

發明專利說明書

(本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※ 申請案號：96115773

※ 申請日期：96 年 5 月 3 日

※IPC 分類：G06F 9/44 (2006.01)

一、發明名稱：(中文/英文)

在執行中作業系統下啟動超管理器之電腦程式產品和方法

LAUNCHING HYPERVISOR UNDER RUNNING OPERATING
SYSTEM

二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

美商·微軟公司

Microsoft Corporation

代表人：(中文/英文)

艾華那諾爾 D 巴特萊

EPPENAUER, D. BARTLEY

住居所或營業所地址：(中文/英文)

美國華盛頓州列德蒙微軟路 1 號

One Microsoft Way, Building 8, Redmond, WA 98052-6399, U.S.A.

國 籍：(中文/英文)

美國/USA

三、發明人：(共 4 人)

姓 名：(中文/英文)

1. 千古立蘇瓦巴特/GANGULY, SHUVABRATA

2. 多頓安德魯 J/THORNTON, ANDREW J.

3. 偉德韓約翰 F/WIEDERHIRN, JOHN F.

4. 雷肯尼斯 D/RAY, KENNETH D.

國 籍：(中文/英文)

1. 印度/INDIA
2. 英國/UK
3. 美國/USA
4. 美國/USA

四、聲明事項：

☐ 主張專利法第二十二條第二項 ☐ 第一款或 ☐ 第二款規定之事實，其事實發生日期為： 年 月 日。

☒ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☒ 有主張專利法第二十七條第一項國際優先權：

美國；2006 年 5 月 15 日；11/383,455

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

國 籍：(中文/英文)

1. 印度/INDIA
2. 英國/UK
3. 美國/USA
4. 美國/USA

四、聲明事項：

☐ 主張專利法第二十二條第二項 ☐ 第一款或 ☐ 第二款規定之事實，其事實發生日期為： 年 月 日。

☒ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☒ 有主張專利法第二十七條第一項國際優先權：

美國；2006 年 5 月 15 日；11/383,455

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明係有關於一種在執行中作業系統下啟動超管理器之電腦程式產品和方法。

【先前技術】

作業系統的一項主要功能是與計算系統上的實體資源介接。典型的作業系統可防衛防止以不正當方式存取實體資源，例如：當一個應用程式正在使用記憶體의特定區段，作業系統會保護該記憶體區段避免遭到相同作業系統所管理的其他應用程式修改。否則應用程式無法如預期產生作用。這種存取防衛通常以作業系統為計算系統上運行的唯一作業系統之假設。

不過，有時候可在相同計算系統上運行多重作業系統。在該情況下，每個作業系統內確保安全作業資源的暗中保護可能不再足夠。作業系統可能無法控制其他作業系統存取相同實體資源，並且甚至沒有機制可以知道存在其他運行中的作業系統。

超管理器屬於一種軟體層，其經設置成介於一或更多個運行中作業系統與受保護的實體資源(像是處理器、I/O連接埠、記憶體、岔斷等等)之間。超管理器加倍保護作業系統中的實體資源，並且以虛擬化方式將資源顯示給每個作業系統。例如，針對簡單範例，假設在具有一個處理器以及 1GB(Gigabyte)隨機存取記憶體(Random Access

Memory, RAM)的計算系統上運行兩套作業系統，超管理器可自行將一半處理器週期配置給每個作業系統，並且將一半記憶體(512 MB(Megabyte) RAM)配置給每個作業系統。更進一步，超管理器可提供定址給每套作業系統的RAM虛擬範圍，如此就像是每套作業系統都只有512 MB RAM可用。

當作業系統嘗試與實體資源通訊或反之，超管理器執行適當的緩衝與轉換，以允許每套作業系統體驗到其環境，猶如其為計算系統上所運行的唯一作業系統。更進一步，超管理器以計算系統上的實體資源即使受到保護也可讓多套作業系統共享之方式來達成此目的。

傳統上，超管理器會在運行作業系統之前啟動。這讓超管理器利用呈現出實體資源的虛擬狀態來在虛擬機器內啟動作業系統。為了立即在虛擬機器內啟動作業系統，超管理器包括用於發現實體資源及其基本特性的擴充碼(extensive code)。因為實體資源發現是在任何運行的作業系統之前完成，所以作業系統無法依靠此發現處理。因此，超管理器內用於發現實體資源的程式碼相當複雜。

【發明內容】

雖然本發明的原理並不受限於本發明說明內彙總的具體實施例，其間說明的某些具體實施例係關於在已經有一運行作業系統之後，一超管理器的啟動步驟。雖然不要求，不過還是可使用運行中的作業系統取代超管理器來發現在

計算系統上運行的實體資源。如此，若想要的話，超管理器可依賴作業系統發現資源，而不是擁有執行相同功能的程式碼。

本發明內容用於導入簡單形式中概念的選擇，在底下實施方式中有進一步說明。本發明內容並不在於識別所主張標的之關鍵特色或基本特色，也不在於用來幫助決定所主張標的之範圍。

【實施方式】

根據本發明的具體實施例，超管理器可在已經有運行中的作業系統之後啟動。可使用運行中的作業系統取代超管理器來發現在計算系統上運行的實體資源。在超管理器已經運作之後可啟動其他作業系統。首先將參閱第 1 圖說明其中可實現本發明原理的一般計算環境。然後將參閱後續圖式進一步說明有關本發明具體實施例的細節。

此時計算系統增加出許多型態，計算系統可例如為手持裝置、設備、膝上型電腦、桌上型電腦、主機電腦、分散式計算系統或甚至是並非一般考量的計算系統之裝置。在此說明與申請專利當中，術語「計算系統」廣泛定義為包含其中內含至少一個處理器以及記憶體（其具有處理器可執行的電腦可執行指令）之任何裝置或系統（或其組合）。記憶體可為任何形式，並且可取決於計算系統的天性與形式。計算系統可透過網路環境散佈，並且可包含多重構造計算系統。

