NAME

e4crypt − ext4 file system encryption utility

SYNOPSIS

e4crypt add_key -S [**-k** *keyring*] [**-v**] [**-q**] [**-p** *pad*] [*path ...*]
e4crypt new_session
e4crypt get_policy *path ...*
e4crypt set_policy [**-p** *pad*] *policy path ...*

DESCRIPTION

e4crypt performs encryption management for ext4 file systems.

COMMANDS

e4crypt add_key [**-vq**] [**-S** *salt*] [**-k** *keyring*] [**-p** *pad*] [*path ...*]

Prompts the user for a passphrase and inserts it into the specified keyring. If no keyring is specified, e4crypt will use the session keyring if it exists or the user session keyring if it does not.

A salt is used to convert the passphrase into an encryption key, and ensures that if the user uses the same passphrase in different contexts, different salt values will result in different encryption keys. By default, **e4crypt** will examine all mounted ext4 file systems, and insert an encryption key salted with each file system with encryption enabled with its default salt value.

Alternatively, if the user specifies an explicit salt, that salt value will be used to calculate the encryption key from the passphrase. If the first two characters of *salt* are "s:", then the rest of the argument will be used as a text string and used as the salt value. If the first two characters are "0x", then the rest of the argument will be parsed as a hex string and the hex value will be used as the salt. If the first characters are "f:" then the rest of the argument will be interpreted as a filename from which the salt value will be read. If the string begins with a '/' character, it will similarly be treated as filename. Finally, if the *salt* argument can be parsed as a valid UUID, then the UUID value will be used as a salt value.

The *keyring* argument specifies the keyring to which the key should be added.

The *pad* value specifies the number of bytes of padding will be added to directory names for obfuscation purposes. Valid *pad* values are 4, 8, 16, and 32.

If one or more directory paths are specified, e4crypt will try to set the policy of those directories to use the key just added by the **add_key** command. If a salt was explicitly specified, then it will be used to derive the encryption key of those directories. Otherwise a directory-specific default salt will be used.

e4crypt get_policy *path ...*

Print the policy for the directories specified on the command line.

e4crypt new_session

Give the invoking process (typically a shell) a new session keyring, discarding its old session keyring.

e4crypt set_policy [**-p** *pad*] *policy path ...*

Sets the policy for the directories specified on the command line. All directories must be empty to set the policy; if the directory already has a policy established, e4crypt will validate that the policy matches what was specified. A policy is an encryption key identifier consisting of 16 hexadecimal characters.

AUTHOR

Written by Michael Halcrow <mhalcrow@google.com>, Ildar Muslukhov <muslukhovi@gmail.com>, and Theodore Ts'o <tytso@mit.edu>

SEE ALSO

keyctl(1), **mke2fs**(8), **mount**(8).