NASTEL
Driving Business Transaction Performance ®

LE 100.001

Log Expert
Installation and Usage Guide
Version 1.0

PUBLISHED BY:

RESEARCH & DEVELOPMENT

NASTEL TECHNOLOGIES, INC.

88 SUNNYSIDE BLVE, SUITE 101

PLAINVIEW, NY 11803

DOCUMENT TITLE: **LOG EXPERT INSTALLATION AND USAGE GUIDE**

VERSION: **1.0**

DOCUMENT RELEASE DATE: **MAY 2017**

NASTEL DOCUMENT NUMBER: **LE 100.001**

ACKNOWLEDGEMENTS:

THE FOLLOWING TERMS ARE TRADEMARKS OF NASTEL TECHNOLOGIES CORPORATION IN THE UNITED STATES OR OTHER COUNTRIES OR BOTH: TRANSACTIONWORKS, M6 AUTOPILOT, AUTOPILOT/IT, AUTOPILOT/ENTERPRISE, M6 FOR WMQ, AUTOPILOT/WMQ, M6 WEB SERVER, M6 WEB CONSOLE, AUTOPILOT/WEB, MQCONTROL, MQCONTROL EXPRESS, AUTOPILOT/TRANSACTION ANALYZER, AUTOPILOT/WAS, AUTOPILOT/TRANSACTION MONITOR, AUTOPILOT/OS MONITOR

THE FOLLOWING TERMS ARE TRADEMARKS OF THE IBM CORPORATION IN THE UNITED STATES OR OTHER COUNTRIES OR BOTH: IBM, MQ, MQSERIES, WEBSPHERE, WEBSPHERE MQ WIN-OS/2, AS/400, OS/2, DB2, AND AIX, Z/OS

THE FOLLOWING TERMS ARE TRADEMARKS OF HEWLETT-PACKARD IN THE UNITED STATES OR OTHER COUNTRIES OR BOTH: OPENVIEW, HP-UX

COMPAQ, THE COMPAQ LOGO, ALPHASERVER, COMPAQ INSIGHT MANAGER, CDA, DEC, DECNET, TRUCLUSTER, ULTRIX, AND VAX REGISTERED IN U.S. PATENT AND TRADEMARK OFFICE. ALPHA AND TRU64 ARE TRADEMARKS OF COMPAQ INFORMATION TECHNOLOGIES GROUP, L.P IN THE UNITED STATES AND OTHER COUNTRIES

SNMPC, SNMPC, WORKGROUP, AND SNMPC ENTERPRISE ARE TRADEMARKS OF CASTLE ROCK COMPUTING IN THE UNITED STATES OR OTHER COUNTRIES, OR BOTH.

SUN, SUN MICROSYSTEMS, THE SUN LOGO, IFORCE, JAVA, NETRA, N1, SOLARIS, SUN FIRE, SUN RAY, SUNSPECTRUM, SUN STOREDGE, SUNTONE, THE NETWORK IS THE COMPUTER, ALL TRADEMARKS AND LOGOS THAT CONTAIN SUN, SOLARIS, OR JAVA, AND CERTAIN OTHER TRADEMARKS AND LOGOS ARE TRADEMARKS OR REGISTERED TRADEMARKS OF SUN MICROSYSTEMS, INC. IN THE UNITED STATES AND OTHER COUNTRIES.

INSTALLANYWHERE IS A REGISTERED TRADEMARK OF ZEROG SOFTWARE IN THE UNITED STATES OR OTHER COUNTRIES, OR BOTH.

THIS PRODUCT INCLUDES SOFTWARE DEVELOPED BY THE APACHE SOFTWARE FOUNDATION (HTTP://WWW.APACHE.ORG/). THE JAKARTA PROJECT" AND "TOMCAT" AND THE ASSOCIATED LOGOS ARE REGISTERED TRADEMARKS OF THE APACHE SOFTWARE FOUNDATION

INTEL, PENTIUM AND INTEL486 ARE TRADEMARKS OR REGISTERED TRADEMARKS OF INTEL CORPORATION IN THE UNITED STATES, OR OTHER COUNTRIES, OR BOTH

MICROSOFT, WINDOWS, WINDOWS NT, WINDOWS XP, AND THE WINDOWS LOGOS ARE REGISTERED TRADEMARKS OF THE MICROSOFT CORPORATION.