請參閱第 1 圖，在其最基本的組態中，計算系統 100 通常包含至少一處理單元 102 以及記憶體 104。記憶體 104 可為實體系統記憶體，其可為揮發性、非揮發性或這兩者的組合。揮發性記憶體的範例包含隨機存取記憶體 (RAM)。非揮發性記憶體的範例包含唯讀記憶體 (Read Only Memory, ROM)、快閃記憶體等等。此處也用術語「記憶體」來稱呼非揮發性大量儲存元，像是實體儲存媒體。這種儲存元可為可移除式或不可移除式，並且可包含(但不受限於) PCMCIA 卡、磁碟與光碟、磁帶等等。

如此處所使用，「模組」或「組件」等詞可為在計算系統上執行的軟體物件或例式。此處所說明的不同組件、模組、引擎以及服務都可為在計算系統上實施的物件或處理(例如當成個別處理緒)。雖然此處說明的系統與方法可在軟體內實施、在硬體內實施並且也可能並預期在軟體與硬體組合內實施。

在接下來的說明中，將參考由一或更多計算系統所執行的步驟來說明本發明具體實施例。若這種步驟在軟體內實施，則執行步驟的相關計算系統之一或更多個處理器會指引計算系統的作業，來回應已經執行的電腦可執行指令。這種作業的範例牽涉到資料的操縱。電腦可執行指令(以及操縱的資料)都可儲存在計算系統 100 的記憶體 104 內。

計算系統 100 也可包含讓計算系統 100 可透過像是網路 110 與其他計算系統通訊之通訊通道 108。通訊通道 108

為通訊媒體的範例。通訊媒體一般具體實施電腦可讀取指令、資料結構、程式模組或其他調變資料信號內的資料，像是載波或其他傳輸機構並且包含任何資訊傳遞媒體。藉由範例並且不受限於此範例，通訊媒體包含像是有線網路或直接有線連線的有線媒體，以及像是聲音、無線電、紅外線以及其他無線媒體的無線媒體。此處所使用的術語「電腦可讀取媒體」包含儲存媒體以及通訊媒體。

本發明範疇內的具體實施例也包含攜帶或具有電腦可執行指令或其上所儲存資料結構的電腦可讀取媒體。這種電腦可讀取媒體可為一般用途或特殊用途電腦可存取的任何可用媒體。藉由範例並且不設限，這種電腦可讀取媒體可包含實體儲存元以及/或記憶體媒體，像是 RAM、ROM、EEPROM、CD-ROM 或其他光碟儲存元、磁碟儲存元或其他磁性儲存裝置，或可用於以電腦可執行指令或資料結構型態攜帶或儲存所要程式碼並且可由一般用途或特殊用途電腦存取之其他任何媒體。當資訊透過網路或其他通訊連線(有線、無線或有線與無限的組合)傳輸或提供給電腦，電腦會適當將連線看待成電腦可讀取媒體。如此，任何這種連線都適當看待為電腦可讀取媒體。上述組合也應該包含在電腦可讀取媒體的範疇內。

電腦可執行指令包含例如導致一般用途電腦、特殊用途電腦或特殊用途處理裝置執行特定功能或功能群組的指令與資料。雖然以特定結構特色語言以及/或方法步驟來說明所主張標的，吾人可瞭解，後附申請專利範圍內所定義

的主張標的並不必然受限於此處的特定特色或步驟。而此處的特定特色與步驟僅當成用於實施申請專利範圍之範例型式。

第 2 圖說明運行中作業系統啟動超管理器的方法 200 之流程圖。在此說明與申請專利範圍內，「超管理器」為一軟體層，其係設置成於一或更多執行中作業系統與受保護實體資源之間所佈置。該超管理器將該等作業系統中的受保護實體資源予以功能性地多工，並且以虛擬化方式將資源顯示給每個作業系統。如此，超管理器當成作業系統與計算系統實體資源之間的特殊種類抽象層。

例如，針對簡單範例，假設在具有一個處理器以及 1GB 隨機存取記憶體 (RAM) 的計算系統上運行兩套作業系統，超管理器可自行將一半處理器週期配置給每個作業系統，並且將一半記憶體 (512 MB RAM) 配置給每個作業系統。更進一步，超管理器可提供定址給每套作業系統的 RAM 虛擬範圍，如此就像是每套作業系統都只有 512 MB RAM 可用。當作業系統嘗試與實體資源通訊或反之，超管理器執行適當的緩衝與轉換，以允許每套作業系統體驗到其環境，猶如其為計算系統上唯一運行的作業系統。

不像傳統超管理器組態，本發明具體實施例在已經啟動作業系統之後才啟動超管理器，即使作業系統已經發現計算系統的實體資源也一樣。啟動超管理器的作業系統將所發現的實體資源狀態資訊傳遞給超管理器，如此超管理器不需要個別程式碼來發現計算系統的實體資源。

一旦作業系統啟動超管理器並將有關所發現的計算系統實體資源之資訊傳遞給超管理器，則作業系統會暫停執行並將控制權交給超管理器。然後超管理器設定虛擬機器實體來控制未來對於計算系統實體資源的任何受保護資源之存取要求。虛擬機器實體以和受保護實體資源的作業系統概念一致之狀態初始化。當達成此狀態，作業系統會在虛擬機器環境內繼續。不過，在虛擬機器環境內，作業系統透過超管理器與實體資源介接，而非直接介接。因為專門與作業系統通訊的虛擬機器得知該作業系統已於先前發現有關實體資源的資訊，所以該改變對作業系統而言為透明 (transparent)。

在某些情況下以及對於某些受保護的實體資源而言，在不使用超管理器之下不可能讓作業系統發現受保護的實體資源，然後稍後透過超管理器以通透方式間接與相同受保護的實體資源介接。在該情況下，作業系統可經設置成瞭解到稍後會透過超管理器來作業，如此忽略稍後無法用通透方式虛擬化的任何實體資源。例如：作業系統載入器可經設置成通知其他作業系統組件不要使用特定受保護的實體資源。

