Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'setfiles.8' command

$ man setfiles.8

setfiles(8) SELinux User Command setfiles(8)

NAME

setfiles - set SELinux file security contexts.

SYNOPSIS

setfiles [-c policy] [-C] [-d] [-l] [-m] [-n] [-e directory] [-E] [-p]

[-s] [-v] [-W] [-F] [-I|-D] [-T nthreads] spec_file pathname ...

DESCRIPTION

This manual page describes the setfiles program.

This program is primarily used to initialize the security context fields (extended attributes) on one or more filesystems (or parts of them). Usually it is initially run as part of the SELinux installation process (a step commonly known as labeling).

It can also be run at any other time to correct inconsistent labels, to add support for newly-installed policy or, by using the -n option, to passively check whether the file contexts are all set as specified by the active policy (default behavior) or by some other policy (see the -c option).

If a file object does not have a context, setfiles will write the de? fault context to the file object's extended attributes. If a file ob? ject has a context, setfiles will only modify the type portion of the security context. The -F option will force a replacement of the entire context.

OPTIONS

-c check the validity of the contexts against the specified binary policy.

-C If only relabeling errors are encountered during the file tree walks, exit with status 1 rather than 255.

-d show what specification matched each file.

-e directory

directory to exclude (repeat option for more than one direc? tory).

-E treat conflicting specifications as errors, such as where two hardlinks for the same inode have different contexts.

-f infilename

infilename contains a list of files to be processed. Use ?-? for stdin.

-F Force reset of context to match file_context for customizable files, and the default file context, changing the user, role, range portion as well as the type.

-h, -? display usage information and exit.

-i ignore files that do not exist.

-I ignore digest to force checking of labels even if the stored SHA256 digest matches the specfiles SHA256 digest. The digest will then be updated provided there are no errors. See the NOTES section for further details.

-D Set or update any directory SHA256 digests. Use this option to enable usage of the security.sehash extended attribute.

-l log changes in file labels to syslog.

-m do not read /proc/mounts to obtain a list of non-seclabel mounts to be excluded from relabeling checks. Setting this option is useful where there is a non-seclabel fs mounted with a seclabel fs mounted on a directory below this.

-n don't change any file labels (passive check).

-o outfilename

Deprecated - This option is no longer supported.

-p show progress by printing the number of files in 1k blocks un?

less relabeling the entire OS, that will then show the approxi? mate percentage complete. Note that the -p and -v options are mutually exclusive.

-q Deprecated and replaced by -v. Has no effect on other options or on program behavior.

-r rootpath

use an alternate root path. Used in meta-selinux for OpenEmbed? ded/Yocto builds to label files under rootpath as if they were at /

-s take a list of files from standard input instead of using a pathname from the command line (equivalent to ?-f -?).

-v show changes in file labels and output any inode association pa? rameters. Note that the -v and -p options are mutually exclu? sive.

-W display warnings about entries that had no matching files by outputting the selabel_stats(3) results.

-0 the separator for the input items is assumed to be the null character (instead of the white space). The quotes and the backslash characters are also treated as normal characters that can form valid input. This option finally also disables the end of file string, which is treated like any other argument. Use? ful when input items might contain white space, quote marks or backslashes. The -print0 option of GNU find produces input suitable for this mode.

-T nthreads

use up to nthreads threads. Specify 0 to create as many threads as there are available CPU cores; 1 to use only a single thread (default); or any positive number to use the given number of threads (if possible).

ARGUMENTS

spec_file

The specification file which contains lines of the following form:

regexp [type] context | <<none>>

The regular expression is anchored at both ends. The op? tional type field specifies the file type as shown in the mode field by the ls(1) program, e.g. -- to match only regular files or -d to match only directories. The con? text can be an ordinary security context or the string <<none>> to specify that the file is not to have its con? text changed.

The last matching specification is used. If there are multiple hard links to a file that match different speci? fications and those specifications indicate different se? curity contexts, then a warning is displayed but the file is still labeled based on the last matching specification other than <<none>>.

pathname ...

The pathname for the root directory of each file system to be relabeled or a specific directory within a filesystem that should be recursively descended and relabeled or the pathname of a file that should be relabeled. Not used if the -f or the -s option is used.

EXIT STATUS

setfiles exits with status 0 if it encounters no errors. Fatal errors result in status 255. Labeling errors encountered during file tree walk(s) result in status 1 if the -C option is specified and no other kind of error is encountered, and in status 255 otherwise.

NOTES

1. setfiles operates recursively on directories. Paths leading up the final component of the file(s) are not canonicalized before label? ing.
2. If the pathname specifies the root directory and the -v option is set and the audit system is running, then an audit event is auto? matically logged stating that a "mass relabel" took place using the message label FS_RELABEL.

3. To improve performance when relabeling file systems recursively the -D option to setfiles will cause it to store a SHA256 digest of the spec_file set in an extended attribute named security.sehash on each directory specified in pathname ... once the relabeling has been completed successfully. These digests will be checked should setfiles -D be rerun with the same spec_file and pathname parame? ters. See selinux_restorecon(3) for further details.

The -I option will ignore the SHA256 digest from each directory specified in pathname ... and provided the -n option is NOT set, files will be relabeled as required with the digests then being up? dated provided there are no errors.

AUTHOR

This man page was written by Russell Coker <russell@coker.com.au>. The program was written by Stephen Smalley <sds@tycho.nsa.gov>

SEE ALSO

restorecon(8), load_policy(8), checkpolicy(8)

10 June 2016 setfiles(8)