Rocky Enterprise Linux 9.2 Manual Pages on command 'sos-clean.1'

C:\>man sos-clean.1

SOS(CLEAN) SOS(CLEAN)

NAME

sos clean - Obfuscate sensitive data from one or more sosreports

SYNOPSIS

sos clean TARGET [options]

[--domains]

[--disable-parsers]

[--keywords]

[--keyword-file]

[--map-file]

[--jobs]

[--no-update]

[--keep-binary-files]

[--archive-type]

DESCRIPTION

sos clean or sos mask is an sos subcommand used to obfuscate sensitive information from previously generated sosreports that is not covered by the standard plugin-based post processing executed during report generation, for example IP addresses. Data obfuscated via this utility is done so consistently, meaning for example an IP address of 192.168.1.1 in an unprocessed sosreport that gets obfuscated to, for ex? ample, 100.0.0.1, will be changed to 100.0.0.1 in all occurrences found in the re? port.

Additionally, by default all such obfuscations are stored in "maps" that will be persistently saved to /etc/sos/cleaner/default_mapping and be re-used on subsequent runs.

This utility may also be used in-line with sos report and sos collect by specify? ing the --clean or --mask option.

When called directly via sos clean, the obfuscated archive is written as an addi? tional file, meaning the original unprocessed report still remains on the filesys? tem. When called via report or collect, the changes are done in-line and thus only an obfuscated archive is written and available. In either case, a mapping file containing the relationships between unprocessed and obfuscated elements will be written in the same location as the resulting archive. This mapping file should be kept private by system administrators.

REQUIRED ARGUMENTS

TARGET

The path to the archive that is to be obfuscated. This may be an archive or an un? built sos temporary

directory. If an archive, it will first be extracted and then after obfusca? tion is complete re-compressed using the same compression method as the original.

OPTIONS

--domains DOMAINS

Provide a comma-delimited list of domain names to obfuscate, in addition to those matching the hostname of the system that created the sosreport. Subdo? mains that match a domain given via this option will also be obfuscated.

For example, if --domains redhat.com is specified, then 'redhat.com' will be obfuscated, as will 'www.redhat.com' and subdomains such as 'foo.red? hat.com'.

--disable-parsers PARSERS

Provide a comma-delimited list of parsers to disable when cleaning an ar? chive. By default all parsers are enabled.

Note that using this option is very likely to leave sensitive information in place in the target archive, so only use this option when absolutely neces? sary or you have complete trust in the party/parties that may handle the

generated report.

Valid values for this option are currently: hostname, ip, mac, keyword, and username.

--keywords KEYWORDS

Provide a comma-delimited list of keywords to scrub in addition to the de? fault parsers.

Keywords provided by this option will be obfuscated as "obfuscatedwordX" where X is an integer based on the keyword's index in the parser. Note that keywords will be replaced as both standalone words and in substring matches.

--keyword-file FILE

Provide a file that contains a list of keywords that should be obfuscated.

Each word must be specified on a newline within the file.

--map-file FILE

Provide a location to a valid mapping file to use as a reference for exist? ing obfuscation pairs. If one is found, the contents are loaded before parsing is started. This allows consistency between runs of this command for obfuscated pairs. By default, sos will write the generated private map file to /etc/sos/cleaner/default_mapping so that consistency is maintained by de? fault. Users may use this option to reference a map file from a different run (perhaps one that was done on another system).

Default: /etc/sos/cleaner/default_mapping

--jobs JOBS

The number of concurrent archives to process, if more than one. If this utility is called by sos collect then the value of the jobs option for that utility will be used here.

Default: 4

--no-update

Do not write the mapping file contents to /etc/sos/cleaner/default_mapping

--keep-binary-files

Keep unprocessable binary files in the archive, rather than removing them.

Note that binary files cannot be obfuscated, and thus keeping them in the archive may result in otherwise sensitive information being included in the final archive. Users should review any archive that keeps binary files in

place before sending to a third party.

Default: False (remove encountered binary files)

--archive-type TYPE

Specify the type of archive that TARGET was generated as. When sos inspects a TARGET archive, it tries to identify what type of archive it is. For ex? ample, it may be a report generated by sos report, or a collection of those reports generated by sos collect, which require separate approaches.

This option may be useful if a given TARGET archive is known to be of a spe? cific type, but due to unknown reasons or some malformed/missing information in the archive directly, that is not properly identified by sos.

The following are accepted values for this option:

auto Automatically detect the archive type

report An archive generated by sos report

collect An archive generated by sos collect

insights An archive generated by the insights-client package

The following may also be used, however note that these do not attempt to pre-load any information from the archives into the parsers. This means that, among other limitations, items like host and domain names may not be obfuscated unless an obfuscated mapping already exists on the system from a previous execution.

data-dir A plain directory on the filesystem.

tarball A generic tar archive not associated with any known tool

SEE ALSO

sos(1) sos-report(1) sos-collect(1) sos.conf(5)

MAINTAINER

Jake Hunsaker <jhunsake@redhat.com>

AUTHORS & CONTRIBUTORS

See AUTHORS file in the package documentation.