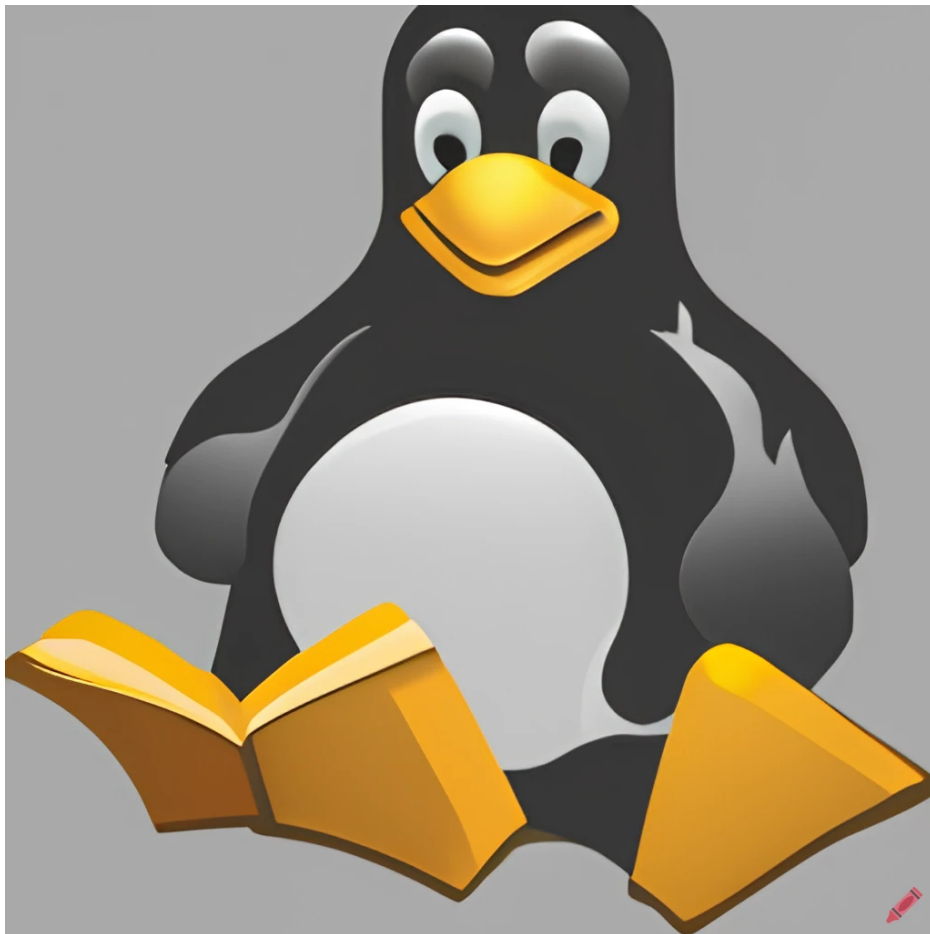


The Linux Process Journey

version 1.0 (beta)
Feb-2023

By Shlomi Boutnaru



Created using [Craiyon AI Image Generator](#)

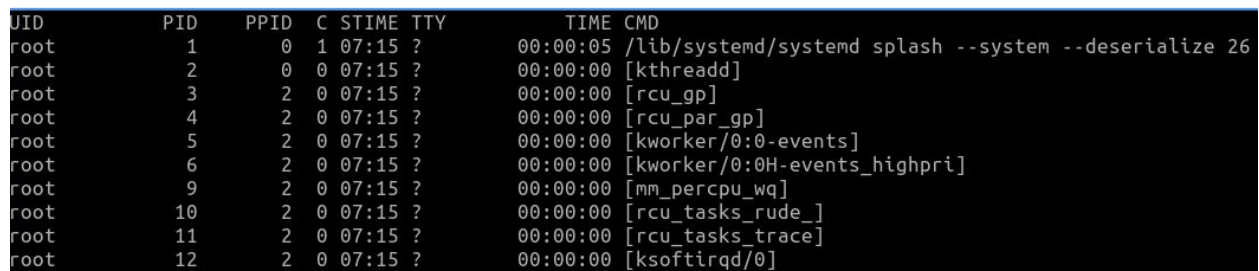
| | |
|---|-----------|
| Introduction | 3 |
| swapper (PID 0) | 4 |
| init (PID 1) | 5 |
| Kernel Threads | 6 |
| kthreadd (PID 2) | 7 |
| migration | 9 |
| charger-manager | 11 |
| idle_inject | 12 |
| kworker | 13 |
| kdevtmpfs | 14 |
| cpuhp | 15 |
| khungtaskd | 16 |
| kswapd | 17 |
| kcompactd | 18 |
| md (Multiple Device Driver) | 20 |
| mld (Multicast Listener Discovery) | 22 |
| ksmd (Kernel Same Page Merging) | 23 |
| ttm_swap | 24 |
| watchdogd | 26 |
| zswap-shrink | 28 |
| khugepaged | 29 |
| krfcommd | 30 |
| ksgxd | 31 |

Introduction

When starting to learn OS internals I believe that we must understand the default processes executing (roles, tasks, etc). Because of that I have decided to write a series of short writeups named "Process ID Card" (aimed at providing the OS vocabulary).

Overall, I wanted to create something that will improve the overall knowledge of Linux in writeups that can be read in 1-3 mins. I hope you are going to enjoy the ride.

In order to create the list of processes I want to explain, I have installed a clean Ubuntu 22.10 VM (Desktop version) and executed ps (as can be seen in the following image - not all the output was included).



| UID | PID | PPID | C | STIME | TTY | TIME | CMD |
|------|-----|------|---|-------|-----|----------|---|
| root | 1 | 0 | 1 | 07:15 | ? | 00:00:05 | /lib/systemd/systemd splash --system --deserialize 26 |
| root | 2 | 0 | 0 | 07:15 | ? | 00:00:00 | [kthreadd] |
| root | 3 | 2 | 0 | 07:15 | ? | 00:00:00 | [rcu_gp] |
| root | 4 | 2 | 0 | 07:15 | ? | 00:00:00 | [rcu_par_gp] |
| root | 5 | 2 | 0 | 07:15 | ? | 00:00:00 | [kworker/0:0-events] |
| root | 6 | 2 | 0 | 07:15 | ? | 00:00:00 | [kworker/0:0H-events_highpri] |
| root | 9 | 2 | 0 | 07:15 | ? | 00:00:00 | [mm_percpu_wq] |
| root | 10 | 2 | 0 | 07:15 | ? | 00:00:00 | [rcu_tasks_rude_] |
| root | 11 | 2 | 0 | 07:15 | ? | 00:00:00 | [rcu_tasks_trace] |
| root | 12 | 2 | 0 | 07:15 | ? | 00:00:00 | [ksoftirqd/0] |

Probably the best way to do it is to go over the processes by the order of their PID value.

The first one I want to talk about is the one we can't see on the list, that is PID 0 (we can see it is the PPID for PID 1 and PID 2 - on them in the next posts).

Lastly, you can follow me on twitter - @boutnaru (<https://twitter.com/boutnaru>). Also, you can read my other writeups on medium - <https://medium.com/@boutnaru>.

Lets GO!!!!!!

swapper (PID 0)

Historically, old Unix systems used swapping and not demand paging. So, swapper was responsible for the “Swap Process” - moving all pages of a specific process from/to memory/backing store (including related process’ kernel data structures). In the case of Linux PID 0 was used as the “idle process”, simply does not do anything (like nops). It was there so Linux will always have something that a CPU can execute (for cases that a CPU can’t be stopped to save power). By the way, the idle syscall is not supported since kernel 2.3.13 (for more info check out “man 2 idle”). So what is the current purpose of swapper today? helping with pageout ? cache flushes? idling? buffer zeroning? I promise we will answer it in more detail while going through the other processes and explaining the relationship between them.

But how can you believe that swapper (PID 0) even exists? if you can’t see it using ps. I am going to use “bpftrace” for demonstrating that (if you don’t know about bpftrace, I strongly encourage you to read about it). In the demo I am going to trace the kernel function “hrtimer_wakeup” which is responsible for waking up a process and move it to the set of runnable processes. During the trace I am going to print the pid of the calling process (BTW, in the kernel everything is called a task - more on that in future posts) and the executable name (the comm field of the task_struct [/include/linux/sched.h]). Here is the command: `sudo bpftrace -e 'kfunc:hrtimer_wakeup { printf("%s:%d\n",curtask->comm,curtask->pid); }'`.



```
Attaching 1 probe...
swapper/0:0
swapper/2:0
swapper/0:0
swapper/2:0
swapper/2:0
swapper/0:0
swapper/2:0
swapper/0:0
swapper/2:0
swapper/0:0
```

From the output we can see we have 3 instances of swapper: swapper/0, swapper/1 and swapper/2 all of them with PID 0. The reason we have three is because my VM has 3 virtual CPUs and there is a swapper process for each one of them - see the output of the command in the following image.

init (PID 1)

After explaining about PID 0, now we are going to talk about PID 1. Mostly known as “init”. init is the first Linux user-mode process created, which runs until the system shuts down. init manages the services (called demons under Linux, more on them in a future post). Also, if we check the process tree of a Linux machine we will find that the root of the tree is init.

