**大量啟用規劃指南**

**Windows 7 與 Windows Server 2008 R2**

Microsoft Corporation

發佈日期：2009 年 6 月

摘要

大量啟用能夠協助大量授權客戶將大量授權媒體的啟用程序自動化，並加以管理。大量授權客戶和特殊程式（例如 Microsoft Partner Program、MSDN® 和 Microsoft® TechNet）的訂閱者，都能夠大量授權其軟體和媒體。本指南適用於其組織正在規劃部署大量啟用版本之Windows® 7 與 Windows Server® 2008 R2 作業系統的資訊技術 (IT) 專業人員。

此文件與其中任何參照文件僅供參考之用，Microsoft 不針對此文件進行明示或暗示保證。此文件的資訊（包含 URL 及其他網際網路網站的參考）如有變更，怒不另行通知。使用者必須擔負使用此文件或使用此文件後所導致任何結果的全部風險。除非另有特別說明，否則在此案例中描述的公司、組織、產品、網域名稱、電子郵件位址、標誌、人員、處所及事件皆為虛構。其中未影射任何真實的公司、組織、產品、網域名稱、電子郵件位址、標誌、人員、處所或事件。使用者必須負責遵守所有適用的著作權法。未經 Microsoft Corporation 明確的書面許可，不得針對任何目的或以任何方式或形式（電子、機械、影印、記錄或其他方式）將本文件任何部分予以重製、儲存或放入檢索系統或予以傳送，此規定未限制著作權許可之權利。

Microsoft 可能擁有本文件所提及內容中所含之專利權、專利申請權、商標、著作權或其他智慧財產權。除非 Microsoft 書面授權合約明確規定者外，提供本文件並未授予貴用戶上述專利權、商標、著作權或其他智慧財產權。

© 2009 Microsoft Corporation。保留所有權利。

Microsoft、Active Directory、Hyper-V、MSDN、Windows、Windows 標誌、Windows Server、Windows Vista 和 Windows Web Server 為 Microsoft 公司集團的商標。

此文件提及的實際公司及產品的名稱為個別擁有者的商標。

**內容**

[簡介 5](#_Toc231550947)

[瞭解產品啟用 6](#_Toc231550948)

[啟用選項 6](#_Toc231550949)

[零售 6](#_Toc231550950)

[原始設備製造商 7](#_Toc231550951)

[大量授權 7](#_Toc231550952)

[大量啟用模式 8](#_Toc231550953)

[金鑰管理服務 8](#_Toc231550954)

[多重啟用金鑰 9](#_Toc231550955)

[萬一未啟用系統該怎麼辦？ 9](#_Toc231550956)

[限定期限 9](#_Toc231550957)

[限定期限到期 10](#_Toc231550958)

[產品金鑰 10](#_Toc231550959)

[檢視可用的啟用模式 11](#_Toc231550960)

[金鑰管理服務 11](#_Toc231550961)

[最低電腦需求 11](#_Toc231550962)

[KMS 的運作方式 13](#_Toc231550963)

[規劃 KMS 部署 15](#_Toc231550964)

[多重啟用金鑰 18](#_Toc231550965)

[大量啟用管理工具 18](#_Toc231550966)

[MAK 架構 19](#_Toc231550968)

[評估用戶端連線能力 20](#_Toc231550969)

[核心網路 23](#_Toc231550970)

[隔離網路 23](#_Toc231550971)

[高安全性區域 23](#_Toc231550972)

[分公司位置 25](#_Toc231550973)

[未連接的個別電腦 26](#_Toc231550974)

[測試和研發實驗室 27](#_Toc231550975)

[將電腦對應至啟用方法 28](#_Toc231550976)

[決定產品金鑰的需求 29](#_Toc231550977)

[選擇 MAK 產品金鑰群組 30](#_Toc231550978)

[選擇 KMS 金鑰 31](#_Toc231550979)

[選擇 KMS 主機 33](#_Toc231550980)

[決定監控與報告的需求 35](#_Toc231550981)

[Windows Management Instrumentation 35](#_Toc231550982)

[System Center Configuration Manager 35](#_Toc231550983)

