amount of messages that will be forwarded to host in a given second, messages over that rating will be dropped. If no <eps rate> is specified (i.e. No @10 or no @50) then all messages will be forwarded up the the eps key rating of the Collector itself.

Should a host be added to the forwarding configuration file after the Collector has started, the Collector will need to be restarted in order to forward messages to the newly added host.

**Record Processor:**

The Record Processor generates summary data from events stored by the Collector. This summary data is then stored into a database for ease of access.

**Route Processor usage:**

The Route Processor takes two command line arguments which are required for startup. These are the location of the Logstore database and the location of its own property files. The command lines are as follows;

***-Dsyslogdir=*** <full path to the Logstore database> The full path to the configured Logstore database.

***-Dperpetualhome=*** <full path to the RP res/properties directory> This is the full path to APPLICATION_HOME/rp/res/properties.

**Route Processor configuration file:**

The Record Processor's (RP) configuration file lives in APPLICATION_HOME/rp/res/properties/config and is called rp.properties. The following options may be set prior to the RP startup (note, if a change is made to this file the RP will have to be restarted).

***rp.threadpool.max.size=*** The maximum number of threads the RP will create when running. The threads are used in processing individual summaries for domains.

***rp.threadpool.init.size=*** The initial number of threads the RP will create on startup. If this value is set to 0 the RP will create threads are required up to the maximum setting of ***rp.threadpool.max.size***

***rp.db.refresh.interval=*** The RP looks at the database to get information about what summaries are required to run, the domain they belong to and the time to start them. This value indicates how often the RP will re-check the database for configuration changes.

***rp.lag.time=*** This value is in miliseconds and indicates the time the RP will lag when starting and stopping a scheduled summary.

## Viewer:

The Viewer is the primary user interface to the LogBOSS Application. It provides for both operaters and administrators to view, schedule, export event data, create domain specific sets of access rights for operaters and create new message patterns. This section of the guide is not intended to provide a users manual for the Viewer.

## Viewer usage:

The viewer takes two command line arguments which are required for startup. These are the location of the Logstore database the the RP configuration files.

***-Dsyslogdir=*** <full path to the Logstore database> The full path to the configured Logstore database.

***-Dperpetualhome=*** <full path to the RP res/properties directory> This is the full path to APPLICATION_HOME/rp/res/properties.

## Logging:

All system level events that are generated by the LogBOSS Application are stored via Log4j. The following are the locations of the various component level logfiles.

Collector – APPLICATION_HOME/collector/collector.log

Route Processor – APPLICATION_HOME/rp/rp.log

Viewer – APPLICATION_HOME/jboss-3.2.1/server/default/log/server.log

The default logging level is set to INFO. Do not change the logging level without prior to consulting Perpetual IP Systems GmbH or your reseller.