Rocky Enterprise Linux 9.2 Manual Pages on command 'cryptsetup-tcryptDump.8'

$ man cryptsetup-tcryptDump.8

CRYPTSETUP-TCRYPTDUMP(8)   Maintenance Commands   CRYPTSETUP-TCRYPTDUMP(8)

NAME

    cryptsetup-tcryptDump - dump the header information of a TCRYPT

    (TrueCrypt or VeraCrypt compatible) device

SYNOPSIS

    cryptsetup tcryptDump [<options>] <device>

DESCRIPTION

    Dump the header information of a TCRYPT (TrueCrypt or VeraCrypt

    compatible) device.

    If the --dump-volume-key option is used, the TCRYPT device volume key

    is dumped instead of TCRYPT header info. Beware that the volume key (or

    concatenated volume keys if cipher chain is used) can be used to

    decrypt the data stored in the TCRYPT container without a passphrase.

    This means that if the volume key is compromised, the whole device has

    to be erased to prevent further access. Use this option carefully.

    <options> can be [--dump-volume-key, --key-file, --tcrypt-hidden,

    --tcrypt-system, --tcrypt-backup, --veracrypt (ignored),

    --disable-veracrypt, --veracrypt-pim, --veracrypt-query-pim, --cipher,

--hash, --header, --verify-passphrase, --timeout].

The keyfile parameter allows a combination of file content with the

passphrase and can be repeated.

OPTIONS

    --hash, -h <hash-spec>

        Specifies the passphrase hash. Applies to plain and loopaes device

        types only.

        For tcrypt device type, it restricts checked PBKDF2 variants when

        looking for header.

    --cipher, -c <cipher-spec>

        Set the cipher specification string for plain device type.

        For tcrypt device type it restricts checked cipher chains when

        looking for header.

    --verify-passphrase, -y

        When interactively asking for a passphrase, ask for it twice and

        complain if both inputs do not match. Ignored on input from file or

        stdin.

    --key-file, -d name

        Read the passphrase from file.

        If the name given is "-", then the passphrase will be read from

        stdin. In this case, reading will not stop at newline characters.

        See section NOTES ON PASSPHRASE PROCESSING in cryptsetup(8) for

        more information.

    --dump-volume-key, --dump-master-key (OBSOLETE alias)

        Print the volume key in the displayed information. Use with care,

        as the volume key can be used to bypass the passphrases, see also

        option --volume-key-file.

    --timeout, -t <number of seconds>

        The number of seconds to wait before timeout on passphrase input

        via terminal. It is relevant every time a passphrase is asked. It

        has no effect if used in conjunction with --key-file.

        This option is useful when the system should not stall if the user

        does not input a passphrase, e.g. during boot. The default is a

value of 0 seconds, which means to wait forever.

--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.

--tcrypt-hidden, --tcrypt-system, --tcrypt-backup

Specify which TrueCrypt on-disk header will be used to open the

device. See TCRYPT section in cryptsetup(8) for more info.

--veracrypt

This option is ignored as VeraCrypt compatible mode is supported by

default.

--disable-veracrypt

This option can be used to disable VeraCrypt compatible mode (only

TrueCrypt devices are recognized). Only for TCRYPT extension. See

TCRYPT section in cryptsetup(8) for more info.

--veracrypt-pim, --veracrypt-query-pim

Use a custom Personal Iteration Multiplier (PIM) for VeraCrypt

device. See TCRYPT section in cryptsetup(8) for more info.

--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-TCRYPTDUMP(8)