



Manuale Criptsetup-luks

MANDRIVA

Davide Garatti



Davide_01



Release 0.3

3 gennaio 2008

Indice Generale

1	Informazioni iniziali.....	3
2	Software necessario.....	3
3	Criptare FS /home.....	4
3.1	Fase preliminare.....	4
3.2	Crittografare la Partizione.....	5
3.3	Creare FS nella partizione criptata.....	6
3.4	TEST.....	7
3.5	NUOVO S.O.	9
4	Criptare Dispositivo USB.....	10
4.1	Uso della penna criptata.....	11
5	Creare cancellare passphrase.....	12

1 Informazioni iniziali

A cosa può servire criptare una partizione? Nella maggior parte dei casi e per la maggior parte delle persone a poco o a nulla. Tuttavia in particolari casi, ed in particolari campi, può essere necessario se non assolutamente richiesto, avere un FS criptato per salvaguardare le informazioni contenute nel proprio PC soprattutto se portatile.

Per l'utente normale potrebbe essere un modo per custodire file particolari come liste di password o altro. Magari poste in una partizione particolare o un dispositivo USB criptato da montare e smontare solo in determinati momenti.

Questo manuale avrà due diversi obbiettivi, il primo la creazione di una /home criptata, sarà pertanto necessario predisporre una partizione, separata di sufficiente capienza, che utilizzeremo per ospitare proprio la nostra /home criptata.

Il secondo obbiettivo sarà quello di criptare un dispositivo USB.

Criptare la partizione significa perdere completamente i dati in essa contenuti, per limitare gli sforzi profusi per il backup ed il ripristino di dati e impostazioni, e da prendere in seria considerazione l'esecuzione di questo procedimento a Sistema appena installato.

Aggiungo qualche riferimento esterno :

Luks home page	http://luks.endorphin.org/dm-crypt
Wiki vari	http://www.saout.de/tikiwiki/tiki-index.php
freeotfe	http://www.freeotfe.org/

2 Software necessario

Cryptsetup

luks-tool

Installarli tramite il solito comando da terminale

```
#urpmi scryptsetup luks-tool <INVIO>
```

oppure da installa software su Mandriva Control Center.

3 Criptare FS /home

3.1 Fase preliminare

Eseguiamo alcuni passi prima di iniziare le vere operazioni:

prendere nota del nome del dispositivo che ospita home (/dev/sdaX, /dev/hdaX o altro) lo si fa semplicemente con il comando:

```
#df <INVIO>
```

ogni riga farà riferimento ad una partizione di un disco

verificare quindi nella colonna "filesystem" in corrispondenza di /home il nome del dispositivo

Prima di smontare la partizione si deve fare il backup delle informazioni e delle impostazioni degli user presenti su /home

quindi copiare tutti i file necessari ed in particolare per le impostazioni copiare i file nascosti di ogni utente:

```
#cp -rf /home/davide/* /DISCO3/Backup/Davide/ <INVIO>
```

```
#cp -rf /home/alessia/* /DISCO3/Backup/Alessia/ <INVIO>
```

Termina la sessione e fai il login come root in modo tale che sia possibile SMONTARE la partizione /home.

Potrebbe essere impedito il login grafico come root (per motivi di sicurezza) pertanto sarà necessario premere i tasti CTRL+F2 per passare ad un altro terminale (puoi sostituire F2 con un tasto funzione da F1 a F6, mentre l'interfaccia grafica rimarrà ancora su F7).

Ci troveremo davanti ad un terminale da cui faremo login come "root".

Cancellare gli utenti con il comando userdel

```
#userdel davide <INVIO>
```

```
#userdel alessia <INVIO>
```

Smonta la partizione

```
#umount /home <INVIO>
```

(puoi verificare rapidamente il corretto smontaggio di /home con il comando df)

Una volta eseguito il login come superuser, con la partizione /home smontata e gli utenti cancellati, passiamo a controllare e riempire la nostra partizione con dei dati casuali.

Questo è un passo fondamentale e che richiederà diverse ore a seconda della dimensione della partizione da criptare e delle prestazioni del PC/DISCO

Si può scegliere tra due metodi (il secondo offre una maggiore sicurezza).

1)

```
# /sbin/badblocks -c 10240 -s -w -t random -v /dev/vg0/home
```

(wait several hours...)

Checking for bad blocks in read-write mode

From block 0 to 295360984

done

Reading and comparing: done

Pass completed, 0 bad blocks found.

```
#
```

2)

```
#dd if=/dev/urandom of=/dev/hdaX
```

dove /dev/hdaX deve essere il dispositivo associato alla partizione home

Manuale-GnuCash_Garatti.pdf.zip

Lanciando questo comando non vedremo nessun tipo di messaggio fino al completo intasamento del dispositivo, a quel punto verranno visualizzate alcune informazioni tra cui il tempo trascorso, nel mio caso e con il mio hardware 2,1GB <>12 minuti circa.

