Discovering VMX Features  
Assignment 1  
Virtual Technologies

Team Members:   
Puja Kumari  
Tonja Jean

December 2023

**Table of Contents**

[1 Project Scope 2](#_Toc153755716)

[1.1 GitHub Repo 2](#_Toc153755717)

[2 Prerequisite: 2](#_Toc153755718)

[3 Terms and Definitions 2](#_Toc153755719)

[4 Implementation 3](#_Toc153755720)

[4.1 Dynamic Teamwork – Team Contribution 3](#_Toc153755721)

[4.2 Environment Set up 4](#_Toc153755722)

[4.2.1 Server Type 4](#_Toc153755723)

[4.2.2 Environment Setup – As completed in assignment 1 and included here for context. 4](#_Toc153755724)

[4.2.3 Install the build essentials. 4](#_Toc153755725)

[4.2.4 Confirm KVM is not already loaded, remove actively loaded, and perform add the kernel modules. 4](#_Toc153755726)

[4.3 Update Kernel Code Files 4](#_Toc153755727)

[4.3.1 Update kvm hypervisor files: cupid.c and vmx.c files 4](#_Toc153755728)

[4.4 Create L2 VM and Test CPUID Assignment 6](#_Toc153755729)

[4.4.1 Create Nested L2 VM 6](#_Toc153755730)

[4.4.2 Installed GEMO compatible Ubuntu OS on the inner VM using Chrome Remote Desktop 8](#_Toc153755731)

[4.5 Perform CPUID confirmation test - Results 8](#_Toc153755732)

[Test 1: Tested functionality for %eax=04xFFFFFFF 8](#_Toc153755733)

[4.6 Debugging 10](#_Toc153755734)

[5 Summary and Questions 13](#_Toc153755735)

# Project Scope

This assignment is designed to demonstrate how to discover VMX features that are available in the processor. The lab explores several MSRs and their capabilities and includes building a system that supports vmx flags for use in the more subsequent assignments.

GitHub Repo

<https://github.com/tlavette/cmpe283assignment-1.git>

# Prerequisite:

Prerequisites: A base system running Linux version of OS with an Intel CPU Processor native to the hardware. In this lab we will be building an environment using the Google Cloud Platform.

# Terms and Definitions

|  |  |
| --- | --- |
| CPUID leaf node | The most significant or highest EAX command parameter of the EAX set |
| KVM | Kernel Based Virtual Machine |
| Kernel | An architecture standpoint it stands in between the Applications and CPU, Memory and Devices and is the main interface between the physical hardware and the processes running on it. |
| Kernel module | Code that can be loaded and unloaded to the Kernel |
| lsmod | Displays loaded modules |
| rmmod | Command used to remove running modules |
| modprobe | Program used to add and remove modules from the Linux Kernel |
| RDTSC | Read time Stamp Counter measures the number of CPU cycles since its reset. |
| CPU | Central Processing Unit |
| module | Are extensions used to create and manage various components of virtual machines such as networking, storage, and networking. |
| SSH | Secure Shell |
| GCP | Google Cloud Platform |

# Implementation

## Dynamic Teamwork – Team Contribution

The first assignment did present several unexpected issues, so the original divide of tasks did overlap as we had to resolve issues ranging from finding the best GCP VM Service, building the VM with the needed storage, and creating the kernel. Overall, the project was divided according to need and we paired on building and resolving issues presented. The general divide of the project was as follows:

Tonja Jean

* Researched system options from various platforms and hardware.
* Perform collaborative review of the requirements to determine the resources needed to complete.
* Created an instance from Google Cloud Platform and performed system requirements for memory, CPU, and nested capabilities.
* Installed Linux build with needed source code, libraries, and components.
* Performed system updates including the .config boot file.
* Modified cmpe283-1.c file and performed the build for the following:
  + IA32\_VMX\_PINBASED\_CTLS 0x481
  + IA32\_VMX\_PROCBASED\_CTLS 0x482
  + IA32\_VMX\_PROCBASED\_CTLS2 0x48B
* Performed test and debug collaboration.
* Collected and compiled documentation.
* Performed final code refactoring and compilation.

