Open in app

Medi

To make Medium work, we log user data. By using Medium, you agree to our <u>Privacy Policy</u>, including cookie policy.

Sign in

X

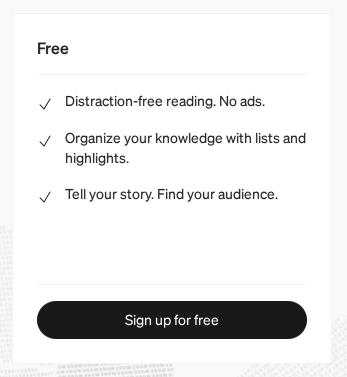


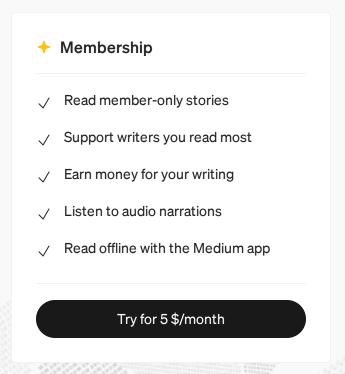
Leveraging Emond on macOS For Persistence



Christopher Ross · Follow

Medium





The launched config file is located where other system daemons reside:

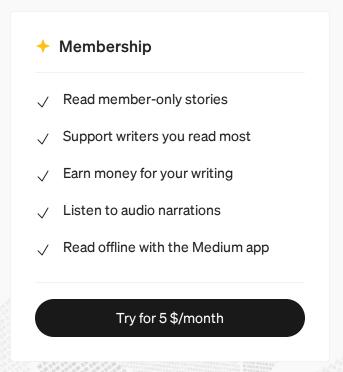
/Sj To make Medium work, we log user data. By using Medium, you agree to our Privacy Policy, including cookie policy.

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

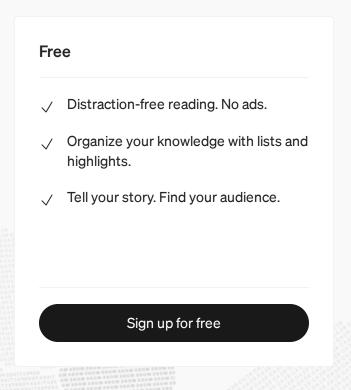




For rules, they're stored in the letelement dirules directory and they should be To make Medium work, we log user data. By using Medium, you agree to our Privacy Policy, including cookie policy.

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

Medium





action. Thus any commands that require notwork access will not work

No make Medium work, we log user data. By using Medium, you agree to our <u>Privacy Policy</u>, 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





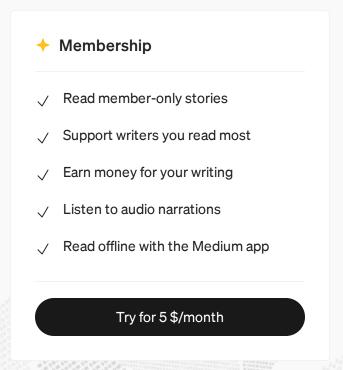
the name if desired. The defined actions need to be modified for the run

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





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

Medium

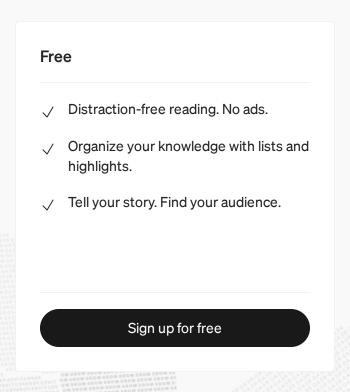
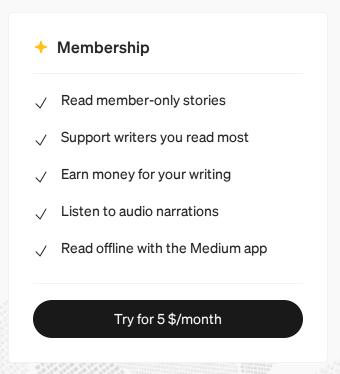




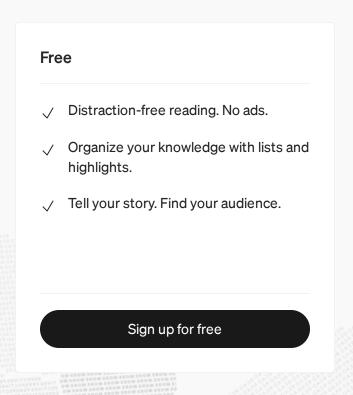
Figure 5: emond error log after starting the service

Medium





Medium





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

Medium

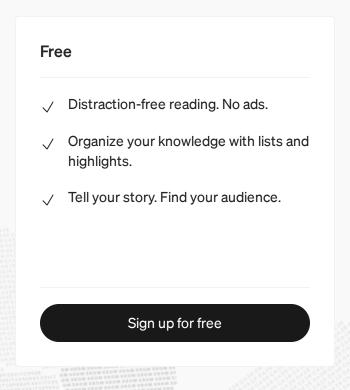




Figure 9. Output When Event Fires

To make Medium work, we log user data. By using Medium, you agree to our <u>Privacy Policy</u>, including cookie policy.

