

硬體對虛擬化的支援，逐漸走向強化周邊裝置的應用

AMD在VMworld大會展示虛擬化創新技術

在VMworld大會上，AMD搶先發表能大幅提升虛擬化應用的新技術，包括繪圖處理虛擬化、I/O虛擬化（I/O Virtualization），以及Hypervisor的安全開機（Secure Boot）等

在今年的VMworld大會上，AMD展示區附近相當熱鬧滾滾，其中最重要的一場活動就是三個概念展示的實際驗證展示，那就是：繪圖處理虛擬化（Graphics Virtualization）、I/O虛擬化（I/O Virtualization），以及Hypervisor的安全開機（Secure Boot）功能，而且這些功能都即將問世。

這些展示的圖片已經由AMD原廠張貼到網路，因此，那些無法去這次大會現場的人也能夠看到。這項史無前例的展示，說明了AMD對於推動虛擬化技術趨於成熟所作的努力。近期，AMD原廠也將這些展示的短片上傳至網路。

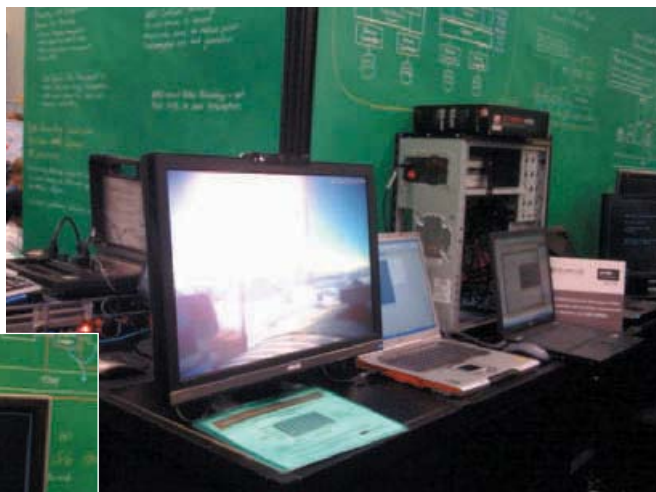
▼ Hypervisor搭配TPM的驗證，可避免虛擬化系統在開機的過程中檢查是否遭到竄改。



繪圖處理虛擬化

當虛擬桌面越來越普及，透過傳統伺服器所支撐的個人端電腦技術來支援更豐富的圖形處理環境，已經不太容易。這項概念驗證的展示呈現了對繪圖卡執行裝置直接配置的作業，可以提升對高度資源要求的圖形應用程式的支援，像是電腦輔助設計（CAD），以及數位內容創作（DCC）。值得注意的是AMD Opteron 6100系列處理器（代號為Magny-Cours），即將於2010年第一季推出。

這項展示執行在AMD工程研發系統上，它包含了2顆12核心的AMD Opteron 6100系列處理器、AMD SR5690晶片組和ATI FirePro專業繪圖卡。這套系統在VMware ESX 4.0系統中的一臺虛擬機器上，執行了3DMark06和Toy Store/Code Zero。在直接裝置對應（direct device mapping）功能後，該項展示也比較了啟動或停用等兩種狀態的繪圖處理效能表現，同時也利用AMD I/O虛擬化技術讓圖形處理可以快速穿透虛擬層。而支援AMD I/O虛擬化技術，也已經屬於VMware ESX 4.0的實驗性功能之一。



▲ 繪圖處理虛擬化增強了伺服器對於圖形運算的處理能力，可讓桌面虛擬化的環境更直接地存取與共享繪圖卡的資源。

I/O虛擬化

在虛擬化早期發展時，對於特定應用程式需要高效能的網路傳輸能力並沒有考慮在內，這是因為虛擬化會帶來相關的負荷。為了達到接近原生網路效能，I/O虛擬化正是設計用來減少這類負擔的一種機制。這項概念驗證的展示，也對照了有無I/O虛擬化的網路效能差異。

這項展示所搭配的硬體環境是AMD工程研發系統，其中包含了4顆12核心的AMD Opteron 6100系列處理器、4組AMD SR5690晶片組和1個Solarflare的10G網路卡。該系統搭配的軟體是在VMware ESX 4.0上，執行了NetPerf的網路效能測試程式。過程中，AMD也使用了VMware針對裝置直接配置的穿透支援。對AMD的I/O虛擬化而言，VMware ESX 4.0對也提供了實驗性支援。

安全啟動

安全性是虛擬化相當重要的考量之一，特別是當越來越多的企業關鍵應用系統轉移到虛擬伺服器的這個時刻。這項概念驗證展示強調了採用AMD技術核心的既有量產型伺服器，如何

對Hypervisor做到安全的設定控制。

該項展示的硬體環境上，主要是搭配2顆六核心AMD Opteron處理器的HP ProLiant DL385 G6，這臺伺服器的主機板也內建TPM (Trusted Platform Module) 安全晶片。AMD展示的安全開機軟體環境，是以VMware ESX 4.0搭配AMD軟體工程師所開發的安全載入器。在開機的過程中，Hypervisor會將設定與儲存在TPM中的設定資訊相比對，確

