HowToSHA256SUM

The program **sha256sum** is designed to verify data integrity using the SHA-256 (SHA-2 family with a digest length of 256 bits). SHA-256 hashes used properly can confirm both file integrity and authenticity. SHA-256 serves a similar purpose to a prior algorithm recommended by Ubuntu, MD5, but is less vulnerable to attack.

Comparing hashes makes it possible to detect changes in files that would cause errors. The possibility of changes (errors) is proportional to the size of the file; the possibility of errors increase as the file becomes larger. It is a very good idea to run an SHA-256 hash comparison check when you have a file like an operating system install CD that has to be 100% correct.

Contents

In terms of security, cryptographic hashes such as SHA-256 allow for authentication of data obtained from insecure mirrors. The SHA-256 hash must be signed or come from a secure source (such as a HTTPS page or a GPG-signed file) of an organization you trust. See the SHA-256 checksum file for the release you're using under http://releases.ubuntu.com, such as http://cdimage.ubuntu.com/daily-live/current/SHA256SUMS . You should verify this file using the PGP signature, SHA256SUMS.gpg (such as http://cdimage.ubuntu.com/daily-live/current/SHA256SUMS.gpg) as described in VerifyIsoHowto.

sha256

sha256sum on Linux

Most Linux distributions come with the `sha256sum` utility (on Ubuntu it is part of the coreutils package). We are going to use the Ubuntu 9.10 LiveDVD for the following example:

Check the iso file

Ubuntu distributes the SHA-256 checksum hashes in a file called **SHA256SUMS** in the same directory listing as the download page for your release http://releases.ubuntu.com.

Manual method

First open a terminal and go to the correct directory to check a downloaded **iso** file:

```
cd download_directory
```

Then run the following command from within the download directory.

```
sha256sum ubuntu-9.10-dvd-i386.iso
```

sha256sum should then print out a single line after calculating the hash:

```
c01b39c7a35ccc3b081a3e83d2c71fa9a767ebfeb45c69f08e17dfe3ef375a7b *ubuntu-9.10-dvd-i386.iso
```

Compare the hash (the alphanumeric string on left) that your machine calculated with the corresponding hash in the SHA256SUMS file.

When both hashes match exactly then the downloaded file is almost certainly intact. If the hashes do not match, then there was a problem with either the download or a problem with the server. You should download the file again from either the same mirror, or from a different mirror if you suspect a server error. If you continuously receive an erroneous file from a server, please be kind and notify the web-master of that mirror so they can investigate the issue.

Semi-automatic method

First download the **SHA256SUMS** and **SHA256SUMS.gpg** files to the same directory as the iso. Then run the following commands in a terminal.

```
cd download_directory
sha256sum -c SHA256SUMS 2>&1 | grep OK
```

The sha256sum line should output a line such as:

```
ubuntu-9.10-dvd-i386.iso: OK
```

If the OK for your file appears, that indicates the hash matches.

Success

Once you have verified the sha256 hash, go ahead and burn the CD. You may want to refer to the BurningIsoHowto page.

Check the CD

So far so good, you have downloaded an iso and verified its integrity. When you boot from the CD you will be given the option to test its integrity. Great, but if the CD is corrupt then you have already wasted time rebooting. You can check the integrity of the CD without rebooting as follows.

Manual method

```
sha256sum /dev/cdrom
```

Check the calculated hash against UbuntuHashes as shown for the iso file above. Depending on your system, you may need to change **cdrom** to **cdrom0** (or even **cdrom1** if you have two CD drives).

Success?

Congratulations, you now have a verified Ubuntu CD. Go ahead and use it (or play frisbee with it if you want).

digest(1) on Solaris

Use the Solaris digest(1) command, specifying the sha256 algorithm with the -a flag. For instance:

```
$ digest -a sha256 ubuntu-9.10-dvd-i386.iso
c01b39c7a35ccc3b081a3e83d2c71fa9a767ebfeb45c69f08e17dfe3ef375a7b
```

SHA256SUM of burnt media

Depending on how you burn your ISOs you can check the burnt media directly. Start by checking that the ISO file is correct:

```
$ grep ubuntu-9.10-dvd-i386.iso SHA256SUMS | tee /proc/self/fd/2 | sha256sum --check -
c01b39c7a35ccc3b081a3e83d2c71fa9a767ebfeb45c69f08e17dfe3ef375a7b *ubuntu-9.10-dvd-i386.iso
ubuntu-9.10-dvd-i386.iso: OK
```

Now burn it from Nautilus (right-click, "Write to Disc ..."). To check the media directly:

```
$ sha256sum /dev/cdrom
c01b39c7a35ccc3b081a3e83d2c71fa9a767ebfeb45c69f08e17dfe3ef375a7b  /dev/cdrom
```

where "/dev/cdrom" is typically a soft-link to your CD/DVD reader/burner. Note that the checksum matches.

External Links

- Wikipedia's Cryptographic Hash Entry

VerifyIsoHowto

CategoryInstallation

HowToSHA256SUM (last edited 2015-12-14 23:05:24 by anthony-geoghegan @ ip-84-203-58-58.broadband.digiweb.ie[84.203.58.58]:anthony-geoghegan)