3.2 Crittografare la Partizione

La vera operazione di crittografia avviene ora dando il comando

```
# cryptsetup --verbose --verify-passphrase luksFormat /dev/hdaX
```

WARNING!

=====

This will overwrite data on /dev/hda7 irrevocably.

Are you sure? (Type uppercase yes): YES (**SCRIVI MAIUSCOLO**)

Enter LUKS passphrase: (enter your passphrase, and write it down somewhere!)

Verify passphrase: (repeat passphrase)

Nota sulla “passphrase” la lunghezza e complessità della frase determina la sicurezza del FS criptato, ovviamente dovremo scriverla e custodirla in luogo sicuro e certamente non insieme al PC.

NOTA: visto che stiamo crittografando la partizione home ad ogni riavvio dovremo inserire la passphrase, di conseguenza dobbiamo utilizzarne una che sia un buon compromesso tra lunghezza, complessità e facilità di **ricordarsela**.

Con il seguente comando si crea un associazione tra il dispositivo e la partizione /home

```
cryptsetup luksOpen /dev/hda7 home
```

Enter LUKS passphrase:

e a seguito di questo comando dovremmo trovare una voce home nella directory /dev/mapper

```
ls -l /dev/mapper/
```

```
total 0
```

```
crw----- 1 root root 10, 63 May 24 06:52 control
```

```
brw-rw---- 1 root disk 253, 4 May 24 10:54 home
```

3.3 *Creare FS nella partizione criptata*

Dopo avere criptato la partizione dobbiamo ancora ricreare il Filesystem, ovviamente possiamo scegliere quello che preferiamo, nel mio caso uso l'oramai classico EXT3.

```
# /sbin/mkfs.ext3 -j -m 1 /dev/mapper/home <INVIO>
```

3.4 TEST

Verifichiamo quello che abbiamo ottenuto, iniziamo con il rimontare la partizione:

```
#mount /dev/mapper/home /home <INVIO>
```

e verificarne le informazioni con

```
# df -h /dev/mapper/home <INVIO>
```

```
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/home 4.0G 80M 3.8G 3% /home
```

ricreiamo a questo punto gli utenti o da MCC oppure da terminale con i comandi:

```
# useradd -m davide
```

```
# passwd davide
```

Changing password for user davide.

New UNIX password:

Retype new UNIX password:

passwd: all authentication tokens updated successfully.

```
#
```

```
# useradd -m alessia
```

```
# passwd alessia
```

Changing password for user alessia.

New UNIX password:

Retype new UNIX password:

passwd: all authentication tokens updated successfully.

```
#
```

ed in caso di backup delle impostazioni ricopiare i file .* precedentemente salvati nuovamente dentro la directory dei relativi utenti.

Usare il comando `cp -rf` con l'opzione `-preserve` che permette di mantenere i permessi originali.

Provare il login degli utenti con il comando

```
# su - davide <INVIO>
```

a questo punto modifichiamo il file /etc/fstab in modo da far montare la partizione /home corretta e non in automatico al boot

la voce relativa ad home non dovrà più puntare al dispositivo /dev/hdaX

```
/dev/hda7 /home ext3 defaults 1 1
```

Ma a quello criptato ad esso associato e posto in /dev/mapper

```
/dev/mapper/home /home ext3 defaults 0 0
```

A questo punto riepiloghiamo i due comandi essenziali già visti:

```
cryptsetup luksOpen /dev/hda7 home
```

Enter LUKS passphrase:

```
#mount /dev/mapper/home /home <INVIO>
```

questi due comandi dobbiamo farli eseguire automaticamente all'avvio, per farlo, il modo più semplice mi sembra quello di creare un file "luks-sistema" nella directory /etc/init.d

contenente:

```
#!/bin/sh  
#  
# /etc/init.d/Luks-Sistema  
# Subsystem file for nomefile  
#  
# chkconfig: 2345 52 05  
# description: mappatura e montaggio /home criptata  
#  
# processname: Luks-Sistema  
  
cryptsetup luksOpen /dev/hda7 home  
  
mount /dev/mapper/home /home  
  
RETVAL=$?  
exit $RETVAL
```


poi creare un link simbolico a questo file in /etc/rc5.d/

```
#cd /etc/rc5.d  
#ln -s /etc/init.d/luks-sistema /etc/rc5.d/S52luks-sistema
```

Questa operazione farà in modo di lanciare i comandi per associazione e montaggio precedentemente visti e provati prima del lancio del Desktop manager.