UNIX IS A REGISTERED TRADEMARK IN THE UNITED STATES AND OTHER COUNTRIES LICENSED EXCLUSIVELY THROUGH X/OPEN COMPANY LIMITED.

"LINUX" AND THE LINUX LOGOS ARE REGISTERED TRADEMARKS OF LINUS TORVALDS, THE ORIGINAL AUTHOR OF THE LINUX KERNEL. ALL OTHER TITLES, APPLICATIONS, PRODUCTS, AND SO FORTH ARE COPYRIGHTED AND/OR TRADEMARKED BY THEIR RESPECTIVE AUTHORS.

SCO CUSA, SCO DOCTOR, SCO DOCTOR FOR NETWORKS, SCO DOCTOR LITE, SCO GLOBAL ACCESS, SCO MPX, SCO MULTIVIEW, SCO NIHONGO OPENSERVER, SCO OK, THE SCO OK LOGO, SCO OPENSERVER, SCO OPEN SERVER, SCO PORTFOLIO, SCO POS SYSTEM, SCO TOOLWARE, AND THE WORLD NEVER STOPS ARE TRADEMARKS OR REGISTERED TRADEMARKS OF CALDERA INTERNATIONAL, INC. IN THE U.S.A. AND OTHER COUNTRIES, ALL RIGHTS RESERVED.

ORACLE® IS A REGISTERED TRADEMARK OF ORACLE CORPORATION AND/OR ITS AFFILIATES

OTHER COMPANY, PRODUCT, AND SERVICE NAMES, MAY BE TRADEMARKS OR SERVICE MARKS OF OTHERS.

Contents

Figures

Tables

This Page Intentionally Left Blank

1 Introduction

The purpose of this document is to explain the basic concepts of Log Expert monitoring with AutoPilot M6.

1.1 History of This Document

Table 1-1. Document History

Release Date	Document Number	Version	Summary
May 2017	LE 100.001	1.0	Initial release

1.2 Architecture Review

The diagram below shows the basic AutoPilot M6 architecture.

