

# CMPE 283: Virtualization Technologies

## Assignment 4: Shadow paging vs Nested paging

Bhavya Tetali (014535144), Supriya Meduri (015262767)

### Contribution of Team Members

Bhavya Tetali & Supriya Meduri:

- Collaborated together in zoom call
- Run the code in assignment 3 with shadow paging and added a screenshot.
- Run the code with shadow paging on i.e; ept=0 and added the screenshot.
- Created the documentation.

**Environment Setup:** We build this homework assignment on assignment-3 and hence used the same environment setup

### Steps Followed:

1. Boot the Guest VM
2. Reboot the guest VM and, Record total exit count information
3. Shutdown the test (inner) VM.
4. Remove the 'kvm-intel' module from your running kernel

```
$ rmmod kvm-intel
```

5. Reload the kvm-intel module with the parameter **ept=0** (this will disable nested paging and force KVM to use shadow paging instead)

```
$ insmod /lib/modules/5  
/kernel/arch/x86/kvm/kvm-intel.ko ept=0
```

6. Boot the VM again, note the exits
7. Reboot the VM and record the exits

## Screenshots

### Nested paging

```

890.876404] CPUID(0x4FFFFFFE), exit number 54 exits=3
890.876539] CPUID(0x4FFFFFFE), exit number 55 exits=3
890.876582] CPUID(0x4FFFFFFE), exit number 56 exits=0
890.876711] CPUID(0x4FFFFFFE), exit number 57 exits=0
890.876757] CPUID(0x4FFFFFFE), exit number 58 exits=0
890.876796] CPUID(0x4FFFFFFE), exit number 59 exits=0
890.876836] CPUID(0x4FFFFFFE), exit number 60 exits=0
890.876878] CPUID(0x4FFFFFFE), exit number 61 exits=0
890.876925] CPUID(0x4FFFFFFE), exit number 62 exits=0
890.876971] CPUID(0x4FFFFFFE), exit number 63 exits=0
890.877017] CPUID(0x4FFFFFFE), exit number 64 exits=0
890.877066] Exit type 65 is not defined by the SDM
890.877116] CPUID(0x4FFFFFFE), exit number 66 exits=0
890.877163] CPUID(0x4FFFFFFE), exit number 67 exits=0
890.877214] CPUID(0x4FFFFFFE), exit number 68 exits=0
1055.585027] perf: interrupt took too long (10260 > 9982), lowering kernel.perf_event_max_sample_rate to 19250
1074.389216] CPUID(0x4FFFFFFE), exit number 1 exits=95662
1160.395254] CPUID(0x4FFFFFFE), exit number 10 exits=145890
1165.853519] CPUID(0x4FFFFFFE), exit number 2 exits=0
1172.538620] CPUID(0x4FFFFFFE), exit number 3 exits=0
1178.273427] CPUID(0x4FFFFFFE), exit number 4 exits=0
1183.900267] CPUID(0x4FFFFFFE), exit number 10 exits=145964
1189.237134] CPUID(0x4FFFFFFE), exit number 12 exits=52303
bhavyalalithya@bhavyalalithya-virtual-machine:~/linux$

```

### Shadow paging

#### Boot

```

2519.335830] CPUID(0x4FFFFFFE), exit number 10 exits=716542
2523.021412] CPUID(0x4FFFFFFE), exit number 3 exits=0
2526.965627] CPUID(0x4FFFFFFE), exit number 1 exits=486389
2543.188624] CPUID(0x4FFFFFFE), exit number 12 exits=163216
2549.202179] CPUID(0x4FFFFFFE), exit number 10 exits=716614
2554.213734] CPUID(0x4FFFFFFE), exit number 2 exits=0
2558.527684] CPUID(0x4FFFFFFE), exit number 4 exits=0
bhavyalalithya@bhavyalalithya-virtual-machine:~/linux$

```

#### After reboot

```

2923.389576] CPUID(0x4FFFFFFE), exit number 12 exits=199643
2925.023645] CPUID(0x4FFFFFFE), exit number 10 exits=998550
2928.662274] CPUID(0x4FFFFFFE), exit number 1 exits=647224
2930.558241] CPUID(0x4FFFFFFE), exit number 2 exits=0
bhavyalalithya@bhavyalalithya-virtual-machine:~/linux$ ~

```

## Observations

**What did you learn from the count of exits? Was the count what you expected? If not, why not?**

The number of exits in shadow paging increases compared to nested paging. It is an expected outcome since, in nested paging, it will only VM exit when an EPT violation occurs. Whereas in shadow paging, it could exit every time VM tries to execute CR0, CR3, CR4 execution, or any paging related exits like a page fault.

### **What changed between the two runs (ept vs no-ept)?**

EPT Mode:

Two-layer page tables are used to translate from Guest VA to Guest PA to Host PA, and more page access is required, the guest VM should own page table and hence all the operations on CR3 is done natively, i.e. no need to exit

No EPT Mode:

Guest VM does not own the page table in shadow paging mode, for it, the VMM must simulate CR3.