

---

# Magic SysRq key

## Touches Magic SysRq key

Les **magic SysRq key** sont une fonctionnalité du noyau Linux qui permet par une combinaison de touches de lancer des commandes de bas niveau. Elle doit être activée à la compilation du noyau.

La principale utilité de cette fonctionnalité est de pouvoir redémarrer un système bloqué sans corrompre le système de fichier.

Sur un ordinateur x86, la combinaison utilisée est formée des 3 touches : **Alt+Imprim écran** ou **Syst** et une autre touche qui détermine l'action à effectuer : **r** « récupère » le clavier, approprié le plus souvent par le système de fenêtrage X Window.

- k** tue tous les processus de la console virtuelle active
- b** redémarre immédiatement le système. Cette fonctionnalité peut provoquer des pertes de données : ce qui est en mémoire cache n'est pas écrit sur les disques ; cette fonctionnalité est beaucoup plus radicale que le Ctrl-Alt-Delete de Microsoft ou que le Ctrl+Alt+Del de Linux
- c** redémarre le processus kexec et affiche le message du crash
- s** synchronise tous les systèmes de fichier montés Cette fonctionnalité peut être très utile si on doit faire un arrêt rapide de l'ordinateur (arrêt électrique ou logiciel) : elle permet de ne pas perdre les données en mémoire cache
- o** arrête le système
- u** passe tous les systèmes de fichier montés en lecture seule
- p** affiche les registres courants et les flags dans la console
- t** affiche la liste des différentes tâches actives ainsi que des informations pour chacune
- m** affiche les informations relatives à la mémoire dans la console (dans cette situation, le noyau n'est pas en mesure de tenir compte de la disposition des touches sur le clavier, et interprète les frappes comme si elles étaient réalisées sur un clavier QWERTY. Dans le cas de l'utilisation d'un clavier AZERTY, il faut donc appuyer sur ', ' la touche qui se trouve à l'emplacement du m du clavier QWERTY)
- de 0 à 9** permet de définir le type de messages du noyau qui s'affichent dans la console
- f** appelle la fonction oom\_kill, elle tue le processus qui consomme toute la mémoire disponible
- e** envoie le signal SIGTERM à tous les processus excepté init
- i** envoie le signal SIGKILL à tous les processus excepté init
- I** envoie le signal SIGKILL à tous les processus init compris

Toutes autres touches non assignées à une commande affiche une aide sommaire dans la console.

## Modifications

Les différentes méthodes pour modifier cette fonctionnalité sont

- méthode la plus rapide : dans le fichier **sysctl.conf**, interdire ces fonctionnalités en mettant **kernel.sysrq=0**. Dans ce cas, le contenu du fichier **/proc/sys/kernel/sysrq** sera '0'.

- Méthode plus longue, mais plus rigoureuse : Avant de générer un noyau, paramétrer le booléen **CONFIG\_MAGIC\_SYSRQ** à **false** dans les paramètres **kernel hacking**

- Méthode de loin la plus rigoureuse, mais aussi la plus complexe et la plus longue : Il peut être tentant de supprimer les fonctionnalités trop dangereuses, et de laisser celles qui peuvent être utiles dans certains cas extrêmes

---

Pour supprimer les fonctions jugées trop dangereuses : Avant de générer le noyau, il faut modifier un des fichiers **sysrq.c** des sources du noyau. Il y a plusieurs fichiers **sysrq.c**, il faut choisir celui correspondant au type de processeur concerné.

## Redémarrer proprement un système bloqué

**Pour redémarrer un système Linux qui ne répond plus, il faut utiliser la séquence de touches suivante :**

1. **unraw** — récupérer le contrôle du clavier X ;
2. **terminate** — envoyer SIGTERM a tous les processus, pour leur permettre de s'arrêter proprement ;
3. **kill** — envoyer SIGKILL a tous les processus, pour les forcer à s'arrêter immédiatement ;
4. **sync** — synchroniser les disques, écrire le contenu du tampon sur le disque ;
5. **unmount** — remonter tous les systèmes de fichiers en lecture seule, pour ne pas devoir lancer fsck au redémarrage ;
6. **boot**.

Il faut commencer par maintenir simultanément les touches **Alt** et **Syst**, puis l'une après l'autre les touches dans l'ordre donné, en attendant au moins deux secondes entre chaque touche.

Cela permet de démonter correctement les systèmes de fichiers, ce qui évite de risquer des corruptions de données et de devoir exécuter **fsck** au redémarrage. De plus les processus ont du temps pour enregistrer des sauvegardes d'urgence le cas échéant.