CentOS 磁碟加密 SOP

以移轉 MariaDB 資料目錄為例

版本：v1.0

文件更新日期：2016/07/28

一、 以 dm-crypt 建立 Linux 加密檔案系統

1. 加密的檔案系統可以保障 Hard Disk 不會受到硬體層面的攻擊，於雲端環境中，當用戶自行將個資、資料庫…等機敏資料放置於虛擬機器上加密過的檔案系統上，能保證雲服務提供商之平台維運人員無法碰觸到客戶的 SaaS 資料，任何人將虛擬硬碟弄到手後，依然要用暴力法(Brute-force)猜測加密金鑰，構成取得機敏資料的重大阻礙。而 dm-crypt 透過 cryptsetup 這個工具程式，為 Linux 提供一個簡潔易用的加密檔案系統工具。
2. 硬碟加密的不足之處為，對硬碟加密將造成寫入操作性能略差於原始虛擬硬碟，且每次虛擬機器重開機時，需輸入 Passphrase 以手動開啟加密硬碟以進行後續掛載，若特定服務的檔案目錄置於該加密硬碟上，亦須於掛載後手動啟動服務。

二、 硬碟加密情境說明

1. 以下將於 CentOS 虛擬機器環境，於 CloudBOSS 上額外申租掛載一 EBS 硬碟，並將原先已正常提供服務的 MariabDB 資料目錄移至加密硬碟上，可保證當虛擬機或虛擬硬碟遭複製時，無法竊取其硬碟上已加密的資料。

測試作業系統版本

	CentOS 7	Centos 6
OS Version	CentOS 7.2.1511(Core)	CentOS release 6.8 (Final)
DB Version	MariaDB 10.0.26	MariaDB 10.0.26
cryptsetup Version	cryptsetup 1.2.0	cryptsetup 1.6.7

三、 CentOS 7.2 硬碟加密 SOP - 以移動 MariaDB 檔案目錄為例

- 以下的 SOP 示範之測試指令與截圖將以 CentOS 7.2.1511 版本為例，並經驗證 CentOS 6.8(Final)指令一樣可以通用。
- 首先，確認目前系統之版本
  cat /etc/*release

```
[root@localhost test]# cat /etc/*release
CentOS Linux release 7.2.1511 (Core)
NAME="CentOS Linux"
VERSION="7 (Core)"
ID="centos"
ID_LIKE="rhel fedora"
VERSION_ID="7"
PRETTY_NAME="CentOS Linux 7 (Core)"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:centos:centos:7"
HOME_URL="https://www.centos.org/"
BUG_REPORT_URL="https://bugs.centos.org/"

CENTOS_MANTISBT_PROJECT="CentOS-7"
CENTOS_MANTISBT_PROJECT_VERSION="7"
REDHAT_SUPPORT_PRODUCT="centos"
REDHAT_SUPPORT_PRODUCT_VERSION="7"

CentOS Linux release 7.2.1511 (Core)
CentOS Linux release 7.2.1511 (Core)
```

- 於開始之前，確認已安裝 cryptsetup 相關套件

  cryptsetup --version

```
[root@localhost lib]# cryptsetup --version
cryptsetup 1.6.7
```

- 於此機器上已安裝 MariaDB 並正常啟用服務，

```
[root@localhost /]# mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 6
Server version: 10.0.26-MariaDB-wsrep MariaDB Server, wsrep_25.13.raf7f
02e

Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input sta
tement.

MariaDB [(none)]>
```

- MariaDB 相關資料檔預設安裝目錄置於/var/lib/mysql 內。

```
[root@localhost /]# ls /var/lib/mysql/
aria_log.00000001  ib_logfile1               mysql
aria_log_control   localhost.localdomain.err  mysql.sock
ibdata1            localhost.localdomain.pid  performance_schema
ib_logfile0        multi-master.info          test
```

