Rocky Enterprise Linux 9.2 Manual Pages on command 'integritysetup.8'

$ man integritysetup.8

INTEGRITYSETUP(8)   Maintenance Commands   INTEGRITYSETUP(8)

NAME

       integritysetup - manage dm-integrity (block level integrity) volumes

SYNOPSIS

       integritysetup <options> <action> <action args>

DESCRIPTION

       Integritysetup is used to configure dm-integrity managed device-mapper mappings.

       Device-mapper integrity target provides read-write transparent integrity checking of block

       devices. The dm-integrity target emulates additional data integrity field per-sector. You

       can use this additional field directly with integritysetup utility, or indirectly (for au?

       thenticated encryption) through cryptsetup.

       Integritysetup supports these operations:

       format <device>

              Formats <device> (calculates space and dm-integrity superblock and wipes the de?

              vice).

              <options> can be [--data-device, --batch-mode, --no-wipe, --journal-size, --inter?

              leave-sectors, --tag-size, --integrity, --integrity-key-size, --integrity-key-file,

              --sector-size, --progress-frequency]

       open <device> <name>

       create <name> <device> (OBSOLETE syntax)

              Open a mapping with <name> backed by device <device>.

              <options> can be [--data-device, --batch-mode, --journal-watermark, --journal-com?

              mit-time,   --buffer-sectors,   --integrity,   --integrity-key-size,   --integ?

rity-key-file, --integrity-no-journal, --integrity-recalculate, --integrity-recal?

culate-reset,--integrity-recovery-mode, --allow-discards]

close <name>

    Removes existing mapping <name>.

    For backward compatibility, there is remove command alias for the close command.

    <options> can be [--deferred] or [--cancel-deferred]

status <name>

    Reports status for the active integrity mapping <name>.

dump <device>

    Reports parameters from on-disk stored superblock.

OPTIONS

--verbose, -v

    Print more information on command execution.

--debug

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

    by '#'.

--version

    Show the program version.

--batch-mode

    Do not ask for confirmation.

--progress-frequency <seconds>

    Print separate line every <seconds> with wipe progress.

--no-wipe

    Do not wipe the device after format. A device that is not initially wiped will con?

    tain invalid checksums.

--journal-size, -j BYTES

    Size of the journal.

--interleave-sectors SECTORS

    The number of interleaved sectors.

--integrity-recalculate

    Automatically recalculate integrity tags in kernel on activation. The device can

    be used during automatic integrity recalculation but becomes fully integrity pro?

    tected only after the background operation is finished. This option is available

since the Linux kernel version 4.19.

--integrity-recalculate-reset

Restart recalculation from the beginning of the device. It can be used to change
the integrity checksum function. Note it does not change the tag length. This op?
tion is available since the Linux kernel version 5.13.

--journal-watermark PERCENT

Journal watermark in percents. When the size of the journal exceeds this watermark,
the journal flush will be started.

--journal-commit-time MS

Commit time in milliseconds. When this time passes (and no explicit flush operation
was issued), the journal is written.

--tag-size, -t BYTES

Size of the integrity tag per-sector (here the integrity function will store au?
thentication tag).

NOTE: The size can be smaller that output size of the hash function, in that case
only part of the hash will be stored.

--data-device

Specify a separate data device that contains existing data. The <device> then will
contain calculated integrity tags and journal for this data device.

--sector-size, -s BYTES

Sector size (power of two: 512, 1024, 2048, 4096).

--buffer-sectors SECTORS

The number of sectors in one buffer.

The tag area is accessed using buffers, the large buffer size means that the I/O
size will be larger, but there could be less I/Os issued.

--integrity, -I ALGORITHM

Use internal integrity calculation (standalone mode). The integrity algorithm can
be CRC (crc32c/crc32) or hash function (sha1, sha256).

For HMAC (hmac-sha256) you have also to specify an integrity key and its size.

--integrity-key-size BYTES

The size of the data integrity key. Maximum is 4096 bytes.

--integrity-key-file FILE

The file with the integrity key.

--integrity-no-journal, -D

    Disable journal for integrity device.

