Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Comprobación de la integridad de los ficheros con md5 (md5sum) (40288 lectures)

Per **Carlos Cortes Cortes**, ***carcoco*** (http://bulma.net/~carcoco/)

Creado el 27/03/2002 01:03 modificado el 27/03/2002 01:03

MD5 es un algoritmo que se suele utilizar para realizar la comprobación de la **integridad de ficheros binarios**, siendo muy utilizado, para por ejemplo, la posterior verificación de imagenes **ISO** o programas descargados de Internet ...

Realmente es muy utilizado por su sencillez de uso, potencia y popularidad, siendo relativamente sencillo el comprobar si un determinado archivo se ha descargado correctamente o por el contrario ha ocurrido algun problema y el programa o imagen ISO es inutilizable (es ideal para comprobar las imagenes ISO de CD's, antes de tostarlas). Indicar que en el mundo **Linux**, es muy habitual encontrar las sumas de control **MD5** de todos los paquetes que componen la distribución.

Supongamos que tengo el fichero **xdibu-0.1.tgz** y quiero distribuirlo en Internet, como se supone que es un archivo bastante grande y quiero facilitar que cualquiera lo pueda descargar (usando por ejemplo, los famosos programas de descargas tipo GetRigth, Download Accelerator Plus, NetVampire, Downloader2X, wget, GetLeft, ...).
Lo que voy a hacer es añadir un pequeño fichero con el resultado de la ejecución del comando **md5sum** (o el algunos sistemas simplemente **md5**) sobre el archivo en cuestión:

```
$ md5sum xdibu-0.1.tgz
750726b7df78e9401068b623d47bbf73  xdibu-0.1.tgz

$ md5sum xdibu-0.1.tgz > xdibu-0.1.tgz.asc

$ cat xdibu-0.1.tgz.asc
750726b7df78e9401068b623d47bbf73  xdibu-0.1.tgz
```

De forma que una vez descargado, para verificar la integridad del fichero simplemente tendré que ejecutar la misma instrucción, comprobando carácter por carácter, la suma de control obtenida.
Existen versiones del md5sum, para la práctica totalidad de los sistemas operativos, pudiendo en caso de necesidad recurrir al poderoso **Perl**. Independientemente del sistema operativo utilizado, en cualquiera de ellos, esta suma de control debe coincidir exactamente.

md5sum suele venir incluido dentro del paquete **GNU textutils** (ftp://ftp.gnu.org/gnu/textutils/[1]), que está formado por algunos comandos habituales en linux, como: cat, cksum, comm, csplit, cut, expand, fmt, fold, head, join, md5sum, nl, od, paste, pr, sort, split, sum, tac, tail, tr, unexpand, uniq, y wc.

Como ejemplo de la popularidad del **md5sum**, aquí os dejo las sumas de control de las tres imagenes ISO de la nueva Linux Mandrake 8.2:

```
$ cat md5sums.82

cda56ed1c9e9ace3de44eba1c36069a7  Mandrake82-cd1-inst.i586.iso
6ede8c75fec92e10636b6c0bf5ee9860  Mandrake82-cd2-ext.i586.iso
0b4921ddb67425687a5e053ff288dcba  Mandrake82-cd3-supp.i586.iso
```

Aunque **md5** se utiliza también por motivos de **seguridad**, de forma que permite saber si un determinado fichero, ha sido fraudulentamente modificado, es más recomendable utilizar **PGP** para firmar los paquetes, aunque su uso no está tan extendido como la firma **md5** de paquetes (muchas veces nos encontraremos con ambos métodos).
Por lo tanto cuando lo único que nos importa es la seguridad **PGP** y **GPG** (más conocido como **GnuPG**) es la solución

ideal.

Enlaces relacionados:

- Crear checksums md5 de tus ficheros
  http://bulma.net/body.phtml?nIdNoticia=35[2]
- GnuPG (The GNU Privacy Guard)
  http://www.gnupg.org/[3]
- Using PGP to Verify Digital Signatures
  http://www.cert.org/archive/pdf/PGPsigs_paper2.pdf[4]
- How To Check MD5sums On A Linux Iso Image
  http://www.linuxiso.org/md5sum.html[5]
- rfc1321: The MD5 Message-Digest Algorithm
  http://www.ietf.org/rfc/rfc1321.txt[6]

--
$ alias **carcoco**="echo Carlos Cortes"
http://bulma.net/todos.phtml?id_autor=132 [7]

Lista de enlaces de este artículo:

1. ftp://ftp.gnu.org/gnu/textutils/
2. http://bulma.net/body.phtml?nIdNoticia=35
3. http://www.gnupg.org/
4. http://www.cert.org/archive/pdf/PGPsigs_paper2.pdf
5. http://www.linuxiso.org/md5sum.html
6. http://www.ietf.org/rfc/rfc1321.txt
7. http://bulma.net/todos.phtml?id_autor=132

E-mail del autor: carcoco _ARROBA_ gmail.com
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=1241