[事件記錄檔 35](#_Toc231550984)

[KMS 管理組件 36](#_Toc231550985)

[大量啟用管理工具 36](#_Toc231550986)

[附錄 A：傳送至 Microsoft 的資訊 37](#_Toc231550987)

[附錄 B：授權狀態 38](#_Toc231550988)

[已啟用 39](#_Toc231550989)

[限定期限 39](#_Toc231550990)

[正版 39](#_Toc231550991)

[通知 40](#_Toc231550992)

# 簡介

大量啟用是一種可設定的解決方案，能夠協助 IT 專業人員將執行根據 Microsoft® 大量授權方案和其他提供 Windows 大量授權版本之方案所授權的 Windows Vista®、Windows® 7、Windows Server® 2008 與 Windows Server 2008 R2 作業系統之電腦的產品啟用程序自動化，並加以管理。本指南提供規劃步驟和實例以協助規劃大量啟用部署，尤其是 Windows 7 與 Windows Server 2008 R2 作業系統。

**注：**此文件提供 Windows 7 與 Windows Server 2008 R2 作業系統的大量啟用規劃指南。然而本指南亦說明兩世代產品之間的互通性。如需為 Windows Vista 與 Windows Server 2008 規劃大量啟用的詳細資訊，請參閱 Microsoft 網站上的《Volume Activation 2.0 技術指南》(<http://go.microsoft.com/fwlink/?LinkID=75674>)。

大量啟用部署包含以下步驟：

1. 瞭解產品啟用。
2. 檢視可用的啟用模式。
3. 評估用戶端連線能力。
4. 將實體電腦或虛擬機器對應至啟用方法。
5. 決定產品金鑰的需求。
6. 決定監控與報告的需求。

# 瞭解產品啟用

產品啟用 是向製造商驗證軟體的程序。啟用可確認產品確為正版且產品金鑰未遭洩漏。這與啟用信用卡或全新的行動電話類似。啟用可在軟體產品金鑰及裝置上安裝的特定軟體間建立關聯性。

Microsoft 使用的所有啟用方法均是為了協助保護使用者的隱私權。在啟用期間傳送的資料不會追蹤至電腦或使用者。收集的資料是要用來確認軟體為合法的授權版本，然後進行彙總用於統計分析。Microsoft 不會使用這些資訊來識別或連絡使用者或組織。

例如，在線上啟用期間，軟體版本、語言、產品金鑰、網際網路通訊協定 (IP) 位址等資訊，以及關於裝置硬體的資訊會傳送至 Microsoft。IP 位址僅用來驗證要求的位置，因為某些 Windows 版本（例如 Windows 7 Starter）僅可以在特定的目標市場地理位置啟用。

## 啟用選項

Windows 7 與 Windows Server 2008 R2 的授權可以透過下列三個基本管道的其中一個取得：零售、原始設備製造商 (OEM) 或大量授權。每個管道都有獨特的啟用方法。由於組織可以透過這三個可用管道取得作業系統，因此能夠選擇多種啟用方法的組合。

### 零售

透過零售店取得的 Windows 7 與 Windows Server 2008 R2 產品皆為獨立授權，其啟用方法與零售版本的 Windows Vista 和 Windows Server 2008 作業系統的啟用方法相同。每套購買的產品都附有唯一產品金鑰（列印於產品包裝上），使用者必須在產品安裝期間輸入。作業系統安裝完成後，電腦會使用這個產品金鑰完成啟用。最後的啟用步驟也可以在線上或透過電話完成。

### 原始設備製造商

大部分的 OEM 會銷售包含標準建置的 Windows 7 或 Windows Server 2008 R2 作業系統。硬體廠商會藉由建立作業系統與電腦韌體（基本輸入/輸出系統，或 BIOS）的關聯來執行 OEM 啟用。此程序在電腦交付給客戶前即完成，因此使用者不需要進行其他任何動作。這個啟用方法稱為 OEM 啟用。

