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 'cryptsetup-resize.8' command

$ man cryptsetup-resize.8

CRYPTSETUP-RESIZE(8) Maintenance Commands CRYPTSETUP-RESIZE(8)

NAME

cryptsetup-resize - resize an active mapping

SYNOPSIS

cryptsetup resize [<options>] <name>

DESCRIPTION

Resizes an active mapping <name>.

If --size (in 512-bytes sectors) or --device-size are not specified, the size is computed from the underlying device. For LUKS it is the size of the underlying device without the area reserved for LUKS header (see data payload offset in luksDump command). For plain crypt device, the whole device size is used.

Note that this does not change the raw device geometry, it just changes how many sectors of the raw device are represented in the mapped device.

If cryptsetup detected volume key for active device loaded in kernel keyring service, resize action would first try to retrieve the key using a token. Only if it failed, it?d ask for a passphrase to unlock a keyslot (LUKS) or to derive a volume key again (plain mode). The kernel keyring is used by default for LUKS2 devices.

<options> can be [--size, --device-size, --token-id, --token-only, --token-type, --key-slot, --key-file, --keyfile-size, --keyfile-offset, --timeout, --disable-external-tokens, --disable-locks,

--disable-keyring, --verify-passphrase, --timeout].

OPTIONS

--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.

--keyfile-offset value

Skip value bytes at the beginning of the key file.

--keyfile-size, -l value

Read a maximum of value bytes from the key file. The default is to read the whole file up to the compiled-in maximum that can be queried with --help. Supplying more data than the compiled-in maximum aborts the operation.

This option is useful to cut trailing newlines, for example. If --keyfile-offset is also given, the size count starts after the offset.

--key-slot, -S <0-N>

For LUKS operations that add key material, this option allows you to specify which key slot is selected for the new key.

The maximum number of key slots depends on the LUKS version. LUKS1 can have up to 8 key slots. LUKS2 can have up to 32 key slots based on key slot area size and key size, but a valid key slot ID can always be between 0 and 31 for LUKS2.

--size, -b <number of 512 byte sectors>

Set the size of the device in sectors of 512 bytes.

--device-size size[units]

Sets new size of the device. If unset real device size is used.

If no unit suffix is specified, the size is in bytes.

Unit suffix can be S for 512 byte sectors, K/M/G/T (or KiB,MiB,GiB,TiB) for units with 1024 base or KB/MB/GB/TB for 1000 base (SI scale).

--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.

--disable-external-tokens

Disable loading of plugins for external LUKS2 tokens.

--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.

--token-id

Specify what token to use. If omitted, all available tokens will be checked before proceeding further with passphrase prompt.

--token-only

Do not proceed further with action if token based keyslot unlock failed. Without the option, action asks for passphrase to proceed further.

--token-type type

Restrict tokens eligible for operation to specific token type. Mostly useful when no --token-id is specified.

--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/>.