回頭參閱第 2 圖，當啟動根作業系統後(步驟 201)開始方法 200。一「根」作業系統為啟動超管理器的作業系統，相對於可在超管理器運作之後啟動的作業系統。第 4A 圖說明此作業階段上的組態 400A，其中作業系統 401 在缺少超管理器的情況下直接 404 與計算系統的實體資源 402

通訊。

然後根作業系統執行許多第 2 圖的左欄「根作業系統」標題之下的步驟。例如：根作業系統發現至少一個實體資源(步驟 211A)。作業系統通常具有在啟動作業系統之後立刻執行的指令，來發現計算系統的實體資源。請參閱第 4A 圖，例如作業系統 401 發現實體資源狀態 403。發現計算系統的實體資源是一項複雜的工作。

為了在超管理器啟動之前的狀態下恢復作業系統，作業系統會在啟動超管理器之前擷取實體機器的狀態。在一個具體實施例內，擷取的狀態包含所有實體處理器與實體 APIC 的狀態。實體處理器狀態包含：

1. 一般用途暫存器。
2. 浮點與 XMM 緩衝器。
3. 控制暫存器 (Control Register, CR)。
4. 偵錯暫存器 (Debug Register, DR)。
5. 指令指示器(RIP)、堆疊指示器(RSP)以及旗標暫存器(RFLAGS)。
6. CS、DS、SS、ES、FS、GS 以及 TR 區段的區段狀態，包含區段基座、限制以及存取權限。
7. 全域描述器表格暫存器(Global Descriptor Table Register, GDTR)、中斷描述器表格暫存器(Interrupt Descriptor Table Register, IDTR)以及本機描述器表格暫存器(Local Descriptor Table Register, LDTR)。
8. 某模型特定暫存器 (Model Specific Register,

MSR)，其包含 KemeIgsBase、Star、Lstar、Cstar、Sfinask、SysenterCs、SysenterEip、SysenterEsp 以及 ApicBase MSR。

實體本機 APIC 狀態包含：

1. 本機 APIC ID
2. 高要求暫存器 (hi-Request-Register, IRR)
3. 高服務暫存器 (hi-Service-Register, ISR)
4. 工作優先權暫存器 (Task Priority Register, TPR)

此外，當超管理器已啟動時，某些其他硬體態樣可提供給超管理器當成根參數。這可包含：

1. 目前與潛在邏輯處理器，包含可能在執行時間上熱插拔的處理器
2. BIOS 內的超執行緒 (hyperthreading) 是否啟用或停用
3. 目前的實體 RAM 範圍 - 在超管理器開機時用 RAM 傳播的系統實體位址範圍
4. 實體節點 (包含在開機時無相關資源但是在執行時間上傳播的那些節點)
5. 實體節點之間的記憶體存取率
6. 超管理器必須存取的特定硬體功能之位址 (例如電源管理計時器)

作業系統也啟動該於作業系統與實體資源之間所插入的超管理器 (步驟 211B)。例如：請參閱第 4B 圖，超管理器 405 插入根作業系統 401 與實體資源 402 之間。針對此啟動部分，作業系統提供要保護的至少實體資源的狀態資

訊給超管理器(步驟 212)。此狀態資訊包含關於超管理器必須發現由超管理器所防衛之受保護實體資源的相關狀態的所有資訊。在一個具體實施例內，狀態資訊可包含上述的擷取狀態。至少，狀態資訊包含至少對應的實體資源之識別。

另外，針對啟動部分，作業系統將控制權傳遞給超管理器。然後超管理器執行第 2 圖右欄「超管理器」標題下的步驟。尤其是，超管理器執行需要將計算系統受保護的實體資源虛擬化至根作業系統所需之工作(步驟 221)。

例如：超管理器可建立用於根作業系統的虛擬機器實體(步驟 231)。請參閱第 4B 圖，區塊 421 表示用於作業系統 401 的虛擬機器實體。一旦初始化並作業，虛擬機器實體 421 將當成用於作業系統 401 的實體資源 402 之代理主機。虛擬機器實體 421 將接收來自作業系統 401 用於實體資源的服務要求，並且將根據虛擬機器實體 421 可存取的狀態資訊來執行要求的適當轉換與緩衝。然後虛擬機器實體 421 將導致超管理器 405 要求來自實體資源 402 的適當服務。虛擬機器實體 421 也將潛在地依照需求以適當轉換與緩衝方式將需求結果回報給作業系統 401。

虛擬機器實體 421 將根據虛擬機器實體可存取的狀態資訊而有不同行為。超管理器知道作業系統 401 已經發現有關實體資源 402 的狀態資訊。因此，超管理器 405 用作業系統提供的至少某些狀態資訊將虛擬機器實體 421 初始化(步驟 232)。例如：超管理器 405 可使用作業系統提供

的擷取狀態將虛擬機器初始化。在此方式中，虛擬機器實體 421 使用與代表作業系統所偵測實體資源的資訊一致之狀態來初始化。然後作業系統在虛擬機器環境內恢復(步驟 233 和步驟 214)。在此環境內，如第 4B 圖內所示，取代作業系統 401 直接與實體資源 402 介接，透過使用虛擬機器實體 421 與超管理器 405 將實體資源 402 虛擬化給作業系統 401。因為虛擬機器 421 所使用的狀態資訊與作業系統 401 所發現的狀態資訊一樣，則在某些具體實施例內之變更對於作業系統 401 為透明。

