Mid-term Homework

Terminologies of virtualization (20pts)

(1) Define virtualization in 100 words? (2 pts)

Virtualization, in fact, is a kind of technology which based on software. It aims at virtual something like stoage, networking or applications. The key which let virtualiztion reliable is hypervisor which is a software runs between pysical machine and virtual machine. The thing which hypervisor do is that they fetch the resource from the pysical machine sand give it to the virtual machine. The hypervisor is very common lkie VMware. In conclusion, virtualization s a tech to create virtual software (whatever OS or other) in host and managed by hypervisors.

(2) Please explain the three usage models of virtualization: workload isolation, workload consolidation, workload migration. (6 pts)

wokload isolation

workload isolation is used to enhance the security of the system since the stack in different virtul machines are isolated. As a result, when one virtual machine were hacked, it won't affect others. It can also improve the reliable since if one crashed, it will also not affect others.

worklod consolidation

workload consolidation solve the problem that with this tech, the compputation resources or other things are consolidated into one or fewer machine to run which can lower the maintenance costs, decreased complexity and esay in scaling when the amount of virtual machine growth.

workload migration

it can be used when virtual machine crashed. using workload migration, the data fof other things can be migrate to a brand new platform. That is becuase the virtual machine can be decouple with the handware.

(3) List 3 well-known VMMs. (2 pts)

the Red Hat **Virtual Machine Manager**

VMware workstation

Parellels Desktop in MAC

(4) Explain the following terms: paravirtualization, full virtualization, binary translation, hardware-assisted virtualization, hybrid virtualization. (10 pts)

paravirtualization

paravirtualization is like half virtualization. Compared to full virtualization, it is more energy-saving and coan improve the consolidation of server since Vms are controlled by some kind of adminstaor os. Therefore, it is less protable adn it may bring some risk since the VMs are not full isolated.

full virtualization

Full virtualization is most commonly as we think. VMS runs seperately adn for every VM, they has its own operating system and configuration like run enviroment. As a result, VMs are isolated and portable.

binary translation

Binary translationis to translate the binary code of the insturction set from orgianal set to target set. It is uesd in virtulization to solve the problem that the original insturstion can't run in VMs.

hardware-assisted virtualization

Haedware-assisted virtualization solve the prolem about the performance. Normally, operating system running in the VM needs to use the hypervisor to access some resource like network card. However, with hardware-assisted. Like mordern cpu, they can suppoert to virtualizaed as muliple cpu for virtulization so they can call the hardware directly to better the performance. I

hybrid virtualization

Hybrad-virtualiaztion combine the advantage of full and para virtualization. It inserts a kernel-level driver into the host operating system kernel. This driver is like a manager to coordinate hardware access between the VMS and the host operating system. So it ensure the isolation and portable and use the technology compatibiable.

Privilege levels (25 pts)

(1) How many privilege levels does x86 (IA-32) provide? How are they used by OS and user processes (considering an ordinary OS without virtualization)? Please provide three examples of the importance of privilege separation. (5 pts)

1. 4
2. The mode 0 for kernel/os use. The mode 3 for application/user processes use
3. Firstly, it will improve the security of the system since when a little application can access whatever the thing in computer it is quiet dangerous since the application can blackmail the user. With privilage separation, the application can only have the smalllest privilege Secondly, the privilege separation can also abstract the development of a software since the application do not need do implement the system by themselves. At last, the privilege separation can make the management of a team more

resoanable since the team memeber can only access the thing that they allow to. With privilege mode when a memeber wants to something like remove the syustem file the privilege separation will prevetn him/her.

(2) What is ring compression? (3 pts)

The ring compression is a problem that since the VMM guest can only run in IA-32 paging do not seperate the ring for 0 to 2 so the guest os can only run in the in the level three just like the application.

(3) Without Intel VT-x, how does Xen address ring compression for X86 (IA-32)? (3 pts)

(4) Without Intel VT-x, how does Xen address ring compression for x86-64? (3 pts)

(5) What is ring aliasing? (3 pts)

The ring alasing is that the os will read some secify regiseters to know that the current ring is 0 and os may change its behavior wihch aginst the transparentcy of the os.

(6) What are VMX root and VMX non-root in VT-x? (4 pts)

At first the VMX is defined as the support of the IA-32 processor. The processor or cpu support the virtualzation by the VMX. There are two mode of VMX called VMX root and VMX non-root. The VMM run in VMM root and the guest application runs on non-root. They can both support two operation. There are two translation of VMX. The first one called VM entry is to enter the the root. Contrarily. The VM exit will eixt from the VMX root.

