

I'm Richard

Welcome

To my talk about an easy to use, small, fast and flexible realtime filesystem activity monitoring tool

FSpy

Based on inotify

Implemented since 2.6.13

Why?

Just a single, opt controlled,
executable

No need to install or modify
the OS

Usage: fspy [options] [file/dir]

Options:

- F, --filter STRING/REGEX a string or regular expression which will be used to filter the output. (the regex will be matched against the whole path e.g. [/etc/passwd])
- I, --inverted STRING/REGEX its the same like -F/--filter but inverted. you can combine both. e.g. -F '.conf' -I 'wvdial.conf' will filter for files with ".conf" in its name but without "wvdial.conf" in it.
- R, --recursive NUMBER enables the recursive engine to look at a depth of NUMBER.
- A, --adaptive (HIGHLY-EXPERIMENTAL) enables the adaptive mode. e.g. if new items will be added within the path fspy will automatically add those items to the watch list.
- D, --diff VALUE (EXPERIMENTAL) enables the diffing feature. VALUE may be a comma separated list of:
 - s - element size (byte)
 - A - last access time (e.g. Mon Jul 21 21:32:31 2008)
 - M - last modification time (e.g. Mon Jul 21 21:32:31 2008)
 - S - last status change time (e.g. Mon Jul 21 21:32:31 2008)
 - O - permissions (octal)
 - U - owner (uid)
 - G - group (gid)
 - I - inode number
 - D - device id
- T, --type VALUE specifies the type of objects to look for. VALUE may be a comma separated list of:
 - f - regular file
 - d - directory
 - s - symlink
 - p - FIFO/pipe
 - c - character device
 - b - block device
 - o - socketdefault is any.
- O, --output VALUE specifies output format. VALUE may be a comma separated list of:
 - f - filename
 - p - path
 - d - access description
 - t - element type
 - s - element size (byte)
 - w - watch descriptor (inotify manpage)
 - c - cookie (inotify manpage)
 - m - access mask (inotify manpage | src/fsevents.h)
 - l - len (inotify manpage)
 - A - last access time (e.g. Mon Jul 21 21:32:31 2008)
 - M - last modification time (e.g. Mon Jul 21 21:32:31 2008)
 - S - last status change time (e.g. Mon Jul 21 21:32:31 2008)
 - O - permissions (octal)
 - U - owner (uid)
 - G - group (gid)
 - I - inode number
 - D - device id
 - T - date and time (for this event) (e.g. Tue Mar 25 09:23:16 CET 2008)e.g.: '[,T,],,d,:,p,f' would result in:
'[Mon Sep 1 12:31:25 2008] file was opened:/etc/passwd'
(take a look at the README).
- h, --help this short help.
- version version information.

file was accessed:/var/run/utmp size: 5760 atime: Sun Dec 28 13:52:44
file was accessed:/var/run/utmp size: 5760 atime: Sun Dec 28 13:52:44
file was accessed:/var/run/utmp size: 5760 atime: Sun Dec 28 13:52:44
file was accessed:/var/run/utmp size: 5760 atime: Sun Dec 28 13:52:44
writeable file was closed:/var/run/utmp size: 5760 atime: Sun Dec 28 13:52:44
file was modified:/var/log/messages size: **451441** atime: Sun Dec 28 13:52:44
file was modified:/var/log/messages size: **451497** atime: Sun Dec 28 13:52:44
file was opened:/var/run/utmp size: 5760 atime: Sun Dec 28 13:52:44 20
file was accessed:/var/run/utmp size: 5760 atime: Sun Dec 28 13:52:44
writeable file was closed:/var/run/utmp size: 5760 atime: Sun Dec 28 13:52:44
file was modified:/var/log/messages size: **451599** atime: Sun Dec 28 13:52:44
dir access (2):/var/log size: **4096** atime: **Wed Jan 30 17:03:55 2008**
dir access (2):/var/log/ size: 4096 atime: Wed Jan 30 17:03:55 2008
dir access (1):/var/log size: 4096 atime: Wed Jan 30 17:03:55 2008
dir access (1):/var/log/ size: 4096 atime: Wed Jan 30 17:03:55 2008
file was opened:/var/run/utmp size: 5760 atime: Sun Dec 28 13:52:44 20
file was accessed:/var/run/utmp size: 5760 atime: Sun Dec 28 13:52:44

Can be usefull for

Application Testing

System Monitoring

■ ■ ■

Warning: This is a PoC!

You can get it

Here:

<http://mytty.org/fspy>

Thank you

Private Contact

richard.sammet@gmail.com
<http://www.mytty.org>

Business Contact

Deloitte.

Deloitte & Touche GmbH
Wirtschaftsprüfungsgesellschaft

Franklinstraße 50
60486 Frankfurt
Germany

Richard Sammet
Senior Security Consultant

rsammet@deloitte.de

Member of
Deloitte Touche Tohmatsu