

---

# rngd

Vérifie et remplit le pool d'entropie du kernel depuis une source d'entropie

rngd fonctionne sur des blocks de 20000bits à la fois en utilisant les tests FIPS 140-2 pour vérifier le caractère aléatoire des données. Si la donnée est bien aléatoire, le block est envoyée, random-step\*8bits à la fois dans le pool d'entropie du kernel, jusqu'à ce que le pool soit plein.

## OPTIONS

- b, --background** met en tâche de fond
- f, --foreground** Ne fork pas ni ne détache du terminal
- R, --rng-driver=name** Pilote de source d'entropie. 'stream' est un pilote d'entrée de flux Unix généraliste capable de recevoir des données depuis un fichier, un pipe donné, ou un périphérique caractère Unix. 'viapadlock' est un pilote de l'espace utilisateur pour TRNG embarqué sur certains CPU VIA qui ont le moteur de sécurité VIA PadLock
- o, --random-device=file** Périphérique pour la sortie de l'entropie. Défaut : /dev/random
- r, --rng-device=file** Pilote kernel, fifo ou fichier utilisé pour l'entrée d'entropie. Défaut : /dev/hwrng
- hrng=name** Sélectionne un HRNG connu. help liste les HRNG connus.
- H, --rng-entropy=n.n** Entropie par bit de donnée d'entrée. C'est un nombre à virgule flottante entre 0 et 1. Défaut : 1.0
- Q, --rng-quality=quality** Sélectionne la qualité de la donnée aléatoire qu'une source d'entropie génère. 'default', 'low', 'medium' ou 'high'. N'utiliser que high si la donnée aléatoire est obtenue directement.
- B, --rng-buffers=n** Nombre de tampons 20000bits à utiliser. Défaut : 3
- s, --random-step=n** Nombre d'octets écrits dans le périphérique aléatoire à la fois, entre 8 et 2500. Défaut : 64
- W, --fill-watermark=n [%]** Remplis le pool d'entropie jusqu'à atteindre % de données d'entropie dans le pool. Défaut : 50%
- t, --feed-interval=n** non-zéro, rngd force en remplir le pool même si celui-ci est plein
- T, --rng-timeout=n** Temps à attendre les données pour démarrer. 0 attend indéfiniment. Défaut : 10
- p, --pidfile=file** Fichier contenant le pid du processus

rngd dump certaines statistiques dans son canal de sortie chaque heure, et à la réception de SIGUSR1. Ce canal est soit stderr en mode foreground, ou syslog en mode background.

## Codes de sortie

- 0** aucune erreur ne s'est produite
- 1** La source a un problème
- 10** problème de paramètres, ou rngd échoue à bloquer son pidfile, ou le périphérique ne peut être ouvert
- 11** Une erreur d'entrée/sortie s'est produite
- 12** Une erreur de ressource ou de l'os s'est produite