只要客戶在系統上使用由 OEM 提供的映像，OEM 啟用就會生效。若要建立自訂的映像，客戶可以使用由 OEM 提供的映像作為建立自訂映像的基礎。否則就需要使用不同的啟用方法。如需自訂 Windows 與啟用影響的詳細資訊，請參閱以下的[白皮書](http://go.microsoft.com/fwlink/?LinkID=137292&clcid=0x409)。

**注：**OEM 啟用適用於透過 OEM 管道所購買之已安裝 Windows 的電腦。

### 大量授權

Microsoft 大量授權可針對您組織規模及購買偏好提供量身訂做的自訂方案。這些方案提供簡單、靈活及實惠的解決方案，讓組織能夠輕鬆管理授權。若要成為大量授權客戶，組織需要與 Microsoft 簽訂大量授權合約。

有兩種合法的方式可以為安裝 Windows 用戶端作業系統的新電腦取得完整的授權。第一種且最經濟實惠的方式就是透過原始設備製造商預先安裝授權。另一種選項是購買完整包裝的零售產品。

Microsoft 大量授權方案（例如開放式授權、選用授權和企業合約）僅包含 Windows 用戶端作業系統的升級。每部電腦需要一份合格的 OS 授權，才能在這些電腦中行使透過大量授權取得的升級權限。

如需大量授權的詳細資訊，包括合格的 OS 清單，請移至   
<http://go.microsoft.com/fwlink/?LinkId=73076>。

**注：**某些 Windows 版本（例如 Windows 7 Enterprise）僅可以透過大量授權管道取得。

## 大量啟用模式

大量啟用可以讓大量授權客戶將啟用程序自動化，因此它對使用者是透明的。大量啟用適用於大量授權方案所涵蓋的電腦。它僅作為啟用的工具，與授權發票開立或收費無關。

大量啟用提供兩種模式來完成大量啟用：金鑰管理服務 (KMS) 與多重啟用金鑰 (MAK)。KMS 可以讓組織在其網路中啟用系統，MAK 則藉由使用 Microsoft 所提供之裝載的啟用服務以單次為基礎啟用系統。客戶可以在他們的環境中使用其中一種或兩種金鑰類型來啟用系統。

### 金鑰管理服務

透過 KMS，IT 專業人員可以在其區域網路中完成啟用，無需將個別電腦連接至 Microsoft 以完成產品啟用。KMS 屬於輕量服務，不需要專屬的系統，並可輕鬆一同裝載於提供其他服務的系統上。依預設，Windows 7 與 Windows Server 2008 R2 的大量授權版本會連接至裝載要求啟用之 KMS 服務的系統。使用者無需執行任何動作。

KMS 需要網路環境中具有最低數量的電腦（實體或虛擬機器）。組織必須至少有 5 部電腦才能啟用 Windows Server 2008 R2，必須至少有 25 部電腦才能啟用執行 Windows 7 的用戶端。這些最低數量稱為啟用臨界值。

若要為 Windows 7 進行 KMS 啟用，電腦必須有合格的 OS 授權（通常透過 OEM 作為新 PC 採購的一部份取得），同時 BIOS 中必須包含 Windows 標記。

### 多重啟用金鑰

MAK 是透過 Microsoft 裝載的啟用服務進行的單次啟用。有兩種使用 MAK 啟用電腦的方法。第一種方法是 MAK 獨立啟用，它會要求每部電腦透過網際網路或電話獨立連接至 Microsoft 並進行啟用。第二種方法是 MAK Proxy 啟用。透過這種方法，電腦會像 MAK Proxy 一樣在網路中的多部電腦中收集啟用資訊，然後代表這些電腦傳送集中的啟用要求。使用大量啟用管理工具 (VAMT) 可設定 MAK Proxy 啟用。

**注：**KMS 是大量啟用用戶端的預設金鑰。使用 MAK 啟用需要安裝 MAK 金鑰。如需將 KMS 用戶端轉換為 MAK 的詳細資訊，請參閱[大量啟用部署指南](http://go.microsoft.com/fwlink/?LinkId=150083)。