Puja Kumari

* Researched system options from various platforms and hardware.
* Perform collaborative review of the requirements to determine the resources needed to complete.
* Created an instance from Google Cloud Platform and performed system requirements for memory, CPU, and nested capabilities.
* Installed Linux build with needed source code, libraries, and components.
* Modified cmpe283-1.c file and performed the build for the following:
  + IA32\_VMX\_EXIT\_CTLS 0x483
  + IA32\_VMX\_ENTRY\_CTLS 0x484
  + IA32\_VMX\_PROCBASED\_CTLS3 0x492
* Performed test and debug collaboration.
* Performed final code refactoring and compilation.
* Collected and compiled documentation.

## Create the environment

The steps used in completing this lab is as follows. The user will need to consider the libraries and components needed may vary by CPU type, Server OS, memory etc. Please note it is required to use an Intel CPU Platform that supports nested environments. For this lab we used the following:

### Server Type

Google Cloud Platform VM Server Machine Type: n1-standard-8 CPU Platform: Intel Haswell Architecture: x86/64 Boot Disk: debian-11-bullseye-v20231115 200G

A screenshot of a computer

Description automatically generated

This system was selected because it has the Intel Haswell CPU which does support vmx flags.

Confirmed VMX flags are available.

cat /proc/cpuinfo

A black screen with white text

Description automatically generated

### Environment Setup – Increased storage capacity to 200G

A screenshot of a computer

Description automatically generated

### Download Linux Source Code Cloned the GitHub repository-

<https://github.com/torvalds>

Login to GitHub

Press Fork

Press code and copy the link for the repository.

Login to the local VM and clone the fork of the Linux Source Code repo

$git clone <https://github.com/torvalds/linux.git>

### Download Files from Canvas

cmpe283-1.c

Makefile

### Install the build essentials.

Perform apt-get update and apt-get install for needed libraries

apt-get install build-essential kernel-package fakeroot

libncurses5-devlibssl-dev ccache bison flex libelf-dev

### Update Kernel Source Code

mkdir linux

cd linux

uname -a - to determine the kernel needed

cp /boot/6.7.0-rc3+ . .config

ma

# Results:

1. **Pinbased SDM Volume 3C Section 25.6.2**

IA32\_VMX\_PINBASED\_CTLS

A close-up of a document

Description automatically generated

268.235381] cmpe283\_1: loading out-of-tree module taints kernel.

[ 268.242312] CMPE 283 Assignment 1 Module Start

[ 268.246948] Pinbased Controls MSR: 0x7f00000016

[ 268.253008] External Interrupt Exiting: Can set=Yes, Can clear=Yes

[ 268.259517] NMI Exiting: Can set=Yes, Can clear=Yes

[ 268.264724] Virtual NMIs: Can set=Yes, Can clear=Yes

[ 268.270006] Activate VMX Preemption Timer: Can set=Yes, Can clear=Yes

[ 268.276760] Process Posted Interrupts: Can set=No, Can clear=Yes

tonja\_jean@centralnested:~$

1. **Procbased**

MSR IA32\_VMX\_PROCBASED\_CTLS2

**SDM Vol 3D 25.6.2**

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

1. **Secondary Procbased**

**SDM Vol 3D 25.6.2**

IA32\_VMX\_PROCBASED\_CTLS2

{

{ 0, "Virtualize APIC accesses" },

{ 1, "Enable EPT" },

{ 2, "Descriptor-table exiting" },

{ 3, "Enable RDTSCP" },

{ 4, "Virtualize x2APIC mode" }.

