

LUKS - Disk Encryption

Encryption on Debian 9

1. Install dm-crypt

```
apt-get install cryptsetup
```

2. If you encrypted data drives during initial system setup, your swap space will be encrypted as well. First remove the swap encryption.

```
sudo mkswap -f /dev/sda6  
sudo swapon /dev/sda6
```

3. Add the swap space to /etc/fstab. If you have swap on multiple drives, where the remaining space is allocated to a software RAID, add the swap partitions with the same priority.

```
/dev/hda6 none swap sw,pri=1 0 0
```

4. Remove the fstab entry for mounting the encrypted volume
5. Add the following commands to [rc.local](#) executed as root

```
echo "volume password" | sudo cryptsetup luksOpen /dev/mapper/vg-lv  
my_encrypted_volume  
mount /dev/mapper/my_encrypted_volume /mount/point
```

6. To lock the container again, it needs to be unmounted first

```
sudo umount /media/my_device  
sudo cryptsetup luksClose my_encrypted_volume
```

Encrypt volume

1. Find the Block Device Name of Your Partition

```
lsblk
```

2. Set Up LUKS Header

```
sudo cryptsetup luksFormat /dev/mapper/<vg name>-<lv name>
```

3. Create a Filesystem on the Partition. You have to map this physical device to a virtual device. What gets written to the virtual device will be encrypted before being stored on the physical device.

```
sudo cryptsetup luksOpen /dev/mapper/<vg name>-<lv name> <vg name>-<lv  
name>_crypt
```

```
sudo mkfs.ext4 /dev/mapper/<vg name>-<lv name>_crypt
```

4. Mount Encrypted Partition

```
sudo mount /dev/mapper/<vg name>-<lv name>_crypt /mountpoint
```

5. If you need a directory tree to be copied from a backup location back to the newly encrypted drive, do it with rsync

```
rsync -av --progress --exclude '/home/user/VirtualBox VMs' /home/user /mountpoint/
```

6. Or, for an entire BackupPC structure

```
rsync -avxHAWX --info=progress2 /backup/ /new-backup/
```

7. Verify the structure between source and destination

```
rsync -avcn /backup/ /new-backup/
```

Increase size of Raid Disk Array with LVM and LUKS

These steps have to be taken to increase a Raid Disk Array with the following configuration: RAID → LVM → LUKS → ext4.

1. Increase size of Raid explained in [RAID - mdadm \(Software RAID\)](#)
2. Unmount the file system:

```
sudo umount /backup
```

3. Close LUKS:

```
cryptsetup luksClose vg_backup-lv_backup_crypt
```

4. Resize the physical volume to consume all free space in LVM:

```
pvresize /dev/md3
```

5. Resize the logical volume to consume all free space in LVM:

```
lvresize -l+100%FREE /dev/vg_backup/lv_backup
```

6. Open LUKS and enter the volume password:

```
cryptsetup luksOpen /dev/mapper/vg_backup-lv_backup vg_backup-lv_backup_crypt
```

7. Check the filesystem:

```
e2fsck -f /dev/mapper/vg_backup-lv_backup_crypt
```

8. Extend the filesystem to consume all free space:

```
resize2fs /dev/mapper/vg_backup-lv_backup_crypt
```

9. Mount file system:

```
mount /dev/mapper/vg_backup-lv_backup_crypt /backup
```

- You could do an online resize by avoiding to unmount the file system and closing LUKS, but I find this approach safer. If you decide to do an online resize, skip steps 2 and 3, and instead of step 6 (open LUKS) do a crypt resize:

```
cryptsetup resize vg_backup-lv_backup_crypt
```

Links

- <https://bobcares.com/blog/raid-resync/>
- <https://www.ducea.com/2009/03/08/mdadm-cheat-sheet/>
- <https://unix.stackexchange.com/questions/546218/debian-full-disk-encryption-does-debian-installer-use-luks-1-or-2>
- <https://www.lisenet.com/2013/install-luks-and-create-an-encrypted-luks-partition-on-debian/>
- <https://www.lisenet.com/2013/install-luks-and-create-an-encrypted-luks-partition-on-debian/>
- <https://www.cyberciti.biz/security/how-to-change-luks-disk-encryption-passphrase-in-linux/>
- <https://www.digitalocean.com/community/tutorials/how-to-use-rsync-to-sync-local-and-remote-directories>

Links

- [How To: Linux Hard Disk Encryption With LUKS](#)
- [Resizing a LUKS volume on LVM](#)
- [Extend a LUKS encrypted partition to fill disk](#)
- [How to grow ext4+lvm+LUKS+RAID](#)
- [Encrypt an existing Linux installation with LUKS and LVM](#)
- [Replace LUKS partition with ext4 partition with same contents](#)
- [What's the difference between LUKS, cryptsetup, and dm-crypt?](#)
- [Mount encrypted volumes from command line?](#)
- [How to Encrypt Your Partitions on Linux with dm-crypt](#)
- [Where is rc.local in Debian 9 \(Debian Stretch\)](#)
- [dm-crypt/Encrypting an entire system](#)
- [LVM \(Debian Wiki\)](#)
- [dm-crypt/Swap encryption](#)
- [Setting up swap space](#)
- [How to wipe free disk space in Linux?](#)
- [Best order of RAID, LVM and LUKS](#)
- [Setting Up Full Disk Encryption on Debian 9 Stretch](#)
- [VirtualBox: Encryption of Disk Images](#)
- [dm-crypt/Encrypting an entire system](#)

- [Create a luks encrypted partition on Linux Mint](#)
- [dm-crypt/Swap encryption](#)
- [How to Clone a Partition or Hard drive in Linux](#)
- [How to Clone Your Linux Hard Drive: 4 Methods](#)
- [How to Clone an Encrypted Hard Drive](#)
- [Cloning HDD containing /boot and LVM to new HDD](#)
- [Migrate Linux RAID 1+LVM System To Larger Disks HOWTO](#)
- [create software raid1 on one disk, later add second disk?](#)
- [how to resize / extend a volume group](#)
- [How to resize RAID1 array with mdadm?](#)
- [Moving RAID 5 to another computer](#)
- [Copy entire file system hierarchy from one drive to another](#)
- [How to clone a LUKS encrypted home/root/swap partition from a HDD to an SSD?](#)

From:

<https://wiki.condrau.com/> - **Bernard's Wiki**

Permanent link:

<https://wiki.condrau.com/deb9:luks>

Last update: **2024/03/31 13:38**