## 萬一未啟用系統該怎麼辦？

啟用旨在向使用者提供透明化的啟用方式。如果未在安裝作業系統後立即啟用，Windows 7 與 Windows Server 2008 R2 仍會在限定時間或限定期限 內提供作業系統的完整功能。Windows 7 與 Windows Server 2008 R2 的限定期限長度為 30 天。限定期限到期後，兩套作業系統都會透過通知提醒使用者啟用電腦。

### 限定期限

在初始限定期限中，會有定期通知提醒電腦需要啟用。每天都會在登入程序期間出現一次通知，提醒使用者啟用作業系統。這會一直持續到限定期限剩下 3 天的時候。在限定期限最後 3 天的前兩天，每 4 個小時就會出現通知。在限定期限的最後 1 天，每 1 個小時就會在整點出現通知。

### 限定期限到期

在初始限定期限到期或啟用失敗後，Windows 7 與 Windows Server 2008 R2 會持續通知使用者其作業系統需要啟用。電腦必須啟用的提醒會出現在產品的許多地方，直到作業系統啟用為止：

* 在登入期間，輸入使用者認證後會出現通知對話方塊。
* 螢幕下方通知區域的上方會出現通知。
* 會持續出現桌面通知且桌面背景為黑色。
* 當使用者開啟特定 Windows 應用程式時可能會出現提醒。

## 產品金鑰

大量啟用不會變更大量授權客戶取得產品金鑰的方式。他們可以透過大量授權服務中心 (VLSC) 網站 <http://go.microsoft.com/fwlink/?LinkId=107544> 或致電啟用客服中心取得 MAK 及 KMS 金鑰。服務提供商授權合約 (SPLA) 合作夥伴只能夠致電啟用客服中心取得金鑰。美國客戶可以撥打 1-888-352-7140。美國地區以外的客戶可以與當地支援中心連絡。如需全球啟用客服中心的電話號碼，請移至 <http://go.microsoft.com/fwlink/?LinkId=107418>。致電支援中心時，客戶必須要有大量授權合約。

大量授權客戶可以隨時登入 VLSC 網站，檢視 KMS 金鑰的資訊。VLSC 網站也包含如何要求及使用 MAK 的資訊。如需 MAK 和 KMS 金鑰的詳細資訊，包括增加允許啟用數量的資訊，請參閱 <http://go.microsoft.com/fwlink/?LinkId=74008> 的 **Existing Customers（現有客戶）**頁面。

# 檢視可用的啟用模式

大量啟用提供以下啟用模式：

* 金鑰管理服務 (KMS)
* 多重啟用金鑰 (MAK)

所選擇的模式需視組織的規模、網路基礎結構、連線能力和安全性需求而定。IT 專業人員可以選擇僅使用一種啟用模式或使用這些啟用模式的組合。

**注：**權杖型啟用是特殊的啟用選項，適用於已核准的 Microsoft 大量授權客戶。它是設計用於終端系統完全與網路或電話中斷連接的特殊情況。透過此選項，客戶可以使用公開金鑰基礎結構 (PKI) 和數位憑證（或通常儲存在智慧卡中的*權杖* ）在本機啟用 Windows 7 Enterprise 與 Windows Server 2008 R2，無需透過 MAK 連絡客戶裝載的 KMS 或 Microsoft 裝載的啟用服務。如需權杖型啟用的詳細資訊，請連絡 Microsoft 帳戶團隊或服務代表。

## 金鑰管理服務

KMS 可以在區域網路中啟用電腦，因此個別電腦不需要連接至 Microsoft。若要這麼做，KMS 會使用用戶端 – 伺服器拓撲。KMS 用戶端電腦可以使用網域名稱系統 (DNS) 或靜態設定找到 KMS 主機電腦。KMS 用戶端可以使用遠端程序呼叫 (RPC) 連絡 KMS 主機。KMS 可以裝載於執行 Windows Vista、Windows 7、Windows Server 2003、Windows Server 2008 或 Windows Server 2008 R2 作業系統的電腦上。

