KVM 虚拟化技术及其安全策略研究

李诚鑫 罗亚丽

四川大学锦城学院 计算机与软件学院 四川 成都 611731

【摘 要】:在网络科学技术发展的时代，云计算成为了最热门的词汇之一。构建云基础架构的技术中，有一种技术称为虚拟化。在云计算的背景下，虚拟化技术的形式种类也随着它的扩展而增添不少。而 KVM 就是庞大的虚拟化技术家族成员之一，随着 x86 硬件对虚拟化技术的支持越来越成熟，KVM 虚拟化技术也有了很大的提高。本文将围绕 KVM 虚拟化展开研究，首先分析为何选择 KVM 而放弃 XEN，再了解 KVM 的优势及其安全威胁，并作出安全策略，最后分析 KVM 的发展情况和未来趋势。

【关键词】：KVM 虚拟化技术；KVM 安全性；KVM 发展趋势

1 引言

由于互联网科技的进步，使得人们日常生活和工作有了非常大的变化。云计算和虚拟化就在此环境下产生的，虚拟化作为云计算核心组成的成员，具备了可以提高 IT 资源利用率以及实现资源的动态分配，跨域共享，灵活调度等优势。对于多样化用户的需求，虚拟化也可以满足。在 IT 行业中，虚拟化技术早已产生了深刻的影响。KVM 就是虚拟化技术其中之一。在互联网行业中，由于 Linux 服务器的广泛应用，促使 Linux 内核原生的虚拟化技术——KVM，也受到了许多企业的关注和使用以及用户的青睐。

2 KVM 虚拟化

2.1KVM 虚拟化技术的概述

KVM 英文全称是 Kernel-based Virtual Machine，而中文全称是基于内核的虚拟机，它是一个可通过 Linux 自身的调度器进行管理的 Linux 内核模块，KVM 以高性能、高安全性、扩展性、低成本来面向用户。

KVM 本身不执行任何模拟，它需要一个客户机虚拟服务器的地址空间，地址空间是用户空间程序通过/dev/kvm 接口设置而成，提供模拟的 I/O 给 KVM，并将其视频显示映射回宿主的显示屏，这个应用程序就是 QEMU，QEMU 是一套以 GPL 许可证分发源码的模拟处理器程序[1]。图 1 是 KVM 的基本结构：

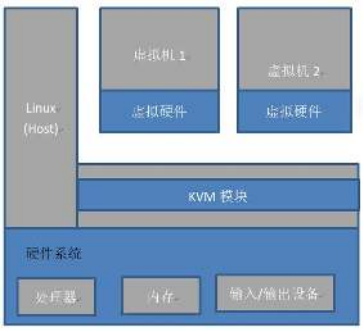

图 1：KVM 的基本结构

2.2 为何淘汰 XEN 而选择 KVM

XEN 是一个软件层，可以直接在计算机硬件之上运行，从而代替操作系统，也可以同时运行多个客户端操作系统。在 2006 年，Qumranet 公司对外宣布 KVM 的诞生，Linux 正式接纳 KVM 模块的源代码，使之成为内核源代码的一部分，Linux 内核最新开发成果可以被 KVM 直接获取。而 XEN 对于其他 Linux 功能的适应性非常差，最大的缺点是 XEN 被 Linux 内核社区抵制，与 XEN 相关的内核更改无法被内核源代码所接纳，并且无法支持内核的最新开发结果[2]。从而引起了开发人员的抵触，Linux 厂商也慢慢从 XEN 的领域撤退。比如红帽公司将 XEN 运用到之前的 RHEL5 版本中，却在新推出的 RHEL 6 版本中，将所有 XEN 相关组件移除，从而采用了 KVM 来替代，并且还提供了方便 XEN 到 KVM 虚拟机的迁移工具。

2.3 KVM 虚拟化的优势和弱势

KVM 也是一个具有优势的虚拟化产品。优势在于：①KVM 是可提供虚拟化处理方案的免费开源软件。②更好的进程调度支持③更广泛的物理硬件平台的驱动④更高的代码质量⑤KVM 还可用于改进虚拟网络的支持，增强安全性等方面。