There are multiple implementations for init, each of them provide different advantages among them are: SysVinit, launched, systemd, runit, upstart, busybox-init and OpenRC (those are examples only and not a full list). Thus, based on the implementation specific configuration files are read (such as /etc/inittab - SysVinit), different command/tools to manage demons (such as service - SysVinit and systemctl - systemd), and different scripts/profiles might be executed during the boot process (runlevels of SysVinit vs targets in systemd).

The creation of init is done by the kernel function “rest_init”¹. In the code we can see the call to “user_mode_thread” which spawns init, later in the function there is a call to “kernel_thread” which creates PID 2 (more information about it in the upcoming pages ;-).

Now we will go over a couple of fun facts about init. First, in case a parent process exits before all of its children process, init adopts those child processes. Second, only the signals which have been explicitly installed with a handler can be sent to init. Thus, sending “kill -9 1” won’t do anything in most distributions (try it and see nothing happens). Remember that different init implementations handle signals in different ways.

Because they are multiple init implementations (as we stated before) we can determine the one installed in the following manner. We can perform “ls -l /sbin/init”. If it is not a symlink it is probably SysVinit, else if it points to “/lib/systemd/systemd” than systemd is in use (and of course they are other symlinks to the other implementation - you can read about it in the documentation of each init implementation). As you can see in the attached screenshot Ubuntu 22.10 uses systemd.

¹ <https://elixir.bootlin.com/linux/v6.1.8/source/init/main.c#L683>

Kernel Threads

Before we will go over kthreadd I have decided to write a short post about kernel threads (due to the fact kthreadd is a kernel thread). We will go over some characteristics of kernel threads. First, kernel threads always execute in Kernel mode and never in User mode. Thus, kernel threads have basically all privileges and have no userspace address associated with them.

Second, both user mode process and kernel threads are represented by a task_struct inside the Linux kernel. As with all other user tasks, kernel threads are also part of the OS scheduling flow and can be executed on any CPU (there are cases in which there is a specific kernel thread for each CPU, we have seen it with swapper in the first post). Third, all kernel threads are descendants of kthreadd - Why is that? We will explain it in the next post focused on kthreadd.

Lastly, let's investigate kernel threads using /proc and see the difference in information retrieved from a regular user process (aka user task). There are multiple file entries in "/proc/pid" that contain information in case of a user mode process but are empty in case of a kernel thread, such as: "maps", "environ", "auxv", "cmdline" (I suggest reading "man proc" to get more info about them). Also, the fd and fdinfo directories are empty and the link "exe" does not point to any executable. In the attached screenshot we can see some of the difference between PID 1 [example of a regular user mode process] and PID 2 [example for a kernel thread]. BTW, the screenshot below was taken from an online/browser based Linux implementation called JSLinux - <https://bellard.org/jslinux>.

```
localhost:/# uname -a
Linux localhost 4.12.0-rc6-g48ec1f0-dirty #21 Fri Aug 4 21:02:28 CEST 2017 i586
Linux
localhost:/# cat /etc/issue
Welcome to Alpine Linux 3.12
Kernel \r on an \m (\l)

localhost:/# ls -l /proc/1/exe
lrwxrwxrwx    1 root    root              0 Aug 11 23:17 /proc/1/exe -> /bin/busybox
localhost:/# ls -l /proc/2/exe
ls: /proc/2/exe: cannot read link: No such file or directory
lrwxrwxrwx    1 root    root              0 Aug 11 23:16 /proc/2/exe
localhost:/# cat /proc/1/environ
HOME=/TERM=linuxTZ=UTC+07:00localhost:/#
localhost:/# cat /proc/2/environ
```

kthreadd (PID 2)

After explaining about PID 1, now we are going to talk about PID 2. Basically, kthreadd is the “kernel thread daemon”. Creation of a new kernel thread is done using kthreadd (We will go over the entire flow). Thus, the PPID of all kernel threads is 2 (checkout ps to verify this). As explained in the post about PID 1 (init) the creation of “kthreadd” is done by the kernel function “rest_init”². There is a call to the function “kernel_thread” (after the creation of init).

Basically, the kernel uses “kernel threads” (kthreads from now on) in order to run background operations. Thus, it is not surprising that multiple kernel subsystems are leveraging kthreads in order to execute async operations and/or periodic operations. In summary, the goal of kthreadd is to make available an interface in which the kernel can dynamically spawn new kthreads when needed.

Overall, kthreadd continuously runs (infinite loop³) and checks “kthread_create_list” for new kthreads to be created. In order to create a kthread the function “kthread_create”⁴ is used, which is a helper macro for “kthread_create_on_node”⁵. We can also call “kthread_run”⁶ could also be used, it is just a wrapper for “kthread_create”. The arguments passed to the creating function includes: the function to run in the thread, args to the function and a name.

While going over the source code we have seen that “kthread_create” calls “kthread_create_on_node”, which instantiates a “kthread_create_info” structure (based on the args of the function). After that, that structure is queued at the tail of “kthread_create_list” and “kthreadd” is awakened (and it waits until the kthread is created, this is done by “__kthread_create_on_node”⁷). What “kthreadd” does is to call “create_thread” based on the information queued. “create_thread” calls “kernel_thread”, which then calls “kernel_clone”. “kernel_clone” executes “copy_process”, which creates a new process as a copy of an old one - the caller needs to kick-off the created process (or thread in our case). By the way, the flow of creating a new task (recall every process/thread under Linux is called task and represented by “struct task_struct”) from user mode also gets to “copy_process”.

For the sake of simplicity, I have created a flow graph which showcases the flow of creating a kthread, not all the calls are there, only those I thought are important enough. Also, in both cases of macros/functions I used the verb “calls”. The diagram appears at the end of the post. Let me know if it is clear enough or do you think I should change something.

² <https://elixir.bootlin.com/linux/v6.1.8/source/init/main.c#L683>

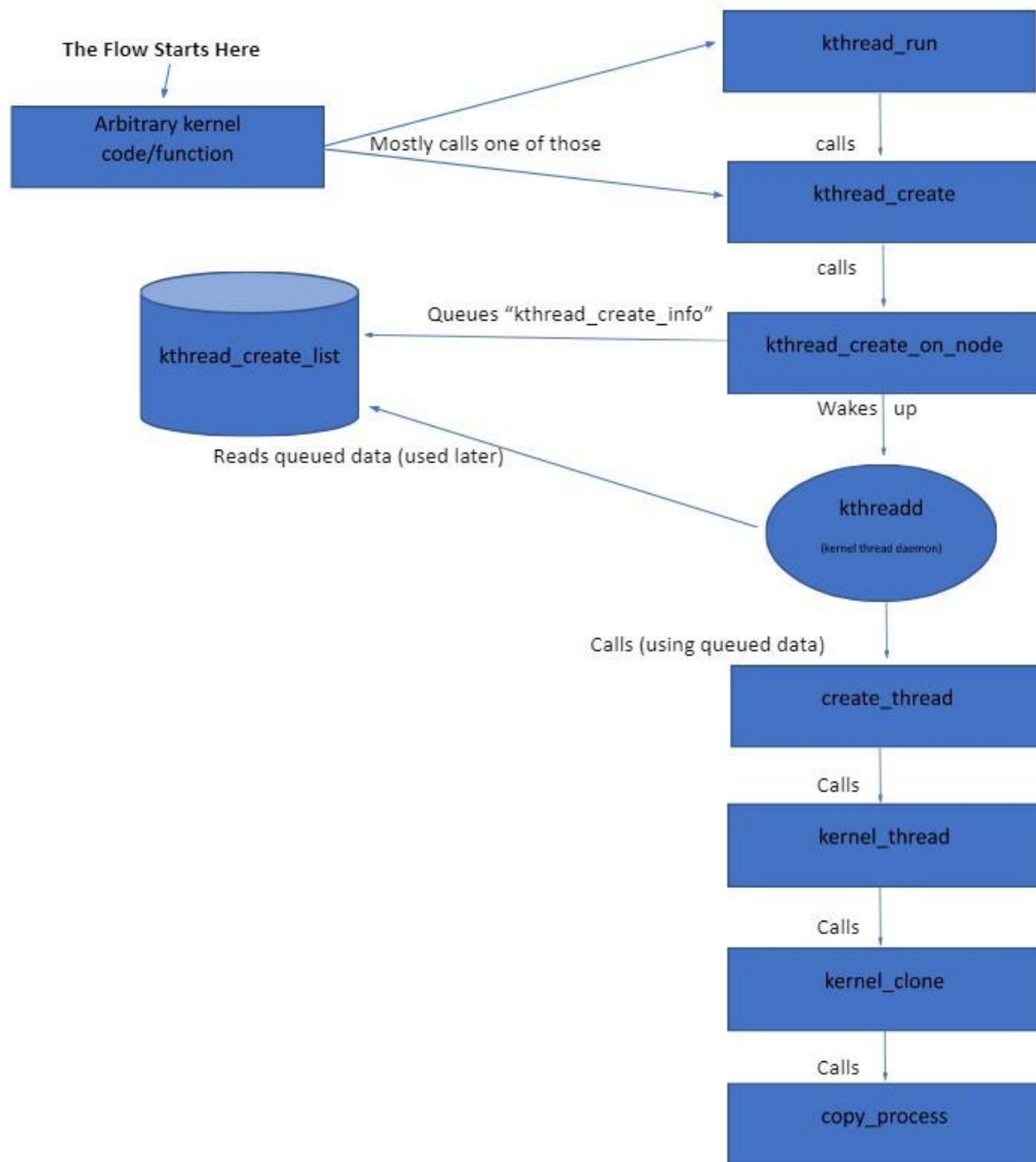
³ <https://elixir.bootlin.com/linux/v6.1.12/source/kernel/kthread.c#L731>

