系統程式-期中報告

翁瑋泓

虛擬機研究

目錄

[虛擬機 (Virtual Machine) 的基本原理 2](#_Toc40380101)

[虛擬機的基本名詞與類型 4](#_Toc40380102)

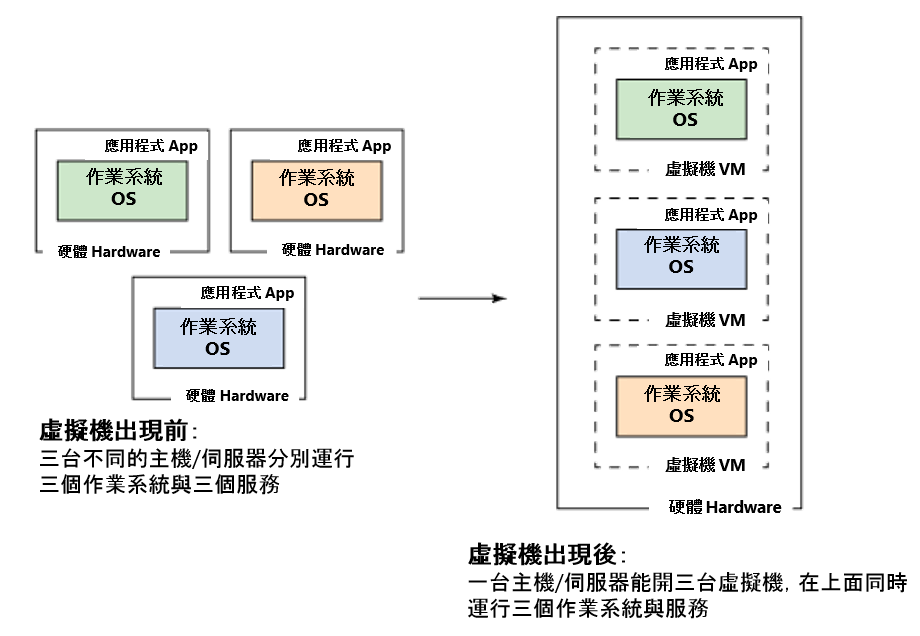
[QEMU介紹 5](#_Toc40380103)

## 虛擬機 (Virtual Machine) 的基本原理

根據「切割硬體資源進行彈性分配」與「安全的系統測試環境」等需求的背景下，，IBM 開發出了「**虛擬機**」(Virtual Machine) 作為解方。

運用軟體技術、如 CPU 排程與虛擬記憶體，作業系統就能創造出一個多處理程式的假象：每個程式都具備自己的記憶體 (雖然是虛擬的)，且在屬於自己的處理器上面運作。

也就是**藉由軟體虛擬技術，提供一個與底層硬體功能一模一樣的介面**，這樣系統就能為每個程式都提供了一份底層硬體的 Copy，稱為虛擬機 (Virtual Machine)。簡單來講，就是用軟體技術模擬出一個硬體的環境。