--integrity-bitmap-mode. -B

    Use alternate bitmap mode (available since Linux kernel 5.2)   where dm-integrity

    uses bitmap instead of a journal. If a bit in the bitmap is 1, the corresponding

    region's data and integrity tags are not synchronized - if the machine crashes, the

    unsynchronized regions will be recalculated. The bitmap mode is faster than the

    journal mode, because we don't have to write the data twice, but it is also less

    reliable, because if data corruption happens when the machine crashes, it may not

    be detected.

--bitmap-sectors-per-bit SECTORS

    Number of 512-byte sectors per bitmap bit, the value must be power of two.

--bitmap-flush-time MS

    Bitmap flush time in milliseconds.

WARNING:

    In case of a crash, it is possible that the data and integrity tag doesn't match if

    the journal is disabled.

--integrity-recovery-mode. -R

    Recovery mode (no journal, no tag checking).

NOTE: The following options are intended for testing purposes only.

    Using journal encryption does not make sense without encryption the data, these op?

    tions are internally used in authenticated disk encryption with cryptsetup(8).

--journal-integrity ALGORITHM

    Integrity algorithm for journal area. See --integrity option for detailed specifi?

    cation.

--journal-integrity-key-size BYTES

    The size of the journal integrity key. Maximum is 4096 bytes.

--journal-integrity-key-file FILE

    The file with the integrity key.

--journal-crypt ALGORITHM

    Encryption algorithm for journal data area. You can use a block cipher here such

    as cbc-aes or a stream cipher, for example, chacha20 or ctr-aes.

--journal-crypt-key-size BYTES

The size of the journal encryption key. Maximum is 4096 bytes.

--journal-crypt-key-file FILE

The file with the journal encryption key.

--allow-discards

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

since the Linux kernel version 5.7.

--deferred

Defers device removal in close command until the last user closes it.

--cancel-deferred

Removes a previously configured deferred device removal in close command.

The dm-integrity target is available since Linux kernel version 4.12.

NOTE: Format and activation of an integrity device always require superuser privilege be?

cause the superblock is calculated and handled in dm-integrity kernel target.

LEGACY COMPATIBILITY OPTIONS

WARNING:

Do not use these options until you need compatibility with specific old kernel.

--integrity-legacy-padding

Use inefficient legacy padding.

--integrity-legacy-hmac

Use old flawed HMAC calclation (also does not protect superblock).

--integrity-legacy-recalculate

Allow insecure recalculating of volumes with HMAC keys (recalcualtion offset in su?

perblock is not protected).

RETURN CODES

Integritysetup returns 0 on success and a non-zero value on error.

Error codes are:

1 wrong parameters

2 no permission

3 out of memory

4 wrong device specified

5 device already exists, or device is busy.

EXAMPLES

Format the device with default standalone mode (CRC32C):

integritysetup format <device>

Open the device with default parameters:

integritysetup open <device> test

Format the device in standalone mode for use with HMAC(SHA256):

integritysetup format <device> --tag-size 32 --integrity hmac-sha256 --integrity-key-file

<keyfile> --integrity-key-size <key_bytes>

Open (activate) the device with HMAC(SHA256) and HMAC key in file:

integritysetup open <device> test --integrity hmac-sha256 --integrity-key-file <keyfile>

--integrity-key-size <key_bytes>

Dump dm-integrity superblock information:

integritysetup dump <device>

REPORTING BUGS

Report bugs, including ones in the documentation, on the cryptsetup mailing list at <dm-

crypt@saout.de> or in the 'Issues' section on LUKS website. Please attach the output of

the failed command with the --debug option added.

AUTHORS

The integritysetup tool is written by Milan Broz <gmazyland@gmail.com> and is part of the

cryptsetup project.

COPYRIGHT

Copyright ? 2016-2021 Red Hat, Inc.

Copyright ? 2016-2021 Milan Broz

This is free software; see the source for copying conditions. There is NO warranty; not

even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

SEE ALSO

The project website at https://gitlab.com/cryptsetup/cryptsetup

The integrity on-disk format specification available at https://gitlab.com/crypt?

setup/cryptsetup/wikis/DMIntegrity

integritysetup   January 2021   INTEGRITYSETUP(8)