

Open in app

Sign in

Medium

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.



Leveraging Emond on macOS For Persistence



Christopher Ross · [Follow](#)



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

The `launchd` config file is located where other system daemons reside:

`/System/Library/LaunchDaemons/com.specterops.emond.plist` 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.

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

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

For rules, they're stored in the `/etc/emond.d/rules/` directory and they should be disabled by default. To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

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

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

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

Ne To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

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">
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

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

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Figure 3: Example persistence rule

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

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 enable

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

file specifically but emond will stop complaining about not finding any

ru

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Figure 5: emond error log after starting the service

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

FSEvent log files are stored in a gzip compressed format and follow a

he
To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#),
including cookie policy.

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

Medium

Sign up to discover human stories that deepen your understanding of the
world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

Figure 9: Output When Event Fires

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

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

de To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

References

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

Dennis, L. (2016, April). *What is user 12*. Retrieved from

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Written by Christopher Ross

109 Followers · Writer for Posts By SpecterOps Team Members

Follow



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

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...

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

W buildable folders instead of groups

A great language strangled by governance

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

★ 6d ago



★ 3d ago



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month



To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.



F. Perry Wilson, MD MSCE 



Karthick Dkk in devsecops-community

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month