⁴ <https://elixir.bootlin.com/linux/v6.1.12/source/include/linux/kthread.h#L27>

⁵ <https://elixir.bootlin.com/linux/v6.1.12/source/kernel/kthread.c#L503>

⁶ <https://elixir.bootlin.com/linux/v6.1.12/source/include/linux/kthread.h#L51>

⁷ <https://elixir.bootlin.com/linux/v6.1.12/source/kernel/kthread.c#L414>



migration

One of the goals of an operating system is to handle and balance resources across the hardware of the compute entity. In order to do that, Linux has a kernel thread named “migration” which has an instance on every vCPU. By the way, the naming format is “migration/N” where N is the id of the vCPU.

By default threads are not constrained to a vCPU and can be migrated between them in the next call to “schedule()” (which calls the main scheduler function, which is “__scheduler()”⁸). It is done mainly in case the scheduler identifies an unbalanced across the runqueues (the queue in which processes which are in ready/runnable state are waiting to use the processor) of the vCPUs.

It is important to state that we can influence this flow by setting the affinity of a thread (for more read “man 2 sched_setaffinity”. We will talk about that in a future post). There could be performance, cache and other impacts for doing that (but that is also a topic for a different writeup).

I have created a small demo which shows the working of “migration”. For that I have created a VM running Ubuntu 22.04 with 3 vCPUs. In order to trace the usage of “move_queue_task” I have used bpftrace with the following command: **sudo bpftrace -e 'kfunc:move_queued_task { printf("%s moved %s to %d CPU\n",curtask->comm,args->p->comm,args->new_cpu); }'**. The output of the command is shown below. The one-liner prints: the name of the task calling “move_queue_task”, the name of the task which is moved and id the vCPU which the task is moved to.

```
Attaching 1 probe...
migration/2 moved sudo to 1 CPU
migration/1 moved dpkg to 2 CPU
migration/1 moved apt to 0 CPU
migration/1 moved update-motd-upd to 0 CPU
migration/1 moved (snap) to 0 CPU
migration/2 moved friendly-recover to 0 CPU
migration/2 moved lvm2-activation to 0 CPU
migration/0 moved (direxec) to 2 CPU
migration/2 moved (direxec) to 0 CPU
migration/1 moved (direxec) to 2 CPU
migration/2 moved (direxec) to 1 CPU
migration/2 moved (direxec) to 0 CPU
migration/0 moved udiskd to 1 CPU
migration/2 moved bash to 1 CPU
migration/2 moved bash to 0 CPU
migration/1 moved (direxec) to 0 CPU
migration/1 moved (direxec) to 0 CPU
migration/2 moved (direxec) to 0 CPU
migration/1 moved (direxec) to 0 CPU
migration/1 moved (direxec) to 0 CPU
```

⁸ <https://elixir.bootlin.com/linux/latest/source/kernel/sched/core.c#L6544>

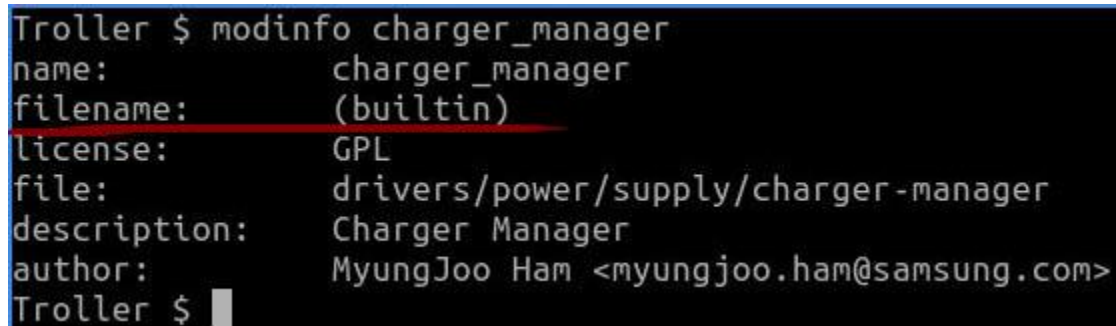
In summary, what the kernel thread “migration” does is to move threads from highly loaded vCPUs to others which are less crowded (by inserting them to a different run-queue). A function which is used by “migration” in order to move a task to a new run-queue is “move_queued_task” (<https://elixir.bootlin.com/linux/latest/source/kernel/sched/core.c#L2325>).

charger-manager

The “charger_manager” kernel thread is created by a freezable workqueue⁹. Freezable workqueues are basically frozen when the system is moved to a suspend state¹⁰. Based on the kernel source code “charger_manager” is responsible for monitoring the health (like temperature monitoring) of the battery and controlling the charger while the system is suspended to memory¹¹. The “Charger Manager” kernel module is written by MyungJoo Ham¹².

Moreover, the kernel documentation states that the “Charger Manager” also helps in giving an aggregated view to user-space in case there are multiple chargers for a battery. In case there are multiple batteries with different chargers on a system, that system would need multiple instances of “Charger Manager”¹³.

On my Ubuntu VM (22.04.1 LTS) this kernel module is not compiled as a separate “*.ko” file. It is compiled into the kernel itself (builtin), as you can see in the output of “modinfo” in the screenshot below.



```
Troller $ modinfo charger_manager
name:                charger_manager
filename:             (builtin)
license:              GPL
file:                 drivers/power/supply/charger-manager
description:          Charger Manager
author:               MyungJoo Ham <myungjoo.ham@samsung.com>
Troller $
```

⁹ <https://elixir.bootlin.com/linux/latest/source/drivers/power/supply/charger-manager.c#L1749>

¹⁰ <https://lwn.net/Articles/403891/>

¹¹ <https://elixir.bootlin.com/linux/latest/source/drivers/power/supply/charger-manager.c>

¹² <https://elixir.bootlin.com/linux/latest/source/drivers/power/supply/charger-manager.c#L1768>

¹³ <https://www.kernel.org/doc/html/v5.3/power/charger-manager.html>

idle_inject

On our plate this time we are going to talk about the kernel thread “idle_inject”, which was merged to the kernel in about 2009. The goal of “idle_inject” is forcing idle time on a CPU in order to avoid overheating.

If we think about it, “idle_inject” adds latency, thus it should be considered only if CPUFreq (CPU Frequency scaling) is not supported. Due to the fact the majority of modern CPUs are capable of running a different clock frequency and voltage configuration we can use CPUFreq in order to avoid overheating.

Overall, there is one “idle_inject” kernel thread per processor (with the name pattern “idle_inject/N”, where N is the id of the processor) - as shown in the screenshot below. Also, all of them are created at init time.

The “idle_inject” kernel threads will call “idle_inject_fn()”->”play_idle_precise()” to inject a specified amount of idle time. After all of the kernel threads are woken up, the OS sets a timer for the next cycle. When the timer interrupt handler wakes the threads for all processors based on a defined “cpu-mask” (affected by idle injection). By the way, when I set a kprobe on “idle_inject_fn()” for 3 hours on my VM it was never called ;-)

```
Troller# ps -eo user,comm,pid,ppid | grep idle_inject
root      idle_inject/0      16        2
root      idle_inject/1      19        2
root      idle_inject/2      25        2
Troller#
```

kworker

A kworker is a kernel thread that performs processing as part of the kernel, especially in the case of interrupts, timers, I/O, etc. It is based on workqueues which are async execution mechanisms, that execute in “process context” (I will post on workqueues in more details separately, for now it is all that you need to know).

