

Process Management - Windows

OPS102 Week 5 Class 2

Tiayyba Riaz/John Sellens

June 4, 2024

Seneca Polytechnic

Outline

Processes Recap

Processes in Windows

Processes Recap

Processes Recap

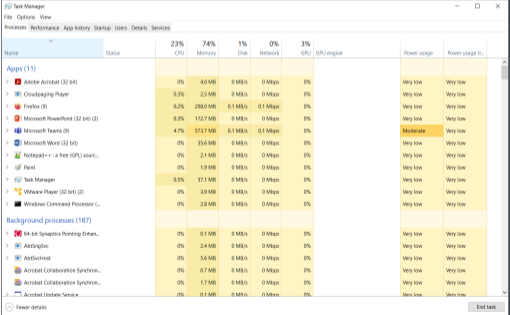
- Everything that runs on a computer is a process
 - Mostly – “threads” are kind of like lightweight processes inside a larger one
- Processes in Linux are hierarchical – every process has a parent
- We have tools like "**ps**", "**ps tree**", and "**top**"
- The shell allows foreground, stopped, and background processes
- We can send signals to processes with the "**kill**" command
 - Signals have default actions, and can usually be caught or ignored by a process
e.g. for cleanup steps
- In code: `fork()`, `exec()` (family of similar functions), `wait()`

Processes in Windows

- Windows generally says “task” rather than “process”
- Generally a hierarchy of parent and child processes
- Running as different users
- In code: `CreateProcess()`, `WaitForSingleObject()`, `CloseHandle()`
- <https://learn.microsoft.com/en-us/windows/win32/procthread/processes-and-threads>

Monitoring Processes in Windows

- Task manager is the unified user interface for monitoring processes in Windows
- You can bring task manager by right clicking in the task bar and selecting the task manager in the context menu.
- Typical view:
 - Monitor resource usage e.g.:
 - CPU
 - Memory
 - Disk
 - Network
 - GPU

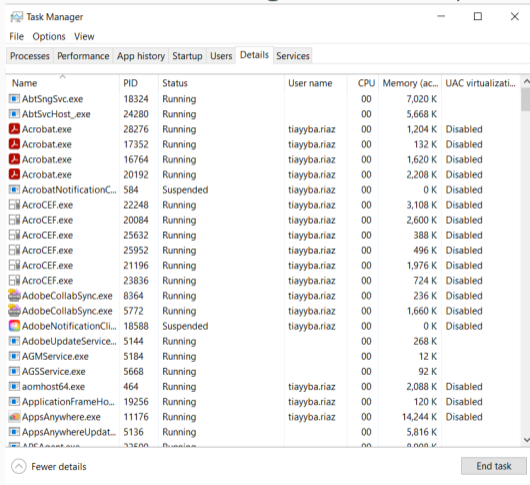


The screenshot shows the Windows Task Manager Performance tab. The top bar indicates overall system usage: CPU 23%, Memory 74%, Disk 1%, Network 0%, and GPU 3%. Below this is a table listing running applications and their resource usage. The 'Power usage' column is highlighted in yellow, with 'Moderate' usage shown for Microsoft PowerPoint.

Name	Status	23% CPU	74% Memory	1% Disk	0% Network	3% GPU	GPU engine	Power usage	Power usage t...
Apps (11)									
Adobe Acrobat (32 bit)		0%	40 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Overlapping Player		0.3%	2.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Firefox (8)		0.2%	298.0 MB	0.1 MB/s	0.1 Mbps	0%		Very low	Very low
Microsoft PowerPoint (32 bit) (2)		0.3%	172.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Microsoft Teams (9)		4.7%	573.7 MB	0.1 MB/s	0.1 Mbps	0%		Moderate	Very low
Microsoft Word (32 bit)		0%	35.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Notepad++ - o free (GPU) sourc...		0%	2.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Paint		0%	1.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Task Manager		0.5%	37.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
VMware Player (32 bit) (2)		0%	3.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Command Processor (...)		0%	2.8 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Background processes (187)									
64-bit Synaptics Pointing Enhanc...		0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
AbtEngSvc		0%	2.4 MB	0 MB/s	0 Mbps	0%		Very low	Very low
AbtSvcHost		0%	5.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Acrobat Collaboration Synthes...		0%	0.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Acrobat Collaboration Synthes...		0%	1.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Acrobat Update Service		0%	0.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low

Process States in Windows

The Details tab of Task Manager shows the process states.

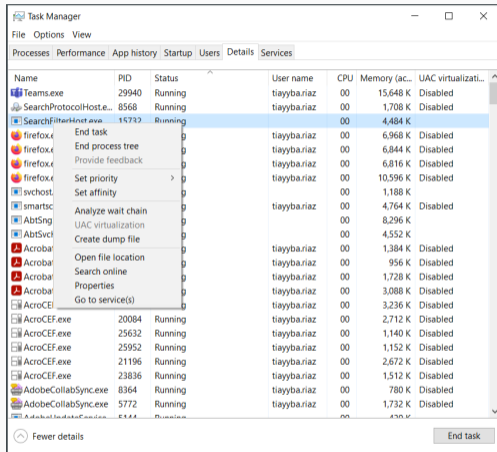


The screenshot shows the Windows Task Manager window with the 'Details' tab selected. The window title is 'Task Manager' and it has a menu bar with 'File', 'Options', and 'View'. Below the menu bar are tabs for 'Processes', 'Performance', 'App history', 'Startup', 'Users', 'Details', and 'Services'. The 'Details' tab is active, displaying a table of processes. The table has columns for Name, PID, Status, User name, CPU, Memory (ac...), and UAC virtualizati... (partially visible). The processes listed include AbtSngSvc.exe, AbtSvcHost_exe, Acrobat.exe (multiple instances), AcrobatNotificationC..., AcroCEF.exe (multiple instances), AdobeCollabSync.exe (multiple instances), AdobeNotificationCi..., AdobeUpdateService..., AGMSvc.exe, AGSSvc.exe, aomhost64.exe, ApplicationFrameHo..., AppsAnywhere.exe, and AppsAnywhereUpdat... (partially visible). At the bottom of the window, there is a 'Fewer details' button on the left and an 'End task' button on the right.

