NAME

cryptsetup-luksResume − resume a suspended device and reinstate the key

SYNOPSIS

cryptsetup *luksResume* **[<options>] <name>**

DESCRIPTION

Resumes a suspended device and reinstates the encryption key. Prompts interactively for a passphrase if no token is usable (LUKS2 only) or −−key−file is not given.

<options> can be [−−key−file, −−keyfile−size, −−keyfile−offset, −−key−slot, −−header, −−disable−keyring, −−disable−locks, −−token−id, −−token−only, −−token−type, −−disable−external−tokens, −−type, −−tries, −−timeout, −−verify−passphrase, −−volume−key−keyring, −−link−vk−to−keyring, −−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−external−tokens

Disable loading of plugins for external LUKS2 tokens.

−−disable−keyring

Do not load the volume key in the kernel keyring; store it directly in the dm−crypt target instead. This option is supported only for the LUKS2 type.

−−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).

−−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.

−−link−vk−to−keyring *<keyring description>::<key description>*
Link the volume key in a keyring with the specified key name. The volume key is linked only if the requested action is successfully finished (with −−test−passphrase, the verified volume key is linked in a keyring without taking further action).

The *<keyring description>* string has to contain the existing kernel keyring description. The keyring name may be optionally prefixed with "%:" or "%keyring:" type descriptions. Or, the keyring may also be specified directly by numeric key id. Also, special keyring notations starting with "@" may be used to select existing predefined kernel keyrings.

The string "::" is a delimiter used to separate the keyring description and key description.

<key description> part describes key type and key name of volume key linked in the keyring described in *<keyring description>*. The type may be specified by adding a "%<type_name>:" prefix in front of the key name. If the type is missing, the default *user* type is applied. If the key of the same name and type already exists (already linked in the keyring), it will get replaced in the process.

See also the **KEY IDENTIFIERS** section of **keyctl**(1).

−−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.

−−token−id
Specify what token to use and allow the token PIN prompt to take precedence over the interactive keyslot passphrase prompt. If omitted, all available tokens (not protected by PIN) will be checked before proceeding further with the passphrase prompt.

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

It allows LUKS2 tokens protected by PIN to take precedence over the interactive keyslot passphrase prompt.

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

It allows LUKS2 *type* tokens protected by PIN to take precedence over the interactive keyslot passphrase prompt.

−−tries, **−T**
How often the input of the passphrase shall be retried. The default is 3 tries.

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

−−usage
Show short option help.

−−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.

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

−−volume−key−keyring <*key description*>
Use a volume key stored in a keyring. This allows one to open *luks* and *plain* device types without giving a passphrase.

For LUKS, the key and associated type have to be readable from userspace so that the volume key digest may be verified before activation. For devices in reencryption, the option may be used twice to specify both old and new volume keys.

For PLAIN type, the user must ensure that the key in the keyring is unchanged since activation. Otherwise, reloading the key can cause data corruption after an unexpected key change.

The <*key description*> uses keyctl−compatible syntax. This can either be a numeric key ID or a string name in the format *%*<*key type*>*:*<*key name*>. See also the **KEY IDENTIFIERS** section of **keyctl**(1). When no *%*<*key type*>*:* prefix is specified, we assume the key type is *user* (default type).

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/>.