

backup, encriptado y copia a remoto

2.2

- disociar parámetros de script en 2 ficheros
 - usar source para incluir las variables necesarias
 - o volver a mirar opciones de usar otro tipo de fichero (INI,JSON)

v2.1

- sustitución **GPG** por **ENCHIVE**
- valorando cambio de cálculo de hash
 - sha1 → md5 (la mitad de tiempo) : las colisiones no son importantes
 - meow hash (por valorar)
- pte: cambiar el nombre del script!

backup_fs_gpg.sh

```
#!/bin/bash

#
# FUNCIONES
#

function calcula_checksum() {
# calcula el SHA1 de los ficheros contenidos en el directorio pasado por
# parámetro

    TMP=$(find "$DIR_ORIGEN/$1" -type f -print0 | xargs -0 shasum | sort |
cut -d " " -f 1 | shasum)
    CHECKSUM_ACT=$(echo $TMP | cut -d " " -f1)
    unset TMP
}

#
# VARIABLES
#

FICHERO="diezminutos_com"
DIR_ORIGEN="/home/diezminutos"
CHECKSUM_ACT=""
CAMBIOS="NO"
DBB_HOST="mysql.10minutosaldia.com"
DBB_USER="mate_backup"
DBB_PASSWORD="ot3trecfe4y5fxx722xekngf"
BACKUP_PATH="{DIR_ORIGEN}/backup"
ENCHIVE_PATH="{BACKUP_PATH}/enchive"
ENCHIVE_PUBKEY="mate_es.pub"

FECHA=`eval date +%y%m%d`
```

```
DIRECTORIOS_TAR=""

# backup BBDD
declare -a BBDD=("10minutos" "10minutosbeta")
for BDD in "${BBDD[@]"; do
    /usr/bin/mysqldump --opt --user=${DBB_USER} --password=${DBB_PASSWORD} --
host=${DBB_HOST} ${BDD} > ${DIR_ORIGEN}/mysqldump/${BDD}.sql
    ${ENCHIVE_PATH} --pub-key=${BACKUP_PATH}/${ENCHIVE_PUBKEY} archive
${DIR_ORIGEN}/mysqldump/${BDD}.sql
    rm ${DIR_ORIGEN}/mysqldump/${BDD}.sql
done

# calcula SHA1 directorios
declare -a DIRECTORIOS=("app.10minutos" "appb.10minutos" "public" "beta"
"backup" "system-3.1.11" "mysqldump")

for directorio in "${DIRECTORIOS[@]"; do

    DIRECTORIOS_TAR="${DIRECTORIOS_TAR} ${directorio}"

    ## leer checksum anterior, si existe
    CHEKSUM_ANT=""
    if [ -e "${DIR_ORIGEN}/${directorio}.checksum" ]; then
        CHEKSUM_ANT=$(cat "${DIR_ORIGEN}/${directorio}.checksum")
    fi

    calcula_checksum $directorio

    if [ "${CHEKSUM_ANT}" != "${CHEKSUM_ACT}" ]; then
        CAMBIOS="SI"
        echo -e "${CHEKSUM_ACT}" > ${DIR_ORIGEN}/${directorio}.checksum
    fi

done

if [ "${CAMBIOS}" == "SI" ]; then
    # compresión
    tar zvcpf ${DIR_ORIGEN}/${FICHERO}.tar.gz --exclude-tag-all=.nobackup
${DIRECTORIOS_TAR} ${DIR_ORIGEN}/*.sh

    #encriptación
    ${ENCHIVE_PATH} --pub-key=${BACKUP_PATH}/${ENCHIVE_PUBKEY} archive
~/${FICHERO}.tar.gz

    # borrado fichero original
    rm -f ~/${FICHERO}.tar.gz

    # renombrado
    mv ${FICHERO}.tar.gz.enchive $FECHA-${FICHERO}.tar.gz.enchive

else
    touch ${DIR_ORIGEN}/${FECHA}-SINCAMBIOS.TXT
```

fi

v2

- instalar llave pública contraseña GPG para encriptado fichero TAR (mover entre servidores sin problema)
 - Para desencriptar, solo hace falta la clave secreta y el comando: `$ gpg --decrypt <fichero>`
- volcado ficheros en \$HOME para que «otro» los recoja ← declarados ARRAY
- volcado BBDD **mysqldump** con usuario poco privilegiado (SELECT) ← declaradas ARRAY

