NAME

veritytab − Configuration for verity block devices

SYNOPSIS

/etc/veritytab

DESCRIPTION

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

Each line is in the form

volume−name data−device hash−device roothash options

The first four fields are mandatory, the remaining one is optional.

The first field contains the name of the resulting verity volume; its block device is set up below /dev/mapper/.

The second field contains a path to the underlying block data device, or a specification of a block device via "UUID=" followed by the UUID.

The third field contains a path to the underlying block hash device, or a specification of a block device via "UUID=" followed by the UUID.

The fourth field is the "roothash" in hexadecimal.

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

ignore−corruption, **restart−on−corruption**, **panic−on−corruption**
: Defines what to do if a data verity problem is detected (data corruption). Without these options kernel fails the IO operation with I/O error. With "−−ignore−corruption" option the corruption is only logged. With "−−restart−on−corruption" or "−−panic−on−corruption" the kernel is restarted (panicked) immediately. (You have to provide way how to avoid restart loops.)

ignore−zero−blocks
: Instruct kernel to not verify blocks that are expected to contain zeroes and always directly return zeroes instead. WARNING: Use this option only in very specific cases. This option is available since Linux kernel version 4.5.

check−at−most−once
: Instruct kernel to verify blocks only the first time they are read from the data device, rather than every time. WARNING: It provides a reduced level of security because only offline tampering of the data device's content will be detected, not online tampering. This option is available since Linux kernel version 4.17.

root−hash−signature=
: A base64 string encoding the root hash signature prefixed by "base64:" or a path to roothash signature file used to verify the root hash (in kernel). This feature requires Linux kernel version 5.4 or more recent.

_netdev
: Marks this veritysetup device as requiring network. It will be started after the network is available, similarly to **systemd.mount**(5) units marked with **_netdev**. The service unit to set up this device will be ordered between remote−fs−pre.target and remote−veritysetup.target, instead of veritysetup−pre.target and veritysetup.target.

  Hint: if this device is used for a mount point that is specified in **fstab**(5), the **_netdev** option should also be used for the mount point. Otherwise, a dependency loop might be created where the mount point will be pulled in by local−fs.target, while the service to configure the network is usually only started *after* the local file system has been mounted.

noauto
This device will not be added to veritysetup.target. This means that it will not be automatically enabled on boot, unless something else pulls it in. In particular, if the device is used for a mount point, it'll be enabled automatically during boot, unless the mount point itself is also disabled with **noauto**.

nofail
This device will not be a hard dependency of veritysetup.target. It'll still be pulled in and started, but the system will not wait for the device to show up and be enabled, and boot will not fail if this is unsuccessful. Note that other units that depend on the enabled device may still fail. In particular, if the device is used for a mount point, the mount point itself also needs to have the **nofail** option, or the boot will fail if the device is not enabled successfully.

x−initrd.attach
Setup this verity protected block device in the initramfs, similarly to **systemd.mount**(5) units marked with **x−initrd.mount**.

Although it's not necessary to mark the mount entry for the root file system with **x−initrd.mount**, **x−initrd.attach** is still recommended with the verity protected block device containing the root file system as otherwise systemd will attempt to detach the device during the regular system shutdown while it's still in use. With this option the device will still be detached but later after the root file system is unmounted.

All other verity protected block devices that contain file systems mounted in the initramfs should use this option.

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

EXAMPLES

Example 1. /etc/veritytab example

Set up two verity protected block devices. One using device blocks, another using files.

```
usr  PARTUUID=783e45ae−7aa3−484a−beef−a80ff9c19cbb PARTUUID=21dc1dfe−4c33−8b48−98a9−918a22eb3e37 36
data /etc/data /etc/hash a5ee4b42f70ae1f46a08a7c92c2e0a20672ad2f514792730f5d49d7606ab8fdf auto
```

SEE ALSO

systemd(1), **systemd-veritysetup@.service**(8), **systemd-veritysetup-generator**(8), **fstab**(5), **veritysetup**(8),