Virtual Machine Monitor，VMM，也称 Hypervisor

Type 1 虚拟机管理程序

Type 1 虚拟机管理程序直接在主机的物理硬件上运行，它被称为裸机虚拟机管理程序;它不必预先加载底层操作系统。通过直接访问底层硬件而无需其他软件(例如操作系统和设备驱动程序)，Type1 虚拟机管理程序被视为用于企业计算的***效、性能***的虚拟机管理程序。Type 1 虚拟机管理程序的示例包括 VMware ESXi、Microsoft Hyper-V 服务器和开源KVM等。

同时，管理程序直接在物理硬件上运行也非常安全，因为裸机虚拟机管理程序可避免操作系统通常存在的安全问题和漏洞。这可确保每个访客 VM 与恶意软件和活动保持逻辑隔离。

在很多情况下，虚拟化系统至少托管一个带有操作系统和管理软件的虚拟机，使管理员能够使用系统管理工具(例如 Microsoft System Center)管理物理系统。

Type2虚拟机管理程序

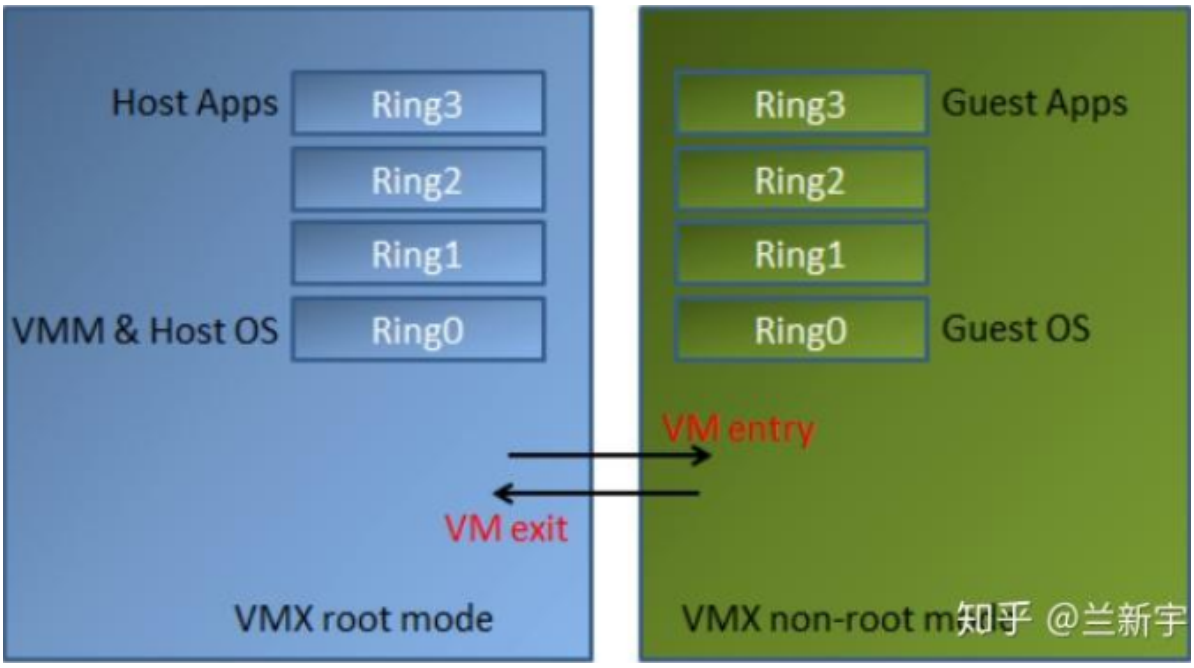
Type2 虚拟机管理程序通常安装在现有操作系统之上，它称为托管虚拟机管理程序，因为它依赖于主机预先安装的操作系统来管理对CPU、内存、存储和网络资源的调用。Type2 虚拟机管理程序包括 VMware Fusion、Oracle VM VirtualBox、适用于 x86 的 Oracle VM Server、Oracle Solaris Zones、Parallels 和 VMware Workstation。

可虚拟化架构

下陷（trap）：指 CPU 特权级从低特权级（如 EL0）切换到高特权级 （如 EL1）

特权指令（prilileged instruction）：指在用户态执行时会触发下陷的指令。（如软中断，和不允许在用户态执行的指令等）
敏感指令（sensitive instruction）：指管理系统物理资源或更换 CPU 状态的指令。（如 I/O 等）
可虚拟化架构：所有敏感指令都是特权指令。（如果有些敏感指令在用户态执行不会触发下陷，那这些指令就不会被虚拟机监控器捕捉到）

硬件虚拟化技术



VMExit

从 guest VM 进入 VMM；non-root mode to root mode

VMEntry

从 VMM 进入 guest VM；root mode to non-root mode

VMCS（Virtual Machine Control data Structures）

负责保存 vCPU 需要的相关状态和上下文信息