CMPE-283 Assignment-3 Report

Evaluate EPT effect on performance

Submitted by Mengshi LI (013818454)

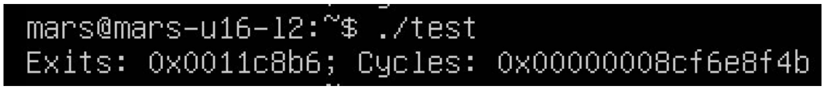
Assignment Purpose

In this assignment we will observe the VM exits times to evaluate the different memory virtualization methods, one is shadow paging, another is nested page table.

Detail Recipe:

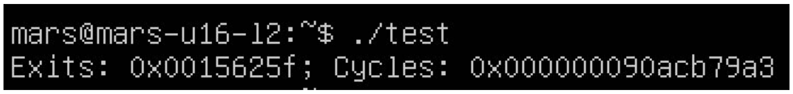
The following steps are setup in VMware fusion, L1 VM and L2 VM are both Ubuntu.

1) Boot into the L2 VM
2) Test exits times with EPT mode
    a) By default the kvm-intel module is loaded with ept=1, i.e. enabled
    b) Boot the guest VM and launch our test program.



```
mars@mars-u16-l2:~$ ./test
Exits: 0x0011c8b6; Cycles: 0x00000008cf6e8f4b
```

    c) Reboot the guest VM and once enter it, record the exits number again.



```
mars@mars-u16-l2:~$ ./test
Exits: 0x0015625f; Cycles: 0x000000090acb79a3
```

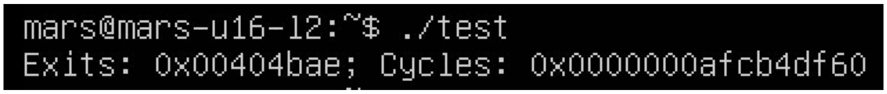
    d) The difference reflects the total exits needed for a reboot, which is approximately 235,945.
    e) The difference reflects the total exits needed for a reboot on the GCP with 1 vCPU + 3.75G memory is approximately 248,829. While for 4 vCPU + 8G memory for the guest VM, Exits = 0x159a66 - 0xfb124 = 0x5E942 = 387,394.
3) Test exits times with shadow paging mode
    a) Remove the kvm-intel module

```
# sudo rmmod kvm-intel
```

    b) Reload the kvm-intel module, but with ept=0, i.e. dis able EPT

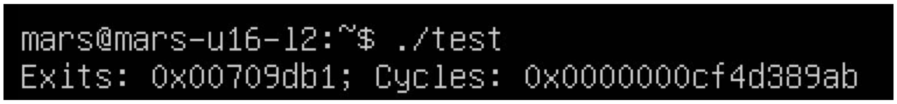
```
# sudo insmod /lib/modules/5.1.0-rc5+/kernel/arch/x86/kvm/kvm-intel.ko ept=0
```

    c) Boot the guest VM record the starting exits number:



```
mars@mars-u16-l2:~$ ./test
Exits: 0x00404bae; Cycles: 0x0000000afcb4df60
```

    d) Reboot the guest VM record the end exits number:

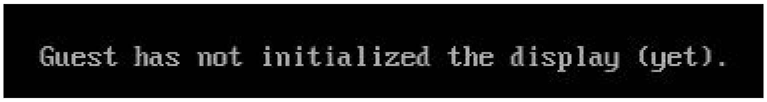


```
mars@mars-u16-l2:~$ ./test
Exits: 0x00709db1; Cycles: 0x0000000cf4d389ab
```

e) The difference reflects the total exits needed for a reboot, which is approximately 3,166,723. Around 13 times of the exits for EPT.

Note:

This experiment seems can't be produced on GCP, as we tried with L1 VM linux kernel from 4.15 to 5.1, none could work; we also tried both virt-manager and qemu-kvm command line, none could work; we also tried different L2 VM image, none could work. The failure is that once we rmmod and insmod with EPT=0, the qemu just shows:



```
Guest has not initialized the display (yet).
```

Also doubt if it is due to the GUI load too heavy and shadow mode can't support it?

Try disable GUI boot by modifying the grub:

```
# sudo vim /etc/default/grub
```

Editions includes:

```
GRUB_CMDLINE_LINUX="3"
GRUB_CMDLINE_LINUX_DEFAULT=”quiet”
GRUB_TERMINAL=console
```

Then update-grub and reboot. Still the same failure.

Questions:

1) What did you learn from the count of exits? Was the count what you expected? If not, why not?
   ANS:
   As expected EPT mode of memory virtualization, i.e. nested paging mode, involves much less exits to handle the paging operations from the guest VM. It will only exit due to EPT violation, while the shadow paging will exit whenever the guest VM access CR3, CR0, CR4, or PF#, execution of INVLPG.

2) What changed between the two runs (ept vs no-ept)?
   ANS:
   For the EPT mode, it is using two layer page table to translate from Guest VA to Guest PA then to Host PA, though more page access is required, but the guest VM could genuinely own the page table and thus any operation on CR3/0/4 and INVLPG instruction is done natively, i.e. no need to exit. it also has hardware registers to help guest VM to notify VMM, its operation and development are much easier.

   While on shadow paging mode, guest VM doesn't really own the page table, the VMM have to emulate CR3/0/4 and INVLPG for it.