### 最低電腦需求

規劃 KMS 啟用時，網路必須達到或超過啟用臨界值 或 KMS 所要求的最低合格電腦數量。IT 專業人員也必須瞭解 KMS 主機如何追蹤網路中的電腦數量。

#### KMS 啟用臨界值

KMS 可以啟用實體電腦和虛擬機器。若要達到 KMS 啟用條件，網路必須有最低的合格電腦數量，稱為啟用臨界值。KMS 主機只會在達到臨界值後才會啟用用戶端。為確保達到啟用臨界值，KMS 主機會計算網路中要求啟用的電腦數量。

KMS 用戶端電腦只會在達到啟用臨界值後才會被啟用。執行 Windows Server 2008 或 Windows Server 2008 R2 之電腦的啟用臨界值為 5。執行 Windows Vista 或 Windows 7 之電腦的啟用臨界值為 25。臨界值包括執行於實體電腦或虛擬機器的用戶端和伺服器。

KMS 主機會針對來自 KMS 用戶端的每個有效啟用要求回應一個計數，表示已有多少部電腦連絡 KMS 主機要求啟用。接收到低於啟用臨界值計數的用戶端不會被啟用。例如，如果連絡 KMS 主機的前兩部電腦執行 Windows 7，則第一部電腦會接收到數目為 1 的啟用計數，而第二部電腦會接收到數目為 2 的啟用計數。如果下一部電腦為 Windows 7 虛擬機器，它會接收到數目為 3 的啟用計數，以此類推。這些電腦都不會被啟用，因為執行 Windows 7 的電腦必須接收到數目 ≥25 的啟用計數才會被啟用。處於限定期限狀態的 KMS 用戶端由於啟用計數太低而無法被啟用者，每兩個小時會連接到 KMS 主機以取得目前的啟用計數，並且在達到臨界值時被啟用。

如果下一部與 KMS 主機連絡的電腦執行 Windows Server 2008 R2，它會接收到數目為 4 的啟用計數，因為啟用計數包含執行 Windows Server 2008 R2 和 Windows 7 的電腦。如果一部執行 Windows Server 2008 或 Windows Server 2008 R2 的電腦收到數目 ≥5 的啟用計數，則它會被啟用。如果一部執行 Windows 7 的電腦收到數目 ≥25 的啟用計數，則它會被啟用。

#### 啟用計數快取

為了追蹤啟用臨界值，KMS 主機會記錄要求啟用的 KMS 用戶端。KMS 主機為每部 KMS 用戶端指定一個用戶端機器識別碼 (CMID)，同時 KMS 主機將每個 CMID 儲存在表格中。每個啟用要求會在表格中保留 30 天。當用戶端更新它的啟用時，會從表格中移除快取的 CMID 並建立新的記錄，然後再次開始 30 天期限。如果 KMS 用戶端未在 30 天內更新它的啟用，KMS 主機便會從表格中移除相對應的 CMID，而啟用計數也會減去 1。

KMS 主機會快取 KMS 用戶端要求之 CMID 數量的兩倍，以確定 CMID 計數不低於啟用臨界值。例如，在用戶端執行 Windows 7 的網路中，KMS 啟用臨界值為 25。KMS 主機會快取最近 50 次啟用的 CMID。Windows Server 2008 R2 的 KMS 啟用臨界值為 5。僅由執行 Windows Server 2008 R2 的 KMS 用戶端連絡的 KMS 主機會快取個最近 10 次的 CMID。如果執行 Windows 7 的用戶端稍後連絡此 KMS 主機，KMS 會將快取大小增加到 50，以配合較高的臨界值。KMS 永遠不會減少快取大小。

### KMS 的運作方式

KMS 啟用需要 TCP/IP 連線。依預設，KMS 主機和用戶端使用 DNS 發佈和尋找 KMS 服務。可以使用只需部分或不需任何管理動作的預設設定，或根據網路設定和安全性需求手動設定 KMS 主機與用戶端。

#### KMS 啟用更新

KMS 啟用的有效期限是 180 天。此即稱為啟用有效間隔。為了維持啟用狀態，KMS 用戶端必須至少每 180 天連接至 KMS 主機一次，以更新啟用。依預設，KMS 用戶端電腦每 7 天會嘗試更新其啟用。如果 KMS 啟用失敗，用戶端每兩個小時會重試。更新用戶端的啟用後，啟用有效間隔會再次開始。