在一個具體實施例內，透過模擬實體處理器行為的虛擬處理器概念提供虛擬化。類似地，其提供模擬實體 APIC 行為的虛擬 APIC。這達成下列狀況：

1. 虛擬處理器的狀態已初始化至實體處理器的擷取狀態。
2. 虛擬 APIC 的狀態已初始化至實體本機 APIC 的擷取狀態。
3. 超管理器安裝岔斷以避免作業系統存取特權實體硬體資源。例如：在啟動超管理器之前已經定位的本機 APIC 之用戶實體位址標示成不存在，如此對於本機 APIC 的所有存取權限都派給超管理器。

在超管理器已經啟動之後，超管理器可啟動額外的作業系統、相同作業系統的實施例或不同作業系統的實施例。例如，請參閱第 4C 圖，由橢圓 414 所表示的作業系統 412 和 413 可另外啟動。第 3 圖說明將實體資源虛擬化

至額外作業系統的方法 300 之流程。當啟動額外的作業系統，超管理器首先啟動對應的虛擬機器實體(步驟 301)，然後透過此實體啟動作業系統(步驟 302)。超管理器使用對應的虛擬機器實體將實體資源虛擬化至對應的額外作業系統(步驟 303)。

當每套作業系統在作業系統啟動時執行實體資源發現，則對應的虛擬機器實體會攔截許多資訊要求。取代找出實體資源相關的實際狀態資訊，對應的虛擬機器提供虛擬狀態資訊給作業系統。

有時候，啟動超管理器的作業系統可在不同的環境類型內。例如：作業系統可能在 32 位元模式內作業，其中正準備啟動的超管理器要在 64 位元模式內作業，或者反之。類似地，作業系統以及超管理器可在不同的傳呼模式內作業。本發明的某些具體實施例允許即使在作業系統與超管理器在不同環境內作業，作業系統也可啟動超管理器。第 5 圖說明讓作業系統進入超管理器環境來準備啟動超管理器的方法 500 之流程圖。從第 5 圖內其中已啟動作業系統的步驟 201 內，作業系統首先呈現不可動作(inactionable)的任何非可遮罩岔斷(步驟 501)，並且遮罩任何可遮罩的岔斷。非可遮罩岔斷可用許多不同方式呈現為不可動作。之後，當作業系統轉換至超管理器作業環境，應小心確定在載入超管理器的初始狀態之前未發生岔斷或例外。若在離開作業系統環境之後但是在進入超管理器環境之前發生岔斷或例外，因為並無岔斷描述器表或堆疊，所以處理器

將可能無法處理岔斷或例外。因為大多數例外都為軟體所初始，所以可輕易避免。利用清除 RFLAGS 暫存器內之 IF 位元，該可遮罩的硬體岔斷可在此處理期間抑制。

非可遮罩岔斷 (Non-maskable Interrupt, NMI) 可由兩機制抑制：

1. 自行傳遞 NMI 並且不執行 IRET 指令：利用暫時修改作業系統岔斷描述器表內的 NMI 處置器位址來指出不同處置器 (handler)，如此就可達成。然後 NMI 可傳遞至目前的處理器。這將導致處理器跳至提供當成 NMI 處置器的位址。在 NMI 處置器，我們可恢復原始 NMI 處置器位址並繼續。這將有效遮罩進一步 NMI，因為在 x86 架構上，會在接收到 NMI 之後到執行 IRET 指令之前遮罩 NMI。

2. 總是運行有效岔斷描述器表 (Interrupt Descriptor Table, IDT) 以及堆疊：這可利用建立暫時 IDT 和堆疊來達成。暫時傳呼表可對映暫時 IDT、NMI 處置器以及堆疊在其原始虛擬位址上以及個別實體位址上。這確定若當處理器正用暫時傳呼表運行時 NMI 到達，則其可正確傳遞至處置器。

一旦岔斷已遮罩或呈現不可動作 (步驟 501)，則可建立暫時虛擬機器實體 (步驟 502)。然後作業系統使用導致一岔斷的指令來初始化暫時虛擬機器實體 (步驟 503)。岔斷為從作業系統傳輸至超管理器的控制權。當暫時虛擬機器實體恢復 (步驟 504)，虛擬機器實體執行導致岔斷的指令，然後產生岔斷 (步驟 505)。因此，暫時虛擬機器實體

使用超管理器狀態開始執行(步驟 506)，藉此導致作業系統持續在超管理器模式內作業(步驟 507)。然後作業系統可啟動超管理器。視需要，暫時虛擬機器實體遭到摧毀(步驟 508)，因為只需要將作業系統放入啟動超管理器所需的超管理器模式即可。

因此，根據本發明的具體實施例，即使在計算系統上已經有運行中的作業系統之後，還是允許啟動超管理器。在某些具體實施例內，即使作業系統與超管理器在不同環境內作業，作業系統也可啟動超管理器。

本發明可在不悖離其精神或基本特性的其他特定型態內實施。所說明的具體實施例全都當成說明並且不做限制。因此，由下附申請專利範圍來指示本發明範疇而非前述說明。所有位於申請專利範圍的意義與範圍內之所有變更都包含在其範疇內。

【圖式簡單說明】

為了進一步闡明本發明上述以及其他優點與特色，因此將參照附圖內所說明的特定具體實施例來呈現本發明更特定之說明。吾人瞭解，這些圖式只是本發明的典型具體實施例，因此並不對發明範疇產生限制。底下將透過附圖，以更特定以及詳細的方式說明與解釋本發明，其中：

第 1 圖說明其中可運用本發明具體實施例的計算環境；

第 2 圖說明使用運行中作業系統啟動超管理器的方法

流程圖；

第 3 圖說明啟動其他作業系統的方法流程圖；

第 4A 圖說明一組態圖，其中缺少超管理器的根作業系統直接與計算系統的實體資源通訊；

第 4B 圖說明一組態圖，其中作業系統已啟動超管理器來當成作業系統與實體資源之間媒介；

第 4C 圖說明一組態圖，其中其他作業系統已經啟動並且受到超管理器支援；以及

第 5 圖說明將作業系統傳輸至超管理器環境的方法流程圖。

【主要元件符號說明】

100	計算系統	403	實體資源狀態
102	處理單元	404	直接通訊
104	記憶體	405	超管理器
108	通訊通道	412	作業系統
110	網路	413	作業系統
200	方法	414	橢圓
400A	組態	421	虛擬機器實體
401	作業系統	300	方法
402	實體資源	500	方法

