Encrypted custom install

Asked 6 years, 7 months ago Modified 6 months ago Viewed 50k times

34

My computer runs Ubuntu. I want to install Ubuntu on another medium. I wish to enable encryption, yet as the ubuntu installer's default choices (erase/alongside/etc...) only concerns the default drive, I have to choose "something else" and create the partitions on the other drive manually, I create ~128mb part for boot, then I'm lost, if I make an encrytped partition with the rest of the space I'm unable to split it, so I have no swap; if instead I create two encrypted partitions, it doesn't seems right because it want to set up two different passwords...

How can I set up the swap then? (During or after install).

system-installation encryption luks

Share Improve this question

Follow

edited May 23, 2017 at 9:01

Zanna ♦

70k 56 218 328

asked May 23, 2017 at 8:10

Yvain

534 1 4 12

See also askubuntu.com/questions/293028/… – Flimm Nov 10, 2018 at 6:16

4 Answers

Sorted by: Highest score (default)

47

Update 2020-07-16: *This may not work with Ubuntu flavors that have moved away from the Ubiquity installer (eg. Lubuntu which now uses Calamares) because some of those installers go so far as to deactivate LVM partitions that they did not, themselves, configure in the pre-installation process. Thus, making unavailable the partitions that were configured for system installation.*

How to accomplish this *with* LVM and a single encrypted partition##

Warning

First of all 128M is too small for boot! I use 1G. Otherwise, what is bound to happen is that you may forget to remove old kernels and /boot will fill up, and you'll have to deal with the pain of trying to remove old kernels from the system so that you can get `apt` or `apt-get` to work again. Even with 1G, make sure you remove old kernels from time to time.

The next steps are not intended for novice users.
UPDATE: I have created a script that will perform the following operations for you and more! All you have to do is run it from the Live OS before installation. You can find a write-up on my blog.

Pre-installation from live OS

You want to setup LUKS and LVM while manually partitioning! I tested this on Ubuntu 16.04.2 / 18.04 / 20.04

Boot Ubuntu from a Live OS and select the option to try Ubuntu without installing. Follow the steps I've outlined below. Let's assume you're installing to /dev/sdb.

1. Partition the drive with your tool of choice: I used fdisk to set mine up on an msdos partition table as follows:
    - other partitions: existing OSs -- we don't care about these
    - sdb1: /boot (1G)
    - sdb2: LUKS partition (the rest of the disk)
2. Setup LUKS
    - `sudo cryptsetup luksFormat --hash=sha512 --key-size=512 --cipher=aes-xts-plain64 --verify-passphrase /dev/sdb2`
    - `sudo cryptsetup luksOpen /dev/sdb2 CryptDisk`
    - While not necessary, it is a good idea to fill your LUKS partition with zeros so that the partition, in an encrypted state, is filled with random data. `sudo dd if=/dev/zero of=/dev/mapper/CryptDisk bs=4M` *BEWARE, this could take a really long time!*

3. Setup LVM on /dev/mapper/CryptDisk
    - `sudo pvcreate /dev/mapper/CryptDisk`
    - `sudo vgcreate vg0 /dev/mapper/CryptDisk`
    - `sudo lvcreate -n swap -L 2G vg0`
    - `sudo lvcreate -n root -L 10G vg0`
    - `sudo lvcreate -n home -l +100%FREE vg0`

Installation from live OS

4. Now you're ready to install. When you get to the "Installation type" portion of the install, choose the "Something else" option. Then manually assign the /dev/mapper /vg0-* partitions as you would like to have the configured. Don't forget to set /dev/sdb1 as /boot. the /boot partition must not be encrypted. If it is, we won't be able to boot. Change the "Device for boot loader installation" to /dev/sdb, and continue with installation.
5. When installation is complete, **don't reboot**! Choose the option to "Continue Testing".

Post-installation configuration from live OS

This bit is really important if you want your system to boot! I spent quite a bit of time researching this to figure out these post-installation steps. In my case I was actually doing it because I wanted to customize the size of /boot on /dev/sda, but all that work should carry over to your situation as well.

6. In a terminal, type the following and look for the UUID of /dev/sdb2. Take note of that UUID for later.
    - `sudo blkid | grep LUKS`
    - The important line on my machine reads `/dev/sdb2: UUID="bd3b598d-88fc-476e-92bb-e4363c98f81d" TYPE="crypto_LUKS" PARTUUID="50d86889-02"`
7. Next lets get the newly installed system mounted again so we can make some more changes.
    - `sudo mount /dev/vg0/root /mnt`
    - `sudo mount /dev/vg0/home /mnt/home` # this is probably not necessary
    - `sudo mount /dev/sdb1 /mnt/boot`
    - `sudo mount --bind /dev /mnt/dev` # I'm not entirely sure this is necessary
    - `sudo mount --bind /run/lvm /mnt/run/lvm`
    - *(Only if you're using EFI):* `sudo mount /dev/sd*/your/efi/partition /mnt/boot/efi`
8. Now run `sudo chroot /mnt` to access the installed system

9. From the chroot, mount a couple more things
    - `mount -t proc proc /proc`
    - `mount -t sysfs sys /sys`
    - `mount -t devpts devpts /dev/pts`
10. Setup crypttab. Using your favorite text editor, create the file /etc/crypttab and add the following line, changing out the UUID with the UUID of your disk.

