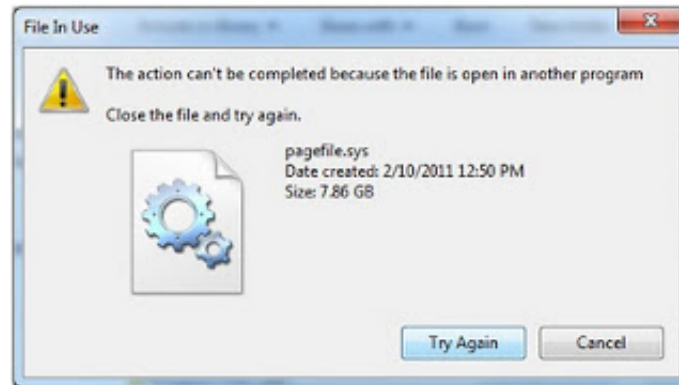


Windows how to check which process locks file command - A M\$ Windows equivalent of lsof command

Author : admin



I've had a **task** today to *deploy a new WAR (Web Application Archive) Tomcat file on Apache Tomcat server running on Windows server 2008 R2 UAT environment.*

The client Tomcat application within war is providing a frontend to an proprietary [Risk Analysis application called Risiko Management \(developed by a German vendor called Schleupen\)](#).

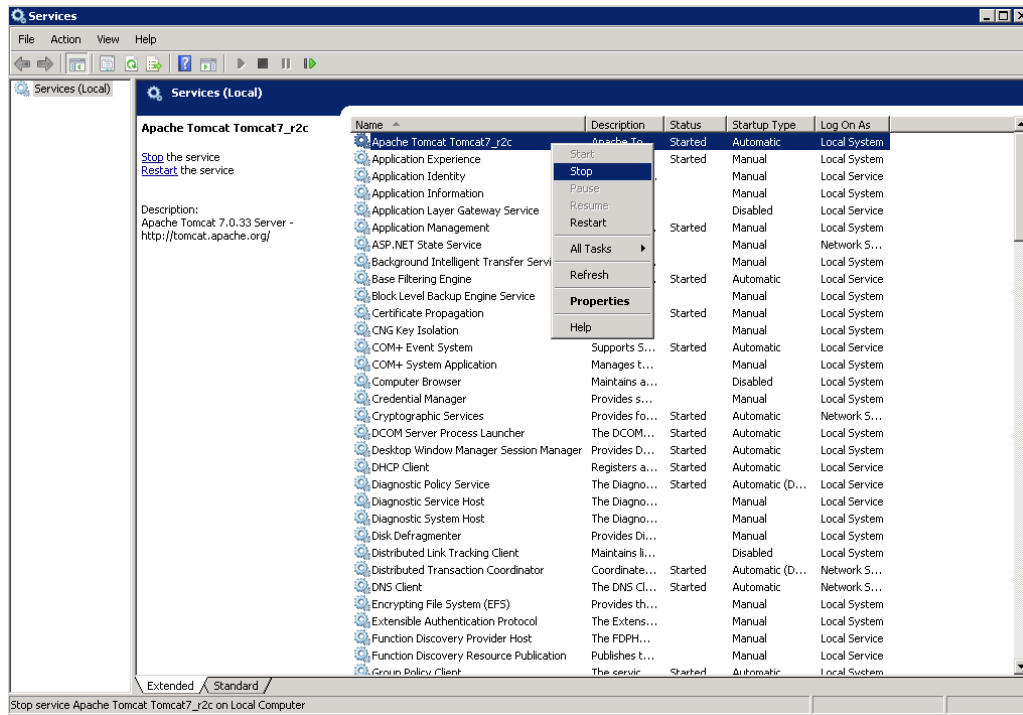
The update of WAR file was part of a version upgrade of application so, both "Risk Analysis" desktop standalone server *RiskKit* and the Web frontend was developed by Schleupen had to be updated.

In order to update I followed the **usual .WAR Tomcat Javafile update Tomcat process.**

1. Stopped Tomcat running service Instance via *services.msc* command e.g.

Start (menu) -> Run

services.msc



2. Move (by Renaming) old *risk-analysis.war* to *risk-analysis_backup_2015.war*

and also rename the automatically Tomcat extracted folder (named same name as the **WAR archive file**

directory - **D:\web\Apache-Tomcat-7.0.33\webapps\Risiko-Analysis** *to* **:\web\Apache-**

Tomcat-7.0.33\webapps\Risiko-Analysis_backup_2015, i.e. run:

C:\Users\risk-analysis> D:

