

# 操作系統虛擬化之保安

2008 年 2 月

© 香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

**免責聲明：**政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

## 目錄

摘要.....	2
I. 介紹.....	3
II. 虛擬化之管理考慮.....	4
促進虛擬化之因素.....	4
虛擬化之優點.....	4
虛擬化之缺點.....	6
III. 給資訊科技從業人員有關虛擬化的建議.....	7
部署虛擬化.....	7
保安威脅.....	7
IV. 結論.....	9

## 摘要

當伺服器與桌上電腦陸續為資訊科技經理帶來管理、彈性和保安等問題時，由虛擬機器（virtual machines）所提供的獨立執行環境（isolated execution environment）也許可解決此問題。另一項優點是假如有人遺失手提電腦，虛擬化技術可幫助保護機構的數據，以免意外地向外間洩露。在用戶手提電腦中的加密檔案夾，也可預先建立鎖定的桌上電腦環境。隨著主要微處理器（microprocessor）供應商日趨增加虛擬化硬件的供應，虛擬化產品已成為資訊科技管理的實務解決方案。在此文中，我們將討論虛擬化技術的管理議題，並提供在伺服器與桌上環境上部署虛擬化技術時可用的選擇。

## I. 介紹

當研究人員首次提出 **Multi-Programming** 和 **time-sharing** 概念時，「虛擬機器」此名詞最早便出現在 1960 年的學術文章中。早期虛擬機器概念的例子可追溯到 1960 年代的 **IBM M44/44X** 計畫，與之後發展出如 **IBM 360/67** 和 **VM/370**<sup>1</sup>等 **IBM** 大型主機系統。在當時，電腦計算能力仍是稀有資源，充分利用有限的硬件是很重要的，而虛擬化技術便是其一解決方案。

虛擬化 (Virtualisation) 已被定義為「*a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, and many others*」<sup>2</sup>，意即虛擬化是利用硬件和軟件分割、分時(time-sharing)、部份或全部機器模擬(simulation)、仿效(emulation)的概念，把電腦資源分割為數個執行環境。虛擬化技術可使電腦資源能夠被最有效地使用，以增加投資回報，從用戶觀點來看，虛擬化可使在同一個實體電腦中運行多個操作系統。

與 1960 年代和 1970 年代比較，現在的電腦硬件相對便宜，且更有威力而供應更加充足，資訊科技管理仍視虛擬化是一項有效的管理策略，當今伺服器虛擬化技術的驅動力包括：

1. 可減少執行特定任務或操作系統的實體伺服器數量；
2. 任何實體伺服器之合併策略，可降低數據中心所需的硬件空間；
3. 可輕易更新已分割成專有虛擬伺服器的個別應用程式，因為改變其中一個虛擬伺服器的應用程式，並不會影響其它虛擬伺服器的應用程式<sup>3</sup>。

為了實現實務上的虛擬化，便需要軟件的子層 (sub-layer)，以控制虛擬化程序。該軟件層稱為虛擬機監視器 (Virtual Machine Monitor, VMM)<sup>4</sup>或虛擬機管理程式 (hypervisor)，VMM 有兩個類別：第一個類別是 VMM 直接在硬件中執行，而本身亦可供其它虛擬機器在其上面執行的操作系統，我們稱此類 VMM 為第一類虛擬機管理程式 (Type 1 hypervisor 或 bare-metal hypervisor)，另一類的 VMM 是在事先已存在 (或主機) 的操作系統上，以應用程式模式執行。舉例而言，當用戶在 Windows XP 桌上電腦上執行虛擬 Linux 電腦系統，Windows XP 會被當成主機操作系統 (host operating system)，而我們稱在 Windows XP 上執行的虛擬 Linux (虛擬) 電腦系統為 guest operating system，該類 VMM 也稱為第二類虛擬機管理程式 (Type 2 hypervisor 或 hosted hypervisor)。

---

<sup>1</sup> <http://www.kernelthread.com/publications/virtualization/>

<sup>2</sup> 同上

<sup>3</sup> [http://utilitycomputing.itworld.com/4824/nls\\_windowsserver050411/page\\_1.html](http://utilitycomputing.itworld.com/4824/nls_windowsserver050411/page_1.html)

<sup>4</sup> <http://www.kernelthread.com/publications/virtualization/>

## II. 虛擬化之管理考慮

### 促進虛擬化之因素

如前所述，虛擬化並不是一個新概念，可支援在同一個實體電腦上執行多個操作系統的虛擬化軟件已出現一陣子了，且可在如 Sun Microsystems SPARC 工作站這類舊電腦平台上找到。幾年前，Sun Microsystems 提供 WABI (Windows Application Binary Interface)，讓 Unix 用戶在數個執行 X 視窗系統的 UNIX 操作環境中執行微軟視窗應用程式<sup>5</sup>，但是，因為在有限的 CPU 處理能力下，模擬程序需依賴軟件驅動程式，所以其執行結果並不令人滿意。

