NAME

/etc/crypttab - encrypted block device table

DESCRIPTION

The **/etc/crypttab** file describes encrypted block devices that are set up during system boot.

Empty lines and lines starting with the **#** character are ignored. Each of the remaining lines describes one encrypted block device, fields on the line are delimited by white space. The first two fields are mandatory, the remaining two are optional.

The first field contains the *name* of the resulting encrypted block device; the device is set up at **/dev/mapper/***name*.

The second field contains a path to the underlying block device. If the block device contains a LUKS signature, it is opened as a LUKS encrypted partition; otherwise it is assumed to be a raw dm-crypt partition.

The third field specifies the encryption password. If the field is not present or the password is set to **none**, the password has to be manually entered during system boot. Otherwise the field is interpreted as a path to a file containing the encryption password. This field does not support spaces, whether escaped with back slashes or quotes. Back slashes or quotes will cause this field to be interpreted as a path to a password file. If you wish to use a password with spaces in it, please use a password file. If using a password file, please note that the entire contents of the password file is used, including new lines and non-printable characters. A password file without a line feed can be created with the "echo" command's "-n" option. For example: echo -n "pass phrase" > MyPasswordFile For swap encryption **/dev/urandom** can be used as the password file; using **/dev/random** may prevent boot completion if the system does not have enough entropy to generate a truly random encryption key.

The fourth field, if present, is a comma-delimited list of options. The following options are recognized:

cipher=*cipher*
: Specifies the cipher to use; see **cryptsetup**(8) for possible values and the default value of this option. A cipher with unpredictable IV values, such as **aes-cbc-essiv:sha256**, is recommended.

size=*size*
: Specifies the key size in bits; see **cryptsetup**(8) for possible values and the default value of this option.

hash=*hash*
: Specifies the hash to use for password hashing; see **cryptsetup**(8) for possible values and the default value of this option.

verify If the the encryption password is read from console, it has to be entered twice (to prevent typos).

swap The encrypted block device will be used as a swap partition, and will be formatted as a swap partition after setting up the encrypted block device. The underlying block device will be formatted again as an unencrypted swap partition after destroying the encrypted block device. (This allows sharing a single swap partition between operating system installations, with some of them encrypting the swap partitions and some of them not.)

WARNING: Using the **swap** option will destroy the contents of the named partition during every boot, so make sure the underlying block device is specified correctly.

tmp The encrypted block device will be prepared for using it as tmp partition: it will be formatted using **mke2fs** and its root directory will be set to mode 01777. The warning about the **swap** option applies here as well.

No options can be specified for LUKS encrypted partitions.

COMPATIBILITY

The **/etc/crypttab** file format is based on the Debian cryptsetup package, and is intended to be compatible.

SEE ALSO

cryptsetup(8)