保Hypervisor未因惡意或無心疏忽而遭到竄改。不論安全與否，Hypervisor的狀態都會回報到vSphere的管理主控臺。這能讓IT人員避免在資料中心環境中，使用錯誤設定的或被竄改的Hypervisor。想了解更多相關的資訊嗎？你可以連線至VMworld.com網站上的專屬展示攤位AMD Virtual Booth (<http://www.vmworld.com/community/exhibitors/amd>)

處理器大幅支援虛擬化已成技術主流，下一步將針對I/O

I/O虛擬化的重要性

近幾年來，處理器對虛擬化的協助已經有長足的進步，但I/O虛擬化的發展是落後的。而AMD在IOMMU (I/O Memory Management Unit) 1.2規格中，已經首度揭露了I/O虛擬化的進展

為什麼你需要I/O虛擬化的架構？當系統實作的虛擬化裝置類型越來越廣泛時，AMD IOMMU在虛擬系統當中需要設法加速周邊的效能，才能減少日常作業的不必要負擔。

由AMD所開發出的IOMMU架構，並非專屬封閉的規格，它目前相容於PCI-SIG組織所定義的新標準，而有了這些標準作為依據，可讓獨立硬體製造商用來提供新的效能等級。IOMMU也能改善驅動程式的可靠性，而且對於未來系統所需的安全開機功能來說，相當重要。

PCI-SIG IOV的周邊虛擬化標準

I/O虛擬化目前已推出一些業界標準，像是PCI-SIG組織所定義的新標準PCI-SIG IOV (PCI-SIG I/O Virtualization)，這項規格和系統虛擬化的技術搭配後，能讓不同的作業系統能在單一臺電腦上模擬執行，並且能以原生的方式彼此共享PCI-E介面的周邊裝置。它可細分成三大領域：另類路由ID解析 (Alternative Routing-ID Interpretation, ARI)、單源I/O虛擬化 (Single Root IOV, SR-IOV)、多源I/O虛擬化 (Multi-Root IOV, MR-IOV)。它們都屬於硬體周邊的虛擬化。

以ARI的作用來說，是讓單各PCIe多功能周邊設備能提供更多PCI功能，提供一組交易方式讓PCI-E元件能夠交換與使用經過轉譯過的位址，藉以支援I/O虛擬化。Single Root IOV則是在既有的PCI-E拓樸下，透過單一根源的複合結構來提供I/O虛擬化，讓PCI-E周邊能呈現多個實體（也就是虛擬化功能）、執行管理的相關功能（像是建置與移除），並且能建立具穿透力的裝置 (virtual function _ virtual machine)。至於Multi-Root IOV則主要基於Single Root IOV的規格，在新的拓樸下去提供I/O虛擬化，例如刀鋒伺服器，在這種系統上會有個

根源的複合結構來共享PCI-E的階層。

其他I/O虛擬化相關的規格，還包括位址轉譯服務 (Address Translation Services, ATS)，針對虛擬化負責保護周邊啟用時的位址轉譯，能從IOMMU當中取得周邊快取的分頁表與需要的交易資料；以及讓周邊分頁能與ATS連接的系統分頁需求介面 (Page Request Interface, PRI)，它能夠透過IOMMU，向作業系統提供周邊需求的記憶體存取服務。

I/O虛擬化的效益

以這樣的標準所建立的I/O虛擬化，可以做到那些事情？首先是提供具備多種功能的網路介面，包含管理、網路交換、獨立虛擬網卡，可根據不同裝置代號轉譯給IOMMU了解（也就是PCI BDF），並且保護每一個周邊裝置。其次是加速存取，可透過I/O轉換旁觀式緩衝 (I/O Translation Look-aside Buffer, IOTLB) 來做到受控裝置的轉譯。最後還有記憶體超載 (Memory Overcommit)，可透過PRI，讓分頁錯誤處理能允許記憶體超量使用。

整體而言，IOMMU處理了周邊的所有存取行為，它能提供虛擬環境與實體環境之間的硬體位址轉譯，同時驗證每一個PCI功能的存取許可、重新將中斷處理對應至新的面向與目標處理器；此外，也提供上述的ATS與PRI服務，分別處理轉譯資訊與分頁錯誤與存取變更等作業。這可以讓因為傳輸漏失所導致的延遲，降到最低。

事實上，IOMMU帶來的好處多多。舉例來說，像是記憶體保護，能確保系統受到隔離，提升安全性，並且限制周邊裝置對記憶體的存取，避免竄改或窺伺，一方面也能開放讓虛擬機器直接存取I/O裝置，進而減少I/O作業的負荷。