RHEL: Manually encrypting a filesystem with LUKS

Article Number: 68 | Rating: Unrated | Last Updated: Sun, May 27, 2018 8:49 PM

```
# Tested on RHEL  7

# LUKS, Linux Unified Key Setup-on-disk-format, allow encrypting
partitions. By default, the
# option to encrypt the file systems is unchecked during the
installation, otherwise we will
# be prompted for a passphrase every time the system boots up.

# The default cipher used for LUKS is aes-cbc-essiv:sha256 (ESSIV -
Encrypted Salt-Sector
# Initialization Vector). The installation program, Anaconda, uses by
default XTS mode
# (aes-xts-plain64). The default key size for LUKS is 256 bits whit
LUKS with Anaconda is
# 512 bits.



# First of all create a new logical volume (or use an existing one).

lvcreate -L 1G -n lv_crypted rootvg
   Logical volume "lv_crypted" created.



# Format, initialize, the LUKS partition and set the initial
passphrase

cryptsetup --verbose --verify-passphrase luksFormat
/dev/rootvg/lv_crypted

   WARNING!
   ========
```

```
   This will overwrite data on /dev/rootvg/lv_crypted irrevocably.

   Are you sure? (Type uppercase yes): YES
   Enter passphrase:
   Verify passphrase:
   Command successful.

ls -l /dev/mapper | grep crypted
   lrwxrwxrwx. 1 root root       7 Feb  5 18:29 rootvg-lv_crypted ->
../dm-5 3


# Open the newly encrypted device

cryptsetup luksOpen /dev/rootvg/lv_crypted crypted_vol
   Enter passphrase for /dev/rootvg/lv_crypted:

ls -l /dev/mapper | grep crypted
   lrwxrwxrwx. 1 root root       7 Feb  5 18:33 crypted_vol ->
../dm-6
   lrwxrwxrwx. 1 root root       7 Feb  5 18:33 rootvg-lv_crypted ->
../dm-5



# Create a filesystem and mount it

mkfs.xfs /dev/mapper/crypted_vol
   meta-data=/dev/mapper/crypted_volisize=256    agcount=4,
agsize=65408 blks
            =                       sectsz=512   attr=2,
projid32bit=1
            =                       crc=0        finobt=0
   data     =                       bsize=4096   blocks=261632,
imaxpct=25
            =                       sunit=0      swidth=0 blks
   naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
   log      =internal log           bsize=4096   blocks=853,
```

```
version=2
           =                       sectsz=512   sunit=0 blks, lazy-
count=1
   realtime =none                   extsz=4096   blocks=0,
rtextents=0
```

```
mkdir /crypted_fs
mount /dev/mapper/crypted_vol /crypted_fs

df -h | grepcrypted
   /dev/mapper/crypted_vol     1019M   33M  987M   4% /crypted_fs
```

```
# If encrypting an existing directory, it may be necessary to restore
default SELinux
# security contexts:
# Ex.: /sbin/restorecon -v -R /home
# ----------------------------------------------------------------
----------------------
# If desired, add the following lines to /etc/fstab and /etc/crypttab
respectively in order
# for the volume to be opened and mounted automatically during system
start-up. Bear in mind
# that, in this case, boot process will block to ask for the
passphrase to be able to open
# the LUKS volume

vi /etc/fstab
   [...]
   /dev/mapper/crypted_vol      /crypted_fs    xfs    defaults    1 2

vi /etc/crypttab
   crypted_vol    /dev/mapper/rootvg-lv_crypted    none
```