Overall, there are a couple of kworkers running on a Linux machine. The naming pattern of kworkers includes: the number of the core on which it is executed, the id of the thread and can contain also string that hints what the kworker does (check the output of ‘ps -ef | grep kworker’).

```
  6      2  0 07:15 ?          00:00:00 [kworker/0:0H-events_highpri]
 82      2  0 07:15 ?          00:00:02 [kworker/0:1H-kblockd]
113      2  0 07:15 ?          00:00:00 [kworker/u3:0]
46277    2  0 11:11 ?          00:00:00 [kworker/u2:1-events_unbound]
46547    2  0 11:20 ?          00:00:01 [kworker/0:1-events]
46624    2  0 11:23 ?          00:00:00 [kworker/u2:2-kcryptd/253:0]
46867    2  0 11:28 ?          00:00:00 [kworker/0:0-inet_frag_wq]
47091    2  0 11:33 ?          00:00:00 [kworker/u2:0-events_unbound]
47299    2  0 11:36 ?          00:00:00 [kworker/0:2-events]
```

The big question is - “How do we know what each kworker is doing?”. It’s a great question, the way in which we are going to answer it is by using ftrace (function tracing inside the kernel - I suggest reading more about that - <https://www.kernel.org/doc/Documentation/trace/ftrace.txt>). The command we are going to use are:

```
echo workqueue:workqueue_queue_work > /sys/kernel/debug/tracing/set_event
cat /sys/kernel/debug/tracing/trace_pipe > /tmp/trace.log
```

The first one enables the tracing regarding workqueues. The second reads the tracing data and saves it to a file. We can also run “cat /sys/kernel/debug/tracing/trace_pipe | grep kworker” and change the grep filter to a specific kworker process. In the trace we will see the function name that each kworker thread is going to execute.

```
kworker/u2:2-46624 [000] d... 17855.481276: workqueue_queue_work: work struct=00000000da1e6721 function=flush_to_ldisc
workqueue=events_unbound req_cpu=8192 cpu=4294967295
kworker/u2:1-48183 [000] d... 17855.525798: workqueue_queue_work: work struct=00000000be96cc25 function=ata_sff_pio_ta
< workqueue=ata_sff req_cpu=8192 cpu=0
kworker/u2:1-48183 [000] d... 17856.038232: workqueue_queue_work: work struct=000000001e1ee94f function=kcryptd_crypt
dm_crypt] workqueue=kcryptd/253:0 req_cpu=8192 cpu=4294967295
kworker/u2:1-48183 [000] d... 17857.542509: workqueue_queue_work: work struct=00000000be96cc25 function=ata_sff_pio_ta
< workqueue=ata_sff req_cpu=8192 cpu=0
kworker/u2:1-48183 [000] d... 17859.558293: workqueue_queue_work: work struct=00000000be96cc25 function=ata_sff_pio_ta
< workqueue=ata_sff req_cpu=8192 cpu=0
kworker/u2:1-48183 [000] d... 17860.134032: workqueue_queue_work: work struct=000000001e1ee94f function=kcryptd_crypt
dm_crypt] workqueue=kcryptd/253:0 req_cpu=8192 cpu=4294967295
kworker/u2:1-48183 [000] d... 17860.134074: workqueue_queue_work: work struct=00000000e0b6b12c function=kcryptd_crypt
dm_crypt] workqueue=kcryptd/253:0 req_cpu=8192 cpu=4294967295
```

kdevtmpfs

“kdevtmpfs” is a kernel thread which was created using the “kthread_run” function¹⁴. “kdevtmpfs” creates a devtmpfs which is a tmpfs-based filesystem (/dev). The filesystem is created during bootup of the system, before any driver code is registered. In case a driver-core requests a device node it will result in a node added to this filesystem¹⁵.

We can see the specific line of code that is used in order to create the mounting point “/dev”¹⁶. The mountpoint is created using the function “init_mount”¹⁷. A nice fact is that it is part of “init_*” functions which are routines that mimic syscalls but don’t use file descriptors or the user address space. They are commonly used by early init code¹⁸.

Thus, we can say the “kdevtmpfs” is responsible for managing the “Linux Device Tree”. Also, by default the name created for nodes under the filesystem is based on the device name (and owned by root) - as shown in the screenshot below (taken from copy.sh based Linux). By the way, not all devices have a node in “/dev” think about network devices ;-)

```
root@localhost:/dev# mount | grep "/dev"| head -1
dev on /dev type devtmpfs (rw,nosuid,relatime,size=10240k,nr_inodes=58635,mode=755)
root@localhost:/dev# ls -lah | head -20
total 1.0K
drwxr-xr-x 11 root root  3.4K Nov  7 02:51 .
drwxrwxrwx 17 root root    0 Nov  7 02:50 ..
crw-r--r--  1 root root 10, 235 Nov  7 02:50 autofs
drwxr-xr-x  2 root root  2.5K Nov  7 02:50 char
crw-----  1 root root   5,  1 Nov  7 02:51 console
lrwxrwxrwx  1 root root   11 Nov  7 02:50 core -> /proc/kcore
drwxr-xr-x  3 root root   60 Nov  7 02:50 cpu
crw-----  1 root root 10, 125 Nov  7 02:50 cpu_dma_latency
drwxr-xr-x  2 root root   60 Nov  7 02:50 dma_heap
drwxr-xr-x  2 root root   60 Nov  7 02:51 dri
crw-----  1 root root 29,  0 Nov  7 02:51 fb0
lrwxrwxrwx  1 root root   13 Nov  7 02:50 fd -> /proc/self/fd
crw-rw-rw-  1 root root   1,  7 Nov  7 02:50 full
drwxr-xr-x  2 root root   80 Nov  7 02:50 input
crw-r--r--  1 root root   1, 11 Nov  7 02:50 kmsg
crw-r-----  1 root root   1,  1 Nov  7 02:50 mem
drwxrwxrwt  2 root root   40 Nov  7 02:50 mqueue
crw-rw-rw-  1 root root   1,  3 Nov  7 02:50 null
crw-----  1 root root 10, 144 Nov  7 02:50 nram
```

¹⁴ <https://elixir.bootlin.com/linux/v6.2-rc1/source/drivers/base/devtmpfs.c#L474>

¹⁵ <https://elixir.bootlin.com/linux/v6.2-rc1/source/drivers/base/devtmpfs.c#L3>

¹⁶ <https://elixir.bootlin.com/linux/v6.2-rc1/source/drivers/base/devtmpfs.c#L377>

¹⁷ <https://elixir.bootlin.com/linux/v6.2-rc1/source/fs/init.c#L16>

¹⁸ <https://elixir.bootlin.com/linux/v6.2-rc1/source/fs/init.c#L3>

cpuhp

This kernel thread is part of the CPU hotplug support. It enables physically removing/adding CPUs on a specific system. There is one kernel thread per vCPU, and the pattern of the thread's name is "cpuhp/N" (where N is the id of the vCPU) - as can be seen in the screenshot below. Also, today the CPU hotplug can be used to resume/suspend support for SMP (Symmetric Multiprocessing).

If we want our kernel to support CPU hotplug the CONFIG_HOTPLUG_CPU should be enabled (it's supported on a couple of architectures such as: MIPS, ARM, x86 and PowerPC). The kernel holds the current state for each CPU by leveraging "struct cpuhp_cpu_state"¹⁹.

We can configure the CPU hotplug mechanism using sysfs (/sys/devices/system/cpu). For example we can shut down and bring up a CPU by writing "0" and "1" respectively to the "online" file in the directory representing the CPU (for which we want to change the status) - checkout the screenshot below (the Linux VM I am testing on has 3 vCPUs).

In order to bring the CPU down the function "cpu_device_down"²⁰ is called. In order to bring up a CPU function "cpu_device_up"²¹ is called.

```
Troller # pwd
/sys/devices/system/cpu
Troller # ls
cpu0  cpufreq  isolated  offline  power  uevent
cpu1  cpuidle  kernel_max  online  present  vulnerabilities
cpu2  hotplug  modalias  possible  smt
Troller # echo 0 > ./cpu2/online
Troller # dmesg | tail -2
[147586.057954] kvm-clock: cpu 1, msr b7001041, secondary cpu clock
[148846.125346] smpboot: CPU 2 is now offline
Troller # echo 1 > ./cpu2/online
Troller # dmesg | tail -2
[148846.125346] smpboot: CPU 2 is now offline
[148874.835266] smpboot: Booting Node 0 Processor 2 APIC 0x2
```

¹⁹ <https://elixir.bootlin.com/linux/latest/source/kernel/cpu.c#L65>

²⁰ <https://elixir.bootlin.com/linux/latest/source/kernel/cpu.c#L1225>

²¹ <https://elixir.bootlin.com/linux/latest/source/kernel/cpu.c#L1439>

khungtaskd

This kernel thread “khungtaskd” is used in order to help with identifying and debugging “Hung Tasks”. This kernel thread is scheduled every 120 seconds (that is the default value). We can say “khungtaskd” is used for detecting tasks which are stuck in uninterruptible sleep (state “D” in ps output). The code of the kernel thread can be read in the following link https://elixir.bootlin.com/linux/latest/source/kernel/hung_task.c.

The basic algorithm of “khungtaskd” is as follows: Iterate over all running tasks on the system and if there are ones marked as TASK_UNINTERRUPTIBLE and it was scheduled at least once in the last 120 seconds it is considered as hung. When a task is considered hung it’s “call stack” is dumped and if the CONFIG_LOCKDEP is also enabled then all of the locks held by the tasks are outputted also.

If we want we can change the sampling interval using the sysctl interface, “/proc/sys/kernel/hung_task_timeout_secs”. We can also verify that the default is 120 seconds by reading it - as shown in the screenshot below.