#### KMS 服務發佈

KMS 服務會使用 DNS 中的服務 (SRV) 資源記錄 (PR) 來儲存 KMS 主機的位置，並與這些主機進行通訊。KMS 主機使用 DNS 動態更新通訊協定（若可供使用）來發佈 KMS SRV RR。如果動態更新無法使用或 KMS 主機沒有權限發佈 RR，則必須手動發佈 DNS 記錄或 IT 專業人員必須設定用戶端電腦以連接特定 KMS 主機。

**注：**視網路的複雜性和拓撲的不同，DNS 變更可能需要一些時間傳播到所有 DNS 主機中。

#### KMS 服務的用戶端探索

依預設，KMS 用戶端會查詢 DNS 以取得 KMS 服務資訊。KMS 用戶端第一次查詢 DNS 以取得 KMS 服務資訊時，會隨機從 DNS 傳回的 SRV RR 清單中選擇一部 KMS 主機。

DNS 伺服器的位址包含 SRV RR，可作為字尾輸入列在 KMS 用戶端，如此可以通告一部 DNS 伺服器中 KMS 的 SRV RR，並且讓其他主要 DNS 伺服器的 KMS 用戶端找到它。

可以在 **DnsDomainPublishList** 登錄值中為 KMS 新增優先順序 和權數 參數。建立 KMS 主機優先順序群組和每個群組中的權數，可以讓 IT 專業人員指定用戶端必須先嘗試哪部 KMS 主機，並平衡多部 KMS 主機的流量。只有 Windows 7 和 Windows Server 2008 R2 提供優先順序 和權數 參數。

如果用戶端選取的 KMS 主機沒有回應，KMS 用戶端會從其 SRV RR 清單中移除該 KMS 主機，並從清單中隨機選取另一部 KMS 主機。當 KMS 主機回應時，KMS 用戶端會快取 KMS 主機的名稱，以用於後續的啟用及更新嘗試。如果快取的 KMS 主機在後續更新時沒有回應，KMS 用戶端會查詢 DNS 取得 KMS SRV RR，以探索新的 KMS 主機。

依預設，用戶端電腦會使用匿名 RPC 透過 TCP 連接埠 1688 連接至 KMS 主機以進行啟用。（IT 專業人員可以變更預設連接埠）與 KMS 主機建立 TCP 工作階段後，用戶端會傳送單一要求封包。KMS 主機會以啟用計數進行回應。如果計數達到或超過該作業系統的啟用臨界值，用戶端便會被啟用，而工作階段會結束。KMS 用戶端針對更新要求使用相同的程序。每個方向的通訊為 250 個位元組。

### 規劃 KMS 部署

KMS 服務不需要專屬的伺服器。KMS 服務能夠與其他服務一同裝載，例如 Active Directory® 網域服務 (AD DS) 網域控制站和唯讀網域控制站 (RODC)。KMS 主機也可以在執行任何支援之 Windows 作業系統（包括 Windows Server 2003）的實體電腦或虛擬機器中執行。雖然執行 Windows Server 2008 R2 的 KMS 主機可以啟用任何支援大量啟用的 Windows 作業系統，但執行 Windows 7 的 KMS 主機只能啟用執行 Windows 7 和 Windows Vista 用戶端的電腦。一部 KMS 主機可以支援不限數量的 KMS 用戶端，但是 Microsoft 建議至少部署兩部 KMS 主機，以進行容錯移轉。大部分的組織只需要在整個基礎結構中使用兩部 KMS 主機。

**注：**KMS 並未自動包括在 Windows Server 2003 中。如需將 KMS 裝載在執行 Windows Server 2003 的電腦中，請從下列網站之一下載並安裝 KMS：

* 針對 x86 型的電腦：Key Management Service 1.1 (x86) for Windows Server 2003 SP1 and Later（Windows Server 2003 SP1 及更高版本的金鑰管理服務 1.1 (x86)）   
  (<http://go.microsoft.com/fwlink/?LinkID=82964>)
* 針對 x64 型的電腦：Key Management Service 1.1 (x64) for Windows Server 2003 SP1 and Later（Windows Server 2003 SP1 及更高版本的金鑰管理服務 1.1 (x64)）   
  (<http://go.microsoft.com/fwlink/?LinkId=83041>)