Name	PID	Status	User name	CPU	Memory (ac...	UAC virtualizati...
AbtSngSvc.exe	18324	Running		00	7,020 K	
AbtSvcHost_exe	24280	Running		00	5,668 K	
Acrobat.exe	28276	Running	tiayyba.riaz	00	1,204 K	Disabled
Acrobat.exe	17352	Running	tiayyba.riaz	00	132 K	Disabled
Acrobat.exe	16764	Running	tiayyba.riaz	00	1,620 K	Disabled
Acrobat.exe	20192	Running	tiayyba.riaz	00	2,208 K	Disabled
AcrobatNotificationC...	584	Suspended	tiayyba.riaz	00	0 K	Disabled
AcroCEF.exe	22248	Running	tiayyba.riaz	00	3,108 K	Disabled
AcroCEF.exe	20084	Running	tiayyba.riaz	00	2,600 K	Disabled
AcroCEF.exe	25632	Running	tiayyba.riaz	00	388 K	Disabled
AcroCEF.exe	25952	Running	tiayyba.riaz	00	496 K	Disabled
AcroCEF.exe	21196	Running	tiayyba.riaz	00	1,976 K	Disabled
AcroCEF.exe	23836	Running	tiayyba.riaz	00	724 K	Disabled
AdobeCollabSync.exe	8364	Running	tiayyba.riaz	00	236 K	Disabled
AdobeCollabSync.exe	5772	Running	tiayyba.riaz	00	1,660 K	Disabled
AdobeNotificationCi...	18588	Suspended	tiayyba.riaz	00	0 K	Disabled
AdobeUpdateService...	5144	Running		00	268 K	
AGMSvc.exe	5184	Running		00	12 K	
AGSSvc.exe	5668	Running		00	92 K	
aomhost64.exe	464	Running	tiayyba.riaz	00	2,088 K	Disabled
ApplicationFrameHo...	19256	Running	tiayyba.riaz	00	120 K	Disabled
AppsAnywhere.exe	11176	Running	tiayyba.riaz	00	14,244 K	Disabled
AppsAnywhereUpdat...	5136	Running		00	5,816 K	
APCAsst.exe	23500	Running		00	6,000 K	

Process Control in Windows

- Whenever an application is started, a process is created.
- This can be viewed in the task manager
- Right clicking on the process name shows actions that can be taken on the specific process. This includes(among others):
 - End task
 - Set Priority
 - Set Affinity



Managing Processes Using PowerShell

- Windows PowerShell provides the following commands for managing process.

Get-Process	Get a list of running Windows processes
Start-Process	Start a process/program
Stop-Process	Forcibly stop (kill) a process
Debug-Process	Debug a process
Wait-Process	Wait until a process ends

- Monitoring processes using Get-Process

```
PS C:\Users\tiayba.riaz> Get-Process
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
314	23	23872	34280		9332	0	AbtSngSvc
688	37	31140	45900		18104	0	AbtSvcHost_
444	26	43924	37576	0.25	54604	1	AcrobatNotificationClient
422	21	8748	23064	1.13	16640	1	AdobeCollabSync
582	28	13044	25420	540.03	22040	1	AdobeCollabSync
434	25	43648	36800	0.30	15400	1	AdobeNotificationClient
166	12	5892	13264		5532	0	AdobeUpdateService
243	16	9040	18968		5540	0	AGMServic

Managing Processes Using PowerShell

Monitoring a specific process using Get-Process

```
PS C:\Users\tiayba.riaz> Get-Process firefox
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
218	14	20292	19464	0.17	17132	1	firefox
881	67	298540	322252	24.38	23620	1	firefox
253	18	26428	31548	0.08	28196	1	firefox
322	31	65148	95496	8.72	29760	1	firefox
1875	114	248104	333156	42.95	42932	1	firefox
329	22	39708	34388	0.17	43640	1	firefox
317	49	130784	158768	6.80	43680	1	firefox
316	25	37392	53520	0.41	50812	1	firefox
253	17	20708	19748	0.14	51880	1	firefox
253	18	26528	31700	0.08	55476	1	firefox
253	18	26540	31652	0.09	56896	1	firefox
183	14	20860	18164	0.06	63492	1	firefox
339	27	41328	69204	0.70	64508	1	firefox
345	51	195056	233072	21.73	64860	1	firefox
210	18	20324	18416	0.06	65256	1	firefox
317	30	51260	78016	1.31	66640	1	firefox
314	22	27872	42884	0.25	67532	1	firefox

Stopping a specific process using Stop-Process

```
PS C:\Users\tiayyba.riaz> Stop-Process -Name Notepad  
PS C:\Users\tiayyba.riaz>
```

Summary – Same as Last Class

- Process management is an important component of every operating system.
- As users, we should monitor the processes for better system performance.