Sysinternals Process Utilities

Article • 03/23/2021 • 2 minutes to read

Autoruns

See what programs are configured to startup automatically when your system boots and you login. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

Handle

This handy command-line utility will show you what files are open by which processes, and much more.

ListDLLs

List all the DLLs that are currently loaded, including where they are loaded and their version numbers. Version 2.0 prints the full path names of loaded modules.

PortMon

Monitor serial and parallel port activity with this advanced monitoring tool. It knows about all standard serial and parallel IOCTLs and even shows you a portion of the data being sent and received. Version 3.x has powerful new UI enhancements and advanced filtering capabilities.

ProcDump

This new command-line utility is aimed at capturing process dumps of otherwise difficult to isolate and reproduce CPU spikes. It also serves as a general process dump creation utility and can also monitor and generate process dumps when a process has a hung window or unhandled exception.

Process Explorer

Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

Process Monitor

Monitor file system, Registry, process, thread and DLL activity in real-time.

PsExec

Execute processes remotely.

PsGetSid

Displays the SID of a computer or a user.

PsKill

Terminate local or remote processes.

PsList

Show information about processes and threads.

PsService

View and control services.

PsSuspend

Suspend and resume processes.

PsTools

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

ShellRunas

Launch programs as a different user via a convenient shell context-menu entry.

VMMap

See a breakdown of a process's committed virtual memory types as well as the amount of physical memory (working set) assigned by the operating system to those types. Identify the sources of process memory usage and the memory cost of application features.