{ 5, "Enable VPID" },

{ 6, "WBINVD exiting" },

{ 7, "Unrestricted guest" },

{ 8, " APIC-register virtualization" },

{ 9, "Virtual-interrupt delivery" }

{ 10, "PAUSE-loop exiting" },

{ 11, "RDRAND exiting" },

{ 12, "Enable INVPCID" },

{ 13, "Enable VM functions" },

{ 14, "VMCS shadowing" }

{ 15, "Enable ENCLS exiting" },

{ 16, "RDSEED exiting" },

{ 17, "Enable PML" },

{ 18, "EPT-violation #VE" },

{ 19, "Conceal VMX from PT" }

{ 20, "Enable XSAVES/XRSTORS" },

{ 21, "PASID translation" },

{ 22, " Mode-based execute control for EPT" },

{ 23, "Sub-page write permissions for EPT" },

{ 24, "Intel PT uses guest physical addresses" }

{ 25, "Use TSC scaling" },

{ 26, "Enable user wait and pause" },

{ 27, "Enable PCONFIG" },

{ 28, "Enable ENCLV exiting" },

{ 30, "VMM bus-lock detection" }

{ 31, "Instruction timeout" },

};

[70512.726139] CMPE 283 Assignment 1 Module Start

[70512.730848] Procbased Controls MSR: 0x51ff00000000

[70512.735771] Virtualize APIC accesses: Can set=Yes, Can clear=Yes

[70512.742111] Enable EPT: Can set=Yes, Can clear=Yes

[70512.747230] Descriptor-table exiting: Can set=Yes, Can clear=Yes

[70512.753606] Enable RDTSCP: Can set=Yes, Can clear=Yes

[70512.758986] Virtualize x2APIC mode: Can set=Yes, Can clear=Yes

[70512.765145] Enable VPID: Can set=Yes, Can clear=Yes

[70512.770354] WBINVD exiting: Can set=Yes, Can clear=Yes

[70512.775816] Unrestricted guest: Can set=Yes, Can clear=Yes

[70512.783187] APIC-register virtualization: Can set=Yes, Can clear=Yes

[70512.789976] Virtual-interrupt delivery: Can set=No, Can clear=Yes

[70512.798233] PAUSE-loop exiting: Can set=No, Can clear=Yes

[70512.804140] RDRAND exiting: Can set=No, Can clear=Yes

[70512.809602] Enable INVPCID: Can set=Yes, Can clear=Yes

[70512.815081] Enable VM functions: Can set=No, Can clear=Yes

[70512.820900] VMCS shadowing: Can set=Yes, Can clear=Yes

[70512.826359] Enable ENCLS exiting: Can set=No, Can clear=Yes

[70512.832369] RDSEED exiting: Can set=No, Can clear=Yes

[70512.839177] Enable PML: Can set=No, Can clear=Yes

[70512.844253] EPT-violation #VE: Can set=No, Can clear=Yes

[70512.849900] Conceal VMX from PT: Can set=No, Can clear=Yes

[70512.855721] Enable XSAVES/XRSTORS: Can set=No, Can clear=Yes

[70512.863058] PASID translation: Can set=No, Can clear=Yes

[70512.868687] Mode-based execute control for EPT: Can set=No, Can clear=Yes

[70512.875875] Sub-page write permissions for EPT: Can set=No, Can clear=Yes

[70512.883262] Intel PT uses guest physical addresses: Can set=No, Can clear=Yes

[70512.890896] Use TSC scaling: Can set=No, Can clear=Yes

[70512.896526] Enable user wait and pause: Can set=No, Can clear=Yes

[70512.903117] Enable PCONFIG: Can set=No, Can clear=Yes

[70512.909862] Enable ENCLV exiting: Can set=No, Can clear=Yes

[70512.916031] VMM bus-lock detection: Can set=No, Can clear=Yes

[70512.922270] Instruction timeout: Can set=No, Can clear=Yes

tonja\_jean@centralnested:~$

1. **IA32\_VMX\_PROCBASED\_CTLS3 Tertiary Procbased**

**SDM Vol 3D 25.6.2**

{

{ 0, "LOADIWKEY exiting" },

{ 1, "Enable HLAT" },

{ 2, "EPT paging-write control" },

{ 3, "Guest-paging verification" },

{ 4, "IPI virtualization " },

{ 7, "Virtualize IA32\_SPEC\_CTRL" },

};

