Contents

[**Entropy** 1](#_Toc503470434)

[ **/dev/random** 1](#_Toc503470435)

[ **/dev/urandom** 1](#_Toc503470436)

[ **To increase entropy** 2](#_Toc503470437)

[Method-1(Preferable) 2](#_Toc503470438)

[Method-2(Not Preferable) 2](#_Toc503470439)

# **Entropy**

* RNG (Random Number Generator)

It is a mechanism to generate pseudo random numbers.

* Pseudo random numbers are used to for generating SSH keys, random PIDs for processes, TCP sequence numbers, UUIDs, GIDs, encryption methods, etc.
* Entropy provided by
* Internal resources: keyboard timings, network traffic, mouse movement, interrupts and IDE timings.
* Processor instruction: RDRAND
* Dedicated external physical devices like TPM (Trusted Platform Module)
* Kernel devices: /dev/random & /dev/urandom

## **/dev/random**

* When requested for random numbers, /dev/random device will only return random bytes within estimated number such that entropy pool doesn’t become empty.
* When entropy pool is empty, reads from /dev/random will block until additional noise is gathered to fill random numbers in entropy pool.

## **/dev/urandom**

* When requested for random numbers, /dev/urandom device will return as many bytes as required. Due to that, entropy pool level is reduced drastically.
* When reads, it doesn’t estimate numbers in entropy pool and even if level of pool is low, it doesn’t block reads.
* The entropy pool is maintained under /var/lib/random-seed
* rngd service is used to generate random numbers.
* Command: yum install rng-tools
* Command: service rngd status
* Command: service rngd start
* To check current value,

Command: cat /proc/sys/kernel/random/entropy\_avail



* **To increase entropy**:

Method-1(Preferable):

* Check current entropy value,

Command: cat /proc/sys/kernel/random/entropy\_avail

* Take backup of /etc/sysctl.conf

Command: cp -p /etc/sysctl.conf /etc/sysctl.conf-$(date '+%Y.%m.%d.%H%M%S')

* Add lines to configuration files.

Command: echo "# Add support for intel rdrand to provide hardware entropy." >> /etc/sysctl.conf

Command: echo "kernel.random.read\_wakeup\_threshold = 2048" >> /etc/sysctl.conf

Command: echo "kernel.random.write\_wakeup\_threshold = 3072" >> /etc/sysctl.conf

* Make changes permanent.

Command: sysctl -p

* Check current value

Command: cat /proc/sys/kernel/random/entropy\_avail

Method-2(Not Preferable):

* To check current value,

Command: cat /proc/sys/kernel/random/entropy\_avail

* Manual way,

Command: watch -n 1 cat /proc/sys/kernel/random/entropy\_avail

* Change RNG device,

Command: rngd -r /dev/urandom -o /dev/random -t 1

-r option: select alternative source; default /dev/random

-o option: device used for random number output;

Default: /dev/random; output to which random numbers are stored

* RNGD:

Check and feed random data from hardware device to kernel random device