In order to demonstrate the operation of “khungtaskd” I have executed the following bpftrace one liner - “sudo bpftrace -e 'kfunc:check_hung_uninterruptible_tasks { printf("%s:%d\n",curtask->comm,curtask->pid); }'”. The trace prints the name of the task and it’s pid when the function “check_hung_uninterruptible_tasks” is called (https://elixir.bootlin.com/linux/latest/source/kernel/hung_task.c#L178) - You can see the output in the screenshot below.

```
Troller $ sudo cat /proc/sys/kernel/hung_task_timeout_secs
120
Troller $ sudo bpftrace -e 'kfunc:check_hung_uninterruptible_tasks { printf("%s:%d\n",curtask->comm,curtask->pid); }'
Attaching 1 probe...
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
khungtaskd:34
```


kswapd

The kernel thread “kswapd” is the background page-out daemon of Linux (swaps processes to disk). You can see the creation of the kernel thread in the source of the kernel - <https://elixir.bootlin.com/linux/latest/source/mm/vmscan.c#L4642>. In the code we can see that a dedicated instance of “kswapd” is created for each NUMA zone (on my Ubuntu 22.10 VM I have only “kswapd0” - as shown in the screenshot below).

Overall, the goal of the “kswapd” is to reclaim pages when memory is running low. In the old days, the “kswapd” was woken every 10 seconds but today it is only wakened by the page allocator, by calling “wakeup_kswapd”²². The code of the page allocator is located at “mm/page_alloc.c”²³.

Basically, “kswapd” trickles out pages so the system has some free memory even if no other activity frees up anything (like by shrinking cache). Think about cases in which operations work in asynchronous contexts that cannot page things out.

The major function which is called by “kswapd” is “balance_pgdat()”²⁴. In order to see that process happening we can use the following bpftrace one-liner: “**sudo bpftrace -e 'kfunc:balance_pgdat { printf("%s:%d\n",curtask->comm,curtask->pid); }**” - You can see “kswapd0” calling it in the screenshot below. The flow of “kswapd” is based on limits, when to start shirking and “until when” to shrink (low and high limits).

```
Troller # sudo bpftrace -e 'kfunc:balance_pgdat { printf("%s:%d\n",curtask->comm,curtask->pid); }'
Attaching 1 probe...
kswapd0:97
kswapd0:97
kswapd0:97
kswapd0:97
kswapd0:97
kswapd0:97
kswapd0:97
kswapd0:97
kswapd0:97
kswapd0:97
kswapd0:97
```

²² <https://elixir.bootlin.com/linux/latest/source/mm/vmscan.c#L4555>

²³ https://elixir.bootlin.com/linux/latest/source/mm/page_alloc.c

²⁴ <https://elixir.bootlin.com/linux/latest/source/mm/vmscan.c#L4146>

kcompactd

When a Linux system is up and running, memory pages of different processes/tasks are scattered and thus are not physically-contiguous (even if they are contiguous in their virtual address). We can move to bigger pages size (like from 4K to 4M) but it still has its limitations like: waste of space in case of regions with small sizes and the need for multiple pages in case of large regions that can still be fragmented. Due to that, the need for memory compaction was born²⁵.

“kcompactd” is performing in the background the memory compaction flow. The goal of memory compaction is to reduce external fragmentation. This procedure is heavily dependent on page migration²⁶ to do all the heavy lifting²⁷. In order for “kcompactd” to work we should compile the kernel with “CONFIG_COMPACTIO” enabled. Also, when a Linux system identifies that it is tight low in available memory the “kcompactd” won’t perform memory compaction memory²⁸.

Overall, the “kcompactd” kernel thread is created in “kcompactd_run” function²⁹ which is called by “kcompactd_init”³⁰. The function “kcompactd_init” is started by “subsys_initcall”³¹, which is responsible for initializing a subsystem.

The kernel thread starts the function “static int kcompactd(void *p)”³². An instance of the kernel thread is created for each node (like vCPU) on the system³³. The pattern of the kernel thread name is “kcompactd[IndexOfNode]” for example “kcompactd0” as we can see in the screenshot below.

“kcompactd” can be called in one of two ways: woken up or by using a timeout. It can be woken up by kswapd³⁴. Also, we can configure it using modification of the filesystem (“/proc/sys/vm/compact_memroy” for example). By the way, in the memory compaction flow of the function “compact_zone”³⁵ is executed in the context of “kcompactd”. In order to demonstrate that we can use the following one-liner using bpftrace: **sudo bpftrace -e 'kfunc:compact_zone { printf("%s:%d\n",curtask->comm,curtask->pid); }'** - The output can be seen in the screenshot below.

²⁵ <https://lwn.net/Articles/368869/>

²⁶ <https://lwn.net/Articles/157066/>

²⁷ <https://elixir.bootlin.com/linux/v6.2-rc3/source/mm/compaction.c#L5>

²⁸ <https://www.linux-magazine.com/Issues/2015/179/Kernel-News>

²⁹ <https://elixir.bootlin.com/linux/v6.2-rc3/source/mm/compaction.c#L2996>

³⁰ <https://elixir.bootlin.com/linux/v6.2-rc3/source/mm/compaction.c#L3048>

³¹ <https://elixir.bootlin.com/linux/v6.2-rc3/source/mm/compaction.c#L3065>

³² <https://elixir.bootlin.com/linux/v6.2-rc3/source/mm/compaction.c#L2921>

³³ <https://elixir.bootlin.com/linux/v6.2-rc3/source/mm/compaction.c#L3061>

³⁴ <https://www.slideshare.net/AdrianHuang/memory-compaction-in-linux-kernelpdf>

³⁵ <https://elixir.bootlin.com/linux/v6.2-rc3/source/mm/compaction.c#L2289>

```
Troller # ps -ef | grep -v grep | grep kcompactd
root      37      2  0 00:15 ?                00:00:09 [kcompactd0]
Troller # ls -l /proc/sys/vm/compact_memory
--w----- 1 root root 0 Jan 14 11:54 /proc/sys/vm/compact_memory
Troller # sudo bpftrace -e 'kfunc:compact_zone { printf("%s:%d\n",curtask->comm,curtask->pid); }'
Attaching 1 probe...
kcompactd0:37
kcompactd0:37
kcompactd0:37
```

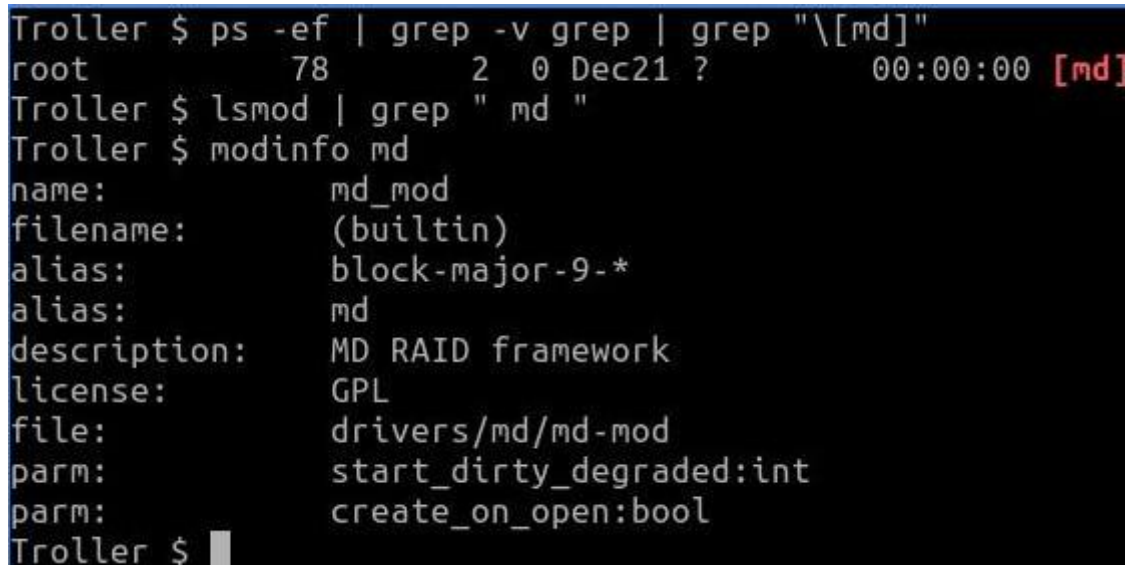
md (Multiple Device Driver)

“md” is a kernel thread which is based on a workqueue³⁶. It is responsible for managing the Linux md (multiple device) driver which is also known as the “Linux software RAID”. RAID devices are virtual devices (created from two or more real block devices). This allows multiple devices (typically disk drives or partitions thereof) to be combined into a single device to hold (for example) a single filesystem³⁷.

By using the “md” driver we can create from one/more physical devices (like disk drivers) a virtual device(s). By the use of an array of devices we can achieve redundancy, which is also known as RAID (Redundant Array of Independent Disks). For more information I suggest reading <https://man7.org/linux/man-pages/man4/md.4.html>.

Overall, “md” supports different RAID types: RAID 1 (mirroring), RAID 4, RAID 5, RAID 6 and RAID 10. For more information about RAID types I suggest reading the following link <https://www.prepressure.com/library/technology/raid>. Besides that, “md” also supports pseudo RAID technologies like: RAID 0, LINAR, MULTIPATH and FAULTY³⁸.