#### 規劃 DNS 伺服器設定

預設的 KMS 自動發佈功能需要 SRV RR 和 DNS 動態更新通訊協定支援。執行 Microsoft 軟體的 DNS 伺服器，或任何支援 SRV RR（根據網際網路工程工作團隊 [IETF] 要求建議 [RFC] 2782）和動態更新（根據 RFC 2136）的其他 DNS 伺服器皆支援 KMS 用戶端預設行為和 KMS SRV RR 發佈。例如：Berkeley Internet Domain Name (BIND) 8.x 和 9.x 版本同時支援 SRV 記錄與動態更新。

必須設定 KMS 主機，讓它有所需的認證以建立與更新 DNS 伺服器上的 SRV、A（網際網路通訊協定版本 4，或 IPv4）和 AAAA（網際網路通訊協定版本 6，或 IPv6）RR，或需要手動建立的記錄。將所需的認證提供給 KMS 主機的建議解決方案是：在 AD DS 中建立安全性群組，然後將所有 KMS 主機新增至該群組。在執行 Microsoft 軟體的 DNS 伺服器中，請確認此安全性群組可以完整控制每個將包含 KMS SRV RR 之 DNS 網域中的 \_VLMCS.\_TCP 記錄。

#### 啟用第一個 KMS 主機

網路中的 KMS 主機需要安裝 KMS 金鑰，然後向 Microsoft 進行啟用。安裝 KMS 金鑰可以啟用 KMS 主機上的金鑰管理服務。KMS 金鑰安裝完成後，透過電話或線上完成 KMS 主機的啟用。初始啟用之後，KMS 主機就不會傳送任何資訊到 Microsoft。

KMS 金鑰僅能安裝於 KMS 主機上，不得安裝於個別的 KMS 用戶端上。Windows 7 與 Windows Server 2008 R2 有安全保護，以協助避免不小心將 KMS 金鑰安裝在 KMS 用戶端電腦上。任何時間當使用者嘗試安裝 KMS 金鑰時，他們會看到如圖 1 所示的警告。

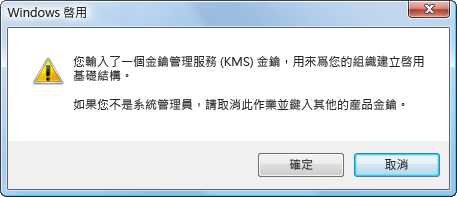


圖 1 安裝 KMS 金鑰

#### 啟用後續的 KMS 主機

每個 KMS 金鑰最多可以安裝於 6 部 KMS 主機，它們可以是實體電腦或虛擬機器。啟用 KMS 主機後，同一部主機最多可以使用相同的金鑰重新啟用 9 次。

如果組織需要 6 部以上的 KMS 主機，IT 專業人員可以致電啟用客服中心要求例外情況，為組織的 KMS 金鑰要求其他啟用。如需詳細資訊，請參閱大量授權網站   
<http://go.microsoft.com/fwlink/?LinkID=73076>。

#### 升級現有的 KMS 主機

執行 Windows Server 2003、Windows Vista 或 Windows Server 2008 的 KMS 主機可以設定成支援執行 Windows 7 和 Windows Server 2008 R2 的 KMS 用戶端。針對 Windows Vista 和 Windows Server 2008，需要一個封包來更新 KMS 主機，其包含支援擴充之 KMS 用戶端的檔案。此封包可透過 Microsoft 下載中心 <http://www.microsoft.com/downloads>，或 Windows Update 和 Windows Server Update Services (WSUS) 取得。將封包安裝於 KMS 主機後，即可依照本指南前面所述的方式安裝並啟用設計用來支援 Windows 7 與 Windows Server 2008 R2 的 KMS 金鑰。支援新版本 Windows 作業系統的 KMS 金鑰同時也為作為 KMS 用戶端之較早的 Windows 大量授權版本提供支援。

