VMCS总结

VMCS是物理内存的一个4KB页面（4KB对齐），包含了6个区域，guest/host状态，VM运行控制，VM entry控制，VM exit控制以及VM exit的信息。

在VMCS架构中，当发生VMX operation模式的Root 与 non Root环境切换时

VMCS用来配置当前发生切换的逻辑处理器的状态及执行环境

一个逻辑处理器管理着多个VMCS

同一时刻 一个逻辑处理器只有一个VMCS是current-VMCS

VMCS三种状态

1) activity属性 包括 active(活动) 及 inactive(非活动)状态

2) current 属性 包括 current(当前的) 及 not current(非当前的)状态

3) launch 属性 包括 clear(干净的) 及 launched(已启动的) 状态

VMCS区域的大小由IA32\_VMX\_BASIC[44:32]域里面得到 以KB得到 最高为4KB

IA32\_VMX\_BASIC[53:50]报告了VMCS区域支持的cache类型 支持UC与WB类型

VMM需要用一个被称为"VMXON region"的区域来管理整个VMX operation模式

VMXON区域大小及所支持的cache类型与VMCS区域一致

一个VMM对应一个VMXON指针 除非在VMM里关闭VMX operation模式后，在使用另一个VMXON

指针来重新开启VMX operation模式，否则，VMXON指针是不会改变的

VMXOFF指令也操作在这个VMXON指针上，用在关闭当前VMXON区域所管理的operation模式

访问VMCS字段必须通过VMREAD 与 VMWRITE指令 每个字段定义一个唯一的ID值来对应

VMCS数据区域包括6个区域

1)guest-state区域 用来保存与guset运行环境相关的信息

1)段寄存器类字段

2)GDTR 与 IDTR字段

base字段，提供描述符表基址

limit字段，提供描述符表的长度

3)MSR字段

4)SMBASE字段 这个字段使用在SMM双重监控处理机制下

5)activity state 字段 用于指示在VM-entry 和 VM-exit时 虚拟处理器的当前活动状态

6)interruptibility state 字段 指示当前虚拟处理器的可中断性

7)pending debug exceptions 字段用来记录和设置guest存在未处理而pending(悬挂)的#DB异常 DebugPoint

8)VMCS link pointer 字段 仅用在SMM双重监控处理机制下

9)VMCS-preemption timer value 字段 用于提供一个32位的定时器初始化计数值

10)PDPTEs字段(Page-Directory Pointer Table Entries 页目录指针表项) 共有4个 PDPTE0 PDPTE1 PDPTE2 PDPTE3 这些字段在支持EPT功能时有效

11)guset interrupt status 字段 作为虚拟local APIC的状态值 处理器使用这个字段来维护虚拟中 断的状态

2)host-state 区域

3)VM-executive 控制区域

主要控制处理器在VMX non-root operation 模式下的行为能力

典型的可以控制某些条件引发VM-exit事件，也控制着VMX的某些虚拟化功能的开启 例如 APIC的虚拟化及EPT机制

4)VM-exit控制区域

1)VM-exit control字段

2)VM-exit MSR-store count 与 VM-exit MSR-store address字段

控制处理器VM-exit时如何保存guest-MSR列表

3)VM-exit MSR-load count 与 VM-exit MSR-load address字段

控制处理器VM-exit时如何保存host-MSR列表

5)VM-entry控制区域

1)VM-entry control字段

2)VM-entry MSR-load count 字段

3)VM-entry MSR-load address 字段

2 3 用来控制VM-entry时guest-MSR列表的加载

4)VM-entry interruption-information字段

5)VM-entry exception error code 字段

6)VM-entry instruction length字段

4 5 6 用于控制事件注入 含有注入事件的VM-entry被称为"向量化的VM-entry"

6)VM-exit信息区域

VM-exit的直接向量事件信息类字段有两个:

VM-exit interruption information 和

VM-exit interruption error code 字段

VM-exit的间接向量事件信息类字段有两个:

IDT-vectoring information 和

IDT-vectoring error code 字段