Medium

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

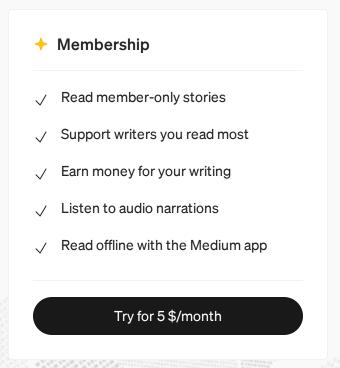
Free

/ Distraction-free reading. No ads.

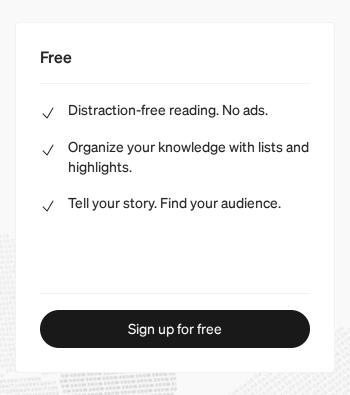
/ Organize your knowledge with lists and highlights.

/ Tell your story. Find your audience.

Sign up for free



Medium





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.

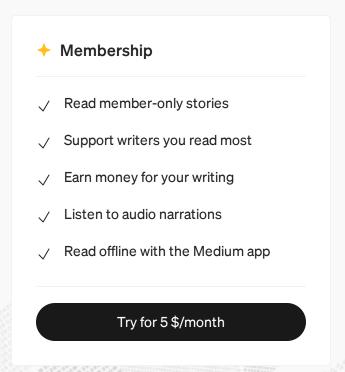
References

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

December 11 1 (2016 April) 11/1 - 4 :- - - 12 Detained 16 -

Medium





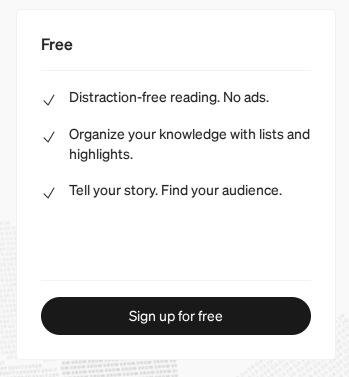
Written by Christopher Ross





109 Followers · Writer for Posts By SpecterOps Team Members

Medium





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

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

Introduction

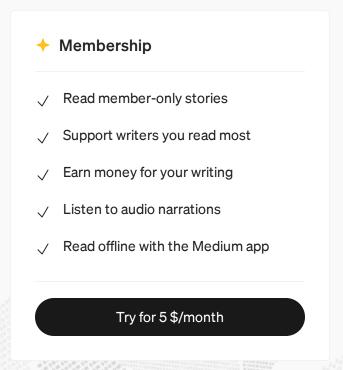
Christopher R... in Posts By SpecterOps Team Me...

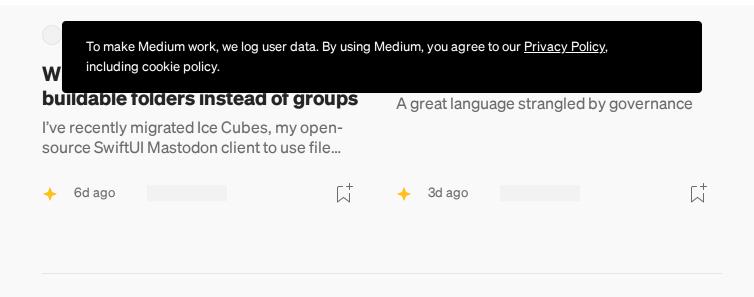
No Place Like Chrome

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

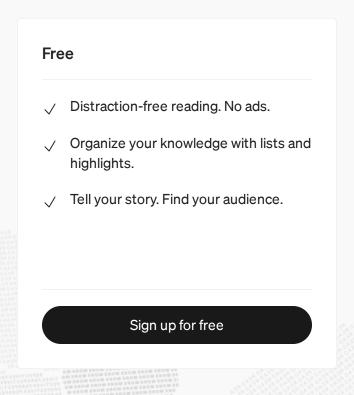
Medium

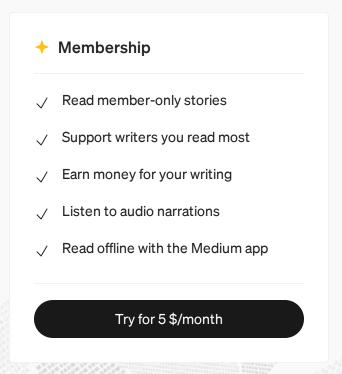


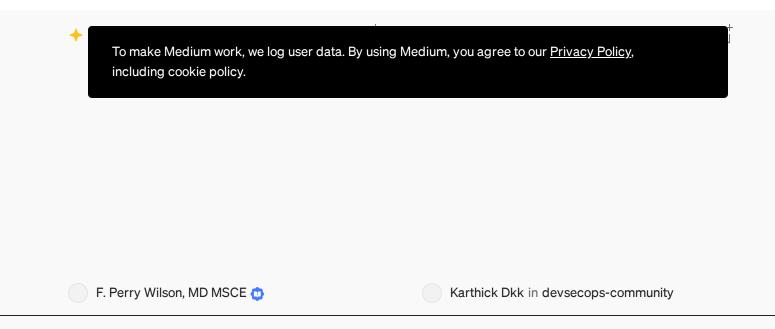




Medium







Medium

