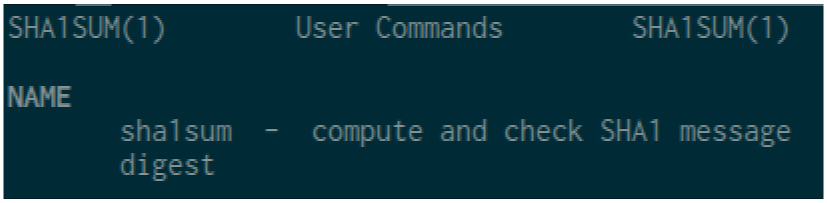
Last updated Saturday, Nov 16, 2019

Linux and Unix sha1sum command tutorial with examples

Tutorial on using sha1sum, a UNIX and Linux command to compute and check a SHA-1 message digest. Examples of reading a SHA-1 message digest, writing a SHA-1 message digest to a file, and checking a SHA-1 message digest.

Estimated reading time: 3 minutes

Table of contents



```
SHA1SUM(1)        User Commands        SHA1SUM(1)

NAME
       sha1sum  -  compute and check SHA1 message
       digest
```

What is the sha1sum command in UNIX?

The `sha1sum` command computes the `SHA-1` message digest of a file. This allows it be compared to a published message digest to check whether the file is unmodified from the original. As such the `sha1sum` command can be used to attempt to verify the integrity of a file. `SHA-1` produces a 160-bit (20 byte) hash value known as a message digest. Although `SHA-1` is no longer considered secure (https://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html) against well funded opponents it is still widely used to verify files.

How to get the SHA-1 of a file

To get the `SHA-1` of a file pass the path of a file to the `sha1sum` command. The `SHA-1` will be printed to standard output printing first the `SHA-1` checksum then the name of the file.

```
sha1sum somefile.txt
da39a3ee5e6b4b0d3255bfef95601890afd80709  somefile.txt
```

How to write the SHA-1 of a file

To write the `SHA-1` of a file standard shell redirection can be used.

```
sha1sum somefile.txt > somefile.txt.sha1
cat somefile.txt.sha1
da39a3ee5e6b4b0d3255bfef95601890afd80709  somefile.txt
```

If the file `somefile.txt` is to be distributed on the Internet the accompanying `SHA-1` file can be distributed with it. This allows anyone downloading or receiving the file to verify (to some extent) that the file has not been tampered with. Normally the canonical author of a file will also publish the `SHA-1` of the file. It is worth verifying that the published `SHA-1` also matches the one published by the author on any webpage relating to the download.

How to check the SHA-1 of a file

If a `SHA-1` file has been provided with a download this can be used to check the integrity of a downloaded file. To check the `SHA-1` of a file use the `-c` option and pass the `SHA-1` checksum file that corresponds to the file or files you wish to check. If not file has been provided with the download the author of the file will normally publish a `SHA-1` message digest and this can be checked manually by comparing the output of `sha1sum [file]` with the published message digest.

```
ls
somefile.txt somefile.txt.sha1
sha1sum -c somefile.txt.sha1
somefile.txt: OK
```

If the `SHA-1` code matches an OK will be printed to standard output along with the filename verified. If the `SHA-1` code fails to match a failure message will be printed to standard output and the file should not be trusted.

```
sha1sum -c somefile.txt.sha1
somefile.txt: FAILED
sha1sum: WARNING: 1 computed checksum did NOT match
```

A note on hashing algorithms

With all issues relating to security things move fast. The `md5` hashing algorithm is now widely considered to be insecure (http://www.dailytech.com/MD5+Is+Officially+Insecure+Hackers+Break+SSL+Certificates+Impersonate+CA/article13842.htm). The `sha1` hashing algorithm is also expected to be insecure (http://arstechnica.com/security/2012/10/sha1-crypto-algorithm-could-fall-by-2018/). As such it is expected that new algorithms will eventually emerge and be widely used. Already there are many checksum commands distributed with Linux and it is expected this will evolve.

```
sha[TAB]
sha1sum    sha224sum  sha256sum  sha384sum  sha512sum  shasum
```

For each of these hashing algorithms the command options and behaviour is the same so when a hashing algorithm changes it is a drop-in replacement.

Further reading

- sha1sum man page (https://linux.die.net/man/1/sha1sum)
- SHA-1 Wikipedia Page (https://en.wikipedia.org/wiki/SHA-1)
- sha1sum for a directory of directories (http://superuser.com/questions/458326/sha1sum-for-a-directory-of-directories)
- GNU Coreutils: sha1sum invocation (https://www.gnu.org/software/coreutils/manual/html_node/sha1sum-invocation.html)