隨著今日十億赫 (gigahertz) 速度和多核心 (multi-core) 的 CPU 技術發展，其運轉速度突飛猛進，而這已加速資訊科技市場中虛擬化技術的採用，透過發展和引進多核心 CPU，如 Intel 和 AMD 等供應商已將虛擬化技術帶入其處理器中，該技術使不同的操作系統可以完全像是不同的實體般地運行，Intel 的 Virtualisation Technology (Intel VT) 旨在「*give virtualisation software the ability to take advantage of offloading workload to the system hardware, enabling more streamlined virtualisation software stacks and "near native" performance characteristics*」<sup>6</sup>，意即讓虛擬化軟件把 offloading workload 使用到系統硬件上，使虛擬軟件群運作更有效率及達到接近完美(near native)的表現。許多 Intel Core 2 Duo 處理器已經將 VT 科技整合於晶片結構中，AMD 也發展了 AMD 虛擬化技術(或 AMD-V、或 Pacifica)，也是要達到增加虛擬化應用程式表現的共同目標<sup>7</sup>。

### 虛擬化之優點

虛擬化的核心優點包括：

1. 當轉換到新的操作系統 (OS) 時，管理和支援傳統應用程式 (Legacy Applications) 在資訊科技管理上是一項普遍的問題。虛擬化提供了符合成本效益的解決方案，在操作系統轉換或更新的過渡時期中，重要的傳統應用程式仍可在虛擬環境中繼續運作，直到更新的解決方案推出為止。
2. 虛擬化提供技術支援人員可以快速地轉換到另一個操作系統的環境，以解決模擬和支援所帶來的問題。
3. 虛擬伺服器提供符合成本效益和有效的方法，讓開發者在數個不同平台上測

<sup>5</sup> <http://docs.sun.com/app/docs/doc/802-6306/6ia0mdt48?a=view>

<sup>6</sup> <http://www.intel.com/technology/platform-technology/virtualization/index.htm>

<sup>7</sup> [http://www.amd.com/us-en/Processors/ProductInformation/0,,30\\_118\\_8796\\_14287,00.html](http://www.amd.com/us-en/Processors/ProductInformation/0,,30_118_8796_14287,00.html)

試和移去軟件中的錯誤。

4. 伺服器虛擬化提供實體伺服器合併的機會，減少數據中心之實體伺服器所需的空間和成本。
5. 虛擬化也提供中央控制環境，幫助保護資料安全，降低基於住家的桌上保安考慮或流動工作者的保安考慮。

此外，對終端用戶桌上環境而言，桌上虛擬化更提供管理、彈性和保安上的優勢。

## 管理

在管理桌上電腦時，通常會分配給每一個使用者一台已安裝全部應用程式的桌上電腦。為了預防公司資產遭竊，與確保符合政策和規例，資訊科技經理通常會鎖定這些桌上電腦，以預防終端用戶安裝未經授權的應用程式，或是更改設定，另外應該實施公司政策和標準，包括安裝電腦病毒保護程式，一般操作系統及系統零件如網站瀏覽器之類的修補程式。

然而，要在機構中達到完全符合規定、完全相同和鎖定的桌上環境是不容易的，但是，資訊科技支援小組可透過虛擬化技術來提供事先內建、保安和鎖定的虛擬機器，而該虛擬機器已事先安裝好許可的應用程式，用戶只能透過受控的虛擬機器接達公司資料。

## 彈性

當資訊科技人員持續面對管理能力和保安挑戰之時，終端用戶喜歡對其桌上電腦有更多控制能力<sup>8</sup>，一方面而言，資訊科技經理須維護保安政策並鎖定桌上電腦，以保護員工可接達到的敏感性數據，另一方面而言，終端用戶傾向對其桌上電腦個人化，例如換上喜愛的桌面或應用程式。桌上虛擬化提供解決該難題的解決方案，透過使用虛擬化技術，資訊科技支援小組可提供兩個或許多個可以在用戶實體電腦上運作的操作系統，當公司提供員工被安全鎖定的虛擬機器以便接達公司資料時，可設定第二個環境，以提供更多個人化應用程式和個人設定的控制權給使用者。透過分割這兩個環境，既可保護公司資產，且讓終端用戶更具彈性及可以個人化自己的電腦。

## 保安

如前所述，機構也能使用桌上虛擬化，亦即透過加密檔案夾、預先建立鎖定之桌上環境，來保護因手提電腦失竊而引起的資料外洩<sup>9</sup>，假如手提電腦遭竊，加密檔案夾可減低公司資訊外洩的機會。

---

<sup>8</sup> [http://searchwinit.techtarget.com/originalContent/0,289142,sid1\\_gci1237943,00.html](http://searchwinit.techtarget.com/originalContent/0,289142,sid1_gci1237943,00.html)

