Cross platform file-access tracking

Asked 16 years, 4 months ago Modified 9 years, 4 months ago

Viewed 575 times

3

I'd like to be able to track file read/writes of specific program invocations. No information about the actual transactions is required, just the file names involved.

Is there a cross platform solution to this?
What are various platform specific methods?
On Linux I know there's strace/ptrace (if there are faster methods that'd be good too).
I think on mac os there's ktrace.
What about Windows?

Also, it would be amazing if it would be possible to block (stall out) file accesses until some later time.

Thanks!

cross-platform filesystems ptrace

Share

Improve this question

Follow

edited Aug 24, 2015 at 9:16

Stefan Steiger

81.9k ● 69 ● 399 ● 454

asked Aug 21, 2008 at 19:16

mgsloan

3,295 ● 22 ● 20

I'm also looking for answers to this question. I had hoped (like you) that I could use ktrace on mac os, but the system call seems to have been removed (or hidden). Have you had any luck with ktrace on the mac? – David Roundy Apr 18, 2015 at 21:19

3 Answers

Sorted by: Highest score (default)

1

The short answer is no. There are plenty of platform specific solutions which all probably have similar interfaces, but they aren't inherently cross platform since file systems tend to be platform specific.

> How do I do it well on each platform?

Again, it will depend on the platform :) For Windows, if you want to track reads/writes in flight, you might have to go with IFS. If you just want to get notified of changes, you can use `ReadDirectoryChangesW` or the NTFS change journal.

I'd recommend using the NTFS change journal only because it tends to be more reliable.

Share Improve this answer

Follow

edited Jul 3, 2012 at 14:52

user142162

answered Aug 21, 2008 at 21:47

Mat Noguchi

1,080 ● 6 ● 7

1 Does the NTFS change journal report which process makes each change? – David Roundy Apr 18, 2015 at 17:53

0

On Windows you can use the command line tool Handle or the GUI version Process Explorer to see which files a given process has open.

If you're looking for a get this information in your own program you can use the IFS kit from Microsoft to write a file system filter. The file system filter will show all file system operation for all process. File system filters are used in AV software to scan files before they are open or to scan newly created files.

Share Improve this answer

Follow

answered Aug 21, 2008 at 20:32

shamer

0

As long as your program launches the processes you want to monitor, you can write a debugger and then you'll be notified every time a process starts or exits. When a process starts, you can inject a DLL to hook the CreateFile system calls for each individual process. The hook can then use a pipe or a socket to report file activity to the debugger.

Share Improve this answer

Follow

answered Jan 14, 2010 at 6:42

Emil

381 ● 3 ● 13

Do you have any hints as to how to do this hooking from C? – David Roundy Apr 18, 2015 at 21:21

Google for DLL hot patch or something like that. Your debugger process can use CreateRemoteThread into the process being debugged to call LoadLibrary that loads your own DLL which becomes part of that process and can use the hot patch technique to intercept all calls to pretty much any function from a system DLL. – Emil Apr 19, 2015 at 22:56