但是 KVM 虚拟化也有不足之处，它具有安全威胁，主要安全威胁有：①流量在虚拟机之间不可控。每台物理机上都承载着多台虚拟机，而虚拟机之间可以通过 KVM 虚拟化平台提供的 vSwitch 来进行通信，同一个 vSwitch 的虚拟机是可以通信的，但虚拟机不属于同一用户则可能造成数据泄露等问题。②虚拟机之间会发生共享资源竞争与冲突。当同一物理机资源被多个虚拟机共享时，会产生资源竞争。若无法将单一虚拟机的可用资源正确配置或限制，则可能会造成某些虚拟机对资源的恶意使用，同时其余的虚拟机不接受服务。另外，如果同一物理机上的虚拟机同时进行病毒扫描等大量消

耗物理资源的动作，当物理机资源枯竭时就会发生瘫痪，虚拟机的业务也会中断[3]。③云平台对虚拟机的控制。如果云平台组件遭到病毒的入侵或者恶意篡改，可能会导致用户的数据泄露，虚拟机资源被非法用户占用，云服务的运营将会受到影响。④云数据安全存在风险问题。当大量用户数据集中存储时，容易吸引黑客大规模攻击。⑤云计算管理权限问题。倘若用户失去了对于物理机的控制，然而管理员拥有了更高的权限，则可能因为管理员的操作停止用户服务或造成数据遗失。

2.4 KVM 增加安全性的措施：

①给镜像文件加密。数据的完整性和一致性在信息安全中变得越来越重要，对数据进行加密处理是对其一致性和完整性较好的保障方式。有一种类型的攻击叫“离线攻击”。在系统关机状态下，如果攻击者可以物理接触到磁盘或者其他存储介质，这种表现形式就属于“离线攻击”。此外，在企业内部，不同岗位的人有不同的职责和权限。系统处于启动状态时，使用者是 A，而系统关机后，会存放在可以获得该系统物理硬件的其他位置 B。如果没有保护措施，那么 B 会很容易地越权获得系统中的内容。如果有良好的加密保护，就可以防护这样的攻击或者内部数据泄露事件的发生。在 KVM 虚拟化环境中，存放虚拟机镜像的存储设备（如磁盘、U 盘等）可以对整个设备进行加密，如果其分区是 LVM，也可以对某个分区进行加密。而虚拟机镜像文件本身，也可以进行加密处理。当“-o encryption”参数支持 qemu-img convert 命令时，可以将未加密处理或者已经加密的镜像文件转化为加密的 qcow2 的文件格式[4]。

②虚拟网络的安全性。在 KVM 宿主机中，为了网络安全，可以使用 iptables 工具，利用 IPv4 协议或者 IPv6 协议可以创建、维护和检查 Linux 内核中 IP 数据报的过滤规则。

③远程管理安全性。如果想要远程访问虚拟机的话可通过 VNC 的方式，考虑到虚拟化管理的安全性，可为 VNC 连接设置密码，同时管理虚拟机可使用 Libvirt，利用‘virsh’和‘virt-manager’等工具。不过安全连接至 Libvirt 有两种简便方法——SSH 通道连接以及简单鉴权和安全层（SASL）。

④普通 Linux 系统的安全准则。KVM 宿主机以及在 KVM 上运行的 Linux 客户端都是普通的 Linux 操作系统。一些常见的 Linux 系统安全策略和准则可用于提高 KVM 环境的安全性。（1）尽可能将传送的数据进行加密。在网络上传输的数据很容易被监听，所以应该使用加密方式对数据进行处理。（2）尽量少安装软件，避免软件漏洞数量增加。（3）尽可能在不同的系统上运行不同的网络服务。当一个服务器只关注一个网络服务时，攻击者即使成功侵入一个网络服务上的软件漏洞并不会影响其他服务的运行。（4）配置一些安全工具去提高系统的鲁棒性。（5）使用尽可能少的权限。只授予最少的必需权限给用户账号和运行软件。