D:\>

```
D:\> CD \Web\Apache-Tomcat-7.0.33\webapps\
```

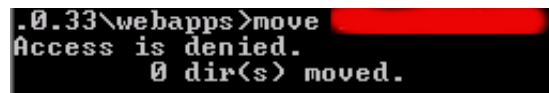
```
D:\Web\Apache-Tomcat-7.0.33\webapps> move risk-analysis.war risk-analysis_2015.war
```

```
D:\Web\Apache-Tomcat-7.0.33\webapps>
```

```
Risiko-Analysis\ Risiko-Analysis_backup_2015\
```

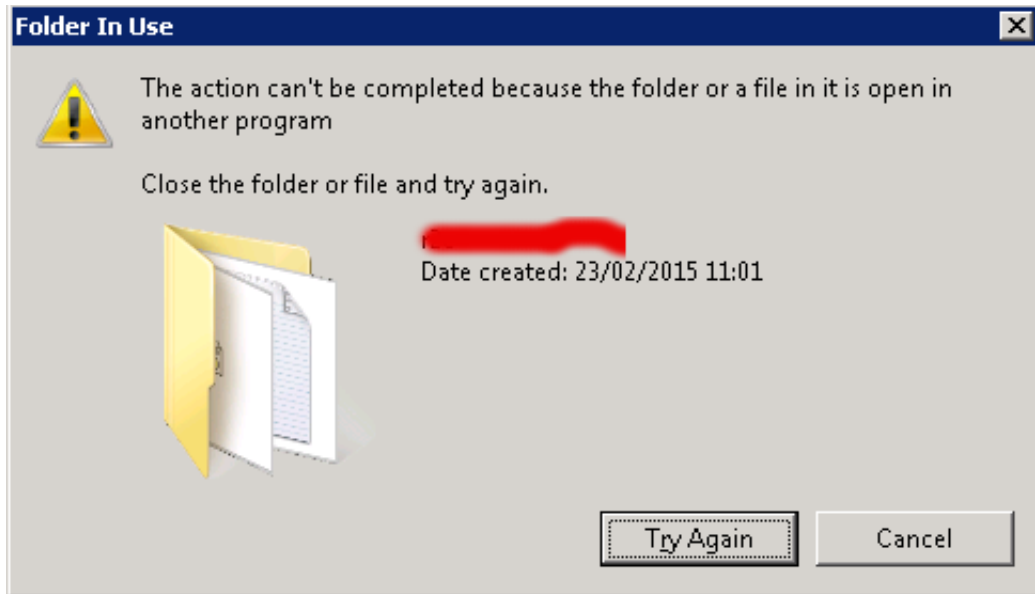
```
move
```

But *unfortunately I couldn't rename it and I got below error:*



```
.0.33\webapps>move [redacted]  
Access is denied.  
0 dir(s) moved.
```

Also I tried copying it using Windows Explorer Copy / Paste but this didn't work either, and I got below error :



3. Finding what Locks a directory or File on MS Windows

Obviously, the reason for unable to copy the directory was something was locking it. Actually there are plenty of locked files many running applications like Explorer do. A good example for all time locked file is Windows (swap file) **pagefile.sys** - this is Windows Linux equivalent of **swap filesystem** (enabled / disabled with **spapon / swapoff** commands).

Having the directory locked was a strange problem, because the Tomcat process was not running as I checked closely both in **Windows taskmgr GUI interface** and manually grepped for the process with **tasklist** command like so:

```
d:\>tasklist /m|find /i "tomcat"
```

```
tomcat7.exe          4396 ntdll.dll, kernel32.dll, KERNELBASE.dll,
```

For people like me who use primary Linux , **above command shows you very precious debugging information, it shows which Windows libraries (DLL) are loaded in memory and used by the process**

(Note that when Tomcat is running, it is visible with command)

```
D:\> wmic.exe process list brief | find /i "tomcat"
526      tomcat7.exe      8      4396      49      156569600
```

Just for those wondering the **156569600** number is number of bytes loaded in Windows memory used by

Tomcat.

After tomcat was stopped above command returned empty string meaning obviously that tomcat is stopped ..

BTW, **wmic** command is very useful to get a list of process names (to list all running processes):

```
D:> wmic.exe process list brief
```

```
Administrator: C:\Windows\system32\cmd.exe
476      iexplore.exe      8      3568      11      31657984
238      mmc.exe          8      4512      4      18370560
526      tomcat7.exe       8      4396      49      154984448
184      ldapconnector.exe 8      844      13      19169280
411      risiko.exe       8      3612      14      143577088
94       MDB-CRON.exe      8      4668      4      6955008
24       cmd.exe          8      4940      1      3248128
52       conhost.exe      8      3912      2      5439488
243      mmc.exe          8      4424      4      17006592
177      WmiPrvSE.exe     8      3052      8      8232960
152      WMIC.exe         8      4168      6      9842688

d:\>
```

Well obviously something was locking this directory (some of its subdirectories or a file name within the directory / folder), so I couldn't rename it just like that.