<sup>9</sup> 同上

此外，虛擬化有助保安事故處理和運作復原，例如，當視窗伺服器或桌上電腦受 Rootkits 或是惡性軟件（malware）感染時，通常的唯一選擇是清除和重新安裝操作系統，此為痛苦和費時的過程，但在虛擬環境下，受惡性軟件感染的虛擬機器副本可被移除，新的副本可從可信賴資源下載，這樣，一個沒有受感染的虛擬環境<sup>10</sup>可在短時間內便完成修復。

## 虛擬化之缺點

當使用虛擬化技術時，資訊科技經理必須意識到以下缺點：

1. 必須分開管理和修補多個操作系統
2. 因安裝於每一個實體電腦的操作系統數量增加，可能增加管理成本。
3. 為了購買適當的虛擬化產品，必須事先花費一筆投資，並增加企業內安裝操作系統和應用程式所需的額外許可證成本。

---

<sup>10</sup> <http://www.securityfocus.com/columnists/397/2>

### III. 給資訊科技從業人員有關虛擬化的建議

#### 部署虛擬化

如同我們所指出的，我們可在一個實體硬件系統中直接放置數個虛擬機器，通常會先在實體電腦上安裝虛擬伺服器，然後在主機上下載並安裝客體操作系統。主機在任何時候皆可提供一個以上的虛擬機器，用戶可在多個虛擬機器之間進行轉換，就像從一個視窗應用程式轉換到另一個應用程式一樣。舉例而言，用戶可在其 Apple Macintosh 桌上電腦執行虛擬 Windows XP 操作系統。一般支援此種機制的虛擬化產品是 VMware VM 伺服器、Microsoft Virtual PC 和 Parallels Desktop。

虛擬化也可用於幫助開發員工能快速地部署和測試新應用程式與平台，開發者可在其桌上電腦或伺服器上直接安裝數個虛擬機器，而不用數個實體伺服器來模擬要求測試的產品環境，在更為有效地使用開發和測試環境之前，此可降低硬件和操作系統安裝的成本。

再者，虛擬化也幫助了資訊科技支援人員，以虛擬化技術去模擬企業內終端用戶遇到之問題，支援人員可回答用戶在不同操作系統中執行應用程式所遇到的問題。與其提供執行不同操作系統的所有機器給支援人員，可使用安裝於單一桌上電腦的虛擬機器，方便選擇不同操作系統或應用程式，以執行他們日常的支援服務，這樣較提供大量機器來執行不同操作系統的方法更加方便。

#### 保安威脅

VMM 軟件也存有錯誤或保安漏洞的可能性，例如有人偵測到 Microsoft Virtual PC 中的保安漏洞，其允許客體操作系統用戶在主機或其它客體操作系統中執行編碼<sup>11</sup>，此漏洞幾乎影響 Microsoft Virtual PC 所有的版本，而需要修補程式以對付該問題。另一個問題是在 1.0.4 版本前的 VMware 伺服器上偵測到尚未具體說明的保安漏洞，在伺服器記錄中記下沒有保護的用戶密碼，這導致未經授權的資訊披露或服務被中斷<sup>12</sup>。

儘管桌上虛擬化提供了許多保安上的優點，應該定期對虛擬化軟件執行最新保安修補程式之一般實務作業。

---

<sup>11</sup> <http://www.microsoft.com/technet/security/bulletin/MS07-049.msp>

<sup>12</sup> <http://nvd.nist.gov/nvd.cfm?cvename=CVE-2007-5619>

此外，虛擬化並不會刪除在任何客體操作系統中找到的一般保安漏洞，應執行和維護主機的操作系統上個別抗電腦病毒軟件、防火牆或其它必要的保安修補程式管理，以達到保安標準的要求。

## IV. 結論

虛擬化技術雖有其悠久歷史，但以這技術的大型部署並不那麼普及。然而，假如要在企業內部署虛擬環境，應該注意以下幾點：

1. 虛擬機器環境提供隔離的環境，不同的虛擬機器如同多個獨立而共存的電腦，但隔離的程度便依賴於如何推行虛擬化技術。一般而言，不應該使虛擬客體操作系統的設定影響其它客體操作系統的運作。
2. 為避免敏感資料儲存於虛擬機器，應推行標準保安最佳作業實務，以保護虛擬機器平台的完整性。例如，儲存虛擬機器於加密檔案夾，如此，客體操作系統和其數據也隨之自動加密。
3. 如同其它操作系統，虛擬機器也應強化及定期執行保安修補程式。

當享受同一個實體單位上數個虛擬機器共存所帶來的便利時，機構應定期檢視有關虛擬機器的保安政策和措施，因為新的威脅會隨著虛擬化技術部署的普及化而出現。