How to password protect gzip files on the command line?

I want to create some tar.gz (and possibly tar.bz2) files, using the tar command on Ubuntu 10.04.

I want to password protect the file.

What is the command to do this (I have Googled, but found nothing that shows how to create and extract compressed files using a password).

Anyone knows how to do this?

ubuntu security tar gzip bzip2

edited Oct 17 '14 at 11:47
pulsarjune
1,115 6 19

asked Jul 12 '10 at 12:50
morpheous
1,178 6 23 27

5 Answers

you have to apply the unix-philosophy to this task: one tool for each task.

tarring and compression is a job for `tar` and `gzip` or `bzip2`, crypto is a job for either `gpg` or `openssl`:

Encrypt

```
% tar cz folder_to_encrypt | \
     openssl enc -aes-256-cbc -e > out.tar.gz.enc
```

Decrypt

```
% openssl enc -aes-256-cbc -d -in out.tar.gz.enc | tar xz
```

Or using gpg

```
% gpg --encrypt out.tar.gz
```

the openssl-variant uses symetric encryption, you would have to tell the receiving party about the used 'password' (aka 'the key'). the gpg-variant uses a combination of symetric and asymetric encryption, you use the key of the receiving party (which means that you do not have to tell any password involved to anyone) to create a session key and crypt the content with that key.

if you go the zip (or 7z) route: essentially that is the same as the openssl-variant, you have to tell the receiving party about the password.

edited Nov 1 '16 at 21:32
Evan
103 1

answered Jul 12 '10 at 13:05
akira
41.1k 10 94 145

20 For anyone wondering how to decrypt the file with openssl: `openssl aes-256-cbc -d -in out.tar.gz.enc -out decrypted.tar.gz` – nathan.f77 Jan 28 '13 at 22:03

1 @nathan.f77 that command also shows how to do things without piping them into openssl. `openssl enc -aes-256-cbc -e -in foo.tar.gz -out bar.tar.gz.enc` – Keith Smiley Mar 6 '14 at 23:48

2 @KeithSmiley if you have large archives and not a lot of space (like it could be on a VPS) it's more space-efficient to pipe. – Andrew Savinykh Jun 2 '14 at 23:15

I can't seem to run this on a mac. Is this different in anyway? – eleijonmarck Dec 20 '16 at 20:46

@eleijonmarck provide the part "does not work because <insert-error-message-here>"… – akira Dec 21 '16 at 8:34

If your intent is to just password protect files, then use the hand zip utility through command line

```
zip -e <file_name>.zip <list_of_files>
```

-e asks the zip utility to encrypt the files mentioned in

Working example:

```
$ touch file_{0,1}.txt # creates blank files file_0 & file_1
$ zip -e file.zip file_* # ask zip to encrypt
$ ENTER PASSWORD:
$ VERIFY PASSWORD:
$ ls file*
```

edited Jul 18 '13 at 4:47

Leo
274 1 9

answered Jun 17 '12 at 20:12

Antony Thomas
257 2 4

7 Zip file encryption is not safe in any way. – Kristopher Ives May 2 '14 at 6:55

1 @KristopherIves can you elaborate on the unsafeness? – tscizzle Jun 2 '16 at 22:26

@tscizzle unix-ag.uni-kl.de/~conrad/krypto/pkcrack/pkcrack-readme.html – Kristopher Ives Jun 4 '16 at 2:09

1 @KristopherIves It requires "another ZIP-archive, containing at least one of the files from the encrypted archive in *unencrypted* form" to work. – Franklin Yu Dec 30 '16 at 20:36

Here's a few ways to do this. One thing to note is that if you're going to use separate compression and encryption tools you should always compress before encryption, since encrypted data is essentially non-compressible.

These examples compress and encrypt a file called `clear_text` .

Using `gpg`

```
$ gpg -c clear_text #Compress & Encrypt
$ gpg -d clear_text.gpg #Decrypt & Decompress
```

gpg will compress the input file before encryption by default, `-c` means to use symmetric encryption with a password. The output file will be `clear_text.gpg` . One benefit of using `gpg` is that is uses standard OpenPGP formats, so any encryption software that supports OpenPGP will be able to decrypt it.

Using `mcrypt`

```
$ mcrypt -z clear_text #Compress & Encrypt
$ mdecrypt -z clear_text.gz.nc #Decrypt & Decompress
```

The `-z` option compresses. By default this outputs a file called `clear_text.gz.nc` .

Using `bcrypt`

```
$ bcrypt -r clear_text #Compress & Encrypt
$ bcrypt -r clear_text.bfe #Decrypt & Decompress
```

bcrypt compresses before encrypting by default, the `-r` option is so that the input file isn't deleted in the process. The output file is called `clear_text.bfe` by default.

Using `gzip` and `aespipe`

```
$ cat clear_text | gzip | aespipe > clear_text.gz.aes #Compress & Encrypt
$ cat clear_text.gz.aes | aespipe -d | gunzip > clear_text #Decrypt & Decompress
```

aespipe is what it sounds like, a program that takes input on stdin and outputs aes encrypted data on stdout. It doesn't support compression, so you can pipe the input through gzip first. Since the output goes to stdout you'll have to redirect it to a file with a name of your own choosing. Probably not the most effective way to do what you're asking but aespipe is a versatile tool so I thought it was worth mentioning.

answered May 1 '14 at 1:38

Graphics Noob
225 4 8

Neither tar, gzip, nor bzip2 supports password protection. Either use a compression format that does, such as zip, or encrypt it with another tool such as GnuPG.

answered Jul 12 '10 at 12:52

Ignacio Vazquez-Abrams
85.1k 4 121 179

Ah, that explains why I couldn't find anything online. I think I'll go for zip. – morpheous Jul 12 '10 at 13:01

Gah!, I'm trying to recursively zip a directory with passwors, and it only creates a zip file with the name foobar as an (empty) directory in it. Here is the command I am using: zip -e foobar.zip foobar. foobar is a non-empty folder in the current directory – morpheous Jul 12 '10 at 13:22

4 Just like the man says, `-r .` – Ignacio Vazquez-Abrams Jul 12 '10 at 13:24

You can use 7zip to create your password protected archive. You can specify the password on the command line (or in a script) the following way:

```
7z a -p<password> <someprotectedfile>.7z file1.txt file2.txt
```

7zip can also read from STDIN as follows:

```
cat <somefile> | 7z a -si -p<password> <someprotectedfile>.7z
```

If it's mandatory to use zip files, you might want to play around with the `-t<type>` parameter (e.g. `-tzip`).

answered Oct 17 '14 at 9:52

SaeX
211 1 11

1 I picked this as the answer because it's the only one that answers the question. The question isn't how to encrypt a message, it's how to password protect an archive. That's all I needed to do. (Gmail was blocking my server backups because it decided there was something unsafe in the attachment, and I just needed to add a password. It doesn't have to be secure.) – felwithe Sep 23 '16 at 16:56