3 Openstack 与 KVM

3.1Openstack 与 KVM 相互辉映

KVM 虚拟化技术被 Openstack 用户大量使用。作为通用的开放虚拟化技术 KVM，可以支持 Openstack 的所有特性。之前，基于 KVM 开发的 Openstack，让 KVM 常常成为默认的虚拟机管理程序，Openstack 与 KVM 都使用相同的开源理念与开发方法。Openstack，拥有强大的行业发展动力，同时还有活力旺盛的社区的云计算平台，KVM 驱动的 Openstack 平台已占据 95%。KVM 会随着 Openstack 的增长而增长。

3.2 企业运用 Opensatck+KVM 的优势

在 2007 年，Linux2.6.20 发布开始，KVM 被并入 Linux 内核，Openstack 完全支持 KVM。在操作系统原生支持或者虚拟操作系统镜像添加 hypervisor 特定驱动进行支持的情况下，KVM 可以提供半虚拟化。并且很多厂商提供 Openstack 和 KVM 的商业支持。

企业可使用 KVM 作为虚拟化软件，利用 KVM 的特点和优势，比如（1）KVM 和 Linux 内核高度集成，可轻易掌握虚拟化进程；（2）KVM 的灵活性，在任何情况下 KVM 都能直接与底层的硬件进行交互，不需要修改虚拟机系统。再结合 Openstack 部署，便可以降低云平台部署的难度。

4 KVM 的发展

4.1KVM 市场现在发展前景

IT 行业的不断发展，促使 KVM 设备被广泛应用，需求量因此增加，国内 KVM 厂商也因技术水平和生产工艺的发展逐渐站稳脚跟。比如 KVM 切换器，被应用到金融、教育、电力等行业中，KVM 切换器已成为智能型控制设备，不再只具有硬件切换功能。由于它提供的便利性，促使它成为管理机房的重要设备。

国内 KVM 产品利用它的特点和优势，以及它合理的价格在市场上占据了越来越高的份额。如果利用一套 KVM 控制台来管理全部设备，会大大提高系统和网络维护人员的工作效率。就比如，在金融行业，由于业务的不断扩展，数据中心的规模也因此增大，促使服务器、键盘、显示器等数量飞速增加，设备增加的同时，所链接线缆也增加使用，这样不仅会增加数据中心的成本，也会占用大量的空间。但应用 KVM 虚拟化技术来处理，数据中心的远程管理不仅可以被很好的

实现，而且数据中心的成本也可以减少。这时，就算是千里之外的系统也会被坐在控制台前的技术人员管理和控制，因此 KVM 受到了越来越多技术人员的喜爱。

4.2KVM 虚拟化技术的未来发展

KVM 作为快速增长的 Linux 虚拟化技术受到了很多制造商的支持。Ubuntu 服务器操作系统作为 Canonical 公司第一个主要的 Linux 发行版，它能提供功能齐全的 KVM 虚拟化堆栈。开放虚拟化联盟（OVA）也在保护 KVM，促进基于内核的虚拟机等开放虚拟化技术的应用，鼓励互操作性，为企业提供更多的虚拟化选择、更高性能和更有魅力的价格。而 KVM 会逐渐成为用户所选择的主流虚拟化产品之一。

结语：

在云计算迅速发展的今天，KVM 作为虚拟化技术家族成员之一，被企业开始关注，并利用其最大的优势来推动平台的搭建、工作的进程等，以此来促进企业的发展和社会的经济发展。但是对于 KVM 虚拟化技术而言，还需要不断地完善和更新，使之成为一种更为稳定地新技术运用于工作和生活之中，以达到最好的效果。未来的虚拟化技术值得我们所有人去关注和期待，KVM 虚拟化技术还在不断创新。

参考文献：

[1] 王培鳞.云计算虚拟化技术与应用，人民邮电出版社 2017.12:86

[2] 任永杰.单海涛.KVM 虚拟化技术：实战与原理解析，机械工业出版社 2013.10：13

[3] 张炜.聂萌瑶.熊晶.云计算虚拟化技术与开发，中国铁道出版社，2018.5:157

[4] 张炜.聂萌瑶.熊晶.云计算虚拟化技术与开发，中国铁道出版社，2018.5:160