基于cells技术方案的Android虚拟化实现

1. 启动篇

本篇以启动两个Android系统为例，主系统起来以后，在主系统的基础上启动辅系统。

1. 文件系统的挂载

* 根文件系统的挂载:在主系统的data目录中mount rootfs文件系统，当做辅系统的根文件系统。
* system文件系统的挂载:直接将主系统的system目录mount成辅系统的system文件系统。
* data文件系统的挂载:在主系统中创建一个临时目录，然后把这个临时目录mount成辅系统的data文件系统。
* sdcard 文件系统的挂载:原理同data文件系统
* 根文件系统的所有文件需要主动拷贝，system文件系统则不需要

mount

主系统

/ 根文件系统

system 文件系统

sdcard 文件系统

data 文件系统

data 文件系统

辅系统

/ 根文件系统

sdcard 文件系统

system 文件系统

1. init进程的启动

* 利用clone系统调用启动辅系统的init进程
* clone 系统调用需要一系列namespace 标记来创建属于辅系统的命名空间
* 然后需要给这个init进程分配cgroup资源
* 最后需要调用chroot函数给辅系统分配根目录，这个根目录就是前文提到的辅系统的根文件系统，实际上它是主系统中的一个目录而已

namespace1

clone

namespace21

chroot -> /

execve -> init

cgroup -> init

1. display的虚拟化

* display虚拟化的重点在于，非当前系统也需要实时更新画面，不能简单粗暴的进行阻截，只是这个非当前系统的画面要隐藏起来，不能投射到屏幕中。
* 当非当前系统使用mmap映射显存时需要映射的是内存，将所有像素数据保存在内存中。
* 当发生系统切换时，就可以将内存中的像素数据复制到显存当中.

1. input的虚拟化

* input的虚拟化在驱动中进行的，它的修改逻辑很简直，阻截非当前系统的event事件上报

1. binder的虚拟化

* binder的虚拟化在驱动中进行的，它的修改逻辑很简单，就是把相关数据结构复制一次，各自挂载到各自的namespace中

1. wifi的虚拟化

* 远程调用wpa模块配置wifi芯片参数
* 远程调用dhcp模块配置ip地址
* 利用虚拟网桥veth联通两个namespace的network

veth

dhcpd

dhcpd\_proxy

wpa\_supplicant\_proxy

wpa\_supplicant

namespace21

namespace11