五、中文發明摘要：

茲揭示一種在已經有運行中作業系統之後，一超管理器之啟動步驟。該作業系統本身可啟動超管理器。可使用運行中的作業系統而不是超管理器來發現在計算系統上運行的實體資源。在超管理器為運算中之後可啟動其他作業系統或作業系統實體。

六、英文發明摘要：

The launching of a hypervisor after there is already a running operating system. The operating system itself may launch the hypervisor. The running operating system may be used instead of the hypervisor to discover the physical resources running on the computing system. Other operating systems or operating system instances may be launched after the hypervisor is operational.

十、申請專利範圍：

1. 一種包含具有一或更多電腦可執行指令之一或更多電腦可讀取媒體的電腦程式產品，其中當該指令由一計算系統的一或更多處理器執行時，該一或更多電腦可執行指令導致該計算系統去執行一使用一執行中作業系統來啟動一超管理器的方法，該方法包含以下步驟：
一作業系統啟動一超管理器的步驟；以及
該已啟動超管理器將該計算系統的至少一實體資源虛擬化至已啟動該超管理器之作業系統之步驟。
2. 如申請專利範圍第 1 項所述之電腦程式產品，其中該一或更多電腦可讀取媒體為實體記憶體以及儲存媒體。
3. 如申請專利範圍第 1 項所述之電腦程式產品，其中該一或更多電腦可讀取媒體為實體記憶體媒體。
4. 如申請專利範圍第 1 項所述之電腦程式產品，其中該一或更多電腦可讀取媒體為實體儲存媒體。
5. 如申請專利範圍第 1 項所述之電腦程式產品，其中該電腦可執行指令另指示當由該計算系統的一或更多處理器執行時，會導致該計算系統另執行下列：
該作業系統發現至少一實體資源的步驟；以及
該作業系統提供該至少一實體資源的狀態資訊給該超管理器之步驟，該狀態資訊包含至少該對應實體資源的一識別。
6. 如申請專利範圍第 5 項所述之電腦程式產品，其中該

電腦可執行指令另指示當由該計算系統的一或更多處理器執行時，會導致該計算系統另執行下列：

該超管理器啟動一用於該作業系統的虛擬機器實體之步驟；

使用由該作業系統提供的狀態資訊將該虛擬機器實體初始化之步驟；

該超管理器在初始化該虛擬機器實體之後恢復該作業系統之步驟；以及

在該作業系統恢復之後，該超管理器使用該虛擬機器實體將該至少一實體資源虛擬化之步驟。

7. 如申請專利範圍第 6 項所述之電腦程式產品，其中該電腦可執行指令另指示當由該計算系統的一或更多處理器執行時，會導致該計算系統另執行下列於該計算系統上啟動的每一額外作業系統：

該超管理器啟動一用於每一額外作業系統的對應虛擬機器實體之步驟；

在該對應的虛擬機器實體已啟動之後啟動該對應的額外作業系統之步驟；以及

該超管理器使用該對應的虛擬機器實體將該至少一實體資源虛擬化至該對應的額外作業系統之步驟。

8. 如申請專利範圍第 1 項所述之電腦程式產品，其中該電腦可執行指令另指示當由該計算系統的該一或更多處理器執行時，會導致該計算系統另執行下列：

該已啟動超管理器將該計算系統的至少一實體資

源虛擬化至已啟動該超管理器之作業系統之步驟。

9. 如申請專利範圍第 1 項所述之電腦程式產品，其中該電腦可執行指令另包含電腦可執行指令，當該指令由該計算系統的該一或更多處理器執行時，會導致該計算系統執行下列：

該作業系統建立一暫時虛擬機器實體之步驟；

使用產生一岔斷的一指令來初始化該暫時虛擬機器實體之步驟；

在該初始化步驟之後恢復該暫時虛擬機器實體之步驟；

在偵測到來自於該暫時虛擬機器實體的恢復步驟的岔斷結果之後，使用超管理器狀態啟動該暫時虛擬機器實體來作業之步驟。

10. 如申請專利範圍第 9 項所述之電腦程式產品，其中該電腦可執行指令另包含電腦可執行指令，當該指令由該計算系統的該一或更多處理器執行時，會導致該計算系統在建立該暫時虛擬機器實體之前執行下列：

呈現不可動作(inactionable)的任何非遮罩岔斷之步驟。

11. 如申請專利範圍第 9 項所述之電腦程式產品，其中該電腦可執行指令另包含電腦可執行指令，當該指令由該計算系統的該一或更多處理器執行時，會導致該計算系統在使用該超管理器狀態起動該暫時虛擬機器實體之後執行下列：

啟動該超管理器的步驟；以及

摧毀該暫時虛擬機器實體之步驟。

12. 如申請專利範圍第 11 項所述之電腦程式產品，其中該作業系統與該超管理器之一者在 32 位元模式內作業，而該作業系統與該超管理器之其他者在 64 位元模式內作業。

