



EMC® Watch4net®

Version 6.4u2

Audit Logging Configuration Guide

P/N: pending

Rev : 40032

EMC²

Copyright ©2011 - 2014 EMC Corporation. All rights reserved. Published in the USA.

Published October, 2014

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC², EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (<https://support.emc.com>).

Contents

Preface	iii
Overview	iii
Intended Audience	iii
Common Abbreviations and Acronyms	iii
Where to get help	v
1 Installation and Configuration	1
1 Installation	1
2 Configuration	1
2 Handlers	3
1 RotateFileHandler	3
2 UDPHandler	4
2.1 Configuration	4
2.2 Examples	5
3 Formatters	7
1 APGLogFormatter	7
1.1 Configuration	7
1.2 formattedString	8
4 Filters	11
1 MDCFilter	11
2 MarkerNameFilter	12
5 Audit Logs	13
1 Configuration	13
2 Line by Line	14

Preface

Overview

During APG execution, log messages are generated by APG's services. These messages are handled using mostly Java Logging. However for specific needs, especially for Audit Logs, some more facilities are provided by APG.

Intended Audience

This guide requires a good knowledge and understanding of the Java Logging API. For an overview see <http://download.oracle.com/javase/6/docs/technotes/guides/logging/overview.html>.

Common Abbreviations and Acronyms

<APG>	refers to the APG installation directory
<instance>	refers to the Tomcat Web-Server instance name

Where to get help

EMC support, product, and licensing information can be obtained as follows:

PRODUCT INFORMATION - For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at:

<https://support.emc.com>

TECHNICAL SUPPORT - Go to EMC Online Support and click Service Center. You will see several options for contacting EMC Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

1

Installation and Configuration

1 Installation

APG Logging is not a module by itself. It is shipped by any APG's module that need to generate log messages.

2 Configuration

Logging is configured in the `logging.properties` configuration file of each APG's service. For Tomcat Web-Server, the configuration file is located at `<APG>/Web-Servers/Tomcat/<instance>/conf/logging.properties`.

2

Handlers

In addition to the standard handlers included in Java:

<http://download.oracle.com/javase/6/docs/technotes/guides/logging/overview.html#1.5>, APG provides two more handlers.

1 RotateFileHandler

The `RotateFileHandler` appends log messages to a file in a configured directory. The file is named using the pattern `<prefix><date><suffix>` where `<prefix>` and `<suffix>` are user specified and `<date>` corresponds to the current date. Each day at midnight a new log file is created with a name reflecting the updated date.

The following configuration properties are available for the Handler:

- `directory` - The directory where to create the log files. If the path is not absolute, it is relative to the current working directory of the application. Default value: `logs`.
- `maxDays` - Log files older than this value in days are deleted. Default value: 30.
- `prefix` - The leading part of the log file name. Default value: `"apg."`.

- `suffix` - The trailing part of the log file name. Default value: `".log"`.
- `bufferSize` - Configures buffering. The value of 0 uses system default buffering (typically an 8K buffer will be used). A negative value deactivate buffering and forces a writer flush upon each log write. A positive value defines the size in bytes of the buffer. In this case, the system default buffering will also be applied. Default value: `-1`.
- `encoding` - Character set used by the log file (for example UTF-8). Default value: the system default character set.
- `level` - The level threshold for this Handler. Default value: `ALL`.
- `filter` - The Filter implementation class name for this Handler. Default value: no Filter.
- `formatter` - The Formatter implementation class name for this Handler. Default value: `java.util.logging.Simple`

For an example of configuration for a `RotateFileHandler` see [Audit Logs](#) on page 13.

2 UDPHandler

This Handler sends every log message it receives through an UDP packet to the specified endpoint.

2.1 Configuration

The following configuration properties are available:

- `address` - The end point where to send the packets. Default value: `localhost`
- `port` - The end point port where to send the packets. Default value: `514`
- `bufferSize` - Configures buffering. The value of 0 uses system default buffering (typically an 8K buffer will be used). A negative value deactivate buffering and forces a writer flush upon each log write. A positive value defines the size in bytes of the buffer. In this case, the system default buffering will also be applied. Default value: `-1`.
- `encoding` - Character set used by the log file (for example UTF-8). Default value: the system default character set.
- `level` - The level threshold for this Handler. Default value: `ALL`
- `filter` - The Filter implementation class name for this Handler. Default value: no Filter.
- `formatter` - The Formatter implementation class name for this Handler. Default value: `java.util.logging.Simple`

2.2 Examples

The following `UDPHandler` sends logs message on port 1234 of `localhost`. Only warnings or more critical messages are sent and they are formatted using the standard `XMLFormatter`. Since the `bufferSize` parameter is not specified, each message is sent immediately through an UDP packet after generation.

```
com.watch4net.apg.logging.jul.handler.UDPHandler.address=localhost
com.watch4net.apg.logging.jul.handler.UDPHandler.port=1234
com.watch4net.apg.logging.jul.handler.UDPHandler.level=WARNING
com.watch4net.apg.logging.jul.handler.UDPHandler.formatter=java.util.logging.XMLFormatter
```

