CMPE283 – Virtualization
Final Exam

Name: **Sunil Tiwari (011825476)**

Select or provide the best answer for each question.

1. (15 points) When optimizing hypervisor performance, it has been stated that optimizing to reduce the total number of exits provides the largest amount of performance improvement, as compared with other optimization techniques. Why is this the case?

Answer:

Already Answered

2. (5 points) ___FALSE__ True or False? A hypervisor author can configure the exception exiting VMX control to exit on any exception of his/her choosing.
(You cannot disable CPUID)

3. (5 points) ______A______ If #PF (page fault) exception exiting is enabled in a VMCS currently loaded on a PCPU, what is the processor behaviour when executing guest VM code with that VMCS when a #PF occurs in that guest VM?

A. The #PF is delivered to the VMM via a #PF exception exit
B. The #PF is delivered to the VM and handled by the guest OS
C. It depends on the privilege level of the faulting instruction
D. It depends on the setting of the #VE exception exiting control

4. (10 points) If a hypervisor author wishes to remove the ability of a guest VM to utilize the RDRAND instruction, what steps must he/she take in the hypervisor code?

Answer:
-mask the feature in cpuid
-turn on rdrand exiting control and handle it in hypervisor

For questions 5-9, consider the following configuration during the processing of the guest instruction shown below. The following assumptions should be made:

- **All pages relevant to the instruction are present and paged-in, and have not been accessed previously. The paging environment is properly configured (eg, valid CR3, and valid EPTP)**
- **No relevant entries are present in the processor's TLB prior to execution**
- **The guest is executing in CPL0.**
- **The paging structures in use are shown below:**

Guest VM Page Table	
VA	**PA**
0x1000	0x12000

Nested Page Table	
GPA	**HPA**
0x12000	0x45000

Consider the following guest VM instruction:

0x1010: mov 0x1080, %rax ; move content in address 0x1080 to rax

5. (3 points) Which addresses (if any) are checked in the TLB during this instruction, and what is the content of the TLB after the instruction (tag info not needed)?

Answer:

0x1000	0x12000
0x12000	0x45000

6. (3 points) ____TRUE___ True or False? This instruction will cause a write to memory.

7. (3 points) ____TRUE____ True or False? This instruction will cause a read from memory.

8. (3 points) ___FALSE____ True or False? This instruction will cause a VM exit.

9. (3 points) ____FALSE_____ True or False? This instruction will cause a #GP (protection violation/privilege violation).

10. Given below are several technologies used by container runtimes. For each technology listed, select the capability/capabilities provided by the technology. A given technology may have more than one capability. Some capabilities listed may not be provided by any of the listed technologies, depending on your exam version. (3 points each, total 15 points) (Not In Syllabus)

Technologies	Capabilities
Example: AUFS	**A, B**
cgroups	
Docker agent	
LXC	
iptables	
devicemapper	

Capability list:

A. Copy on write
B. Layering
C. PID namespace
D. Improved Performance
E. Block (not file) based storage

F. User account (UID) namespace
G. Network isolation
H. Image repository
I. Container provisioning to remote hosts
J. Resource limitation

11. (5 points) _____C_______ Which of the following statements about ARM virtualization is correct?

A. The ARM architecture has built in support for shadow paging
B. An ARM hypervisor making use of hardware virtualization should run in EL0
C. An ARM CPU has a hardware register wherein desired exit controls are enabled
D. An ARM system's devices are typically discovered via probing
E. None of the above

12. (5 points) ____FALSE________ True or False? ARM hardware virtualization extensions are available only for 64 bit hosts (AArch64)?

13. (5 points) Place the following activities that occur during VM live migration into order, from earliest to latest.

Some activities may not be used, if they are not part of VM live migration. Some activities may be used more than once. Assume a single processor VM is being migrated.

A. Migration is paused, final pages are transferred
B. System administrator configures shared storage for VMs
C. VMCS content is transferred
D. Device context is transferred
E. VMCS content is deleted

Answer: **B A D C E**

14. (5 points) _____E_______ Which of the following characteristics are shared between BOTH port-based (IN/OUT) and MMIO based device I/O in a hypervisor?

A. Host devices can be passed through to a guest VM
B. Instruction decoding and emulation by the hypervisor may be required
C. Controlled by VMX exit controls
D. None of A, B, C are correct
E. All of A, B, C are correct

15. (5 points) _____C_______ A guest executing HLT with interrupts disabled will result in which of the following?

A. Triple fault and reset
B. Immediate and unconditional PCPU halt
C. Exiting to the hypervisor based on VMX controls settings
D. None of the above

16. (5 points) ______D______ Which of the following is a characteristic of the paravirtualized device model?

A. Reduces coding complexity at the expense of lower performance
B. Requires access to the guest OS source code
C. Increases coding complexity but provides higher performance
D. Higher performance with the same or less coding complexity as traditional models
E. None of the above

17. (5 points) Give three reasons why virtualizing server workloads in a datacenter environment is beneficial to organizations.

Answer: -higher availability
-cost effective (provide thin devices to employee)
-live migration
-backup/recovery
-ease of maintainance