backup_fs_gpg.sh

```
#!/bin/bash

#
#      FUNCIONES
#

function calcula_checksum() {
# calcula el SHA1 de los ficheros contenidos en el directorio pasado por
# parámetroe

    TMP=$(find "$DIR_ORIGEN/$1" -type f -print0 | xargs -0 shasum | sort
| cut -d " " -f 1 | shasum)
    CHEKSUM_ACT=$(echo $TMP | cut -d " " -f1)
    unset TMP
}

#
#      VARIABLES
#

FICHERO="fruitsmontmany_es"
DIR_ORIGEN="/home/vividumcodex"
FECHA=`eval date +%y%m%d`
CAMBIOS="NO"
DBB_HOST="mysql.vividumcodex.com"
DBB_USER="mate_backup"
DBB_PASSWORD="xxx"
DIRECTORIOS_TAR=""

# backup BBDD
declare -a BBDD=("fruitsmontmany_es")
for BDD in "${BBDD[@]}; do
    /usr/bin/mysqldump --opt --user=${DBB_USER} --password=${DBB_PASSWORD} --
host=${DBB_HOST} ${BDD} > ${DIR_ORIGEN}/mysqldump/${BDD}.sql
done

# calcula SHA1 directorios
declare -a DIRECTORIOS=("fruitsmontmany.es" "mysqldump")
```

```

for directorio in "${DIRECTORIOS[@]"; do

    DIRECTORIOS_TAR="${DIRECTORIOS_TAR} ${directorio}"

    ## leer checksum anterior, si existe
    CHEKSUM_ANT=""
    if [ -e "$DIR_ORIGEN/${directorio}.checksum" ]; then
        CHEKSUM_ANT=$(cat "$DIR_ORIGEN/${directorio}.checksum")
    fi

    calcula_checksum $directorio

    if [ "$CHEKSUM_ANT" != "$CHEKSUM_ACT" ]; then
        CAMBIOS="SI"
        echo -e "$CHEKSUM_ACT" > $DIR_ORIGEN/${directorio}.checksum
    fi

done

if [ "$CAMBIOS" == "SI" ]; then

    # compresión
    tar zvcpf ~/$FICHERO.tar.gz --exclude-tag-all=.nobackup ${DIRECTORIOS_TAR}
    ~/*.sh

    # encriptación
    gpg --trust-model always -r "Miguel Angel Torres Egea (backups)" --encrypt
    ~/$FICHERO.tar.gz

    # borrado fichero original
    rm -f ~/$FICHERO.tar.gz

    # renombrado
    mv $FICHERO.tar.gz.gpg $FECHA-$FICHERO.tar.gz.gpg

    # copia
    ## scp -i ~/.ssh/backups\@seedbox.torresegea.es $FECHA-$FICHERO.tar.gz.gpg
    backups@seedbox.torresegea.es:~/miguelangel.torresegea.es

    # borrado fichero encriptado
    ## rm -f $FECHA-$FICHERO.tar.gz.gpg
else
    touch $DIR_ORIGEN/$FECHA-SINCAMBIOS.TXT
    ## scp -i ~/.ssh/backups\@seedbox.torresegea.es $FECHA-SINCAMBIOS.*
    backups@seedbox.torresegea.es:~/miguelangel.torresegea.es
    ## rm -f $DIR_ORIGEN/$FECHA-SINCAMBIOS.TXT
fi