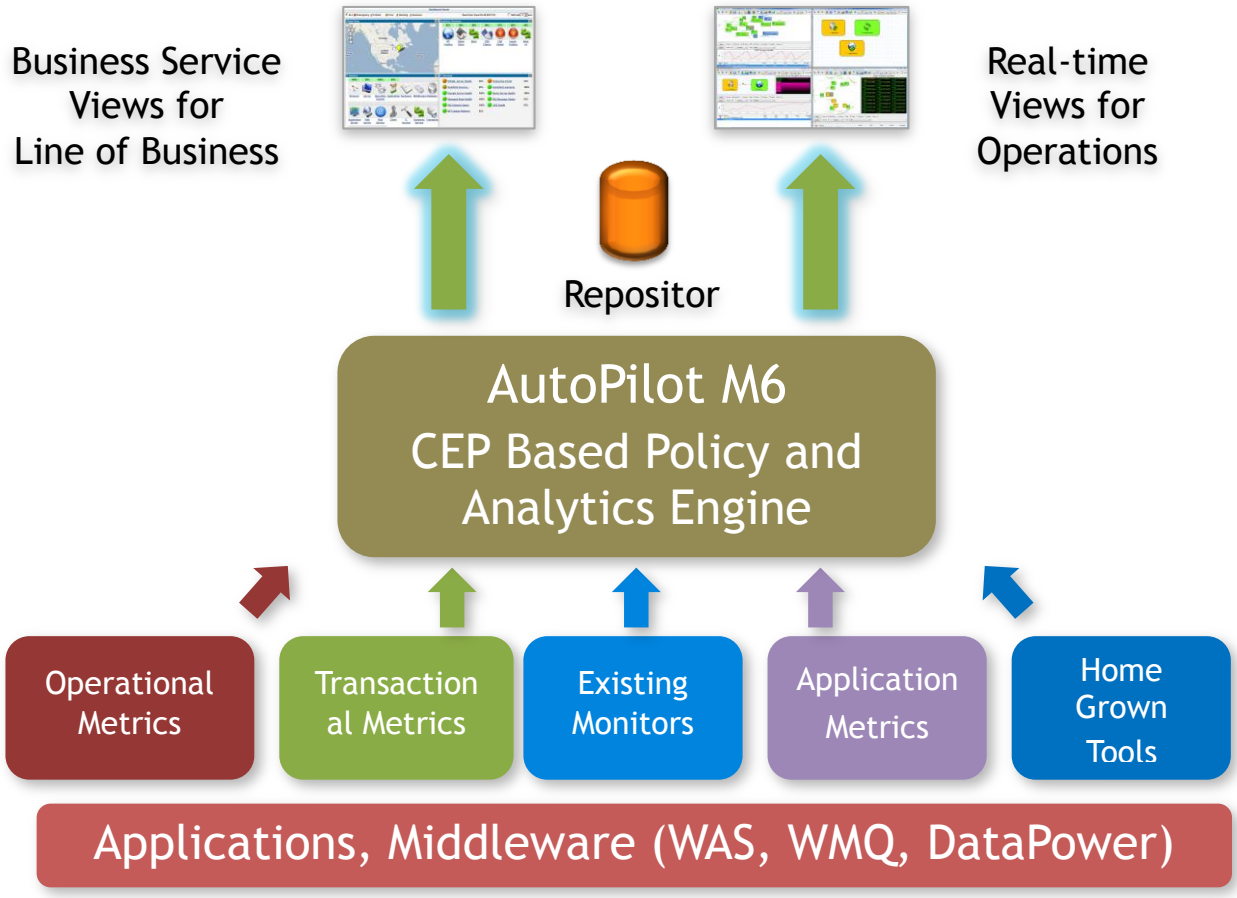

Figure 1. AutoPilot M6 Architecture

2 Log Data Collection

The log file data collection leverages three components:

- Log reader (section 2.1)
- Log analyzer (section 2.2)
- Log expert (section 2.3).

2.1 Log Reader

The log reader is responsible for reading one or more files on each of the target systems. As content is added to the files, that content is forwarded to the log analyzer for parsing. At least one log reader will execute on every target system with the files to be monitored. Multiple readers can be used to increase scalability.

2.2 Log Analyzer

The log analyzer is responsible for processing the log events forwarded from the log reader and identifying patterns that match specified criteria. The matching content is passed on to the log expert. The log analyzer will typically be paired with a log expert on the target system, but an analyzer can process more than one reader when needed. Multiple analyzers can be used to increase scalability.

2.3 Log Expert

The log expert is an instance of an AutoPilot process wrapper which publishes the facts to be used. The facts published are based on the log analyzer definitions. One or more experts can be used to separate the facts based on various conditions although this is not necessary.

The example below shows the most common configuration with one expert processing all log monitor facts:

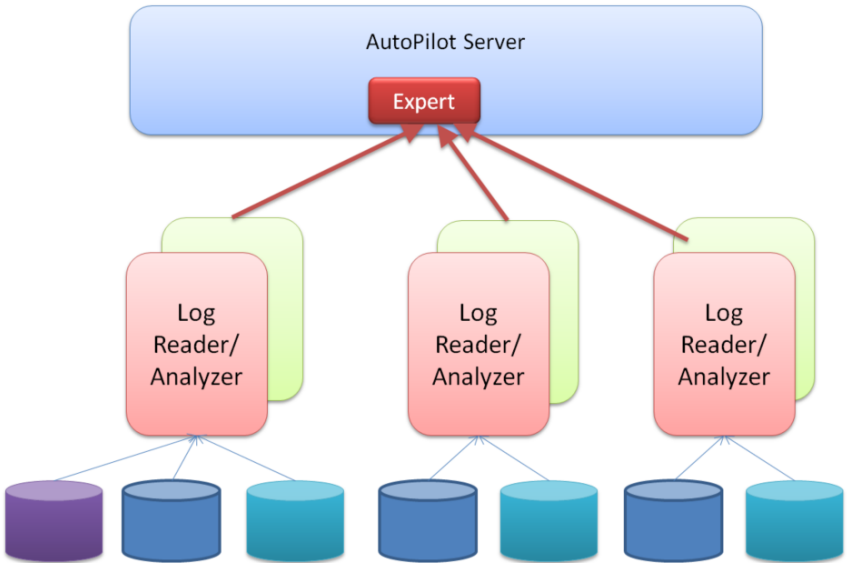

Figure 2. Configuration with One Expert

An alternate approach is with multiple experts receiving facts as shown in the figure below. Other combinations are possible based on configuration options.