13. 如申請專利範圍第 11 項所述之電腦程式產品，其中該作業系統與該超管理器使用一不同傳呼機制來作業。

14. 一種運用一執行中作業系統來啟動一超管理器之方法，該方法包含以下步驟：

一超管理器從一根作業系統處接收代表複數個該作業系統所偵測實體資源的資訊之步驟；

該超管理器啟動一用於該根作業系統的虛擬機器實體之步驟；

使用與該代表該複數個實體資源的資訊一致之狀態來將該虛擬機器初始化，該複數個實體資源係由該作業系統所偵測；

恢復該根作業系統，如此該根作業系統透過已經使用該狀態初始化的該虛擬機器實體間接與該複數個實體資源介接之步驟。

15. 如申請專利範圍第 14 項所述之方法，另包含下列步驟：

在運行該超管理器之後，啟動一或更多額外作業系統之步驟。

16. 如申請專利範圍第 15 項所述之方法，另包含下列用於該一或更多額外作業系統各者之步驟：

將一對應的虛擬機器實體初始化來與該對應的額外作業系統介接之步驟。

17. 一種包含一或更多電腦可讀取媒體的電腦程式產品，該媒體其上具有：

一作業系統；以及

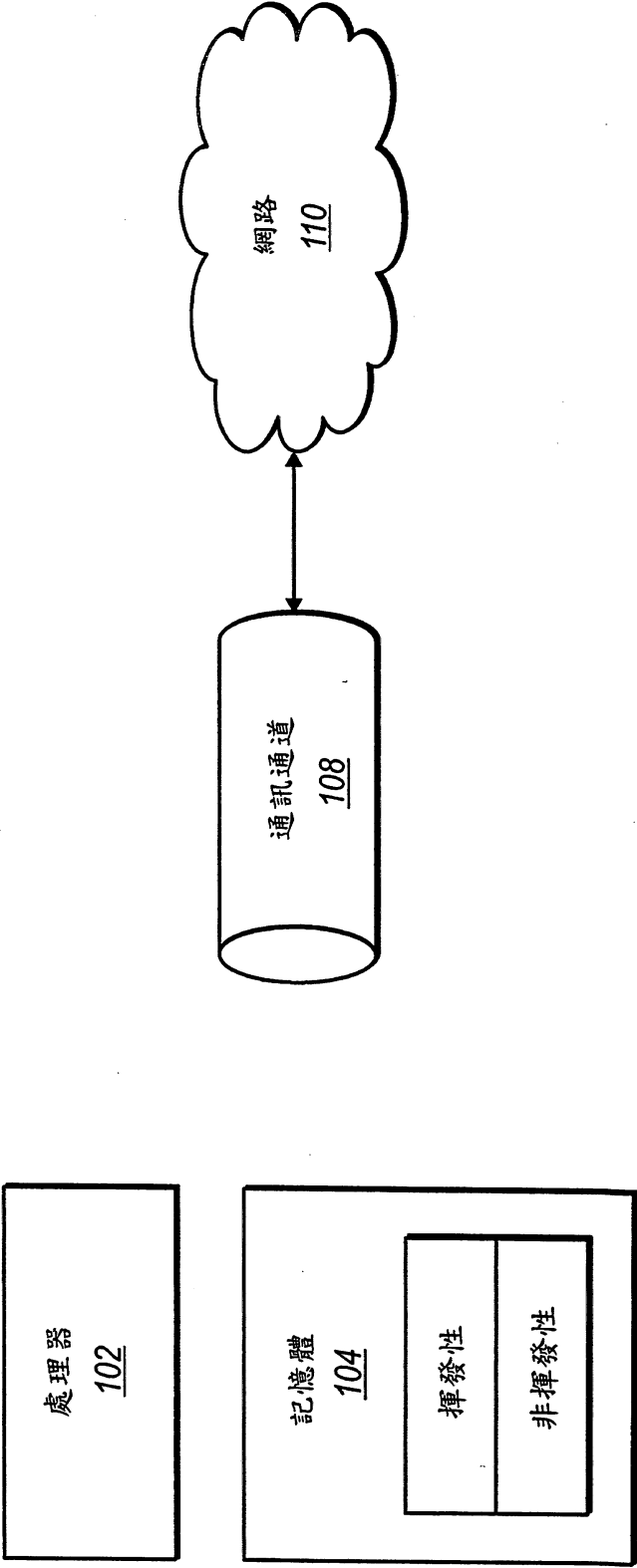
一超管理器，其由該作業系統啟動並且經設置成將該計算系統的至少一實體資源虛擬化至該作業系統。

