Close lid to encrypt

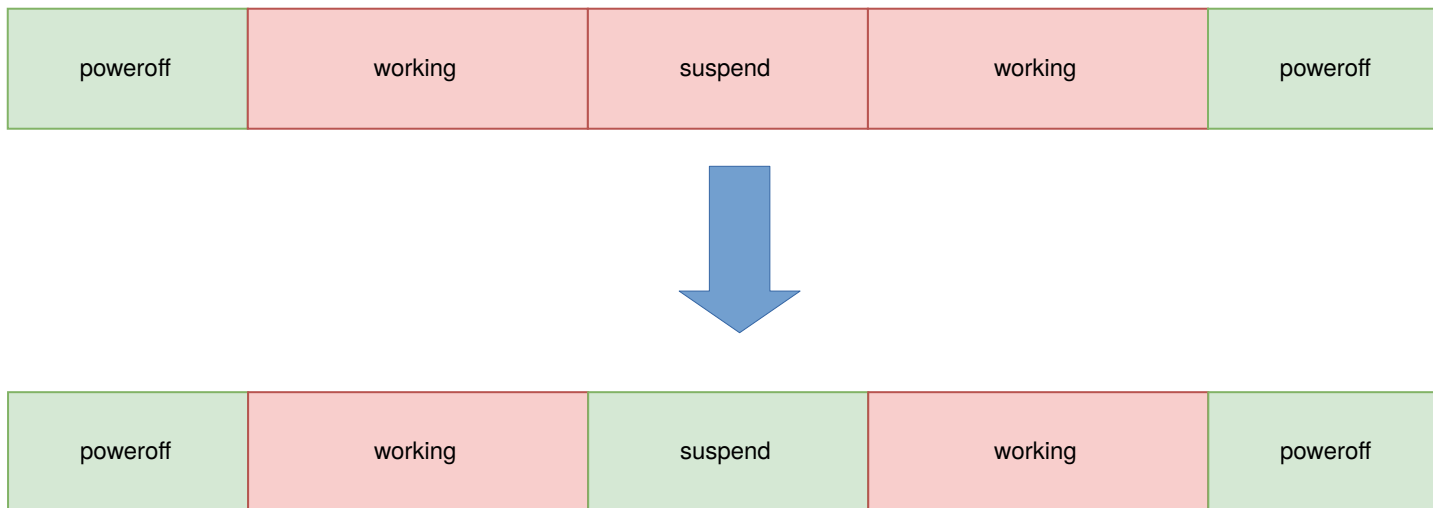## Hard disk encryption in Linux suspend mode

Tim Dittler
FOSDEM, 02.02.2020

What's „Close lid to encrypt"?

- **Project by Jonas Meurer and me**

  – Freelancing systems engineers living in Germany

- **Full-disk encryption in suspend mode**
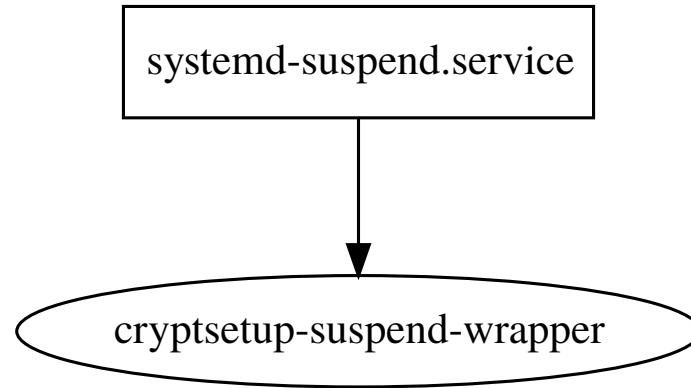
- **For Debian and derivatives**

Why is is useful?

