LUKS encryption

Set up new encrypted volume

Format

```
cryptsetup luksFormat --type luks2 /dev/<dev>
cryptsetup luksDump /dev/<dev>
```

Note the UUID.

Open

```
cryptsetup luksOpen --allow-discards /dev/<dev> <name>
```

Creates new device `/dev/mapper/<name>`.

Format

```
mkfs.btrfs /dev/mapper/<name>
```

Note UUID.

Boot from unencrypted boot partition into encrypted root

Update GRUB configuration

In `/etc/default/grub`:

```
GRUB_CMDLINE_LINUX_DEFAULT="bgrt_disable loglevel=4 rd.luks.uuid=<LUKS UUID> rd.luks.allow-discards"
```

Update boot configuration

Make sure `/boot` and `/boot/efi` are mounted:

```
mount -a
```

Update grub:

```
update-grub
```

Update *initramfs*:

```
xbps-reconfigure -f linux6.6
```

(Re)install grub; make sure `/sys/firmware/efi/efivars` is bound if using `chroot` and `/boot` and `/boot/efi` are mounted:

```
grub-install /dev/<dev>
```

> If running into `symbol `grub_is_shim_lock_enabled` not found` error try removing `/boot/efi/EFI` and `/boot/grub` directories before running grub-install.

Where `<dev>` is the main device (not partition).

Check that grub had good configuration:

```
cat /boot/grub/grub.cfg | egrep 'crypt|luks'
```

Verify that `root=UUID` point to FS UUID and `rd.luks.uuid=` to LUKS UUID.

Revision #12
Created 2024-11-19 17:20:48 GMT by hxd
Updated 2024-11-19 20:32:03 GMT by hxd