18. 如申請專利範圍第 17 項所述之電腦程式產品，其中該一或更多電腦可讀取媒體為實體記憶體以及儲存媒體。

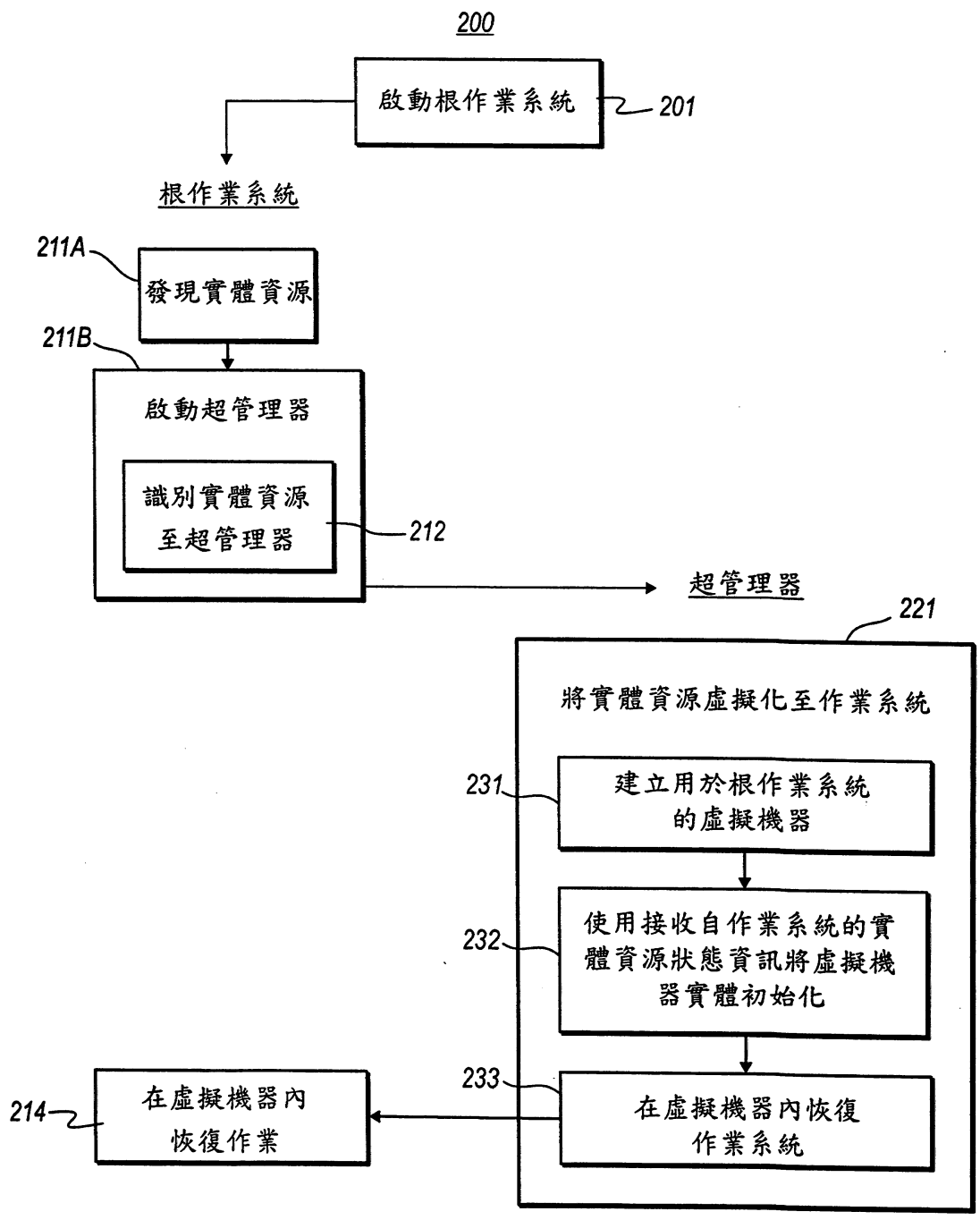
19. 如申請專利範圍第 17 項所述之電腦程式產品，其中該一或更多電腦可讀取媒體為實體記憶體媒體。

