# Leveraging Emond on macOS For Persistence

The launchd config file is located where other system daemons reside: */Sy* …n the … regularly used with LaunchDaemons. The emond.plist config file is located in the */etc/emond.d/* directory. This file defines the locations for rules paths, UID/GID filters, error and event log paths, and a few other options.



**Figure 1: emond.plist contents**

For rules, they're stored in the */etc/emond.d/rules/* directory and they should be



and the action once the event triggers. There are several event types (*startup, periodic, auth.success, auth.failure, etc.*) but for this demonstration we will only use *startup*. The *startup* event type will trigger the rule once it has been loaded by emond. The *periodic* event type will only trigger once the defined 'startTime' has elapsed. The *auth.success* event type will only trigger once a user successfully authenticates, and *auth.failure* will trigger on authentication failure events. There are references to other event types here

action. Thus, any commands that require network access will not work.



To craft a rule file, we will utilize the SampleRule.plist file that already exists and modify it as necessary.

**Figure 2: SampleRules.plist**

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
```

the name if desired. The defined actions need to be modified for the *run* co ble as



**Figure 3: Example persistence rule**

Notice that the first action is to sleep for 10 seconds in order to wait with the hope that network access will become available. The amount of time is just a rough estimate and may vary across hosts. The second action will just curl a

file specifically but emond will stop complaining about not finding any ru



**Figure 5: emond error log after starting the service**

FSEvent log files are stored in a gzip compressed format and follow a he
*/.fs*



caveat for fsevents are that timestamps are not included with entries in the log file. With access to the API, we can use Python or Objective-C to sift through all received events and alert once an event for file creation/modification occurs in the rules directory or the QueueDirectory.

For a simple example, we can use the fswatch open-source project to monitor for changes. It offers support for multiple platforms, thorough

**Figure 9:Output When Event Fires**



This is a very rudimentary example and may not be the best solution in a

The log entry shown above is also available here. These methods of de ut th



## References

Levin, J. (2017) *OS Internals, Volume I: User Space*. North Castle, NY: Technologeeks.com

Reynolds, J. (2016, April). *What is emond?*. Retrieved from:

## Written by Christopher Ross

109 Followers · Writer for Posts By SpecterOps Team Members

Follow

Hope Walk... in Posts By SpecterOps Team Memb...

**An Introduction to Manual Active Directory Querying with Dsquery...**

Introduction

Christopher R... in Posts By SpecterOps Team Me...

**No Place Like Chrome**

Chrome extensions were first introduced to the public in December of 2009 and use...

**W**
**buildable folders instead of groups**

I've recently migrated Ice Cubes, my open-source SwiftUI Mastodon client to use file...

6d ago

A great language strangled by governance

3d ago

F. Perry Wilson, MD MSCE

Karthick Dkk in devsecops-community