## Lab1\_通过QEMU调试ARM Linux内核

熟悉如何使用QEMU调试Linux内核。

### 实验补充说明：

书上说了用如下命令来运行qemu：

$ qemu-system-arm -nographic -M vexpress-a9 -m 1024M -kernel arch/arm/boot/ zImage -append "rdinit=/linuxrc console=ttyAMA0 loglevel=8" -dtb arch/arm/ boot/dts/vexpress-v2p-ca9.dtb -S -s

这里制定了1024M内存，其实不用这么大，指定100M就够了，特别是有的同学在vmware虚拟机里运行优麒麟Linux系统。

书中说了，使用如下脚本来运行：

$ ./run.sh arm32 debug

这个脚本会启动smp，最好还是不要启动smp来进行内核单步调试，比如直接使用如下命令：

$ qemu-system-arm -nographic -M vexpress-a9 -m 100M -kernel arch/arm/boot/ zImage -append "rdinit=/linuxrc console=ttyAMA0 loglevel=8" -dtb arch/arm/ boot/dts/vexpress-v2p-ca9.dtb -S -s

请关注奔跑吧Linux社区微信公众号，里面有更多更有料更好玩的Linux干货：



奔跑吧Linux社区的旗舰篇视频节目，帮您打通Linux和职场任督二脉！





笨叔最新力作，全程约5小时高清，140多页ppt，8大实验，基于x86\_64的Centos 7.6和arm64，提供全套实验素材和环境。全面介绍kdump+crash在死机黑屏方面的实战应用，全部案例源自线上云服务器和嵌入式产品开发实际案例！

不能为客户和老板解决死机黑屏问题的都不是合格的linux运维或者研发攻城狮！





订阅视频请到淘宝店：<https://shop115683645.taobao.com>