The code of “md” is included as a driver/kernel module in the source code of Linux. Thus, it can be compiled directly into the kernel or as a separate “*.ko” file. In my VM (Ubuntu 22.04) it is compiled directly into the kernel image as shown in the screenshot below.

A terminal window with a black background and white text. The prompt is 'Troller \$'. The first command is 'ps -ef | grep -v grep | grep "\[md]"', which shows a process for 'md' with PID 78, PPID 2, and status 0. The second command is 'lsmod | grep " md "', which shows the 'md' module is loaded. The third command is 'modinfo md', which displays detailed information about the 'md' module, including its name, filename, alias, description, license, file path, and parameters.

```
Troller $ ps -ef | grep -v grep | grep "\[md]"
root          78          2   0 Dec21 ?                00:00:00 [md]
Troller $ lsmod | grep " md "
Troller $ modinfo md
name:                md_mod
filename:             (builtin)
alias:                block-major-9-*
alias:                md
description:          MD RAID framework
license:              GPL
file:                 drivers/md/md-mod
parm:                 start_dirty_degraded:int
parm:                 create_on_open:bool
Troller $
```

³⁶ <https://elixir.bootlin.com/linux/v6.1/source/drivers/md/md.c#L9615>

³⁷ <https://linux.die.net/man/8/mdadm>

³⁸ https://doxfer.webmin.com/Webmin/Linux_RAID

The block devices that can be used in order to access the software RAID on Linux are in the pattern “/dev/mdN” (where N is a number [0–255])³⁹. It can also be configured to allow access using “/dev/md/N” or “/dev/md/name”. If we want information about the current state of “md” we can query the file “/proc/mdstat” — for more information you can read <https://raid.wiki.kernel.org/index.php/Mdstat>. There is also the command line utility “mdadm” that can help with managing those devices⁴⁰.

Lastly, the init function is declared using “subsys_initcall” (and not the “module_init”) which ensures that it will run before the device drivers that needs it (if they are using “module_init”) — <https://elixir.bootlin.com/linux/v6.1/source/drivers/md/md.c#L9947>. More information about initcalls will be included on a future writeup.

³⁹ <https://www.oreilly.com/library/view/managing-raid-on/9780596802035/ch01s03.html>

⁴⁰ <https://linux.die.net/man/8/mdadm>

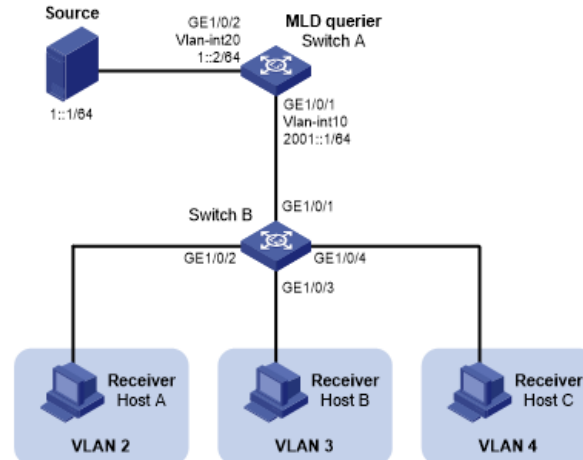
mld (Multicast Listener Discovery)

“mld” is a kernel thread which was created using a workqueue⁴¹. It is the Linux implementation for the multicast listener (MLD) protocol. This protocol is used by IPv6 based routers in order to discover multicast listeners on the local network and identify which multicast addresses are of interest to those listeners. MLD is supported on different operating systems such as Windows⁴² and Linux⁴³.

We can think about it like IGMP⁴⁴ which is used on IPv4 based networks (MLDv1 is derived from IGMPv2 and MLDv2 is similar to IGMPv3). One important difference is that MLD uses ICMPv6 message types, rather than IGMP message types⁴⁵.

Overall, MLD has three major message types: “Multicast Listener Query”, “Multicast Listener Report” and “Multicast Done”. For more information about them I suggest reading the following link⁴⁶. Also, a more detailed explanation about the different MLD operations can be found in <https://ipccisco.com/lesson/mld-operations/>.

What “mld” does is to send MLD report messages⁴⁷ which are sent by an MLD host (see the diagram below⁴⁸) and processes messages⁴⁹. From the source code we can see that there are definitions for structs representing both MLDv1 and MLDv2 headers.



⁴¹ <https://elixir.bootlin.com/linux/latest/source/net/ipv6/mcast.c#L3185>

⁴² <https://learn.microsoft.com/en-us/windows/win32/winsock/igmp-and-windows-sockets>

⁴³ <https://lwn.net/Articles/29489/>

⁴⁴ <https://www.cloudflare.com/learning/network-layer/what-is-igmp/>

⁴⁵ <https://www.ibm.com/docs/en/zos/2.2.0?topic=protocol-multicast-listener-discovery>

⁴⁶ <https://community.cisco.com/t5/networking-knowledge-base/multicast-listener-discovery-mld/ta-p/3112082>

⁴⁷ <https://elixir.bootlin.com/linux/latest/source/net/ipv6/mcast.c#L3185>

⁴⁸ https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3944_ip-multi_cg/content/images/image33.png

⁴⁹ <https://elixir.bootlin.com/linux/latest/source/net/ipv6/mcast.c#L1359>

kmsd (Kernel Same Page Merging)

The kernel thread “ksm” is also known as “Kernel Same Page Merging” (and “kmsd” is ksm demon). It is used by the KVM hypervisor to share identical memory pages (supported since kernel 2.6.32) Those shared pages could be common libraries or even user data which is identical. By doing so KVM (Kernel-based Virtual Machine) can avoid memory duplication and enable more VMs to run on a single node.

In order for “kmsd” to save memory due to de-duplication we should compile the kernel with “CONFIG_KSM=y”. It is important to understand that the sharing of identical pages is done even if they are not shared by fork(). If you want to go over “kmsd” source code you can use the following link - <https://elixir.bootlin.com/linux/latest/source/mm/ksm.c>.

The way “kmsd” works is as follows. Scanning main memory for frames (“physical pages”) holding identical data and collectes the virtual memory address that they are mapped. “kmsd” leaves one of those frames and remaps each duplicate one to point to the same frame. Lastly, “kmsd” frees the other frames. All of the merge pages are marked as COW (Copy-on-Write) for cases in which one of the processes using them will want to write to the page. There is a concern that even if the memory usage is reduced the CPU usage is increased.

The kernel thread “kmsd” is created using the function kthread_run⁵⁰. We can see from the code that the function which is the entry point of the thread is “ksm_scan_therad()” which is calling “ksm_do_scan()” which is the ksm’s scanner main worker function (it gets as input the number of pages to scan before returning). “kmsd” only merges anonymous private pages and not pagecache. Historically, the merged pages were pinned into kernel memory. Today they can be swapped like any other pages.

“kmsd” can be controlled by a sysfs interface (“/sys/kernel/mm/ksm”) - as can be seen in the screenshot below. One of the files exported by sysfs is “run” that can react to one of the following values 0/1/2. “0” means stop “kmsd” from running but keep the merged pages. “1” means run “kmsd”. “2” means stop “kmsd” from running and unmerge all currently merge pages (however leave the mergeable areas registered for next time).

```
Troller # pwd
/sys/kernel/mm/ksm
Troller # ls *
full_scans          pages_shared  pages_unshared  sleep_millisecs  stable_node_dups
max_page_sharing    pages_sharing pages_volatile  stable_node_chains  use_zero_pages
merge_across_nodes  pages_to_scan run            stable_node_chains_prune_millisecs
```

⁵⁰ <https://elixir.bootlin.com/linux/v6.0/source/mm/ksm.c#L3188>

ttm_swap

The kernel thread “ttm_swap” is responsible for swapping GPU’s (Graphical Processing Unit) memory. Overall, TTM (Translation-Table Maps) is a memory manager that is used to accelerate devices with dedicated memory. Basically, all the resources are grouped together by objects of buffers in different sizes. TTM then handles the lifetime, the movements and the CPU mapping of those objects⁵¹.

Based on the kernel documentation, each DRM (Direct Rendering Manager) driver needs a memory manager. There are two memory managers supported by DRM: TTM and GEM (Graphics Execution Manager). I am not going to talk about GEM, if you want you can start reading about in the following link - <https://docs.kernel.org/gpu/drm-internals.html>.

Moreover, “ttm_swap” is a single threaded workqueue as seen in the Linux source code⁵².

Also, the man pages describe TTM as a generic memory-manager provided by the kernel, which does not provide a user-space interface (API). In case we want to use it you should checkout the interface of each driver⁵³.

TTM is at the end a kernel module, you can find the source code and the Makefile in the kernel source tree⁵⁴. Based on the module source code it is written by Thomas Hellstrom and Jerome Glisse⁵⁵. Also, it is described as “TTM memory manager subsystem (for DRM device)”⁵⁶. As you can see it is part of the “drivers/gpu/drm” subdirectory, which holds the code and Makefile of the drm device driver, which provides support for DRI (Direct Rendering Infrastructure) in XFree86 4.1.0+.