```

Llave pública

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

```
mQENBFWTLsBCADPGYcDAMfzYLivjin9FgFGS3xQ0mV4YAmN2poNkfUFSnUHgAZo
6KtelcXBN7TSoCMq7ExXE8xwTAHyMIu0GUfmuLHg/c1Hxfm7fxGdlpRkYXvxNQ3F
8kliCpBq4/Y/7Syeq3rARBX6esyBaLfERmxoUh0l0Br7E8nn52Qmu+k1Xn7ZZYA
8LMpnPR92tEvtSnpUMkk71AaHKEBwd+X0WymMddz0us/8qRkuQ5Ns0hIi7T2pMKt
mSJKGmZVE5MAetJgBQ1Fy8Wak7VTwsxx33E0zAYzZjW6PfUecA67dy/cERnzWy5g
c3oQt9RoLGWQYMBWi2dmTC1dWbBwUIxhwL73ABEBAAG0Nk1pZ3VlbCBBbmdlbCBU
b3JyZXMgRWdlYSAoYmFja3VwcykgPG1hdGVyY25AZ21haWwY29tPokB0AQTAQIA
IgUCVZMsSwIbAwYLCQgHAwIGFQgCCQoLBBYCAwECHgECF4AACgkQaInNFkRv/buM
twf+LFrq4kR2LTG6G6LE+NUIV5vPB9UZ6QNhnh/J5/F709IQWwWxzIy7Nk3LKrRN
QkHl+BLs5nswdUnEhNGah3Eg6eEzQijwsHr7FDr/5culzDZdZHRP6CpGoInqAxUf
qoRTgt00l5793U/uPcE6woRcc6vtMx0v0m8dWRvBNmNd+jLabpuRQ5DSNFYfF4BM
hX0KyBiFvdAHVc6Lz5vhEDzDbnRH5Q+A/loNGPu7vg5tHfQbEicVEssTIy9BoxLJ
FfH/Y3q9htzL7t0dZjosxuTTnwoC5FWUMBAQAoy9njPE+w30Z4H2cwWg/jciQJx+
ZejRkKGuzIQzs3ibc1W/2SV5arkBDQRVkyxLAQgA9xihCubQdVlo6f3LGM3gf5/6
qbhv9J1RYM/59XMcVBt055CgMUiXokleKeZLpliN7tfuz3VL61aw6zkk/b2PCbQF
9nzmaSX7B6LP0ximCNCN6qYpABPPfLv0mVx/sNqv7AQERo2+2YX3YcMmiJuVXNVk
CD3i1VVPJ+YVWBH8A10EjH3eb8KLKG9R0g02ru5UiBK8W48UQlh5XUWQr2oPvU4U
z+wAFyEHr18sMFnimzL1IERmZ2EBwL7p9u/rJVy07E8rLtXQrb0V0ZLuAyUlZXe
UIDkNI1UIeX3DJXvoGwVwM/w+44oP0Lna2DYZuiHGAB3MX+0o40M4BX3yZCXRwAR
AQABiQEfBBgBAgAJBQJVkyxLAhsMAAoJEGiJzRZeb/27lhoIAKVDqP0K5zc4/zKh
bKbuFyLdlqBnLT2w49tgTRRim0fKpZBpQ4xVATC/Vf5WMXn+DJVGPAA0LXRR7BBN
85+sXUfputCXRTCyk0da4fvi424gmFL2/kWyktTFABfW6G1X3I1cB2Pjt25rxKf
2P0K51h0S09YR702g561Aw3tMmyLA9sWYoDXXU0+MK5Fx10zGAo6PKqavp+QvEHQ
HZhNeqYVHfYabPtWgW3RpwKgFDyCGwZ9BYrukq4ReubicyIsthxLhAXK6qUT4hVz
2ZQZ7Tvsoe6Qv2WBT0e7Kpmuhe1n8jrxqD2DFYfrbwN6n/RdWZW6pwL3Uk7LH9Ze
s4ItKkM=
=PS0g
-----END PGP PUBLIC KEY BLOCK-----
```

v1

Instalando GPG y tu clave pública, encriptas el contenido del TAR poniéndote a tí como destinatario, y será el único en poder abrir el fichero. No hace falta poner contraseñas, ni si quiera en el script

```
#!/bin/bash
FICHERO="miguelangel_torresega_es"
FECHA=`eval date +%y%m%d`

# compresión
tar zvcpf ~/${FICHERO}.tar.gz ~/miguelangel.torresegea.es

# encriptación
gpg --trust-model always -r "Miguel Angel Torres" --encrypt ~/${FICHERO}.tar.gz

# borrado fichero original
rm -f ~/${FICHERO}.tar.gz

# renombrado
mv ${FICHERO}.tar.gz.gpg ${FECHA}-${FICHERO}.tar.gz.gpg

# copia
scp -i ~/.ssh/b230993\@hanjin.dreamhost.com ${FECHA}-${FICHERO}.tar.gz.gpg
```

```
b230993@hanjin.dreamhost.com:~/matez
```

```
# borrado fichero encriptado
```

```
rm -f $FECHA-$FICHERO.tar.gz.gpg
```

Para desencriptar, solo hace falta la clave secreta y el comando: `$ gpgp --decrypt <fichero>`

From:

<https://matebcn.eu/> - miguel angel torres egea

Permanent link:

<https://matebcn.eu/linux:scripts:backupgpg>

Last update: **22/03/2020 19:52**