In pratica durante il boot verrà chiesta la passphrase poco prima di entrare nella maschera di login.

NOTA 1: A questo punto lo script viene trattato come se fosse un servizio e quindi lo ritroveremo elencato in Mandriva Control Center | Servizi

Verificare che sia spuntata l'opzione "Al boot"

NOTA 2: Dopo aver configurato questi scripts si può rimuovere dal file /etc/fstab la stringa relativa ad /home.

3.5 NUOVO S.O.

Nel caso in cui si debba reinstallare il sistema operativo per qualsiasi motivo cambio di distribuzione, nuova versione o altro ricordarsi di impostare solo il punto di mount / in modo che il sistema si installi solo su quella partizione dopo di che installare i programmi per criptare i dischi e modificare /etc/fstab e /etc/rc.d/rc.sysinit come già specificato sopra.

L'aggiornamento diretto (senza reinstallare tutto) da Mandriva 2007.1 a Mandriva 2008 usando i repository internet, e quindi da sistema operativo avviato, ha mantenuto tutte le impostazioni perfettamente, senza dare alcun problema.

Nota:

Probabilmente in fase di installazione viene creato nel file /etc/fstab una stringa relativa alla partizione crittografata, questa stringa può essere completamente rimossa.

4 Criptare Dispositivo USB

I passi da seguire sono più o meno gli stessi :

verifica dispositivo associato, inserire la penna USB, montarla, e dare il comando df per verificare il dispositivo occupato:

per esempio

```
/dev/sda1          239M  2,7M  237M   2% /media/USBDISKPRO
```

smontare la penna

Per verificare e riempire di dati casuali la penna usare il comando:

```
badblocks -c 10240 -s -w -t random -v /dev/sda1
```

Seguito dal comando per criptare

```
cryptsetup --verbose --verify-passphrase luksFormat /dev/sda1
```

poi si crea l'associazione:

```
cryptsetup luksOpen /dev/sda1 sda1
```

controllando in /dev/mapper la presenza della voce sda1

a questo punto creiamo il FS con

```
/sbin/mkfs.vfat /dev/mapper/sda1
```

oppure con

```
/sbin/mkfs.ext3 -j -m 1 /dev/mapper/sda1
```

Usare il FS preferito a seconda delle esigenze.

4.1 *Uso della penna criptata*

All'inserzione della penna dovremo creare l'associazione del dispositivo su /dev/mapper tramite il comando

```
#cryptsetup luksOpen /dev/sda1 sda1
```

Completato questo comando comparirà immediatamente la solita finestra per il montaggio del dispositivo.

da qui in poi si utilizzerà esattamente come le altre penne USB, compreso lo smontaggio e la rimozione.

NOTA: anche se si smonta la penna il dispositivo "sda1" associato alla nostra penna in /dev/mapper permane fino a quando non daremo il comando di chiusura **luksClose** :

```
#cryptsetup luksClose /dev/sda1
```

Quindi non rimuovere la penna se non dopo aver dato questo comando, altrimenti reinserendo nuovamente la penna questa richiederà per essere utilizzata gli stessi passaggi eseguiti precedentemente ma per un altro dispositivo, per esempio "sda2".

Solo per conoscenza lascio le seguenti righe, utili se si utilizza un sistema Linux che non prevede l'auto mount del dispositivo

Comando per montare il dispositivo USB crittografato

```
mount -t vfat -o rw /dev/mapper/sda1 /mnt/USB-crypt/
```

Comandi per la rimozione del dispositivo USB crittografato

```
umount /mnt/USB-crypt/
```

```
cryptsetup luksClose /dev/sda1
```

NOTA:

Dopo aver crittografato la penna, nei successivi utilizzi di quest'ultima ci sarà il problema di capire a quale dispositivo verrà associata, questo perché non verrà rilevata. per controllare dare il comando subito dopo l'inserzione della

stessa.

\$dmesg <INVIO>

le ultime righe ci diranno chiaramente il dispositivo associato
sda sdb sdc etc.

5 Creare cancellare passphrase

Si possono creare diverse chiavi (passphrase) con cui accedere alle partizioni criptate,

Per aggiungerne una si usa il comando:

cryptsetup luksAddKey /dev/sda1

Enter any LUKS passphrase: *(enter an existing password for this partition)*
key slot 0 unlocked.

Enter new passphrase for key slot: *(enter the extra password)*

Mentre per rimuovere una chiave si usa il comando:

cryptsetup luksDelKey /dev/sdc1 0

dove 0 sta ad indicare la password eliminata

0 = la prima

1 = la seconda

2 = la terza

.. = e così via.

Per modificare la password usi in sequenza i due comandi creando di fatto una nuova chiave e rimuovendo la vecchia.