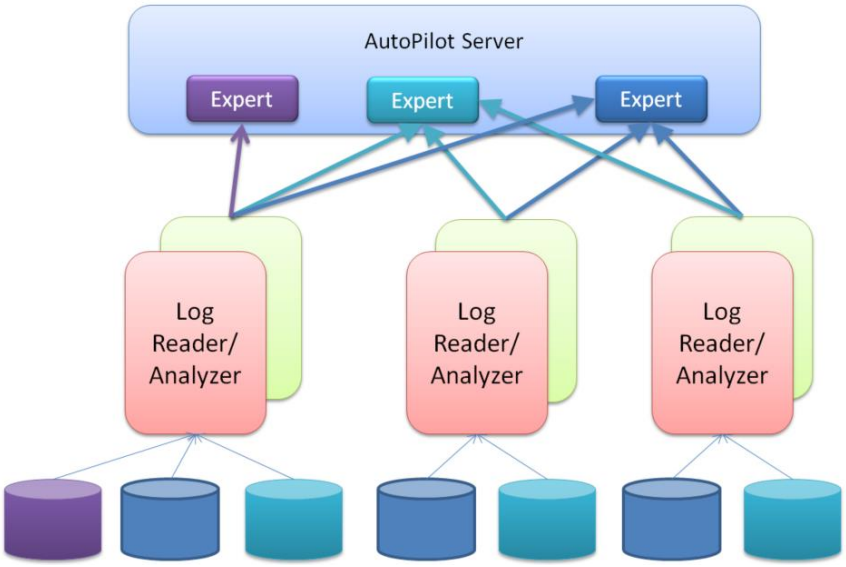

Figure 3. Configuration with Multiple Experts

3 Log Expert Setup

The first step is to add a process wrapper which acts as the log expert to receive the data from the analyzer. To deploy and configure an instance of a process wrapper:

1. Right click the desired CEP server.
2. Select **Deploy Expert > Wrappers > Process Wrapper**

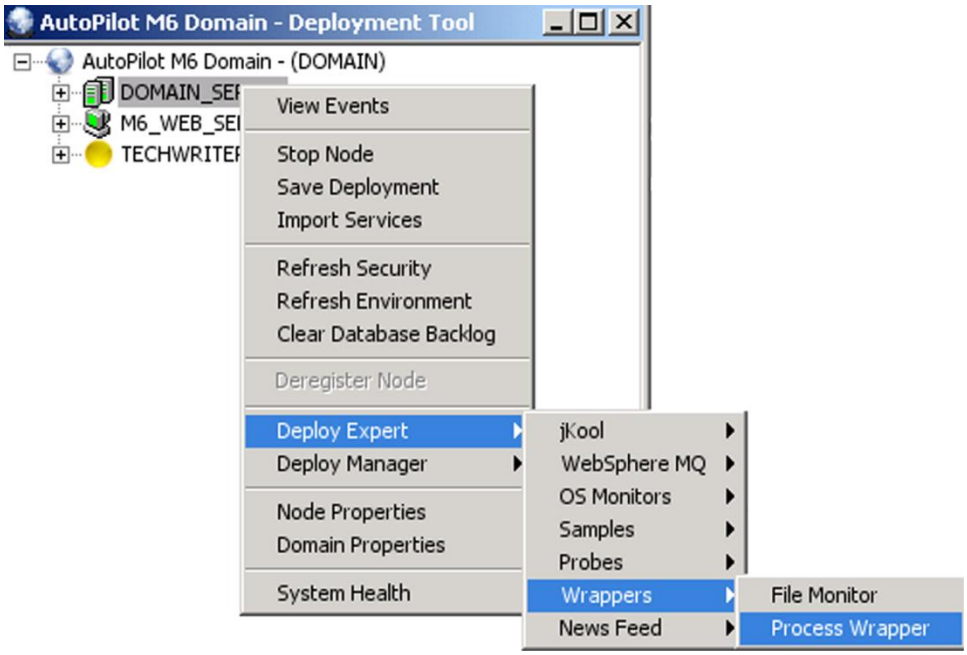

Figure 4. Add Process Wrapper

Give the process wrapper any **Name**, such as **LogExpert** and specify **Context** as **Log_Monitors**.

