NAME

cryptsetup-luksDump − dump the header information of a LUKS device

SYNOPSIS

cryptsetup *luksDump* **[<options>] <device>**

DESCRIPTION

Dump the header information of a LUKS device.

If the −−dump−volume−key option is used, the LUKS device volume key is dumped instead of the keyslot info. With the −−volume−key−file option, the volume key is dumped to a file instead of standard output. Beware that the volume key cannot be changed without reencryption and can be used to decrypt the data stored in the LUKS container without a passphrase and even without the LUKS header. This means that if the volume key is compromised, the whole device has to be erased or reencrypted to prevent further access. Use this option carefully.

A passphrase must be supplied to dump the volume key, either interactively or via −−key−file.

To dump an unbound key (LUKS2 format only), −−unbound parameter, specific −−key−slot id and proper passphrase must be supplied, interactively or via −−key−file. Optional −−volume−key−file parameter enables unbound keyslot dump to a file.

To dump LUKS2 JSON metadata (without basic header information like UUID), use the −−dump−json−metadata option.

If −−dump−volume−key is used with −−key−file and the argument to −−key−file is '−', no validation question will be asked and no warning given.

<options> can be [−−dump−volume−key, −−dump−json−metadata, −−key−file, −−keyfile−offset, −−keyfile−size, −−header, −−disable−locks, −−volume−key−file, −−type, −−unbound, −−key−slot, −−timeout, −−external−tokens−path].

OPTIONS

−−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.

−−disable−locks

Disable lock protection for metadata on disk. This option is valid only for LUKS2 and is 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).

−−dump−json−metadata

For *luksDump* (LUKS2 only), this option prints the content of the LUKS2 header JSON metadata area.

−−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.

−−external−tokens−path *<absolute path>*
Override the system directory path where cryptsetup searches for external token handlers (or token plugins). It must be an absolute path (starting with '/' character).

−−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 the 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.

−−help, **−?**
Show help text and default parameters.

−−key−description *text*
Set the key description in the keyring that will be used for passphrase retrieval.

−−key−file, **−d** *file*
Read the passphrase from the 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 keyslot is selected for the new key.

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

−−timeout, **−t** *seconds*
The number of seconds to wait before a 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.

−−type *type*

Specifies required device type, for more info, read the *BASIC ACTIONS* section in **cryptsetup**(8).

−−unbound
Dumps the existing LUKS2 unbound keyslot.

−−usage
Show short option help.

−−version, **−V**
Show the program version.

−−volume−key−file *file*, −−master−key−file file (OBSOLETE alias)
Use a volume key stored in a file.

The volume key is stored in a file instead of being printed out to standard output.

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 the 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/>.