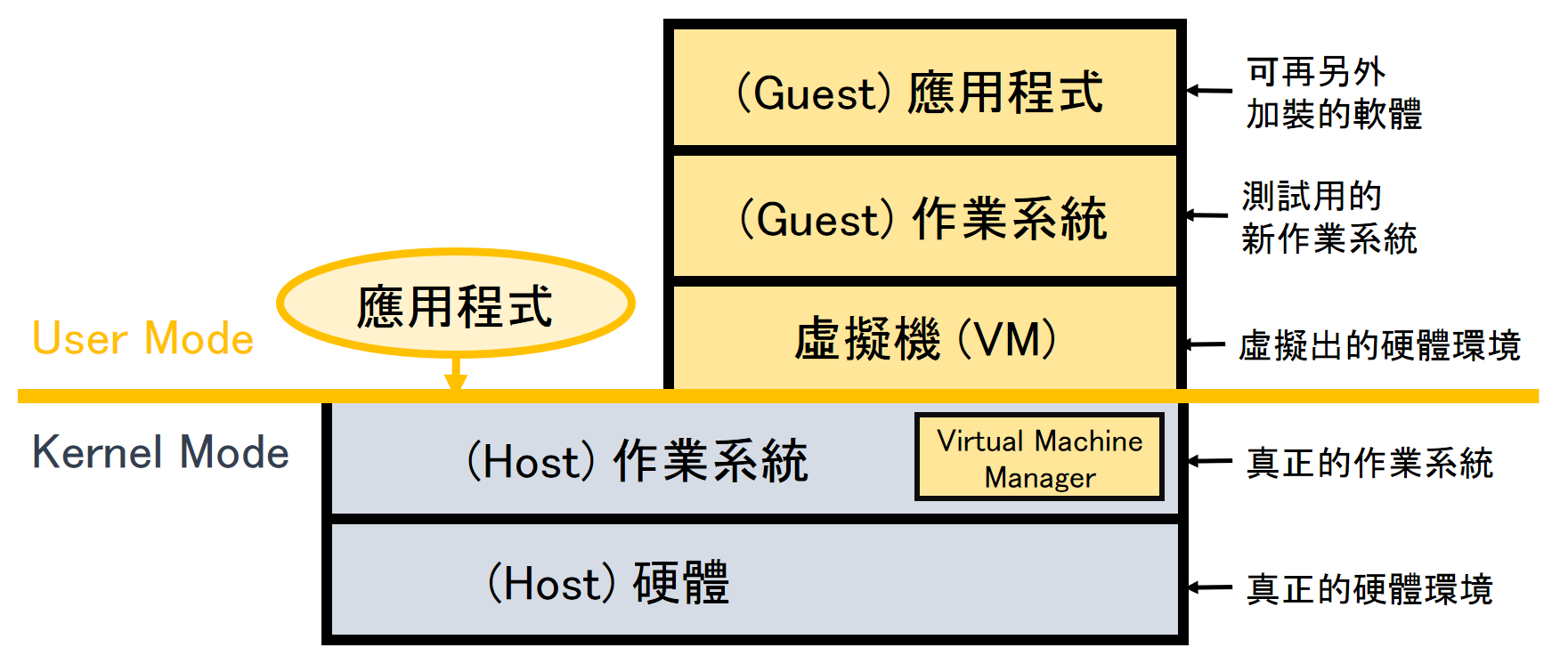
若用更好懂一點的比喻… 現在你有一台實體電腦，可以視為鳴人的本體 (硬體, Host Hardware)。

透過影分身之術 (虛擬化, Virtualization) 變出來分身 (虛擬機, Virtual Machine)，共享鳴人這個單一的實體資源、查克拉都是源於鳴人。但把其中一個影分身打倒，並不會傷到鳴人本身。



## 虛擬機的基本名詞與類型

虛擬機的基本名詞



###### **Host (鳴人的查克拉)**

實際的作業系統和硬體環境。(Underlying hardware system or Operating System)

###### > **Virtual Machine Manager (鳴人的影分身忍術)**

簡稱 VMM、又叫 Hypervisor，用以建立，並管理、執行虛擬機的模組。

###### > **VIRTUAL MACHINE (鳴人的影分身)**

透過 VMM 創造出來、模擬底層硬體 (鳴人本人) 的軟體。

###### > **Guest (鳴人的分身用來打架或做事)**

運行在虛擬機上的作業系統或軟體程式。(Process provided with virtual copy of the host)

## QEMU介紹

QEMU（quick emulator）是一款由Fabrice Bellard等人編寫的免費的可執行硬體虛擬化的（hardware virtualization）開源代管虛擬機器（VMM）。

QEMU是一個代管的虛擬機器鏡像，它通過動態的二進位轉換，類比[CPU](https://zh.wikipedia.org/wiki/CPU)，並且提供一組裝置模型，使它能夠執行多種未修改的客戶機OS，可以通過與[KVM](https://zh.wikipedia.org/wiki/KVM)（kernel-based virtual machine開源加速器）一起使用進而接近本地速度執行虛擬機器（接近真實電腦的速度）。

## 系統模組

QEMU有多種模式[1]

User mod：又稱作「使用者模式」，在這種模組下，QEMU執行針對不同指令編譯的單個Linux或Darwin/macOS程式。系統呼叫與32/64位元介面適應。在這種模式下，我們可以實現交叉編譯（cross-compilation）與交叉偵錯（cross- debugging）。

System mod：「系統模式」，在這種模式下，QEMU類比一個完整的電腦系統，包括外圍裝置。它可以用於在一台電腦上提供多台虛擬電腦的虛擬主機。 QEMU可以實現許多客戶機OS的啟動，比如x86，MIPS，32-bit ARMv7，PowerPC等等。

KVM Hosting：QEMU在這時處理KVM鏡像的設定與遷移，並參加硬體的仿真，但是客戶端的執行則由KVM完成。

Xen Hosting：在這種代管下，客戶端的執行幾乎完全在Xen中完成，並且對QEMU封鎖。QEMU只提供硬體仿真的支援。