In Linux finding which daemon (service) is locking a file is pretty easy with lsof command (for those [new to lsof check my previous article how to how to check what process listens on network port in Linux](#)), however it was unknown to me **how I can check which running service is locking a file** and did a quick google search which pointed me to the famous [handle part of SysInternals tools](#).

The [command tool Handle.exe](#) was exactly what I was looking for.

```
Administrator: C:\Windows\system32\cmd.exe

c:\TEMP>handle /?

Handle v4.0
Copyright (C) 1997-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: handle [[-a [-l]] [-u] ; [-c <handle> [-y]] ; [-s]] [-p <process>] [<pid>]
[<name>]
    -a      Dump all handle information.
    -l      Just show pagefile-backed section handles.
    -c      Closes the specified handle (interpreted as a hexadecimal number).
             You must specify the process by its PID.
             WARNING: Closing handles can cause application or system instability.
    -y      Don't prompt for close handle confirmation.
    -s      Print count of each type of handle open.
    -u      Show the owning user name when searching for handles.
    -p      Dump handles belonging to process <partial name accepted>.
    name    Search for handles to objects with <name> <fragment accepted>.

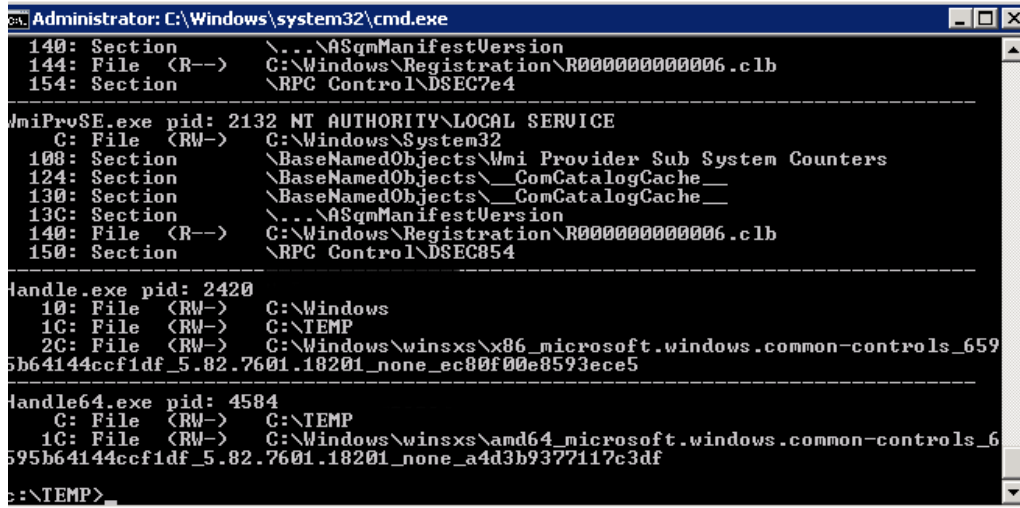
No arguments will dump all file references.

c:\TEMP>
```

To get list of all opened (locked) files and see which application has opened it just exec command

without arguments, you will get

plenty of useful info which will help you to better understand what Windows OS is doing invisible in the background and what app uses what.



```
Administrator: C:\Windows\system32\cmd.exe
140: Section \...\ASqmManifestVersion
144: File (R-->) C:\Windows\Registration\R0000000000006.clb
154: Section \RPC Control\DSEC7e4
-----
wmiprvse.exe pid: 2132 NT AUTHORITY\LOCAL SERVICE
C: File (RW-) C:\Windows\System32
108: Section \BaseNamedObjects\Wmi Provider Sub System Counters
124: Section \BaseNamedObjects\__ComCatalogCache__
130: Section \BaseNamedObjects\__ComCatalogCache__
13C: Section \...\ASqmManifestVersion
140: File (R-->) C:\Windows\Registration\R0000000000006.clb
150: Section \RPC Control\DSEC854
-----
handle.exe pid: 2420
10: File (RW-) C:\Windows
1C: File (RW-) C:\TEMP
2C: File (RW-) C:\Windows\winsxs\x86_microsoft.windows.common-controls_659
5b64144ccf1df_5.82.7601.18201_none_ec80f00e8593ece5
-----
handle64.exe pid: 4584
C: File (RW-) C:\TEMP
1C: File (RW-) C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6
595b64144ccf1df_5.82.7601.18201_none_a4d3b9377117c3df
C:\TEMP>
```