The following `UDPHandler` sends *syslog* formatted messages on `localhost`, port 514.

```
12apgauditsyslog.com.watch4net.apg.logging.jul.handler.UDPHandler.address = 127.0.0.1
12apgauditsyslog.com.watch4net.apg.logging.jul.handler.UDPHandler.port = 514
12apgauditsyslog.com.watch4net.apg.logging.jul.handler.UDPHandler.level = ALL
12apgauditsyslog.com.watch4net.apg.logging.jul.handler.UDPHandler.filter = com.watch4net.apg.
logging.jul.filter.MarkerNameFilter
12apgauditsyslog.com.watch4net.apg.logging.jul.handler.UDPHandler.formatter = com.watch4net.apg.
logging.jul.formatter.APGLogFormatter
12apgauditsyslog.com.watch4net.apg.logging.jul.filter.MarkerNameFilter.regex=AUDIT
12apgauditsyslog.com.watch4net.apg.logging.jul.formatter.APGLogFormatter.formattedString = <{%{
syslogSeverity}>1 {%{date,yyyy-MM-dd'T'HH:mm:ssZ} {%{hostname,-} APG - EDIT [info@32473 module="
{%MDC,application}" code="%{MDC,message.code}" user="%{MDC,username}"] [origin enterpriseId="
32473" software="APG" swVersion="6.0"] {%message}
12apgauditsyslog.com.watch4net.apg.logging.jul.formatter.APGLogFormatter.nullAsEmpty = true
```


Formatters

In addition to the standard formatters included in Java:
<http://download.oracle.com/javase/6/docs/technotes/guides/logging/overview.html#1.6>, APG provides a formatter designed for Audit logs generation.

1 APGLogFormatter

1.1 Configuration

This formatter is defined by two properties:

- `formattedString` - String containing markers which are replaced by information contained in `LogRecord` to produce the final log entry. See section [formattedString](#) for details.
- `nullAsEmpty` - If set to `true`, markers are removed when the corresponding information is missing. If set to `false` they are replaced by the string `"null"`.

For an example of configuration for an `APGLogFormatter` see [Audit Logs](#) on page [13](#).

1.2 formattedString

This string contains markers that follow the pattern: `%{name[, param1, param2, ...]}` where `name` is the name of the property to retrieve and `param<x>` are optional parameters. During log generation, each pattern is replaced by the corresponding information in the `LogRecord`. Other characters in the `formattedString` are left untouched. If the marker is not recognized it is also left unmodified. For example, `%{foobar}` will be formatted as `%{foobar}` because there is no `foobar` marker.

The list of recognized markers in the `formattedString` is:

- `%{date[,format]}` - Returns the `LogRecord` generation time. The time is formatted according to the format specified by the `java.text.SimpleDateFormat` class. If there is no format, the JVM Locale will be used as the default format.
- `%{hostname[,default]}` - Returns the canonical hostname if found or the default value otherwise.
- `%{level}` - Returns the `LogRecord`'s level name.
- `%{loggerName}` - Returns the name of the logger which produces the log.
- `%{markerName}` - Returns the name of the Marker associated to the `LogRecord`.
- `%{MDC, key}` - Returns the value associated to the key-value pair in the MDC context. For further explanation on MDC, see <http://www.slf4j.org/manual.html#mdc>.
- `%{message}` - Returns the message of the `LogRecord`.
- `%{millis}` - Returns the number of milliseconds since January 1st 1970 of the `LogRecord` generation time.
- `%{sequenceNumber}` - Returns the sequence number of this `LogRecord`.
- `%{sourceClassName}` - Returns the Class name where the log comes from.
- `%{sourceMethodName}` - Returns the Method name where the log comes from.
- `%{syslogSeverity, code}` - Returns the severity according to the syslog specification using code as facility (see <http://tools.ietf.org/html/rfc5424#section-6.2.1>). The severity is an association from the `java.util.logging.Level` to a severity code.

Java Level	Syslog Severity
SEVERE	2
WARNING	4
INFO	6
FINE and below	7

- `%{system, property, default}` - Returns the value associated to the specified system property or the default value if the property doesn't exist.
- `%{threadName}` - Returns the thread name where the log comes from.
- `%{threadID}` - Returns the `LogRecord` internal thread Id.
- `%{thrown}` - Returns any `Throwable` associated to the `LogRecord`.

Filters

APG provides two filters which can be used to select only a certain kind of `LogRecord` and discard others.

1 MDCFilter

This Filter acts upon the information available in the MDC context. It is matched against the value of a given MDC property key-value pair in the MDC context. For further explanation on MDC, see <http://www.slf4j.org/manual.html#mdc>.