(7) How does Intel VT-x address the challenges of ring aliasing and ring compression? (4 pts)

Ring compression and ring aliasing are solved by creating a new mode of execution with full access to all four privilege rings. In ring 0, a guest OS runs while the VMM is fully protected against any incorrect behavior.

System calls, interrupts and exceptions (28 pts)

(1) In the context of ordinary OS without virtualization, what are the purpose of system calls? What is the main difference between system calls and function calls? On x86-64 Linux, how are system call parameters passed to the kernel? (5 pts)

1. The system calls are provided to user programs via the Application Program Interface which betwwen a process and os to allow application to use the services of os.
2. A system call is aask for to the kernel to access a resource, whereas a function call is a request from a program to finish a certain kind of job..
3. The system call is passed by the register. In Linux. it will be invoked by call with intrrupt $0x80 and store to the rigister EAX and run in kernel mode.

(2) What is a hypercall in Xen? (2 pts)

In the same way that a syscall links an application to the kernel, a hypercall connects a domain to the hypervisor some kind of like system call. Domains will make use of hypercalls to request privileged tasks like pagetable modifications.

(3) How does Xen virtualize exceptions on x86 (IA-32)? What modifications does Xen make to the original x86 exception handlers? (4 pts)

1. Since Xen the exceution is that the vm entry will load the from the VMCS in geust state. As a result, the Xen can inject some kind of exception to entry to produce the exception.
2. When an exception occurs outside of ring 0, the Xen handler copies the exception stack frame to the guest OS stack and passes control to the appropriate registered handler.

(4) What are the challenges of virtualizing interrupts (especially regarding interrupt masking) on x86 (IA-32)? (3 pts)

The challenges is that the vmm may probobaly refuse to let the geust software to manager the interrupt manage. So in this case, it will make some problem that it will have a bad contribution to the performance of the system since that always iintercepting the geuset.

(5) How does Xen virtualize interrupts on x86 (IA-32)? What is the benefit of such a design? (4 pts)

1. There is a small event delivery mechanism which is to send some notification to the Domain wihc is also asynchronous. The notification is done by the updating the bitmap of a event type.
2. The benefit is that the the notification is asynchronous so the system won't be frequently wake up by it.

(6) What is VMCS in Intel VT-x? What are VM exits and VM entry? How are VMCS used during VM exits and VM entry (4 pts)

1. It is a data structure which has very access and load spped to hodl the reister state of guest and host cpu.
2. The translation form root to not-root mode in VMX is called VM entry. The reverse tranlation is called VM exits.
3. VMCS can control wheter the geust operation will lead to the Vm exits and during the Vm exit, the VMCS will record the detail infromation of the exit reason

(7) How does Xen leverage Intel VT-x to virtualize interrupts? (3 pts)

Xen handle it by introduce a Dom0 instead of hypervisor. Therefor, teh HVM geust will not handle the HVm. The Xen will injects interrupt which is virtual and external to guest in the VM entry.

(8) How does Intel VT-x support exception virtualization? (3 pts)

there is a bit map that allow VMM to choose whter exception should let the VM to exit or not

Address translation (27 pts)

(1) Explain x86 (IA-32) address translation. (3 pts)

X86 has 32-bit address space and a page size of 4 KB. Therefore, 32-bit address is divided into two parts: a 20-bit VPN and a 12-bit offset. The role of the operating system and TLB will convert the VPN into PFN, thus generating a full physical address that can be sent to physical memory to get the correct data.

(2) Explain x86-64 address translation (2 pts)

since the entire 64-bit address is similar to 32 bit but since teh 64 bit is too long, so the first 12-bit are preserved and it suppose 4GB page size.

(3) Explain the relationship between guest virtual memory, guest physical memory, and machine memory. (3 pts)

The guest operating system presents programs with a continuous virtual address space called guest virtual memory.

The memory that is visible to the guest operating system executing in the virtual machine is referred to as guest physical memory.

machine memory is the treu memory of the machine.

so the GPM is in GVM and they are all in MM which need a map to translate.