- 於 CloudBOSS 上額外申租一個儲存空間並掛載至此 VM
- 查看剛申租掛載上 VM 的硬碟，Disk /dev/sdb

  fdisk -l

```
[root@localhost ~]# fdisk -l

Disk /dev/sda: 32.2 GB, 32212254720 bytes, 62914560 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000a7e42

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1            2048     8194047     4096000   82  Linux swap / So
laris
/dev/sda2   *     8194048    62914559    27360256   83  Linux

Disk /dev/sdb: 107.4 GB, 107374182400 bytes, 209715200 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

- 於此案例中以 LVM(Logical Volume Manager)邏輯捲軸管理員架構，依序建立 PV(Physical Volume)實體捲軸、VG(Volume Group)捲軸群組、LV(Logical Volume)邏輯捲軸。
- 首先建立將實體 Partition 建立成為 PV

  pvcreate /dev/sdb

```
[root@localhost ~]# pvcreate /dev/sdb
  Physical volume "/dev/sdb" successfully created
```

- 將/dev/sdb 單獨建立為一個名為 **storage** 的 VG，不額外指定 PE(Physical Extent)實體範圍區塊大小，預設的 PE 大小為 4MB

  vgcreate **storage** /dev/sdb

```
[root@localhost ~]# vgcreate storage /dev/sdb
  Volume group "storage" successfully created
```

- 創造出 storage 這個磁碟後，建立分割區 EncryptedStorage，把整個 VG storage 的容量都分配至 EncryptedStorage 這個 partition 內。
- lvcreate -L 99.9G -n EncryptedStorage storage

```
[root@localhost ~]# lvcreate -L 99.9G -n EncryptedStorage storage
  Rounding up size to full physical extent 99.90 GiB
  Logical volume "EncryptedStorage" created
```

- 接著透過 cryptsetup 此加密工具程式，透過 Block cipher 把該 EncryptedStorage 這個 volume 格式化，以 CBC(cipher block chaining) mode，essiv IV and 256 bits key。

  cryptsetup --verify-passphrase --cipher aes-cbc-essiv:sha256 --key-size 256 luksFormat /dev/storage/EncryptedStorage
- 輸入大寫 YES，並輸入兩次密碼(後續加密硬碟所使用的金鑰也將由此 Passphrase 衍生出來)

```
[root@localhost ~]# cryptsetup --verify-passphrase --cipher aes-cbc-ess
iv:sha256 --key-size 256 luksFormat /dev/storage/EncryptedStorage

WARNING!
========
This will overwrite data on /dev/storage/EncryptedStorage irrevocably.

Are you sure? (Type uppercase yes): YES
Enter passphrase:
Verify passphrase:
```

- 手動開啟加密的 secret 目錄並命名為 **enc_ecrypted_storage**，將要求輸入密碼

  cryptsetup luksOpen /dev/storage/EncryptedStorage **enc_ecrypted_storage**

```
[root@localhost ~]# cryptsetup luksOpen /dev/storage/EncryptedStorage e
nc_ecrypted_storage
Enter passphrase for /dev/storage/EncryptedStorage:
```

- 於/dev/mapper 路徑底下可以看到解密的 partition 目錄

```
[root@localhost ~]# ls /dev/mapper/
control  enc_ecrypted_storage  storage-EncryptedStorage
```

- 將此 enc_ecrypted_storage 格式化成 ext4 格式

```
[root@localhost ~]# mkfs.ext4 /dev/mapper/enc_ecrypted_storage
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
6553600 inodes, 26188288 blocks
1309414 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2174746624
800 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632,
2654208,
        4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

- 開始進行 MariaDB 移轉動作，先將服務停止

  service mysql stop

```
[root@localhost ~]# service mysql stop
Shutting down MySQL... SUCCESS!
```

- 確認資料庫目錄(預設在/var/lib/mysql)，若有調整過目錄位址，可參考 /etc/my.cnf.d/server.cnf 內[mysqld]的 datadir 此 entry

```
[root@localhost ~]# ls /var/lib/mysql/
aria_log.00000001  ib_logfile0               multi-master.info   test
aria_log_control   ib_logfile1               mysql
ibdata1            localhost.localdomain.err  performance_schema
```

- 把/var/lib/mysql 備份一份至 mysql_bak

  cp -a mysql mysql_bak

```
[root@localhost lib]# cp -a mysql/ mysql_bak
```

- 將加密硬碟 enc_ecrypted_storage 掛載至/var/lib/mysql 目錄

  mount /dev/mapper/enc_ecrypted_storage /var/lib/mysql

```
[root@localhost lib]# mount /dev/mapper/enc_ecrypted_storage /var/lib/m
ysql
```

