**问题一：解释Intel VT-x的虚拟化设计方案**

Intel VT中的VT-x技术扩展了传统的IA32处理器架构，为IA32架构的处理器虚拟化提供了硬件支持。VT-x针对X86引入了一种新的模式，这种新的模式被称为VMX，它被设定在R0级以下，可以认为是R-1级。VMX存在两种操作模式：

1）根操作模式( VMX Root Operation)：是VMM运行的模式。在根模式下，所有指令的行为和传统的IA32一样，因此，原来的软件都可以正常运行，与不提供虚拟化时的运行环境兼容。

2）非根操作模式( VMX Non-Root Operation )：是虚拟化客户机运行的模式。在非根模式下，所有敏感指令的行为都被重新定义，使得它们不再经过VMM捕获就直接运行或者通过“陷入再模拟”的方式来处理。

根模式和非根模式都有相应的特权级0—特权级3。所不同的是，在非根模式下，敏感指令会引起“陷入”，被称为VM-Exit。VM-Exit发生时，CPU自动从非根模式切换到根模式，即“陷入”到VMM。与VM-Exit相对应的是VM-Entry，它由VMM发起，通常是VMM调度运行某个客户机时CPU由根模式切换成非根模式。

Intel VT-x(Intel Virtualization Technology for x86)- 处理器虚拟化X

VMCS（Virtual-Machine Control Structure，虚拟机控制结构）用来保存虚拟CPU的状态（如CPU在根模式和非根模式下的特权寄存器的值）。CPU在发生VM-Exit和VM-Entry时会自动查询和更新VMCS。此外，VT-x引入的指令包括：VMLAUNCH/VMRESUME用于发起VM-Entry，VMREAD/VMWRITE用于配置VMCS等。

VT-x可以提高基于软件的虚拟化解决方案的灵活性与稳定性，不仅能够有效减少 VMM 干预，还为 VMM 与客户操作系统之间的传输平台控制提供了有力的硬件支持。在需要 VMM干预时，状态切换更加快速、可靠 和安全。

硬件虚拟化使用vCPU(Virtual CPU)描述符描述虚拟CPU。它类似于操作系统中的进程描述符（或进程控制块），它实际上是一个数据结构，由如下几个部分组成：

1） vCPU标识信息：用于标识vCPU的一些属性，如vCPU的ID号、vCPU属于哪个客户机等。

2） 虚拟寄存器信息：虚拟的寄存器资源，这些内容包含在VMCS中。例如，客户机状态域保存的内容。

3） vCPU状态信息：类似于进程的状态信息，标识该vCPU当前所处的状态（睡眠、运行等），主要供调度器使用。

4） 额外寄存器／部件信息：主要指未包含在VMCS中的一些寄存器或CPU部件。例如，浮点寄存器和虚拟的LAPIC等。

5） 其他信息：用于VMM进行优化或存储额外信息的字段，例如，存放该vCPU私有数据的指针。

vCPU可以划分为两个部分：一个是以VMCS为主，由硬件使用和更新的部分，主要是虚拟寄存器；另一个是由VMM使用和更新的部分，主要是VMCS以外的部分，例如vCPU标识、状态信息等。当VMM创建客户机时，首先要为客户机创建vCPU，整个客户机的运行实际上可以看做VMM在调度不同的vCPU运行。

中断处理

物理机环境下的中断处理： Intel VT-x(Intel Virtualization Technology for x86)- 处理器虚拟化

I/O设备通过中断控制器(I/OAPIC或者PIC）发送中断请求，中断请求经由PCI总线发送到系统总线上，最后目标CPU的Local APIC部件接收中断，目标CPU对中断进行处理。

在虚拟机的环境中，VMM为客户机操作系统提供的中断处理过程如图所示：

Intel VT-x(Intel Virtualization Technology for x86)- 处理器虚拟化

每一个vCPU都对应一个虚拟Local APIC用于接收中断。虚拟平台VMM包含虚拟I/O APIC或者虚拟PIC用于发送中断。虚拟Local APIC、虚拟I/O APIC和虚拟PIC都是由VMM维护的软件实体。

当虚拟设备需要发送中断时，虚拟设备会调用虚拟I/O APIC的接口发送中断；而虚拟I/O APIC根据中断请求，挑选出相应的虚拟Local APIC，向其发出中断请求。虚拟Local APIC进一步利用Intel VT-x的事件注入机制将中断注入到相应的vCPU。

**问题二：为什么说虚拟化技术可以加快灾难恢复的速度，降低灾难恢复所需的成本？**

虚拟机将整个系统，包括硬件配置、操作系统以及应用等封装在文件里，灾难 恢 复时需要重新部署各种软件运行环境，虚拟机和底层的硬件没有直接的绑定 关系，利于无缝迁移，故虚拟化技术加快了部署软件运行环境的速度； 同时， 我们能使用虚拟机保存所有与系统有关的数据，在灾难恢复时 能够在运行中快 速地恢复系统镜像，减少了设置错误以及恢复丢失系统所需要的时间，且无需 维护特定硬件的成本； 在一个计算机上可以运行多个虚拟机，每个应用程序可以在自己的操作系统环境中独立运行，且不会影响其他的工作负载，使得资源的调度更加优化，在灾难恢复时虚拟机可代替多台物理机，降低硬件配置成本 。