How To Show LUKS Passphrase Slots

Unix Tutorial

As you might know, it’s possible to add multiple passphrases to the same LUKS encrypted filesystem. This means each one of these will allow you to decrypt and to mount your filesystem.

Show LUKS Key Slots

This is how you can check how many passphrases or file-based keys are currently in use for managing access to your encrypted filesystem:

```
root@rhel8:~ # cryptsetup luksDump /dev/rhel/06
 LUKS header information for /dev/rhel/06
 Version:          1
```

```
 Cipher name:       aes
 Cipher mode:       xts-plain64
 Hash spec:         sha256
 Payload offset:    4096
 MK bits:           512
 MK digest:         85 84 e1 49 0f c3 7f df 9b fd 62 a0 50 c9
2a 14 a8 86 a8 0e
 MK salt:           58 e4 20 ed ac 01 56 cf cb b7 77 1d c6 11
20 6f
                    4c f2 fd 3a c5 c3 d4 f0 64 41 84 4c f9 58
a2 2f
 MK iterations:     87614
 UUID:              9144c0fe-7758-47ac-886b-330ae8bfa096
 Key Slot 0: ENABLED
     Iterations:             1418912
     Salt:                   65 fd 6c 78 84 7d 1b ae d1 42 13
0b f3 4c f7 41
                             9b 5f d5 e3 6e c5 a2 ce 05 28 02
f1 9b 56 07 b9
     Key material offset:    8
     AF stripes:             4000
 Key Slot 1: DISABLED
 Key Slot 2: DISABLED
 Key Slot 3: DISABLED
 Key Slot 4: DISABLED
 Key Slot 5: DISABLED
 Key Slot 6: DISABLED
 Key Slot 7: DISABLED
```

As you can see, only Key Slot 0 is ENABLED and reporting some setup details. This means I’m only using one passphrase for my encrypted filesytem.

If and when I add more passphrases or encryption keys, they will be occupying next available slot, starting with key slot 1.

See Also

- Red Hat Linux
- **RHEL 8**
- Access encrypted homedir with passwordless SSH logins