Utiliser Process

Command Line Process Viewer/Killer/Suspender for Windows NT/2000/XP

Want a small command line utility to view, kill, suspend or set the priority and affinity of processes, perhaps from a batch file? . . Has a virus disabled your Task Manager? . . or perhaps your Administrator has?

The Command Line Process Utility will function even when the task manager is disabled and/or the dreaded "Task Manager has been disabled by your Administrator" dialog box appears.

Works on remote machines with the Microsoft Telnet Server (tlntsvr) found on Windows 2000 and XP or with BeyondExec for Windows NT4/2000/XP.

View processes, owners, and CPU time . .

```
Command Line Process Viewer/Killer/Suspender for Windows NT/2000/XP
V2.01
Copyright(C) 2002-2003 Craig.Peacock@beyondlogic.org

       ImageName   PID Threads Priority CPU%
[System Process]     0       1        0 100 Error 0x6 : The handle
is invalid.
          System     8      43        8   0 Error 0x5 : Access is
denied.
        SMSS.EXE   180       6       11   0 NT AUTHORITY\SYSTEM
       CSRSS.EXE   204      11       13   0 NT AUTHORITY\SYSTEM
    WINLOGON.EXE   224      16       13   0 NT AUTHORITY\SYSTEM
    SERVICES.EXE   252      33        9   0 NT AUTHORITY\SYSTEM
       LSASS.EXE   264      16        9   0 NT AUTHORITY\SYSTEM
     svchost.exe   436      10        8   0 NT AUTHORITY\SYSTEM
     spoolsv.exe   468      15        8   0 NT AUTHORITY\SYSTEM
    CrypServ.exe   496       3       13   0 NT AUTHORITY\SYSTEM
     svchost.exe   512      28        8   0 NT AUTHORITY\SYSTEM
     hidserv.exe   532       4        8   0 NT AUTHORITY\SYSTEM
  jtagserver.exe   560       3        8   0 NT AUTHORITY\SYSTEM
         mdm.exe   584       6        8   0 NT AUTHORITY\SYSTEM
     nvsvc32.exe   628       2        8   0 NT AUTHORITY\SYSTEM
      regsvc.exe   664       2        8   0 NT AUTHORITY\SYSTEM
      mstask.exe   704       6        8   0 NT AUTHORITY\SYSTEM
      stisvc.exe   728       4        8   0 NT AUTHORITY\SYSTEM
     WinMgmt.exe   804       3        8   0 NT AUTHORITY\SYSTEM
    mspmspsv.exe   876       2        8   0 NT AUTHORITY\SYSTEM
     svchost.exe   896       5        8   0 NT AUTHORITY\SYSTEM
    explorer.exe   616      15        8   0 NEPTUNE\Administrator
       mixer.exe  1092       3        8   0 NEPTUNE\Administrator
    PRISMSTA.exe  1048       1        8   0 NEPTUNE\Administrator
    rundll32.exe   952       2        8   0 NEPTUNE\Administrator
    DIRECTCD.EXE   960       3        8   0 NEPTUNE\Administrator
    internat.exe  1180       1        8   0 NEPTUNE\Administrator
         OSA.EXE  1192       2        8   0 NEPTUNE\Administrator
         Icq.exe  1200      11        8   0 NEPTUNE\Administrator
      devenv.exe  1324       4        8   0 NEPTUNE\Administrator
    IEXPLORE.EXE  1140       7        8   0 NEPTUNE\Administrator
         CMD.EXE  1340       1        8   0 NEPTUNE\Administrator
     Process.exe  1132       1        8   0 NEPTUNE\Administrator
```

Additional switches can be used to display User and Kernel Times (**-t**) or the Creation Time of processes (**-c**).

Kill Processes . . .

Processes can be killed immediately (terminated without saving files or cleaning up) by specifying either the name or the PID (Process IDentifier). In cases where there are multiple processes running with the same name and your desire is to kill a specific process you will need to use the PID.

```
C:\>process -k 748

Command Line Process Viewer/Killer/Suspender for Windows NT/2000/XP
V2.01
Copyright(C) 2002-2003 Craig.Peacock@beyondlogic.org
Killing PID 748 'winword.exe'
```

If an image name such as iexplore.exe is specified, the utility will kill all processes by that name.

```
C:\>process -k iexplore.exe

Command Line Process Viewer/Killer/Suspender for Windows NT/2000/XP
V2.01
Copyright(C) 2002-2003 Craig.Peacock@beyondlogic.org
Killing PID 996 'iexplore.exe'
Killing PID 1832 'iexplore.exe'
Killing PID 1852 'iexplore.exe'
Killing PID 1692 'iexplore.exe'
```

Close Processes . . .