Two configuration fields are available:

- `property` - Name of the MDC property on which the filter is applied. If not configured, the filter discards all `LogRecords`.
- `regex` - The filter only selects `LogRecord` when the value of the selected MDC property matches this regular expression. If not configured and the MDC property is available, the filter accepts all `LogRecords`.

2 MarkerNameFilter

This Filter matches a regular expression against a Marker contained in LogRecords. If the pattern is null, all LogRecords containing a Marker are selected.

To define the regular expression to filter on, the property `regex` must be set to a pattern.

For example this configuration selects only LogRecords having a Marker named "AUDIT".

```
com.watch4net.apg.logging.jul.filter.MarkerNameFilter.regex = AUDIT
```

Audit Logs

APG's Tomcat Web-Server produces specific logs upon user interaction, called Audit Logs. These logs can be retrieved among other logs through their Marker named `AUDIT`. Practically, every `LogRecord` having a marker named `AUDIT` is an audit log.

1 Configuration

In the logging configuration of Tomcat the handler for Audit logs is `RotateFileHandler` and its configuration is:

```
11apgaudit.com.watch4net.apg.logging.jul.handler.RotateFileHandler.prefix = audit.  
11apgaudit.com.watch4net.apg.logging.jul.handler.RotateFileHandler.level = ALL  
11apgaudit.com.watch4net.apg.logging.jul.handler.RotateFileHandler.directory = ${catalina.base  
}/logs  
11apgaudit.com.watch4net.apg.logging.jul.handler.RotateFileHandler.filter = com.watch4net.apg.  
logging.jul.filter.MarkerNameFilter  
11apgaudit.com.watch4net.apg.logging.jul.handler.RotateFileHandler.formatter = com.watch4net.  
apg.logging.jul.formatter.APGLogFormatter
```

```
11apgaudit.com.watch4net.apg.logging.jul.filter.MarkerNameFilter.regex=AUDIT

11apgaudit.com.watch4net.apg.logging.jul.formatter.APGLogFormatter.formattedString = %{date,
yyyy-MM-dd'T'HH:mm:ssZ} - %{level} - %{MDC,application} - %{markerName} - %{MDC,username} : %{
MDC,message_code} - %{message}

11apgaudit.com.watch4net.apg.logging.jul.formatter.APGLogFormatter.nullAsEmpty = true
```

Note: In Tomcat logging.properties file, a prefix may be added to handler names. This allows multiple handlers of a single class to be instantiated. A prefix is a String which starts with a digit, and ends with `'.'`.

2 Line by Line

```
11apgaudit.com.watch4net.apg.logging.jul.handler.RotateFileHandler.prefix = audit.
```

This line defines the names of the generated log files. Only the prefix of the file name is specified, leaving the suffix to its default value (`.log`). Consequently, the Audit log files will be named after the pattern `audit.<date>.log` where date is the date when log files have been generated.

```
11apgaudit.com.watch4net.apg.logging.jul.handler.RotateFileHandler.directory = ${catalina.base}
/logs
```

This line specifies the folder where the Audit log files will be stored. In Tomcat logging.properties file the property `${catalina.base}` can be used. It is automatically replaced by the Tomcat instance's root directory. Consequently, the logs will be stored in `<APG>/Web-Servers/Tomcat/<instance>/logs`.

```
11apgaudit.com.watch4net.apg.logging.jul.handler.RotateFileHandler.level = ALL
```

This line is used to filter log message depending on their severity. In the default configuration, all Audit logs are appended to the log file.

```
11apgaudit.com.watch4net.apg.logging.jul.handler.RotateFileHandler.filter = com.watch4net.apg.
logging.jul.filter.MarkerNameFilter
```

```
11apgaudit.com.watch4net.apg.logging.jul.filter.MarkerNameFilter.regex=AUDIT
```

These two lines setup a filter that selects only Audit logs among all generated logs. For more details on MarkerNameFilter see section [MarkerNameFilter](#) on page 12

```
11apgaudit.com.watch4net.apg.logging.jul.handler.RotateFileHandler.formatter = com.watch4net.apg.logging.jul.formatter.APGLogFormatter
```

```
11apgaudit.com.watch4net.apg.logging.jul.formatter.APGLogFormatter.formattedString = %{date, yyyy-MM-dd'T'HH:mm:ssZ} - %{level} - %{MDC,application} - %{markerName} - %{MDC,username} : %{MDC,message_code} - %{message}
11apgaudit.com.watch4net.apg.logging.jul.formatter.APGLogFormatter.nullAsEmpty = true
```

This is the setup for the Formatter for Audit logs.

This formatter will generate log entries such as:

```
2011-10-04T11:19:07-0400 - INFO - - AUDIT - admin : APPLICATION_ACCESS_000 - Access to web application '/APG' has been granted to user 'admin'.
```

In this log entry example, the application name could not be retrieved from the MDC context and is replaced by an empty string as specified by the field `nullAsEmpty`.