Procevent

This plugin utilizes the Netlink library to monitor process starts and exits. Current configuration options include:

1. BufferLength: The length of a shared-memory ring buffer used by the plugin (see below).
2. Process: The exact name of a specific process (or multiple copies of that process) that we wish to monitor.
3. ProcessRegex: A regular expression to match against process names that we wish to monitor.

While running, two threads are used:

1. The main read thread, to read semaphore-protected shared memory.
2. A blocking listening thread that waits for process messages on a Netlink socket. When a message is received, it is placed in shared memory (a ring buffer).

When the plugin is initialized, the /proc directory of the system is analyzed to find any running processes that match process names or regular expressions enumerated in the plugin configuration. A linked list of process PID/name combos is stored for all running processes that are of interest to the plugin. When a new, matching process is detected during runtime, it will be added to the linked list if its PID/name combo is not already present. When an old, matching process dies during runtime, its PID will be removed from the linked list item and replaced with -1, but the linked list item itself will remain with the process name still present (we do this to reuse the memory rather than freeing the space and reallocating when the process might appear again).

In the case of either a matching process start or exit (in the listening thread), a ring buffer entry is added to the shared memory. The read thread will then read this entry (and any other new entries) when it next wakes, and will use information in the linked list and the buffer entry to construct an event notification to dispatch.