How to change the debugger attached to a process

devblogs.microsoft.com/oldnewthing/20100107-00

Raymond Chen

Suppose your application crashes and debugger X is automatically connected because that's how the system happened to be configured. But you would prefer to use debugger Y. After installing debugger Y, how do you switch the debugger from X to Y? If you try to connect debugger Y to the process, you get the error code `STATUS_PORT_ALREADY_SET`, because only one debugger can be connected to a process at a time. But if you disconnect the old debugger, the application will disappear with it. How do you escape from this Catch-22? Here's what you do.

- Attach the ntsd debugger in non-invasive mode: use -pv instead of -p when specifying the process id.
- The ntsd debugger will suspend all the threads in the process.
- Now tell debugger X to resume the process and detach from it. (If debugger X is ntsd, then the command for this is `qd`.)
- Next, tell debugger Y to attach to the process.
- Finally, go to the ntsd debugger which you attached in non-invasive mode, and tell it to detach with the `qd` command.

This trick works because the non-invasive mode of debugging doesn't actually connect to the process as a debugger. It merely suspends all the threads in the process and lets you snoop around its memory. As a result, when you disconnect the original debugger and tell it to resume execution of the application, the application doesn't actually resume because the non-invasive ntsd is keeping it suspended. You then can attach the new debugger to the process and resume your debugging.

In other words, the non-invasive ntsd acts as a bridge, holding the process frozen while one debugger gets out and another one comes in.

Raymond Chen

Follow