- 從/var/lib/mysql_bak 把該目錄下所有檔案、資料複製進去/var/lib/mysql 內

  cp -a /var/lib/mysql_bak/* /var/lib/mysql

```
[root@localhost lib]# cp -a /var/lib/mysql_bak/* /var/lib/mysql
```

- 檢查/var/lib/mysql 目錄內資料

```
[root@localhost mnt]# ll
total 110644
-rw-rw----. 1 mysql mysql    16384 Jul 27 17:40 aria_log.00000001
-rw-rw----. 1 mysql mysql       52 Jul 27 17:40 aria_log_control
-rw-rw----. 1 mysql mysql 12582912 Jul 27 17:40 ibdata1
-rw-rw----. 1 mysql mysql 50331648 Jul 27 17:40 ib_logfile0
-rw-rw----. 1 mysql mysql 50331648 Jul 27 15:58 ib_logfile1
-rw-r-----. 1 mysql root      2456 Jul 27 17:40 localhost.localdomain.e
rr
drwx------. 2 root  root     16384 Jul 27 17:37 lost+found
-rw-rw----. 1 mysql mysql        0 Jul 27 15:58 multi-master.info
drwx--x--x. 2 mysql mysql     4096 Jul 27 15:58 mysql
drwx------. 2 mysql mysql     4096 Jul 27 15:58 performance_schema
drwxr-xr-x. 2 mysql mysql     4096 Jul 27 15:58 test
```

- 將/var/lib/mysql 該 mountpoint 的目錄權限調整為正確的

  chown mysql:mysql /var/lib/mysql

```
[root@localhost lib]# chown mysql:mysql mysql
```

- 啟動 mysql 服務

  service mysql start

```
[root@centos68 mysql]# service mysql start
Starting MySQL.. SUCCESS!
[root@centos68 mysql]# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 3
Server version: 10.0.26-MariaDB-wsrep MariaDB Server, wsrep_25.13.raf7f
02e

Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input sta
tement.

MariaDB [(none)]>
```

確認無誤後即完成將 mariaDB 相關資料檔案移轉至加密硬碟的流程，後續可以把 mysql_bak 目錄亦移進 mysql 加密 partion 內。

- 於停止服務、並取消掛載以後，可以手動把原/var/lib/mysql 目錄內資料清空

```
[root@localhost lib]# service mysql stop
Shutting down MySQL.. SUCCESS!
[root@localhost lib]# umount /var/lib/mysql
[root@localhost lib]# rm -rf /var/lib/mysql/*
[root@localhost lib]# ll /var/lib/mysql
total 0
```

- 未來重開機時，預設將不會自動將加密硬碟掛載至/var/lib/mysql 目錄，需要重複先前的步驟，手動輸入 Passphrase，解密/dev/storage/EncryptedStorage 成 enc_ecrypted_storage

  cryptsetup luksOpen /dev/storage/EncryptedStorage enc_crypted_storage

```
[root@centos68 ~]# cryptsetup luksOpen /dev/storage/EncryptedStorage en
c_crypted_storage
Enter passphrase for /dev/storage/EncryptedStorage:
```

- 並將/dev/mapper/enc_ecrypted_storage 掛載至/var/lib/mysql

  mount /dev/ mapper/enc_ecrypted_storage /var/lib/mysql

- 即可再次啟動 mysql 服務

```
[root@centos68 mysql]# service mysql start
Starting MySQL.. SUCCESS!
[root@centos68 mysql]# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 3
Server version: 10.0.26-MariaDB-wsrep MariaDB Server, wsrep_25.13.raf7f
02e

Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input sta
tement.

MariaDB [(none)]>
```

四、 參考資料

- https://en.wikipedia.org/wiki/Dm-crypt
- https://wiki.centos.org/zh-tw/HowTos/EncryptedFilesystem
- https://www.linux-geex.com/centos-7-how-to-setup-your-encrypted-filesystem-in-less-than-15-minutes/