Full credit is given to the above companies including the OS that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'integritytab.5'

$ man integritytab.5

```
INTEGRITYTAB(5)            integritytab            INTEGRITYTAB(5)
```

NAME

integritytab - Configuration for integrity block devices

SYNOPSIS

/etc/integritytab

DESCRIPTION

The /etc/integritytab file describes integrity protected 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 verity integrity protected block device. Fields are delimited by white space.

Each line is in the form

```
    volume-name block-device
        [keyfile|-] [options|-]
```

The first two fields are mandatory, the remaining two are optional and only required if user specified non-default options during integrity format.

The first field contains the name of the resulting integrity volume;

its block device is set up below /dev/mapper/.

The second field contains a path to the underlying block device, or a specification of a block device via "UUID=" followed by the UUID, "PARTUUID=" followed by the partition UUID, "LABEL=" followed by the label, "PARTLABEL=" followed by the partition label.

The third field if present contains an absolute filename path to a key file or a "-" to specify none. When the filename is present, the "integrity-algorithm" defaults to "hmac-sha256" with the key length derived from the number of bytes in the key file. At this time the only supported integrity algorithm when using key file is hmac-sha256. The maximum size of the key file is 4096 bytes.

The fourth field, if present, is a comma-delimited list of options or a "-" to specify none. The following options are recognized:

allow-discards

Allow the use of discard (TRIM) requests for the device. This option is available since the Linux kernel version 5.7.

journal-watermark=[0..100]%

Journal watermark in percent. When the journal percentage exceeds this watermark, the journal flush will be started. Setting a value of "0%" uses default value.

journal-commit-time=[0..N]

Commit time in milliseconds. When this time passes (and no explicit flush operation was issued), the journal is written. Setting a value of zero uses default value.

data-device=/dev/disk/by-...

Specify a separate block device that contains existing data. The second field specified in the integritytab for block device then will contain calculated integrity tags and journal for data-device, but not the end user data.

integrity-algorithm=[crc32c|crc32|sha1|sha256|hmac-sha256]

The algorithm used for integrity checking. The default is crc32c. Must match option used during format.

At early boot and when the system manager configuration is reloaded, this file is translated into native systemd units by systemd-integritysetup-generator(8).

EXAMPLES

Example 1. /etc/integritytab

Set up two integrity protected block devices.

```
                                        home     PARTUUID=4973d0b8-1b15-c449-96ec-94bab7f6a7b8     -
journal-commit-time=10,allow-discards,journal-watermark=55%
    data PARTUUID=5d4b1808-be76-774d-88af-03c4c3a41761 - allow-discards
```

Example 2. /etc/integritytab

Set up 1 integrity protected block device using defaults

```
    home PARTUUID=4973d0b8-1b15-c449-96ec-94bab7f6a7b8
```

Example 3. /etc/integritytab

Set up 1 integrity device using existing data block device which contains user data

```
                                        home     PARTUUID=4973d0b8-1b15-c449-96ec-94bab7f6a7b8     -
data-device=/dev/disk/by-uuid/9276d9c0-d4e3-4297-b4ff-3307cd0d092f
```

Example 4. /etc/integritytab

Set up 1 integrity device using a HMAC key file using defaults

```
    home PARTUUID=4973d0b8-1b15-c449-96ec-94bab7f6a7b8 /etc/hmac.key
```

SEE ALSO

systemd(1), systemd-integritysetup@.service(8), systemd-integritysetup-generator(8), integritysetup(8),

systemd 252   INTEGRITYTAB(5)