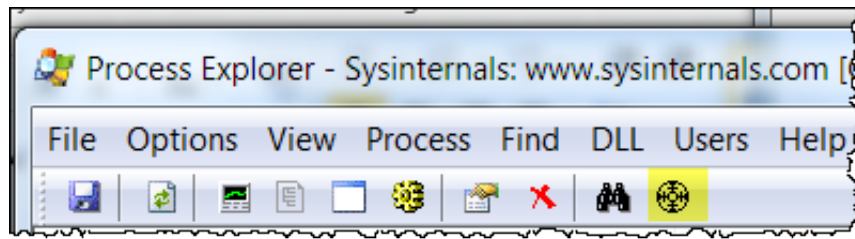
handle is pretty much **Windows equivalent command of Linux lsof**

To get which file was locked by Tomcat I used handle in conjunction with `find /i` command which is pretty much like **Linux's grep equivalent**

```
C:\TEMP> Handle.exe | FIND /I "Tomcat"
```

```
1C: File (RW-) D:\Web\Apache-Tomcat-7.0.33\webapps\Risk-Analysis\images\app
```

Alternatively if you have sysinternals and prefer GUI environment you can use **SysInternals Process Explorer** (press **CTRL + F**) and look for a string:



Next to handle I found also **another GUI program (Internet Explorer extension) [WhoLockMe](#)**, that can be used to *show you all running programs and locked files by this programs*.

WhoLockMe is pretty straight forward to use, though it shows GUI output you have to run the command from cmd line. Below is sample output screenshot of *wholockme*.

Locker Name	PID	Opened File	Handle	Domain	U...	Locker Full Path
explorer.exe	0x01FC (508)	C:\TEMP\LOGISHRD\LVPRCINJ02.DLL	Library	MAIAR	S...	C:\WINDOWS\Explorer.EXE
Skype.exe	0x07B8 (1976)	C:\TEMP\LOGISHRD\LVPRCINJ02.DLL	Library	MAIAR	S...	C:\progs\Skype\Phone\Skype.exe
winamp.exe	0x15A8 (5544)	C:\TEMP\LOGISHRD\LVPRCINJ02.DLL	Library	MAIAR	S...	C:\progs\Winamp\winamp.exe
chrome.exe	0x0EFC (3836)	C:\TEMP\LOGISHRD\LVPRCINJ02.DLL	Library	MAIAR	S...	C:\usr\SLocal Settings\Application Data\Google\Chrome\...
java.exe	0x1624 (5668)	C:\TEMP\LOGISHRD\LVPRCINJ02.DLL	Library	MAIAR	S...	C:\progs\Java\jre6\bin\java.exe
firefox.exe	0x226C (8812)	C:\TEMP\LOGISHRD\LVPRCINJ02.DLL	Library	MAIAR	S...	C:\progs\Mozilla Firefox\Firefox.exe
WhoLockMe...	0x244C (9292)	C:\TEMP\LOGISHRD\LVPRCINJ02.DLL	Library	MAIAR	S...	C:\RegisteredAddins\WhoLockMe.exe
explorer.exe	0x01FC (508)	C:\TEMP\...	0x0E14	MAIAR	S...	C:\WINDOWS\Explorer.EXE
java.exe	0x1624 (5668)	C:\TEMP\hspertdata_Smeagol\5668	0x0754	MAIAR	S...	C:\progs\Java\jre6\bin\java.exe
firefox.exe	0x226C (8812)	C:\TEMP\etlqs_OVBUn0QoDohja5wPR...	0x049C	MAIAR	S...	C:\progs\Mozilla Firefox\Firefox.exe

To Install Wholockme

Unzip "**WhoLockMe.zip**" in a directory (for example : "**C:\Program Files\WhoLockMe**")
 Launch "**Install.bat**" or execute this **Windows registry modification command** :

regsvr32 "C:\Program Files\WhoLockMe\WhoLockMe.dll"

To Uninstall WhoLockMe - if you need to later:

Execute command :

```
regsvr32 /u "C:\Program Files\WhoLockMe\WhoLockMe.dll"
```

Reboot (Or Kill Explorer.exe).

Removes the "**C:\Program Files\WhoLockMe**" directory and its contents.

Probably there are other ways to find out what is locking a file or directory using powershell scripts or .bat (batch) scripting. If you know of other way using default Windows embedded commands, please share in comments.