内核版本：linux-5.8

作者：彭东林

邮箱：[pengdonglin137@163.com](mailto:pengdonglin137@163.com)

在支持VHE的情况下，HOST的内核和应用程序分别运行在EL2和EL0，而GUEST的内核和应用程序则运行在EL1和EL0.

在不支持VHE的情况下，GUEST的内核和应用都运行在EL0，HOST的内核和应用分别运行在EL1和EL0，HOST的内核有一部分运行在EL2.

下面分析的是不支持VHE的情况。

要支持虚拟化，bootloader在跳转到linux kernel时，需要处于EL2.

在arch\arm64\kernel\head.S：

\_head -> primary\_entry -> el2\_setup:

1. 配置在EL2下数据和页表访问的大小端，当前设置为小端（如果没有定义CONFIG\_CPU\_BIG\_ENDIAN的话）
2. 配置HCR\_EL2: EL1运行在Aarch64
3. 配置cnthctl\_el2：允许EL0和EL1访问物理timer和物理counter
4. 将cntvoff\_el2清零，使物理counter和虚拟counter的读数相同，不存在时间差
5. 如果支持以系统寄存器（SRE）的方式访问GICv3和GICv4的cpu interface的话，需要使能EL2\_SRE
6. 设置ID寄存器：将vpidr\_el2和vmpidr\_el2设置为同midr\_el1和mpidr\_el1一样的值
7. 将vttbr\_el2清零，这个寄存器存放的使stage2页表基地址
8. 设置sctrl\_el1，设置EL0和EL1的数据和页表访问时的大小端