



随便xie写 2021.06.07



请问一下作者，在exec的修改中，在用户进程页表重新生成完后，为什么取消进程内核页表之前的映射？我理解的进程内核页表，不是既要有全局内核页表的映射，又要有用户进程页表的映射吗？



随便xie写 回复 解析Ta 2021.06.08



我明白了，博主。你真的太强了!!! 👍



解析Ta 作者 回复 随便xie写 2021.06.08



应该是取消旧进程内核页表中，有关旧进程自己地址空间的映射，保留旧进程内核页表中的内核地址映射

接着添加 `exec()`，该函数的逻辑就是启用了一个新的应用，在新应用上台之前需要完成页表更新工作。所以丢给我们的问题：需要抹掉进程内核页表中对用户态页表的旧映射，然后再将新的用户态页表塞到内核页表中，

Reference

1. <https://blog.csdn.net/u013577996/article/details/109582932>
2. <https://zhuanlan.zhihu.com/p/609350132>