luksman/README.md at main · rigou/luksman

luksman

A simple manager for encrypted volumes
With `luksman` you can easily create, mount and unmount encrypted storage in your GNU/Linux computer. These operations would normally require several arcane commands involving losetup, cryptsetup and filesystem management but with `luksman` you can can do all this with a single command and a couple of options.

Main Repository : https://github.com/rigou/luksman

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY.

Features

you can create / mount / unmount LUKS encrypted volumes with a single command

you can use a container file or a disk to store an encrypted volume

you can enter a passphrase interactively when creating / opening an encrypted volume, or use a key file

key files may conveniently reside in a removable flash drive, allowing you to take them with you when you leave your computer unattended

you can revoke a key file and generate a new one if you suspect it has been compromised

you can delete an encrypted volume and its key file

These features cover 99% of the author's needs. If your requirements are more complex, you can still use cryptsetup on the encrypted volumes created by `luksman` and do whatever you want.

Installation

Install the required package `cryptsetup-bin` for LUKS and dm-crypt support

sudo apt update
sudo apt install cryptsetup-bin

Download the latest release of luksman at https://github.com/rigou/luksman/releases

tar xzf luksman-vx.y.z.tar.gz
sudo chown root: luksman
sudo chmod 770 luksman
sudo mv luksman /usr/local/sbin

optionally, add this convenient alias :

echo "alias lum='sudo /usr/local/sbin/luksman'" >>$HOME/.bashrc

Usage

sudo luksman action [volume_name [options]]

Actions :

create : create an encrypted volume

newkey : add or replace a key file

mount : mount an encrypted volume

unmount : unmount encrypted volume(s)

delete : delete an encrypted volume and its key file

list : list mounted volumes

Volume name :

this name uniquely identifies an encrypted volume. The key file (if any) and the container file (if any) are named after it

the valid characters for a volume name are: letters A-Z (both uppercase and lowercase), numbers 0-9, "@", "-", "_"

Options :

-d location (device path in /dev or UUID) of the disk (or flash drive, or SD card) where the encrypted volume is (or will be) located. UUID is prefered because device path may change unexpectedly. List UUIDs with `lsblk -o NAME,RM,UUID`

-f path of the folder where the container file is (or will be) located. An absolute path is recommended ; a relative path will be interpreted as relative to your home directory. Options -d and -f are mutually exclusive

-s size of the container file which will be created, in MB (1024x1024). Applies only to volumes created with option -f . The minimum size is 17 MB

-k location (device path in /dev, UUID or label) of the disk (or flash drive, or SD card) where the key file is (or will be) located. Label or UUID are prefered because device path may change unexpectedly. List labels and UUIDs with `lsblk -o NAME,RM,LABEL,UUID` . The valid characters of a label are the same as a volume name (see above)

-y do not ask user to confirm actions which may result in existing data loss

1. Create an encrypted volume

sudo luksman create name (-d device | -f folder -s size_MB) [-k keyfile] [-y]

WARNING: when using option -d, the data currently stored at this location will be lost ; use `lsblk` to make certain it is correct

when using option -f, the container file will be created in the specified folder with the given name and the ".dat" extension

when using option -k the key file will be created in the "/luksman" folder of the specified device with the given name and the ".key" extension

► click here to see some examples

2. Add or replace a key file

luksman newkey name (-d device | -f folder) -k keyfile

use this command to change the key of an encrypted volume

this command generates a new key and writes it in a key file, the existing key will be revoked and the key file will be replaced

if the volume was created using a passphrase, a key file will be added and the passphrase will be revoked

the key file will be created in the "/luksman" folder of the specified device with the given name and the ".key" extension

► click here to see some examples

3. Mount an encrypted volume

luksman mount name (-d device | -f folder) [-k keyfile]

if the volume was created using a passphrase, user will be prompted for it

if there is a key file for this volume in the device specified by option -k, it will be used to mount the encrypted volume automatically

after mounting the volume, the device specified by option -k is inactive and can be removed

the mountpoint of volume "name" is /mnt/luksman/name

► click here to see some examples

4. Unmount encrypted volume(s)

luksman unmount (name | all)

this command applies to any encrypted volume, either located in a container file or in a disk

use argument "all" to unmount all volumes that are currently mounted

► click here to see some examples

5. Delete an encrypted volume

luksman delete name (-d device | -f folder) [-k keyfile] [-y]

WARNING: This operation is irreversible

if no key file is specified by option -k, user will be prompted for a passphrase

the LUKS header of the encrypted volume will be overwritten with random characters, making it permanently inaccessible

if the encrypted volume resides in a container file, this file will be deleted

if there is a key file for this volume in the device specified by option -k, this file will be deleted

► click here to see some examples

6. List mounted volumes

this command prints the location and the mountpoint of each currently mounted encrypted volumes

► click here to see an example