- **Full-disk encryption protects your data only at rest**

poweroff	working	suspend	working	poweroff

⬇

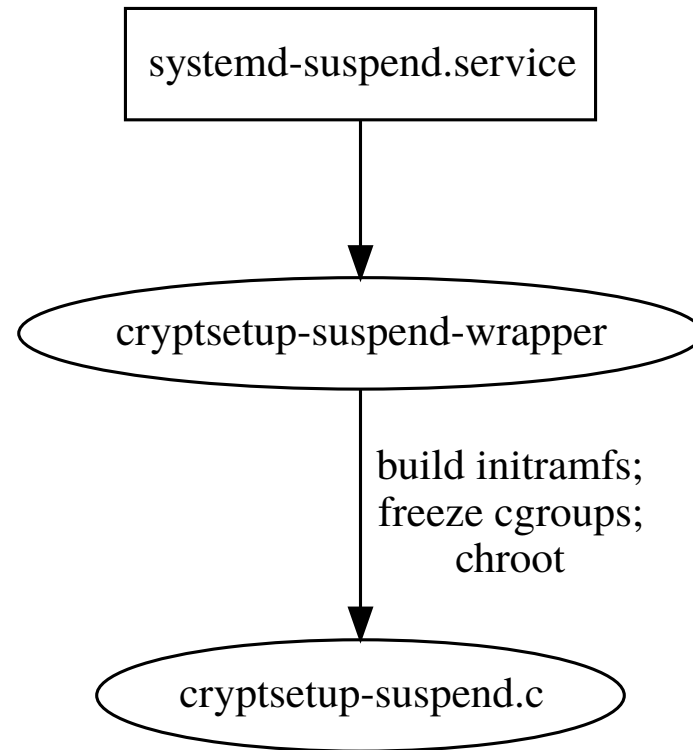| poweroff	working	suspend	working	poweroff

Why is it difficult?

- **Well, we're locking away your running operating system!**
- **Race conditions**
  - Prevent access to locked filesystems
  - Otherwise kernel will wait forever
- **Memory management**
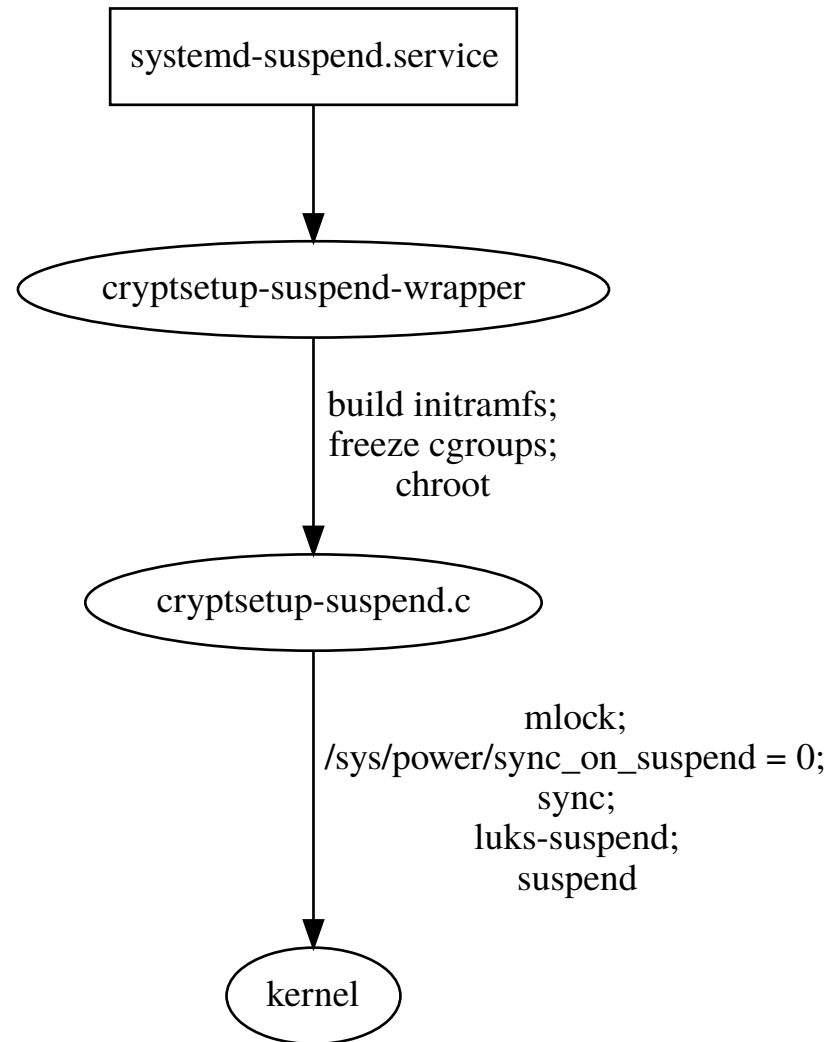 - Swap on harddrive is encrypted

