Red Hat Enterprise Linux Release 9.2 Manual Pages on 'cryptsetup-refresh.8' command

$ man cryptsetup-refresh.8

CRYPTSETUP-REFRESH(8)   Maintenance Commands   CRYPTSETUP-REFRESH(8)

NAME

   cryptsetup-refresh - refresh parameters of an active mapping

SYNOPSIS

   cryptsetup refresh [<options>] <name>

DESCRIPTION

   Refreshes parameters of active mapping <name>.

   Updates parameters of active device <name> without the need to

   deactivate the device (and umount filesystem). Currently, it supports

   parameters refresh on following devices: LUKS1, LUKS2 (including

   authenticated encryption), plain crypt and loop-AES.

   Mandatory parameters are identical to those of an open action for the

   respective device type.

   You may change following parameters on all devices

   --perf-same_cpu_crypt, --perf-submit_from_crypt_cpus,

   --perf-no_read_workqueue, --perf-no_write_workqueue and

   --allow-discards.

   Refreshing the device without any optional parameter will refresh the

   device with default setting (respective to device type).

   LUKS2 only:

   The --integrity-no-journal parameter affects only LUKS2 devices with

   the underlying dm-integrity device.

   Adding option --persistent stores any combination of device parameters

above in LUKS2 metadata (only after successful refresh operation).

The --disable-keyring parameter refreshes a device with volume key

passed in dm-crypt driver.

<options> can be [--allow-discards, --perf-same_cpu_crypt,

--perf-submit_from_crypt_cpus, --perf-no_read_workqueue,

--perf-no_write_workqueue, --header, --disable-keyring,

--disable-locks, --persistent, --integrity-no-journal].

OPTIONS

--allow-discards

Allow the use of discard (TRIM) requests for the device. This is

also not supported for LUKS2 devices with data integrity

protection.

WARNING: This command can have a negative security impact because

it can make filesystem-level operations visible on the physical

device. For example, information leaking filesystem type, used

space, etc. may be extractable from the physical device if the

discarded blocks can be located later. If in doubt, do not use it.

A kernel version of 3.1 or later is needed. For earlier kernels,

this option is ignored.

--perf-same_cpu_crypt

Perform encryption using the same cpu that IO was submitted on. The

default is to use an unbound workqueue so that encryption work is

automatically balanced between available CPUs.

NOTE: This option is available only for low-level dm-crypt

performance tuning, use only if you need a change to default

dm-crypt behaviour. Needs kernel 4.0 or later.

--perf-submit_from_crypt_cpus

Disable offloading writes to a separate thread after encryption.

There are some situations where offloading write bios from the

encryption threads to a single thread degrades performance

significantly. The default is to offload write bios to the same

thread.

NOTE: This option is available only for low-level dm-crypt

performance tuning, use only if you need a change to default

dm-crypt behaviour. Needs kernel 4.0 or later.

--perf-no_read_workqueue, --perf-no_write_workqueue

Bypass dm-crypt internal workqueue and process read or write

requests synchronously.

NOTE: These options are available only for low-level dm-crypt

performance tuning, use only if you need a change to default

dm-crypt behaviour. Needs kernel 5.9 or later.

--header <device or file storing the LUKS header>

Use a detached (separated) metadata device or file where the LUKS

header is stored. This option allows one to store ciphertext and

LUKS header on different devices.

For commands that change the LUKS header (e.g. luksAddKey), specify

the device or file with the LUKS header directly as the LUKS

device.

--disable-locks

Disable lock protection for metadata on disk. This option is valid

only for LUKS2 and ignored for other formats.

WARNING: Do not use this option unless you run cryptsetup in a

restricted environment where locking is impossible to perform

(where /run directory cannot be used).

--disable-keyring

Do not load volume key in kernel keyring and store it directly in

the dm-crypt target instead. This option is supported only for the

LUKS2 type.

--persistent

If used with LUKS2 devices and activation commands like open or

refresh, the specified activation flags are persistently written

into metadata and used next time automatically even for normal

activation. (No need to use cryptab or other system configuration

files.)

If you need to remove a persistent flag, use --persistent without

the flag you want to remove (e.g. to disable persistently stored

discard flag, use --persistent without --allow-discards).

Only --allow-discards, --perf-same_cpu_crypt,

--perf-submit_from_crypt_cpus, --perf-no_read_workqueue,

--perf-no_write_workqueue and --integrity-no-journal can be stored

persistently.

--integrity-no-journal

Activate device with integrity protection without using data

journal (direct write of data and integrity tags). Note that

without journal power fail can cause non-atomic write and data

corruption. Use only if journalling is performed on a different

storage layer.

--batch-mode, -q

Suppresses all confirmation questions. Use with care!

If the --verify-passphrase option is not specified, this option

also switches off the passphrase verification.

--debug or --debug-json

Run in debug mode with full diagnostic logs. Debug output lines are

always prefixed by #.

If --debug-json is used, additional LUKS2 JSON data structures are

printed.

--version, -V

Show the program version.

--usage

Show short option help.

--help, -?

Show help text and default parameters. == REPORTING BUGS

Report bugs at cryptsetup mailing list <cryptsetup@lists.linux.dev> or

in Issues project section

<https://gitlab.com/cryptsetup/cryptsetup/-/issues/new>.

Please attach output of the failed command with --debug option added.

SEE ALSO

Cryptsetup FAQ

<https://gitlab.com/cryptsetup/cryptsetup/wikis/FrequentlyAskedQuestions>

cryptsetup(8), integritysetup(8) and veritysetup(8)

CRYPTSETUP

Part of cryptsetup project <https://gitlab.com/cryptsetup/cryptsetup/>.

cryptsetup 2.6.0   2022-12-14   CRYPTSETUP-REFRESH(8)