2018

by 张益玮

一

1. x 页表不切换，使用共享的0xc0000000到0xffffffff内和空间
2. v
3. x 可以
4. v
5. x 时钟中断
6. v
7. x 缺页异常
8. x 同一特权级
9. v
10. v

二

1.1 pwd;gcc;qemu

1.2 实;GDT;保护;IDT;门；段

1.3 CR3;4k;4k;4k;CR2

1.4 0;20

1.5 用户;内核;PCB;就绪;等待;运行;就绪挂起;等待挂起

三

3.1 1024;死循环调用fork()被称为fork()炸弹，这会导致进程数以指数级别增加，使有进程数限制的系统无法创建新的进程，而没有进程数限制的系统会死机。会大量占用CPU和内存资源，导致系统进程表饱和。因为fork创建的新进程会不断尝试获取资源，即使关闭一个这样的进程也会马上被同样的进程代替。对于使用了Copy-on-write技术的现代操作系统，由于不立即为子进程分配新的物理空间，内存资源不会被耗尽。

3.2 1. 不需要，因为由用户线程管理库函数来实现，不需要用到内核权限。

2. 不需要，因为线程之间共享地址和文件，线程切换需要保存和恢复的只有PC、栈帧和寄存器和其他的一些PID之类的信息，不需要进入内核态。而进程切换需要访问PCB，所以需要进入内核态。
3. http://www.it.uu.se/education/course/homepage/os/vt18/module-4/implementing-threads/

   可以，一个用户态线程可以通过显式地调用yield()方法或者隐式地访问被占用的锁而放弃运行机会从而让用户态线层管理库选择一个已经就绪的用户态线程继续运行；也可以由内核态接到时钟中断之后将控制权交给用户态线程管理库，从而实现线程的调度与切换。

3.3 2362h:10+100+100=210ns 1565h:10+100+10^7+10+100=10,000,220ns(替换出第0页) 25A5h:10+100=110ns

123565h

3.4 34位物理地址可以寻址16G的内存空间

实际上是伪二级页表，需要通过控制位判断是PDE还是直接就是PTE，注意小端

0x3A69A4D2:VPN[1]=0xE9 VPN[0]=0x29A offset=0x4D2 PDE index=0x900003A4 PDE contents=0x28000001 观察控制位，是valid，并且是PDE 则PTE index=0xA0000A68 PTE contents=0x37AB6C09 观察控制位，是valid，并且类型是execute-only page 物理地址是 0xDEADB4D2

0x3A8EB00C:VPN[1]=0xEA VPN[0]=0xEB offset=0xC PDE index=0x900003A8 PDE contents=0x3EB0000F 观察控制位，是valid，并且类型是Read-write-excute page 物理地址是 0xFACEB00C

（这里需要注意的是，因为在一级页表就找到了对应的物理页，所以VPN[0]=0xEB也需要算入offset当中）