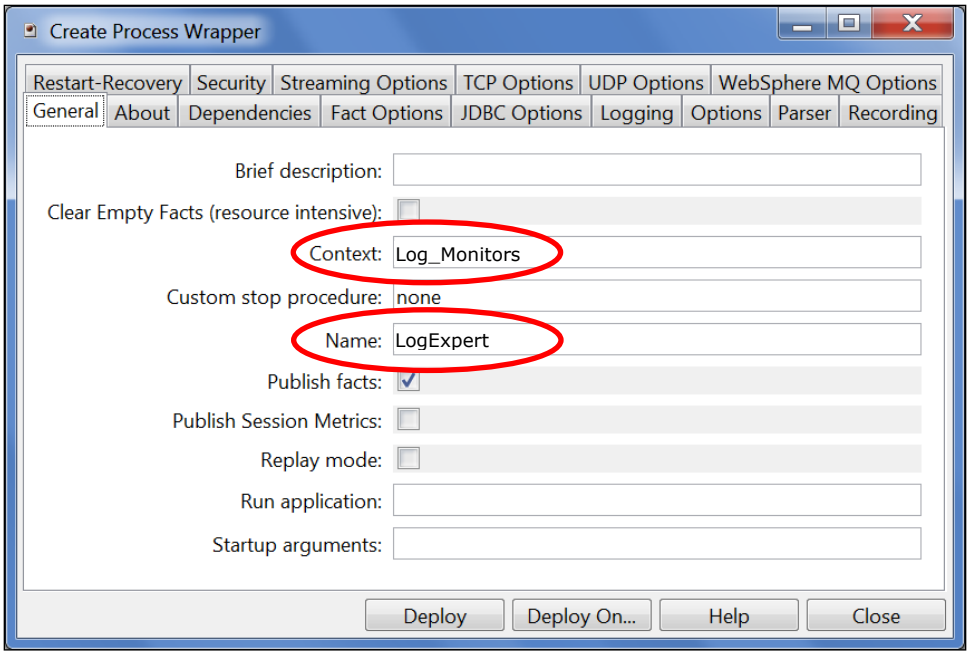

Figure 5. Configure Process Wrapper

The listening port is set on the **TCP Options** tab and can be any available port. In the example the listening pot is set as **8055**.

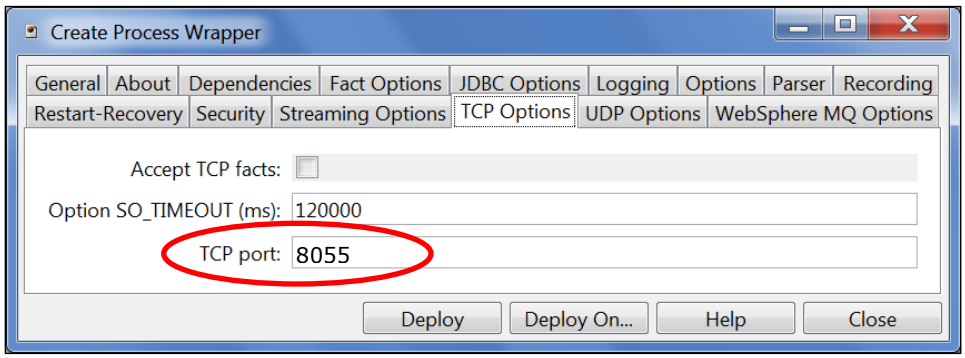

Figure 6. TCP Options

Once deployed, the expert will look similar to the figure below. Session stats will appear automatically over time. Other facts will display as they are published.

