Rocky Enterprise Linux 9.2 Manual Pages on command 'systemd-random-seed.8'

C:\>man systemd-random-seed.8

SYSTEMD-RANDOM-SEED.SERVICE(8) systemd-random-seed.service SYSTEMD-RANDOM-SEED.SERVICE(8)

NAME

systemd-random-seed.service, systemd-random-seed - Load and save the system random seed at boot and shutdown

SYNOPSIS

systemd-random-seed.service

/usr/lib/systemd/random-seed

DESCRIPTION

systemd-random-seed.service is a service that loads an on-disk random seed into the kernel entropy pool during boot and saves it at shutdown. See random(4) for details. By default, no entropy is credited when the random seed is written into the kernel entropy pool, but this may be changed with $SYSTEMD_RANDOM_SEED_CREDIT, see below. On disk the random seed is stored in /var/lib/systemd/random-seed.

Note that this service runs relatively late during the early boot phase, i.e. generally after the initial RAM disk (initrd) completed its work, and the /var/ file system has been mounted writable. Many system services require entropy much earlier than this ? this service is hence of limited use for complex system. It is

recommended to use a boot loader that can pass an initial random seed to the kernel to ensure that entropy is available from earliest boot on, for example systemd-boot(7), with its bootctl random-seed functionality.

When loading the random seed from disk its file is immediately updated with a new seed retrieved from the kernel, in order to ensure no two boots operate with the same random seed. This new seed is retrieved synchronously from the kernel, which means the service will not complete start-up until the random pool is fully initialized. On entropy-starved systems this may take a while. This functionality is intended to be used as synchronization point for ordering services that require an initialized entropy pool to function securely (i.e. services that access /dev/urandom without any further precautions).

Care should be taken when creating OS images that are replicated to multiple systems: if the random seed file is included unmodified each system will initialize its entropy pool with the same data, and thus ? if otherwise entropy-starved ? generate the same or at least guessable random seed streams. As a safety precaution crediting entropy is thus disabled by default. It is recommended to remove the random seed from OS images intended for replication on multiple systems, in which case it is safe to enable entropy crediting, see below.

See Random Seeds[1] for further information.

ENVIRONMENT

$SYSTEMD_RANDOM_SEED_CREDIT

By default, systemd-random-seed.service does not credit any entropy when loading the random seed. With this option this behaviour may be changed: it either takes a boolean parameter or the special string "force". Defaults to false, in which case no entropy is credited. If true, entropy is credited if the random seed file and system state pass various superficial concisistency checks. If set to "force" entropy is credited, regardless of these checks, as long as the random seed file exists.

SEE ALSO

systemd(1), random(4), systemd-boot(7), bootctl(4)

NOTES

1. Random Seeds

   https://systemd.io/RANDOM_SEEDS