On the other hand if you want to gracefully close programs by sending them a WM_CLOSE message first, you can used the -q option. This allows processes to clean up, save files, flush buffers etc. However it can cause deadlocks. e.g trying to close Microsoft Word when a unsaved, but edited document is open will generate a dialog box "Do you want to save changes to document 1?". This will prevent winword.exe from exiting until a user responds to the prompt.

```
C:\>process -q wordpad.exe

Command Line Process Viewer/Killer/Suspender for Windows NT/2000/XP
V2.01
Copyright(C) 2002-2003 Craig.Peacock@beyondlogic.org
Sending PID 1836 'wordpad.exe' WM_CLOSE Message. Timeout is 60
seconds.
wordpad.exe (PID 1836) has been closed successfully.
```

When this option is used a WM_CLOSE message is immediately sent to the process. It then waits up to a default of 60 seconds for the program to clean up and gracefully close before it is killed. The different timeout can be specified as an option after the PID/Image Name.

Suspend & Resume Processes . . .

Processes can be suspended if you need some extra CPU cycles without having to kill the process outright. Once the requirement for the extra CPU cycles has passed you may resume the process and carry on from where you left off. The process is suspended by sleeping all the processes' active threads.

```
C:\>process -s winword.exe

Command Line Process Viewer/Killer/Suspender for Windows NT/2000/XP
V2.01
Copyright(C) 2002-2003 Craig.Peacock@beyondlogic.org
Suspending PID 748 'winword.exe'
Threads [1084][308]
```

Suspending a process causes the threads to stop executing user-mode (application) code. It also increments a suspend count for each thread. Therefore if a process is suspended twice, two resume operations will be required to resume the process (Decrement the suspend count to zero).

Change the priority of processes . . .

When viewing the list of processes, the 4th column shows the base priority of a process. This is a numeric value from zero (lowest priority) to 31 (highest priority). You may set the base priority of a process by specifying one of the priority classes below.

Low	4
BelowNormal	6
Normal	8
AboveNormal	10
High	13
Realtime	24

Please note Windows NT4 does not support the Above Normal and Below Normal priority classes. Specifying these two parameters on a Windows NT4 machine will result in a " The Parameter is incorrect " error.

```
C:\>process -p winword.exe high

Command Line Process Viewer/Killer/Suspender for Windows NT/2000/XP
V2.01
Copyright(C) 2002-2003 Craig.Peacock@beyondlogic.org
Setting PriorityClass on PID 748 'winword.exe' to 128
```

Change the affinity of processes . . .

The affinity is a mask which indicates on which processors (CPUs) a process can run. This is only useful on multiprocessor systems. When the -a option is used in conjunction with a process name or PID, the utility will show the System Affinity Mask and the Process Affinity Mask. The System Affinity Mask shows how many configured processors are currently available in a system. The Process Affinity Mask indicates on what processor(s) the specified process can run on.

```
C:\>process -a wordpad.exe
```

```
Command Line Process Viewer/Killer/Suspender for Windows NT/2000/XP
V2.01
Copyright(C) 2002-2003 Craig.Peacock@beyondlogic.org
Getting Affinity Mask for PID 1084 'wordpad.exe'
System  : 0x0001 0b00000000000000000000000000000011  [2 Installed
Processor(s)]
Process : 0x0001 0b00000000000000000000000000000011
```

To set the affinity mask, simply append the binary mask after the PID/Image Name. Any leading zeros are ignored, so there is no requirement to enter the full 32 bit mask.

```
C:\>process -a wordpad.exe 01

Command Line Process Viewer/Killer/Suspender for Windows NT/2000/XP
V2.01
Copyright(C) 2002-2003 Craig.Peacock@beyondlogic.org
Setting Affinity Mask for PID 1084 'wordpad.exe'
Affinity Mask Successfully Set to 00000000000000000000000000000001
```