How is it implemented?

```
┌─────────────────────────┐
│ systemd-suspend.service │
└─────────────────────────┘
             │
             ▼
   ╭─────────────────────────╮
  ( cryptsetup-suspend-wrapper )
   ╰─────────────────────────╯
```

How is it implemented?

How is it implemented?

/sys/power/sync_on_suspend ???

index : kernel/git/torvalds/linux.git

Linux kernel source tree

about   summary   refs   log   tree   commit   diff   stats

author	🍀 Jonas Meurer <jonas@freesources.org>	2020-01-16 12:53:54 +0100
committer	🐧 Rafael J. Wysocki <rafael.j.wysocki@intel.com>	2020-01-16 21:47:03 +0100
commit	c052bf82c6b00ca27aab0859addc4b3159dfd3a4 (patch)	
tree	5d705708933306bc2c9600133255c8110869bd3a	
parent	5c0e9de06577ba7599b75f97a8bb8cc63f6cb2ad (diff)	
download	linux-c052bf82c6b00ca27aab0859addc4b3159dfd3a4.tar.gz	

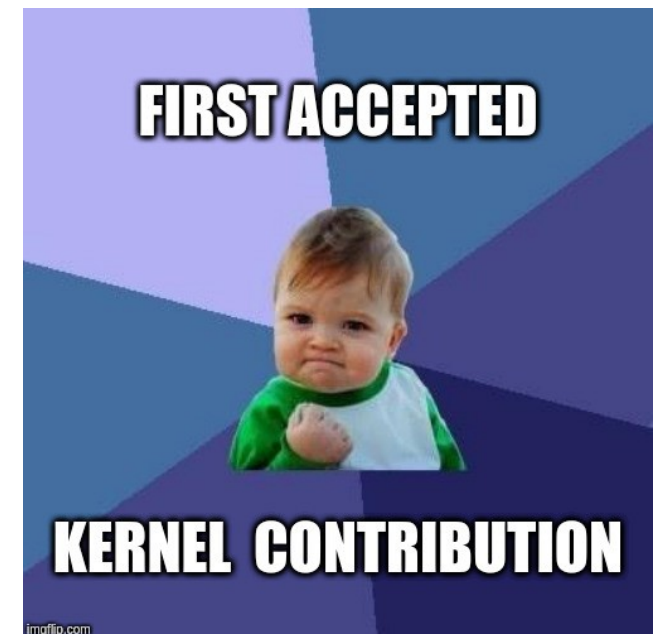**PM: suspend: Add sysfs attribute to control the "sync on suspend" behavior**

The sysfs attribute `/sys/power/sync_on_suspend` controls, whether or not
filesystems are synced by the kernel before system suspend.

