Zygote进程原理

--辅助理解zygote机制和内核设计

1.什么是zygote或者Zygote的主要作用是什么？

zygote是整个系统创建新进程的核心进程。zygote进程在内部会先启动Dalvik虚拟机，继而加载一些必要的系统资源和系统类，最后进入一种监听状态。

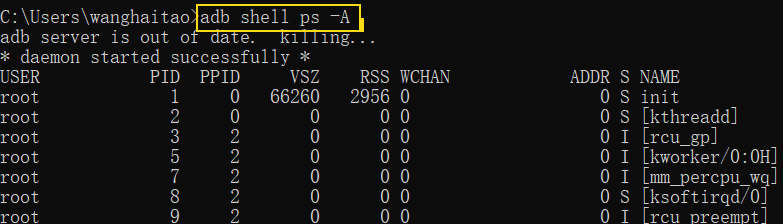
2.为什么会有zygote？

开进程是会占用大量的内存空间，安卓把开进程的这个操作进行统一管理。

3.zygote进程是谁来启动的？

是由init进程开启的。

查看所有进程：adb shell ps -A



各列参数的意思：

USER:进程当前用户；

PID(Process Id):当前进程id;

PPID(Process Parent ID):父进程ID;

VSIZE(Virtual Size):当前进程虚拟内存的大小；

RSS(Resident Set Size):实际驻留在内存中的没存大小；

WCHAN:休眠进程在内核中的地址；

PC(program counter):计算机中提供要从[存储器]中取出的下一个指令地址的[寄存器];

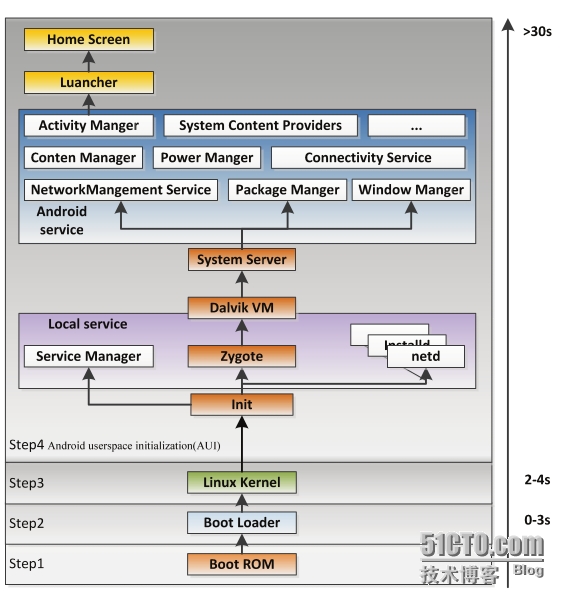
NAME:进程状态值及名称；(这个状态不知道根据什么区分的，试了下没有参考价值)

从下图可以看得出zygote进程是由一个PID=1的进程启动，这个就是init进程。



1. init进程又是什么？

init对应的代码位于：system/core/init/init.c中。



第一阶段：Android设备上电后，首先会从处理器片上ROM的启动引导代码开始执行，片上ROM会寻找Bootloader代码，并加载到内存。（这一步由“芯片厂商”负责设计和实现）

第二阶段：Bootloader开始执行，首先负责完成硬件的初始化，然后找到Linux内核代码，并加载到内存。（这一步由“设备厂商”负责设计和实现）

第三阶段：Linux内核开始启动，初始化各种软硬件环境，加载驱动程序，挂载根文件系统，并执行init程序，由此开启Android的世界。（这一步则是Android内核开发过程中需要涉及的地方）

Android系统以及各大Linux的发行版，他们的Linux内核部分启动过程都是差不多的，他们之间最大的区别就在于init程序的不同，因为init程序决定了系统在启动过程中，究竟会启动哪些守护进程和服务，以及呈现出怎样的一个用户UI界面。

因此，init程序是分析Android启动过程中最核心的程序。

init程序最核心的工作主要有3点：

（1） 创建和挂载一些系统目录/设备节点，设置权限，如：/dev, /proc, and /sys。

（2） 解析 init.rc 和 init.<hardware>.rc，并启动属性服务，以及一系列的服务和进程。

（3） 显示boot logo，默认是“Android”字样。

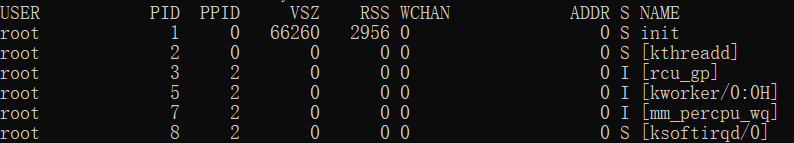
其中第2步包含两部分服务：1.本地服务，2.Android服务

（1）本地服务

本地服务是指运行在C++层的系统守护进程，一部分本地服务是init进程直接启动的，它们定义在init.rc脚本和init.<hardware>.rc中，如 ueventd、servicemanager、debuggerd、rild、mediaserver等。还有一部分本地服务，是由这些本地服务进一步创建的，如mediaserver服务会启动AudioFlinger, MediaPlayerService， 以及 CameraService 等本地服务。

我们可以通过查看init.rc和init.<hardware>.rc文件找出具体有哪些本地服务被init进程直接启动了，这些文件的位置：system/core/rootdir/

注意，每一个由init直接启动的本地服务都是一个独立的Linux进程，在系统启动以后，我们通过adb shell命令进入手机后，输入top命令就可以查看到这些本地进程的存在：



1. Android服务

Android服务是指运行在Dalvik虚拟机进程中的服务，这些服务的创建过程描述如下：

init进程会执行app\_process程序，创建Zygote进程，它是Android系统最重要的进程，所有后续的Android应用程序都是由它fork出来的。

Zygote进程会首先fork出"SystemServer"进程，"SystemServer"进程的全部任务就是将所有的Android核心服务启动起来，这些服务包括：



当所有的服务都启动完毕后，SystemServer会打印出“Making services ready”，然后通过ActivityManager启动Home界面，并发送“ACTION\_BOOT\_COMPLETED”广播消息。

注意，这些Android服务并没有各种运行在独立的进程中，它们由SystemServer以线程的方式创建，所以都运行在同一个进程中，即SystemServer进程中。



1. zygote开进程的流程是什么？