(4) How does Xen manage the per-process page table in the VM and the per-OS page table in the VMM? (4 pts)

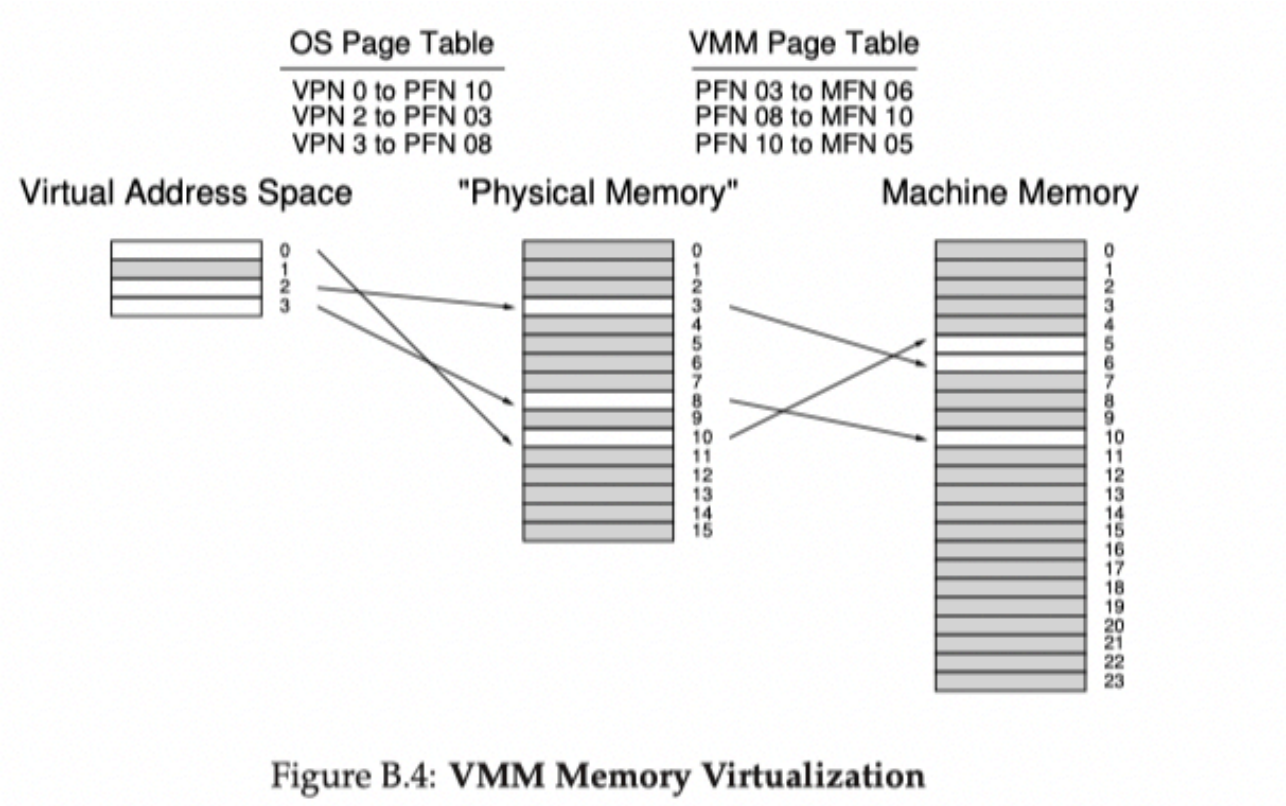

Figure B.4: **VMM Memory Virtualization**

in this graph, the VMM map the "Physical Memory" which is an illusion made by VM and the VMM will use the VMM Page Table to map again to real machine memory.

For every os, there are numbers of processes run on it so the process in the os will have a page table for every os

(5) What does “Address-space compression” mean? (3 pts)

The address space compression means that the although the geust run in its own address space, the problem comes that some struture like IDT or GDT still require control stuture and after that, the guest may know it is in VM and they can change this things to modify outside the VM.

(6) How does Xen address the problem of “Address-space compression”? (4 pts)

every transilation will change the linear address space so that VM can not know the true space.

(7) What is Intel EPT? How to do MMU virtualization with Intel EPT? (5 pts)

EPT is Extended Page Tables which is a virtualization technology to support the MMU. it allows each virtual machine to handle its own page table without granting access to the MMU .

(8) How does Xen allocate physical memory to each domain? (3 pts)

Xen will keep track of who owns and uses each page. Each domain has a physical memory allocation matin the max and current memeory. Besides, a 'balloon driver' can be used by a guest OS whihc is to change the memeory to its limits.