[75429.232473] Procbase tertiary Controls MSR: 0x0

[75429.238542] LOADIWKEY exiting: Can set=No, Can clear=Yes

[75429.244179] Enable HLAT: Can set=No, Can clear=Yes

[75429.249462] EPT paging-write control: Can set=No, Can clear=Yes

[75429.255776] Guest-paging verification: Can set=No, Can clear=Yes

[75429.263569] IPI virtualization : Can set=No, Can clear=Yes

[75429.269542] Virtualize IA32\_SPEC\_CTRL: Can set=No, Can clear=Yes

tonja\_jean@centralnested:~$

1. **IA32\_VMX\_ENTRY\_CTLS**

**Section 25.8.1**

{

{ 2, "Load debug controls" },

{ 9, "IA-32e mode guest" },

{ 10, "Entry to SMM" },

{ 11, "Deactivate dualmonitor treatment" },

{ 13, "Load IA32\_PERF\_GLOBAL\_CTRL" },

{ 14, "Load IA32\_PAT" },

{ 15, "Load IA32\_EFER" },

{ 16, "Load IA32\_BNDCFGS" },

{ 17, "Conceal VMX from PT " },

{ 18, "Load IA32\_RTIT\_CTL" },

{ 19, "Load UINV" },

{ 20, "Load CET state" },

{ 21, "Load guest IA32\_LBR\_CTL" },

{ 22, "Load PKRS" },

};

[76539.905414] Entry Controls MSR: 0xd3ff000011ff

[76539.909993] Load debug controls: Can set=Yes, Can clear=No

[76539.915796] IA-32e mode guest: Can set=Yes, Can clear=Yes

[76539.921505] Entry to SMM: Can set=No, Can clear=Yes

[76539.926827] Deactivate dualmonitor treatment: Can set=No, Can clear=Yes

[76539.934121] Load IA32\_PERF\_GLOBAL\_CTRL: Can set=No, Can clear=Yes

[76539.940549] Load IA32\_PAT: Can set=Yes, Can clear=Yes

[76539.947341] Load IA32\_EFER: Can set=Yes, Can clear=Yes

[76539.952994] Load IA32\_BNDCFGS: Can set=No, Can clear=Yes

[76539.958623] Conceal VMX from PT : Can set=No, Can clear=Yes

[76539.964511] Load IA32\_RTIT\_CTL: Can set=No, Can clear=Yes

[76539.970398] Load UINV: Can set=No, Can clear=Yes

[76539.975336] Load CET state: Can set=No, Can clear=Yes

[76539.980768] Load guest IA32\_LBR\_CTL: Can set=No, Can clear=Yes

[76539.986953] Load PKRS: Can set=No, Can clear=Yes

tonja\_jean@centralnested:~$

1. **IA32\_VMX\_EXIT\_CTLS**

**Section 25.7.1**

struct capability\_info vmxexit[7] =

{

{ 25, "Clear IA32\_RTIT\_CTL" },

{ 26, "Clear IA32\_LBR\_CTL" },

{ 27, "Clear UINV" },

{ 28, "Load CET state" },

{ 29, "Load PKRS " },

{ 30, "Save IA32\_PERF\_GLOBAL\_CTL" },

{ 31, "Activate secondary controls" },

};

[75020.593064] CMPE 283 Assignment 1 Module Start

[75020.597714] Exit Controls MSR: 0x7fefff00036dff

[75020.602397] Clear IA32\_RTIT\_CTL: Can set=No, Can clear=Yes

[75020.608300] Clear IA32\_LBR\_CTL: Can set=No, Can clear=Yes

[75020.614027] Clear UINV: Can set=No, Can clear=Yes

[75020.619371] Load CET state: Can set=No, Can clear=Yes

[75020.626350] Load PKRS : Can set=No, Can clear=Yes

[75020.632912] Save IA32\_PERF\_GLOBAL\_CTL: Can set=No, Can clear=Yes

[75020.640709] Activate secondary controls: Can set=No, Can clear=Yes

tonja\_jean@centralnested:~$