Enabling Syslog Messages as an ESA notification provider on Mac OS X Mavericks.

Table of Contents

Overview

Syslog is one of the user configurable notification providers supported by ESA server notification framework. This document describes the steps needed to enable syslog messages to be received for alert notifications. This document is specific to receiving alerts on the Mac OS X development setup. MessageBus, Mongo and Debug are system level notification providers that are enabled by default.

Mac OS X setup

By default Mavericks doesn't enable the syslogd to listen on the UDP port. The following changes need to be made to support this.

1. Edit the syslogd property list file to enable listening on UDP port
   `sudo /usr/libexec/PlistBuddy /System/Library/LaunchDaemons/com.apple.syslogd.plist`
   This will open a shell prefixed by Command. Type the following in the command shell.

   ```
   add :Sockets:NetworkListener dict

   add :Sockets:NetworkListener:SockServiceName string syslog

   add :Sockets:NetworkListener:SockType string dgram

   save

   exit
   ```

2. Enable printing user facility messages to /var/log/user.log. This requires editing the /etc/asl.conf in sudo. Add the following line to the file
   `? [= Facility user] [<= Level info] file user.log file_max=5M all_max=50M`

3. Restart the syslogd

```
cd /System/Library/LaunchDaemons/

sudo launchctl unload com.apple.syslogd.plist

sudo launchctl load com.apple.syslogd.plist
```

ESA Server configuration

1. Start the esa server.
2. Using the carlos connected esa client add the syslog provider using the command
   `notification-provider-set-syslog --server localhost --name MacOsXSyslog`
   This should add the syslog provider and return the uuid of the provider that has been added. The existing providers can be listed using notification-provider-get. The default syslog provider uses UDP to send messages and the facility is set to USER.
3. Bind this to the existing alert module that has already been loaded using epl-module-set
   `epl-module-bind-notification <alert-module-uuid> --binding p=<syslog-provider-uuid>`
   The alert module uuid is obtained when epl-module-set is invoked to add a new alert module.

With these changes any alerts generated by the bound module will show up in the /var/log/user.log file. An example output looks as follows

```
Aug 24 11:14:17 localhost CEF <Info>: 0|RSA|Security Analytics ESA|10.4|d1f23224-5a83-463d-9e5c-9b42f5fc9d51||5|rt=2014-08-24T18:14Z id=fdadb737-4eb9-4a4d-8bf9-5585c6d5cbbe source=Test:1
```

The output format of the syslog messages is controlled by the syslog.ftl freemarker template file that is available at esa/core/src/main/resources/freemarker/syslog.ftl.