Congruously, the behaviour of build-time switch CONFIG_SUSPEND_SKIP_SYNC
is slightly changed: It now defines the run-tim default for the new sysfs
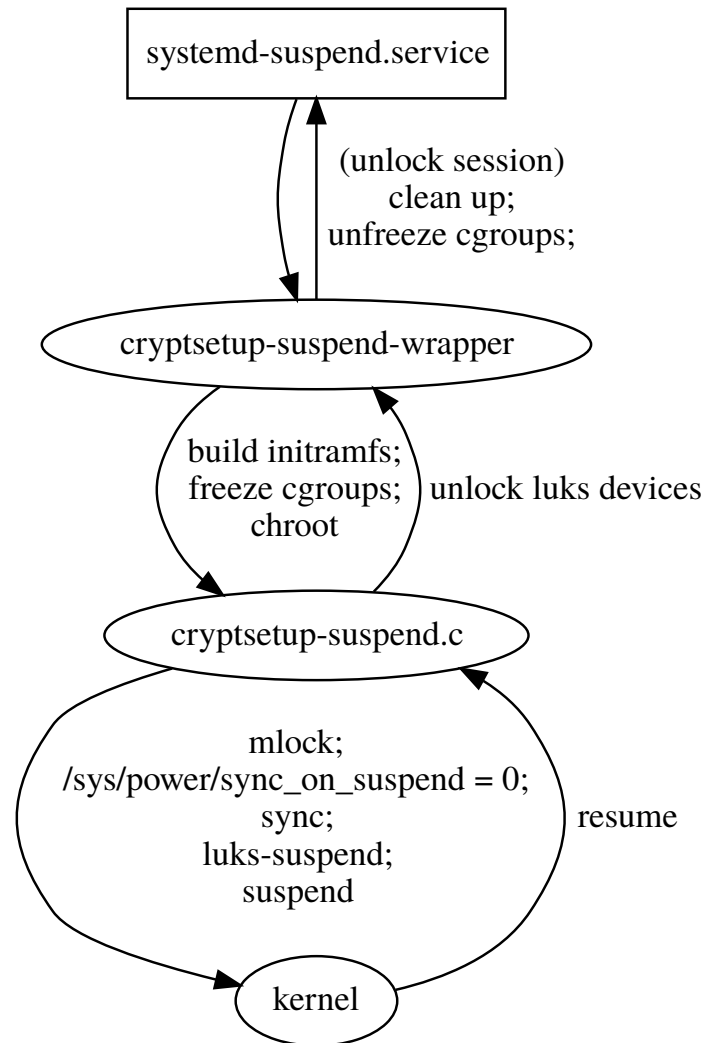attribute `/sys/power/sync_on_suspend`.

The run-time attribute is added because the existing corresponding
build-time Kconfig flag for (`CONFIG_SUSPEND_SKIP_SYNC`) is not flexible
enough. E.g. Linux distributions that provide pre-compiled kernels
usually want to stick with the default (sync filesystems before suspend)
but under special conditions this needs to be changed.

One example for such a special condition is user-space handling of
suspending block devices (e.g. using `cryptsetup luksSuspend` or `dmsetup
suspend`) before system suspend. The Kernel trying to sync filesystems
after the underlying block device already got suspended obviously leads
to dead-locks. Be aware that you have to take care of the filesystem sync
yourself before suspending the system in those scenarios.

Signed-off-by: Jonas Meurer <jonas@freesources.org>
Signed-off-by: Rafael J. Wysocki <rafael.j.wysocki@intel.com>

FIRST ACCEPTED

KERNEL CONTRIBUTION

imgflip.com

How is it implemented?

Demo

Demo

What's next?

- **More testing**
- **Merge upstream**
  - Debian Bullseye: „apt install cryptsetup-suspend"
- **How to handle situations with low available memory?**
- **There are more secrets in your memory than LUKS keys**

Thanks

- **Cryptsetup authors**
  - Jana Saout <jana@saout.de>
  - Clemens Fruhwirth <clemens@endorphin.org>
  - Milan Broz <gmazyland@gmail.com>
  - Ondrej Kozina <okozina@redhat.com>
- **Cryptsetup Debian maintainers**
  - Guilhem Moulin <guilhem@debian.org>
  - Jonas Meurer <jonas@freesources.org>

Thanks

- **Inspiration**
  - Vianney le Clément de Saint-Marcq <vleclement@gmail.com>
    - https://github.com/vianney/arch-luks-suspend
  - Jen Bowen <jen@nailfarmer.com>
    - https://github.com/nailfarmer/debian-luks-suspend/

Thanks

https://salsa.debian.org/
mejo/cryptsetup-suspend/

tim.dittler@systemli.org