期中作业

这项家庭作业占你最终分数的10%。

截止日期：2022.4.26 18:00

这个作业要提交的文件是。

1.报告.pdf

虚拟化是支撑当今许多IT基础架构的核心技术，包括云计算和数据中心。它利用一个被称为虚拟机监控器（VMM或hypervisor）的软件组件，加上一些硬件支持，在计算机硬件上创建一个抽象层，使一台计算机的硬件资源，包括处理器、内存、存储等，可以被多个虚拟机（VM）复用。虚拟机运行自己的操作系统（OS），并像独立的计算机一样运行，尽管它们只使用底层计算机硬件的一部分。虚拟化使物理计算机硬件得到更有效的利用，并使共享资源上的计算得到安全隔离。

在这个作业中，你将通过阅读一些参考资料并将其与你在课堂上所学的知识联系起来，来了解x86（IA-32）和x86-64的虚拟化技术是如何设计和实现的。(RISC-V以后会有对虚拟化的标准支持，敬请期待）。我们为你提供了与Xen虚拟化技术有关的文件，这是一个主导亚马逊AWS云的开源虚拟机实现，以及英特尔用于支持硬件辅助的虚拟化的CPU扩展。你可以参考这些文件，但要随心所欲地超越它们。

为了帮助你组织你的想法，请你回答以下问题。

注意：用自己的话回答问题，避免抄袭!!!如果从参考资料中抄袭了一个连续7个字以上的短语，则该题不得分!!!

1. **虚拟化的术语（20分）**

   (1) 用100个字描述虚拟化？(2分)

   (2) 请解释虚拟化的三种使用模式：工作负载隔离、工作负载整合、工作负载迁移。(6分)

   (3) 列出3个著名的VMMs。(2分)

   (4) 解释以下术语：准虚拟化、完全虚拟化、二进制转换、硬件辅助的虚拟化、混合虚拟化。(10分)

2. **特权等级（25分）**

(1) x86（IA-32）提供多少个权限级别？它们是如何被操作系统和用户进程使用的（考虑到一个没有虚拟化的普通操作系统）？请提供三个例子说明权限分离的重要性。(5分)

(2) 什么是环形压缩？(3分)

(3) 如果没有英特尔VT-x，Xen如何解决X86（IA-32）的环形压缩？(3分)

(4) 如果没有英特尔VT-x，Xen如何解决x86-64的环形压缩？(3分)

(5) 什么是环形混叠？(3分)

(6) 什么是VT-x中的VMX根和VMX非根？(4分)

(7) 英特尔VT-x是如何解决环形混叠和环形压缩的挑战的？(4分)

3. **系统调用、中断和异常（28分）**

(1) 在没有虚拟化的普通操作系统中，系统调用的目的是什么？系统调用和函数调用之间的主要区别是什么？在x86-64 Linux上，系统调用的参数是如何传递给内核的？(5分)

(2) 什么是Xen中的hypercall？(2分)

(3) Xen是如何在x86（IA-32）上虚拟化异常的？Xen对原有的x86异常处理程序做了哪些修改？(4分)

(4) 在x86（IA-32）上虚拟化中断（特别是关于中断屏蔽）的挑战是什么？(3分)

(5) Xen是如何在x86（IA-32）上虚拟化中断的？这种设计的好处是什么？(4分)

(6) 什么是英特尔VT-x中的VMCS？什么是虚拟机退出和虚拟机进入？在虚拟机退出和虚拟机进入时如何使用VMCS（4分）

(7) Xen是如何利用Intel VT-x来虚拟化中断的？(3分)

(8) 英特尔VT-x是如何支持异常虚拟化的？(3分)

4. **地址翻译 (27 分)**

(1) 解释x86（IA-32）地址转换。(3分)

(2) 解释x86-64地址转换（2分）

(3) 解释客户虚拟内存、客户物理内存和机器内存之间的关系。(3分)

(4) Xen如何管理虚拟机中的每进程页表和VMM中的每操作系统页表？(4分)

(5) "地址空间压缩 "是什么意思？(3分)

(6) Xen是如何解决 "地址空间压缩 "的问题的？(4分)

(7) 什么是英特尔EPT？如何用英特尔EPT进行MMU虚拟化？(5分)

(8) Xen是如何为每个域分配物理内存的？(3分)

参考文献

[1] Xen和虚拟化的艺术

[2] Xen 3.0和虚拟化的艺术

[3] 利用英特尔虚拟化技术扩展Xen

[4] 英特尔虚拟化技术

[5] https://sys.readthedocs.io/en/latest/doc/05_calling_system_calls.html

[6] https://pages.cs.wisc.edu/~remzi/OSTEP/vmm-intro.pdf

[7] 混合虚拟化--Linux的增强型虚拟化

[8] Xen* Hypervisor案例研究--设计嵌入式虚拟化英特尔架构平台

[9] 用于x86虚拟化的软件和硬件技术的比较