Lastly, on my VM (Ubuntu 22.04.01) it is compiled as a separate “*.ko” file (/lib/modules/[KernelVersion]/kernel/drivers/gpu/drm/ttm.ko) - as you can see in the screenshot below.

⁵¹ <https://docs.kernel.org/gpu/drm-mm.html>

⁵² https://elixir.bootlin.com/linux/v5.12.19/source/drivers/gpu/drm/ttm/ttm_memory.c#L424

⁵³ <https://www.systutorials.com/docs/linux/man/7-drm-ttm/>

⁵⁴ <https://elixir.bootlin.com/linux/v6.1-rc2/source/drivers/gpu/drm/ttm>

⁵⁵ https://elixir.bootlin.com/linux/v6.1-rc2/source/drivers/gpu/drm/ttm/ttm_module.c#L89

⁵⁶ https://elixir.bootlin.com/linux/v6.1-rc2/source/drivers/gpu/drm/ttm/ttm_module.c#L89


```
Troller # modinfo ttm | head -15
filename:      /lib/modules/5.15.0-52-generic/kernel/drivers/gpu/drm/ttm/ttm.ko
license:      GPL and additional rights
description:   TTM memory manager subsystem (for DRM device)
author:       Thomas Hellstrom, Jerome Glisse
srcversion:   52AE33CCBE42B11150B88C3
depends:       drm
retpoline:    Y
intree:       Y
name:         ttm
vermagic:     5.15.0-52-generic SMP mod_unload modversions
sig_id:       PKCS#7
signer:       Build time autogenerated kernel key
sig_key:      49:B2:3F:66:E1:3B:8B:67:11:CE:17:63:41:27:D0:B1:28:DF:09:8C
sig_hashalgo: sha512
```

watchdogd

This kernel thread “watchdog” is used in order to let the kernel know that a serious problem has occurred so the kernel can restart the system. It is sometimes called COP (Computer Operating Properly). The way it is implemented is by opening “/dev/watchdog”, then writing at least once a minute. Every time there is a write the restart of the system is delayed.

In case of inactivity for a minute the watchdog should restart the system. Due to the fact we are not talking about a hardware watchdog the compilation of the operation depends on the state of the machine. You should know that the watchdog implementation could be software only (there are cases in which it won’t restart the machine due to failure) or using a driver/module in case of hardware support⁵⁷.

If we are talking about hardware support then the watchdog module is specific for a chip or a device hardware. It is most relevant to systems that need the ability to restart themselves without any human intervention (as opposed to a PC we can reboot easily) - think about an unmanned aircraft. We need to be careful because a problem in the watchdog configuration can lead to unpredictable reboot, reboot loops and even file corruption due to hard restart⁵⁸.

The relationship between the hardware and software is as follows: the hardware is responsible to set up the timer and the software is responsible to reset the timer. When the timer gets to a specific value (configured ahead) and it is not elapsed by the software the hardware will restart the system. For an example of using hardware for this functionality you can read the following link <https://developer.toradex.com/linux-bsp/how-to/linux-features/watchdog-linux/>.

The software part is being conducted by the “watchdog” (the software watchdog daemon) which opens “/dev/watchdog” and writes to it in order to postpone the restart of the system by the hardware - for more information you can read <https://linux.die.net/man/8/watchdog>. Examples for different watchdog drives/modules for specific chips can be found in the source tree of linux here <https://elixir.bootlin.com/linux/v6.0.11/source/drivers/watchdog>. Some examples are apple_wdt (Apple’s SOC), ath79_wdt (Atheros AR71XX/AR724X/AR913X) and w83977f_wdt (Winbond W83977F I/O Chip).

We can stop the watchdog without restarting the system by closing “/dev/watchdog”. It is not possible if the kernel was compiled with “CONFIG_WATCHDOG_NOWAYOUT” enabled. Overall, in order for the watchdog to operate the kernel needs to be compiled with CONFIG_WATCHDOG=y and “/dev/watchdog” character device should be created (with major number of 10 and minor number of 130 - checkout “man mknod” if you want to create it).

⁵⁷ <https://github.com/torvalds/linux/blob/master/Documentation/watchdog/watchdog-api.rst>

⁵⁸ <https://linuxhint.com/linux-kernel-watchdog-explained/>

Lastly, if you want to see the status of the watchdog you can use the command “wdctl”⁵⁹ - As can be seen in the screenshot below⁶⁰. For more information about the concept I suggest reading https://en.wikipedia.org/wiki/Watchdog_timer.

```
(root@ako-kaede-mirai)-(12:25am--09/06) r--"
(kousekip) r" wdctl
Device:      /dev/watchdog0
Identity:    SP5100 TCO timer [version 0]
Timeout:     60 seconds
Pre-timeout: 0 seconds
FLAG        DESCRIPTION                STATUS BOOT-STATUS
KEEPALIVEPING Keep alive ping reply                1      0
MAGICCLOSE   Supports magic close char            0      0
SETTIMEOUT   Set timeout (in seconds)             0      0
```

⁵⁹ <https://man7.org/linux/man-pages/man8/wdctl.8.html>

⁶⁰ https://en.wikipedia.org/wiki/Watchdog_timer#/media/File:Wdctl_screenshot.png

zswap-shrink

Based on the kernel source code zswap is a backend for frontswap. Frontswap provides a “transcendent memory” interface for swap pages. In some cases we can get increased performance by saving swapped pages in RAM (or a RAM-like device) and not on disk as swap partition\swapfile⁶¹. The frontends are usually implemented in the kernel while the backend is implemented as a kernel module (as we will show soon). Zswap takes pages that are in the process of being swapped out and attempts to compress and store them in a RAM-based memory pool⁶².

We can say that zswap trades CPU cycles for potentially reduced swap I/O. A significant performance improvement can happen in case the reads from the swap device are much slower than the reads from the compressed cache⁶³. The “zswap_frontswap_store” is the function that attempts to compress and store a single page⁶⁴.

The kernel thread “zswap-shrink” is created based on a workqueue⁶⁵. On my VM (Ubuntu 22.04.1) zswap is compiled part of the kernel itself and not as a separate “*.ko” (kernel module). You can see in the screenshot below that it does not appear in the output of “lsmod” and is marked as builtin (look at the filename field) in the output of “modinfo”.

```
Troller # ps -ef | grep zswap-shrink #show the zswap-shrink kernel thread
root      128          2  0 Oct21 ?        00:00:00 [zswap-shrink]
root     169924    164567  0 20:39 pts/6    00:00:00 grep --color=auto zswap-shrink
Troller # lsmod | grep zswap #check if zswap is loaded outside the kernel
Troller # modinfo zswap #show zswap builtin
name:          zswap
filename:      (builtin)
description:   Compressed cache for swap pages
author:       Seth Jennings <sjennings@variantweb.net>
license:      GPL
file:         mm/zswap
parm:         max_pool_percent:uint
parm:         accept_threshold_percent:uint
parm:         same_filled_pages_enabled:bool
Troller # dmesg | grep zswap
[    1.071279] zswap: loaded using pool lzo/zbud
Troller #
```

For more information like the compression used by zswap (the default one is lzo) and other parameters that can be configured for zswap I suggest reading the following link <https://wiki.archlinux.org/title/zswap>. You can also read the parameter ons “/sys/module/zswap/parameters”.

⁶¹ <https://www.kernel.org/doc/html/v4.18/vm/frontswap.html>

⁶² <https://elixir.bootlin.com/linux/latest/source/mm/zswap.c>

⁶³ <https://www.kernel.org/doc/html/v4.18/vm/zswap.html>

⁶⁴ <https://elixir.bootlin.com/linux/v6.1-rc2/source/mm/zswap.c#L1097>

⁶⁵ <https://elixir.bootlin.com/linux/v6.1-rc2/source/mm/zswap.c#L1511>

khugepaged

The kernel thread “kugepaged” is created using the “kthread_run()” function⁶⁶. It is responsible for the “Transparent Hugepage Support” (aka THP). “kugepaged” scans memory and collapses sequences of basic pages into huge pages⁶⁷.

We can manage and configure TPH using sysfs⁶⁸ or by using the syscalls “madvise”⁶⁹ and “prctl”⁷⁰. The scan of memory is done by calling “khugepaged_do_scan()”⁷¹ which in turn calls “khugepaged_scan_mm_slot()”⁷². In order to demonstrate that I have used the following bpftrace oneliner **“sudo bpftrace -e 'kfunc:khugepaged_scan_mm_slot{ printf("%s:%d\n",curtask->comm,curtask->pid); }”**. The output is shown in the screenshot below.