20. 如申請專利範圍第 17 項所述之電腦程式產品，其中該一或更多電腦可讀取媒體為實體儲存媒體。

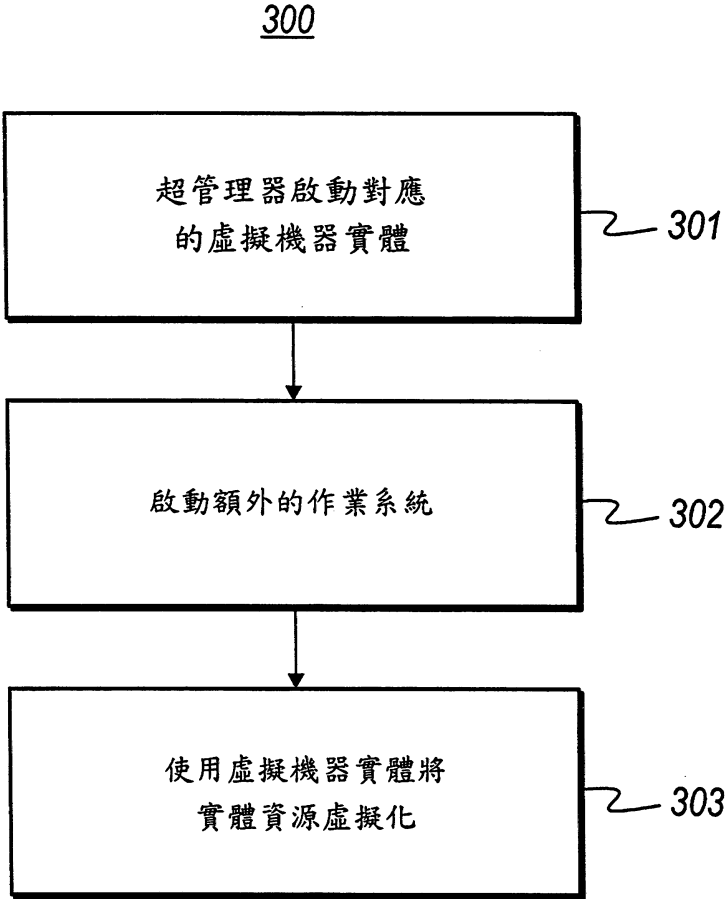
計算系統
100



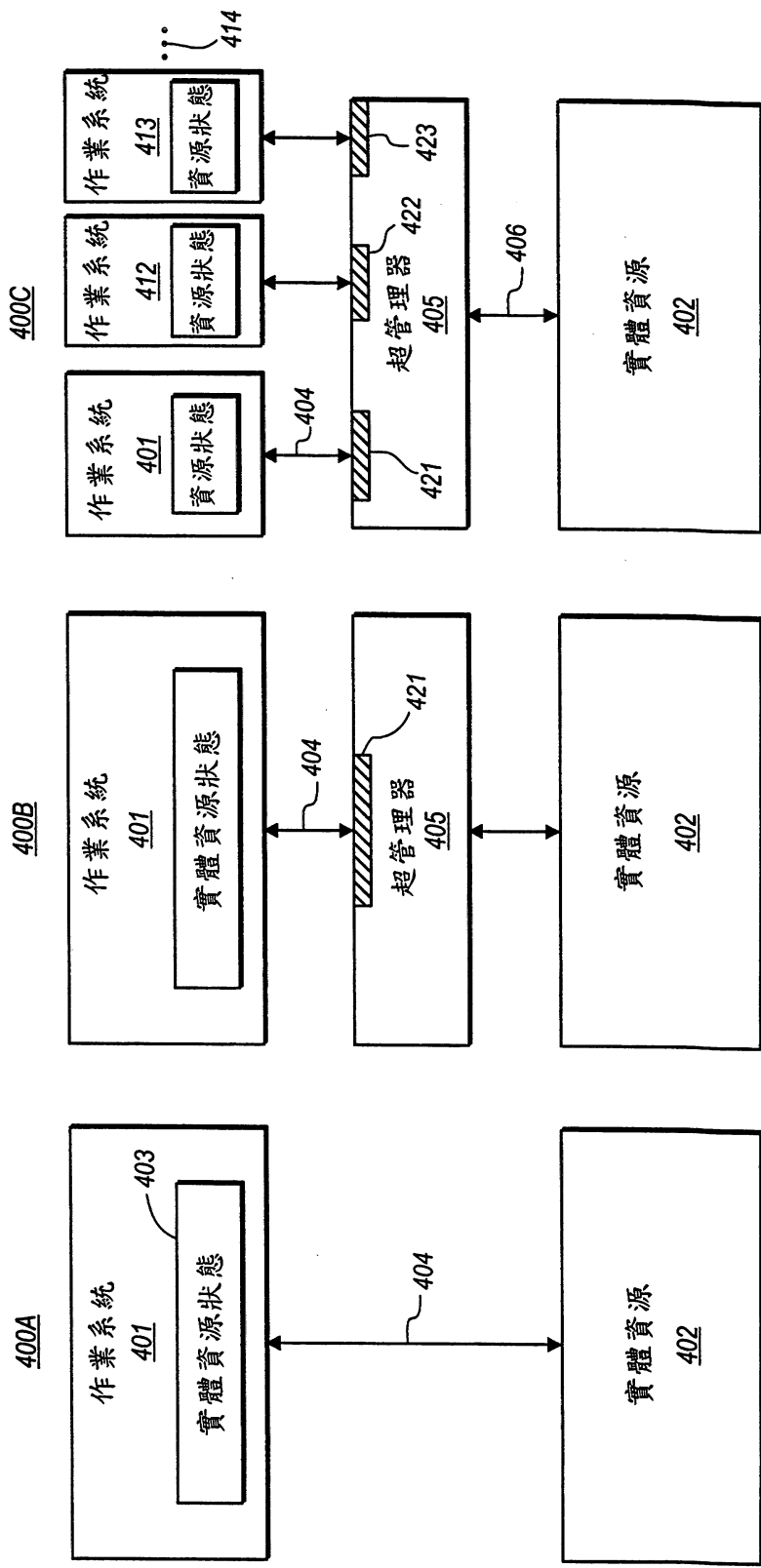
第 1 圖



第 2 圖



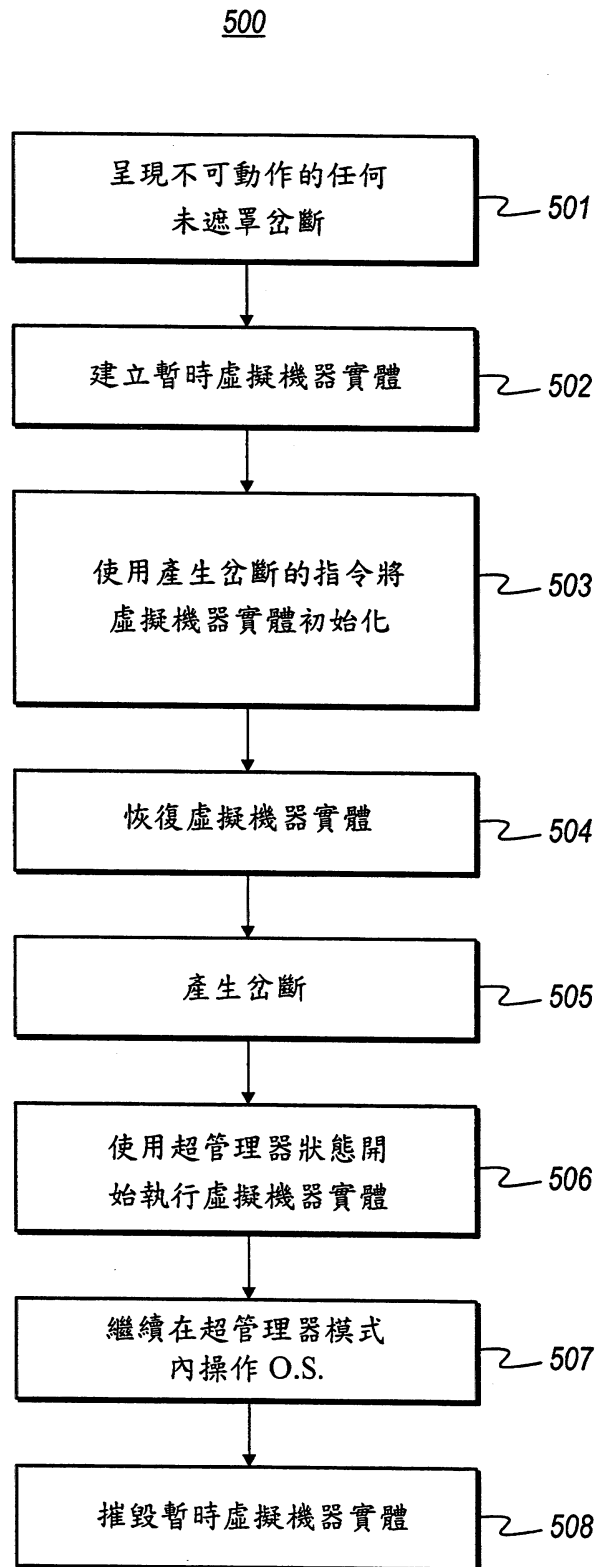
第 3 圖



第 4A 圖

第 4B 圖

第 4C 圖



第 5 圖

七、指定代表圖：

(一)、本案指定代表圖為：第(2)圖。

(二)、本代表圖之元件代表符號簡單說明：

無

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無