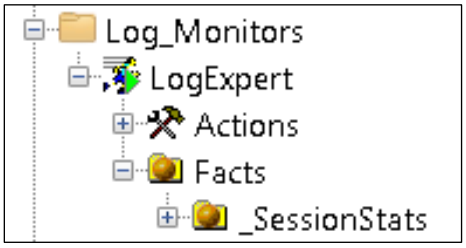

Figure 7. Log Expert

4 Log Reader and Analyzer Setup

The next step is to setup the pair of log readers and analyzers. There are four files which need to be reviewed:

- Two property files (section 4.1)
- Two xml configuration files (section 4.2).

4.1 Property Files

There are two property files. In most cases, these do not require changes.

- **logreader.properties** – contains settings for the reader run time (section 4.1.1)
- **loganalyzer-expert.properties** – contains settings for the analyzer run time (section 4.1.2).

4.1.1 logreader.properties

- Time out value for sending to AutoPilot Expert:
  - execTimeout=0
- Seconds to wait before retrying reading file after read failure:
  - discovery=0
- Reference to file definition file:
  - expertContext=logreader-context.xml
- Log file options:
  - workDirectory=./
  - logFile=logreader-expert.log

4.1.2 loganalyzer-expert.properties

- Reference to search file:
  - expertContext=loganalyzer-expert-context.xml
- Log file options:
  - workDirectory=./
  - logFile=loganalyzer-expert.log
  - logSize=1048576
  - logCount=5
  - logLevel=ALL|INFO|WARNING|SEVERE (ALL is best for debugging)
- Port refresh options:
  - portRefreshConfig=9999

4.2 XML Configuration Files

There are two xml configuration files:

- **logreader-context.xml** – specifies the files to be processed (section 4.2.1)
- **loganalyzer-expert-context.xml** – contains the search strings to be matched (section 4.2.2).

4.2.1 logreader-context.xml

This file specifies the files to be processed. The following attributes are used:

- file (repeat once for each file to be read)
  - **id** – used to reference a specific file scanner. Must match values in the analyzer file.
  - **name** – file name to be scanned
    (follows OS conventions; e.g. `C:\abc.txt` or `/tmp/abc.txt`)
  - **discovery** – the interval, in milliseconds, between scans attempts
  - **host** – the host where the analyzer is running (typically localhost)
  - **port** – the port where the analyzer is listening.

Sample File

```
<?xml version="1.0" encoding="UTF-8"?>
<logreader-config>
   <files>
      <file id="MQLOGFILE">
         <name>/var/mqm/errors/AMQERR01.LOG</name>
         <discovery>1000</discovery>
         <server>
            <host>localhost</host>
            <port>11234</port>
         </server>
      </file>
      <file id="DBLOGFILE">
         <name>/usr/database/mylog.log</name>
         <discovery>5000</discovery>
         <server>
            <host>localhost</host>
            <port>11234</port>
         </server>
      </file>
   </files>
</logreader-config>
```


4.2.2 loganalyzer-expert-context.xml

This file specifies the text strings to be found.. The following attributes are used:

- **autopilot-servers** – may be repeated for multiple log experts
  - **autopilot-server id** – the id for an instance of AutoPilot Server
  - **host** – the host where the log expert is running
  - **port** – the port for the log expert listening for these events
- **events-handlers** – repeated for each incoming content stream from the reader
  - **events-handler fact-name** – the name these facts will be published under
  - **autopilot-server** – the matching server for these facts
  - **port-listener** – the port that the analyzer listens to (must match port reader sends to)
  - **source id** – the source id for the events sent from the reader
  - **event** – repeated for each unique search string
    - **fact-name** – name to identify this matching set
    - **starts-with/contains/ends-with** – content to match from incoming events
    - **text-size** – amount of content to forward to AutoPilot Expert