- `CryptDisk UUID=bd3b598d-88fc-476e-92bb-e4363c98f81d none luks,discard`

11. Lastly, rebuild some boot files.

- `update-initramfs -k all -c - update-grub`

12. Reboot, and the system should ask for a password to decrypt on boot!

Special thanks go to Martin Eve, EGIDIO DOCILE, and the folks at blog.botux.fr for tutorials they posted. By pulling pieces from their posts and doing a little extra trouble shooting, I was finally able to figure this out.

I tried this a number of times and failed over and over. The bit that I had to work out for myself based on error messages was `sudo mount --bind /run/lvm /mnt/run/lvm`

Share Improve this answer Follow

edited Jul 16, 2020 at 13:23

answered May 23, 2017 at 8:46

b_laoshi
4,610 2 23 46

Many thanks, yet I'm stuck at the beginning where i need to setup the luks partition. Cannot find it within fdisk -L output. – Yvain May 24, 2017 at 9:01

And when I try to setup the crypt I get and error: failed to remove headers – Yvain May 24, 2017 at 9:04

1 @Yvain - I believe this is wrong. Sha1 is no longer considered secure. Something more secure (such as the sha512 option suggested) should definitely be used. – some bits flipped Jun 6, 2017 at 16:09

1 +1 @b_laoshi Thanks a lot for the answer, it's helping me a lot :) – Tummala Dhanvi Dec 13, 2017 at 8:54

2 @b_laoshi Fantastic work, however `sudo mount --bind /dev /mnt/dev` was required, otherwise `update-initramfs -k all -c` fails – Nathan Oct 22, 2019 at 9:14

4

This is the answer for those who keep bumping into this question wanting to just slightly change the default partitioning of Ubuntu. For example, remove the `swap` partition and increase the `/boot` size. I think many people would be discouraged to follow b_laoshi's instruction, because of the amount of steps required.

So for simple custom partitioning with encryption I suggest to use "Erase disk and install Ubuntu" with "Encrypt the new Ubuntu installation for security" option. What we will change is the config for this default partitioning.

This configs are contained in `/lib/partman/recipes[-arch]/`. For myself, I've been changing `/lib/partman/recipes-amd64-efi/30atomic`. To get 538M for `efi`, 1024M for `/boot`, and the rest for `/` with ext4, I edited the file to

```
1024 1024 1024 fat32
    $iflabel{ gpt }
    $reusemethod{ }
    method{ efi }
    format{ } .

4096 4096 4096 ext4
    $defaultignore{ }
    $lvmignore{ }
    method{ format }
    format{ }
    use_filesystem{ }
    filesystem{ ext4 }
    mountpoint{ /boot } .

900 10000 -1 ext4
    $lvmok{ }
    method{ format }
    format{ }
    use_filesystem{ }
    filesystem{ ext4 }
    mountpoint{ / } .
```

Note, that once you choose the disk to erase in the installer, it will prompt you with the summary of the partitioning, so you can check if the trick worked and you are getting the desired partitioning. See also https://askubuntu.com/a/678074/47073.

Share Improve this answer Follow

edited Jun 13, 2023 at 20:13

answered Dec 29, 2019 at 2:42

Yrogirg
371 5 16

If I could I would give you 10 upvotes. – netiul Nov 24, 2022 at 16:58

How to accomplish this multiple encrypted partitions and *no* LVM

3

Because my previous answer was so long, I'm posting a second answer that takes a different approach if you do not want to use LVM.

You can create multiple encrypted partitions and use the decrypt_derived script so that you only need to enter the password once. Check out this blog post for step-by-step instructions. The author uses a keyfile, but the decrypt_derived LUKS script would be sufficient as well.

Share Improve this answer Follow

edited Jun 12, 2020 at 14:37
Community Bot
1

answered May 23, 2017 at 9:08
b_laoshi
4,610 2 23 46

I ended up unpluggin the main drive, assisted installs are available to my sd :) lol – Yvain May 24, 2017 at 9:25

2

One way to do the task is to use the ubuntu network installer https://www.ubuntu.com/download/alternative-downloads

It is not a graphical installer. But it offers you the explicit choice of disk after you choose the full disk installation with encryption.

Share Improve this answer Follow

answered Feb 5, 2018 at 20:25
ernstkl
394 1 7