Lastly, we can also monitor the modifications made by “khugepaged” by checking the information on “/proc”. For example we can check the “AnonHugePages”/”ShmemPmdMapped”/”ShmemHugePages” in “/proc/meminfo”, which is global for the entire system. If we want information regarding a specific process/task we can use “/proc/[PID]/smaps” and count “AnonHugePages”/”FileHugeMapped” for each mapping (<https://www.kernel.org/doc/html/latest/admin-guide/mm/transhuge.html>).

```
Troller $ sudo bpftrace -e 'kfunc:khugepaged_scan_mm_slot{ printf("%s:%d\n",curtask->comm,curtask->pid); }'
Attaching 1 probe...
khugepaged:39
khugepaged:39
khugepaged:39
khugepaged:39
khugepaged:39
khugepaged:39
khugepaged:39
```

⁶⁶ <https://elixir.bootlin.com/linux/latest/source/mm/khugepaged.c#L2551>

⁶⁷ <https://www.kernel.org/doc/html/latest/admin-guide/mm/transhuge.html>

⁶⁸ <https://www.kernel.org/doc/html/latest/admin-guide/mm/transhuge.html#thp-sysfs>

⁶⁹ <https://man7.org/linux/man-pages/man2/madvise.2.html>

⁷⁰ <https://man7.org/linux/man-pages/man2/prctl.2.html>

⁷¹ <https://elixir.bootlin.com/linux/latest/source/mm/khugepaged.c#L2404>

⁷² <https://elixir.bootlin.com/linux/v6.1.12/source/mm/khugepaged.c#L2250>

krfcommd

“krfcommd” is a kernel which is started by executing “kthread_run()” function⁷³. The kernel thread executes the “rfcomm_run()” function⁷⁴. Thus, we can say that “krfcommd” is responsible for RFCOMM connections⁷⁵.

RFCOMM (Radio Frequency Communication) is a set of transport protocols on top of L2CAP which provides emulated RS-232 serial ports. It provides a simple reliable data stream (like TCP). It is used directly by many telephony related profiles as a carrier for AT commands, as well as being a transport layer for OBEX over Bluetooth⁷⁶.

Moreover, there is also an “rfcomm” cli tool in Linux. It is used to inspect and maintain RFCOMM configuration⁷⁷. For more information about RFCOMM I suggest reading <https://www.btframework.com/rfcomm.htm>. You can also go over the protocol specification⁷⁸.

Also, RFCOMM protocol supports up to 60 simultaneous connections between two Bluetooth devices. The number of connections that can be used simultaneously is implementation-specific. For the purposes of RFCOMM, a complete communication path involves two applications running on different devices (the communication endpoints) with a communication segment between them⁷⁹.

Lastly, RFCOMM is implemented as a kernel module. Thus, it can be compiled directly to the kernel or separate kernel module - in the screenshot below we can see it compiled as a separate file.

```
root@localhost:~# modinfo rfcomm
filename:       /lib/modules/5.19.7-arch1-1.0/kernel/net/bluetooth/rfcomm/rfcomm.ko.zst
alias:          bt-proto-3
license:        GPL
version:        1.11
description:    Bluetooth RFCOMM ver 1.11
author:         Marcel Holtmann <marcel@holtmann.org>
srcversion:     2787EECAEC282A1A24A7701
depends:         bluetooth
retpoline:      Y
intree:         Y
name:           rfcomm
vermagic:       5.19.7-arch1-1.0 SMP preempt mod_unload 686
sig_id:         PRCS#7
signer:         Build time autogenerated kernel key
sig_key:        30:9a:19:01:ba:9c:ba:d5:c0:8d:f7:a5:39:aa:c7:54:a6:c9:d8:2b
sig_hashalgo:   sha512
signature:      30:64:02:30:6c:ab:da:07:56:cc:36:9d:66:06:e2:8b:98:e9:4a:50:
77:c0:37:08:0a:12:cd:5d:b4:f7:2f:4a:fa:cb:58:68:b9:c4:7b:c0:
08:1c:ec:61:33:fa:7e:a8:69:6b:fd:e7:02:30:69:c8:06:98:12:9c:
e3:b3:25:33:03:12:81:d6:77:59:54:f5:8e:5b:d5:ff:c4:5d:d1:f1:
02:0e:16:68:2e:33:84:97:2d:fd:be:35:1b:30:eb:17:aa:dd:01:ea:
93:0c
parm:           disable_cfc:Disable credit based flow control (bool)
parm:           channel_mtu:Default MTU for the RFCOMM channel (int)
parm:           l2cap_ertm:Use L2CAP ERTM mode for connection (bool)
```

⁷³ <https://elixir.bootlin.com/linux/latest/source/net/bluetooth/rfcomm/core.c#L2215>

⁷⁴ <https://elixir.bootlin.com/linux/latest/source/net/bluetooth/rfcomm/core.c#L2109>

⁷⁵ <https://stackoverflow.com/questions/57152408/what-is-the-internal-mechanics-of-socket-function>

⁷⁶ https://en.wikipedia.org/wiki/List_of_Bluetooth_protocols

⁷⁷ <https://linux.die.net/man/1/rfcomm>

⁷⁸ <https://www.bluetooth.com/specifications/specs/rfcomm-1-1/>

⁷⁹ https://www.amd.e-technik.uni-rostock.de/ma/gol/lectures/wirlec/bluetooth_info/rfcomm.html

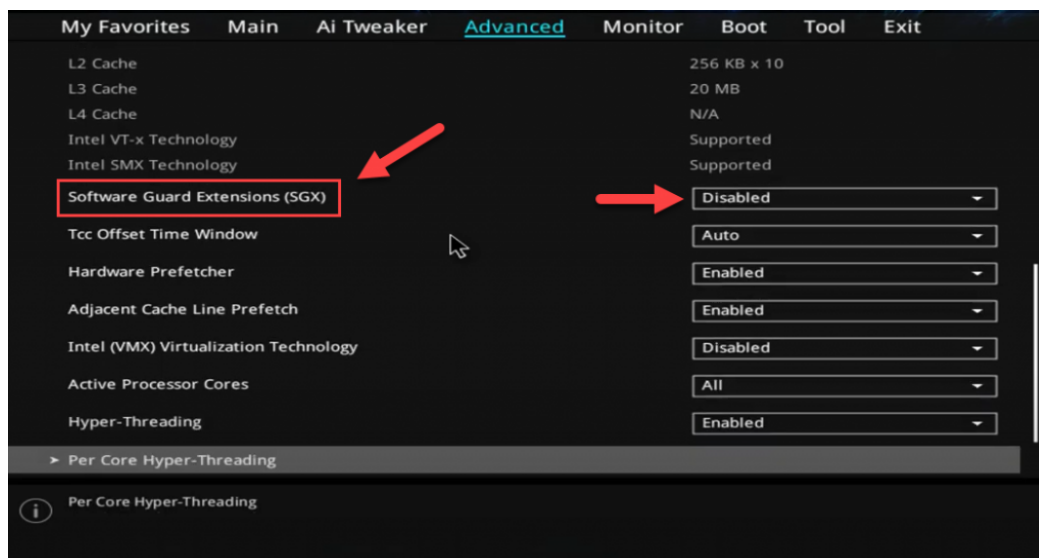
ksgxd

The kernel thread “ksgxd” is part of the Linux support for SGX (Software Guard eXtensions). Overall, SGX is a hardware security feature of Intel’s CPU that enables applications to allocate private memory regions for data and code. There is a privilege opcode “ENCLS” which allows creation of regions and “ENCLU” which is a privilege opcode that allows entering and executing code inside the regions⁸⁰. For more information about SGX you can read my writeup about it⁸¹.

“ksgxd” is a kernel which is started by executing “kthread_run()” function⁸². The kernel thread executes the “ksgxd” function⁸³. “ksgxd” is started while SGX is initializing and at boot time it re-initializes all enclave pages. In case of over commitment “ksgxd” is also responsible for swapping enclave memory⁸⁴ like “kswapd”⁸⁵.

If you want to know if your CPU supports SGX you can use the following command: “cat /proc/cpuinfo | grep sgx” (you can also use lscpu). You can also check your UEFI (legacy BIOS) configuration to check if you - check out the screenshot below⁸⁶.

Lastly, there is a great guide for an example SGX app using a Linux VM on Azure that I encourage you to read⁸⁷. For more information about the Linux stack for SGX I suggest reading https://download.01.org/intelsgxstack/2021-12-08/Getting_Started.pdf and going over the following github repo <https://github.com/intel/linux-sgx>.



⁸⁰ <https://docs.kernel.org/x86/sgx.html>

⁸¹ <https://medium.com/@boutnaru/security-sgx-software-guard-extension-695cab7dbcb2>

⁸² <https://elixir.bootlin.com/linux/v6.1.10/source/arch/x86/kernel/cpu/sgx/main.c#L427>

⁸³ <https://elixir.bootlin.com/linux/v6.1.10/source/arch/x86/kernel/cpu/sgx/main.c#L395>

⁸⁴ <https://elixir.bootlin.com/linux/v6.1.10/source/arch/x86/kernel/cpu/sgx/main.c#L188>

⁸⁵ <https://medium.com/@boutnaru/the-linux-process-journey-kswapd-22754e783901>

⁸⁶ <https://phoenixnap.com/kb/intel-sgx>

⁸⁷ <https://tsmatz.wordpress.com/2022/05/17/confidential-computing-intel-sgx-enclave-getting-started/>