Sample File

```
<?xml version="1.0" encoding="UTF-8"?>
<analyzer-expert-config>
   <autopilot-servers>
      <autopilot-server id="LOGEXPERT1">
         <host>APSERVER.us.com</host>
         <port>8055</port>
      </autopilot-server>
   </autopilot-servers>
   <events-handlers>
       <events-handler fact-name="LOG FILES" autopilot-server="LOGEXPERT1"
disabled="false">
         <port-listener>11234</port-listener>
         <source id="MQLOGFILE">
            <event fact-name="ClientConnectFail">
               <starts-with></starts-with>
               <contains>AMQ9202</contains>
               <ends-with></ends-with>
               <text-size>100</text-size>
            </event>
            <event fact-name="CMDSTART">
               <starts-with></starts-with>
               <contains>AMQ5024</contains>
               <ends-with></ends-with>
               <text-size>100</text-size>
            </event>
         </source>
        <source id="DBLOGFILE">
           <event fact-name="DBFail">
              <starts-with> Failure::</starts-with>
              <contains></contains>
              <ends-with></ends-with>
              <text-size>200</text-size>
           </event>
        </source>
      </events-handler>
   </events-handlers>
</analyzer-expert-config>
```


5 Starting the Log Reader and Analyzer

Once the properties and configuration files have been created, the log reader and log analyzer must be started on the target system. The log reader and analyzer are shipped as jar files.

	NOTE:	For best results, start the log analyzer before the log reader and after AutoPilot server startup.

To start them, issue the following commands:

- **Log Analyzer**
  ```
  java -jar loganalyzer.jar
  ```
- Log Reader
  ```
  java -jar logreader.jar
  ```

5.1 Sample Usage

The following is a walk-through of the processing using the examples in the previous sections.

1. The AutoPilot Server starts and log expert begins listening for facts on port **8055**. (The port was configured in Figure 6.)
2. The log analyzer starts and begins listening for content on port **11234.**
3. The log reader starts and positions at the end of the two files indicated in **logreader-context.xml**, section 4.2.1:
   a. **/var/mqm/errors/AMQERR01.LOG**
   b. **/usr/database/mylog.log**
4. When new content is added to either file, the log reader sends the content to the port **11234** indicating the source of the content (**MQLOGFILE** or **DBLOGFILE**).
5. When the content is received, the log analyzer matches it with the source ids and processes the content according to the source rules:
   a. If **MQLOGFILE**, it searches for **AMQ9202** and **AMQ5024** anywhere in the content
   b. If **DBLOGFILE**, it searches for lines starting with **Failure.**
6. When it gets a match, for example **AMQ9202**, it sends **100** bytes of the message to **LOGEXPERT1** which is defined as port **8055** on server **APSERVER.us.com** identifying that the matching rule as **ClientConnectFail**.
7. The log expert publishes the facts.
8. The process repeats (steps 4 – 7).

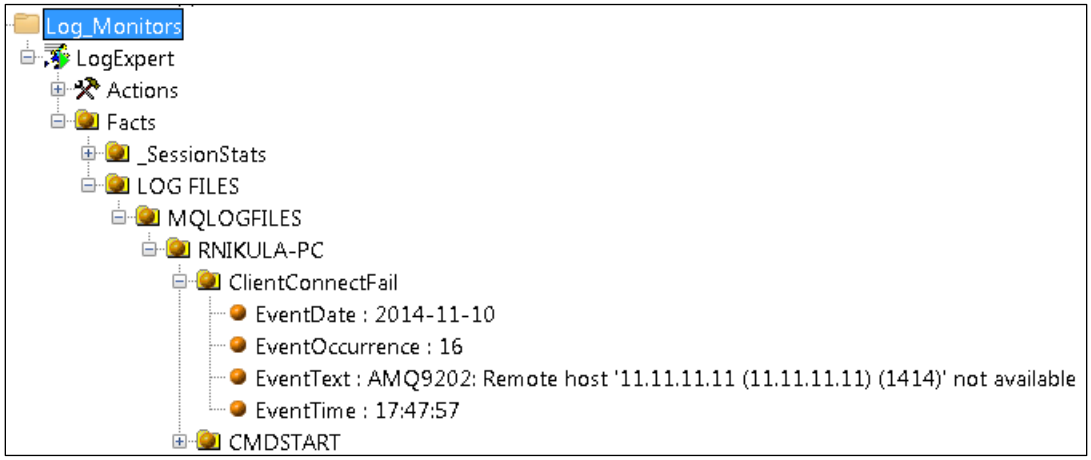

Figure 8. Log Monitor Results