如需更新 Windows Server 2003 KMS 主機，所有必須的檔案都包含於 KMS 1.2 可下載封包中，該封包可透過 Microsoft 下載中心 <http://www.microsoft.com/downloads> 取得。

#### 規劃 KMS 用戶端

依預設，執行 Windows Vista、Windows 7、Windows Server 2008 與 Windows Server 2008 R2 大量授權版本的電腦皆為 KMS 用戶端，不需要其他設定。KMS 用戶端可以藉由查詢 DNS 找出發佈 KMS 服務的 SRV RR，自動找到 KMS 主機。如果網路環境不使用 SRV RR，可以手動設定 KMS 用戶端以使用特定的 KMS 主機。

如需手動設定 KMS 用戶端，請按照[大量啟用部署指南](http://go.microsoft.com/fwlink/?LinkId=150083)中的步驟進行。

#### 作為標準使用者啟用

Windows 7 與 Windows Server 2008 R2 不需要管理員權限即可進行啟用。然而此項變更不允許標準使用者帳戶將 Windows 7 或 Windows Server 2008 R2 從啟用狀態中移除。其他啟用或授權相關的工作仍需要管理員帳戶，例如「重複安裝」。

## 多重啟用金鑰

MAK 是透過 Microsoft 裝載的啟用服務進行的單次啟用。每個 MAK 有預先確定的允許啟用數量；此數量是根據大量授權合約而定，與組織的實際授權計數不相符。使用 Microsoft 裝載啟用服務的每個 MAK 啟用，會累計計數至啟用限制為止。

使用 MAK 啟用電腦的方法有兩種：

* MAK 獨立啟用。每部電腦透過網際網路或電話獨立連接至 Microsoft 並啟用。MAK 獨立啟用最適用於無需固定連接企業網路的組織內的電腦。
* MAK Proxy 啟用。MAK Proxy 啟用會透過連接 Microsoft 的其中一個連線，代表多部電腦啟用集中的啟用要求。使用大量啟用管理工具 (VAMT) 可設定 MAK Proxy 啟用。MAK Proxy 啟用則適用於因安全性考量而限制直接存取網際網路或企業網路的環境。它也適用於缺乏此類連線能力的研發測試實驗室。

MAK 建議用於很少或從未連接至企業網路的電腦，以及需要啟用的電腦數量未達到 KMS 啟用臨界值的環境。MAK 能夠用於個別的電腦，或可使用 Microsoft 部署解決方案進行複製或安裝的映像。MAK 也可以用於原先設定為使用 KMS 啟用的電腦。這在將電腦從核心網路移出至中斷連接的環境時很有用。

### 大量啟用管理工具

VAMT 包含於 Windows 自動化安裝套件 (Windows AIK) 中，是一套獨立的應用程式，會從多部電腦中收集啟用要求，然後再批量傳送至 Microsoft。VAMT 可讓 IT 專業人員指定一個電腦群組，以使用 AD DS、工作群組名稱、IP 位址或電腦名稱來進行啟用。在收到啟用確認碼後，VAMT 會將這些啟用確認碼發佈給要求啟用的電腦。由於 VAMT 也會在本機儲存這些確認碼，因此它可以在重新製作映像後重新啟用先前已啟用的電腦，而無需連絡 Microsoft。此外，VAMT 可以用來在 MAK 和 KMS 啟用方法之間輕鬆轉換電腦。

請從 Microsoft 下載中心下載 Windows Automated Installation Kit (AIK) for Windows 7 RC (<http://go.microsoft.com/fwlink/?LinkId=136976>)。

### MAK 架構

MAK 獨立啟用會在用戶端電腦上安裝 MAK 產品金鑰。金鑰會指示電腦透過網際網路向 Microsoft 伺服器進行啟用。在 MAK Proxy 啟用中，VAMT 會在用戶端電腦上安裝 MAK 產品金鑰，從目標電腦取得安裝識別碼 (IID)，代表用戶端將 IID 傳送給 Microsoft，並且取得確認識別碼 (CID)。然後工具會安裝 CID 以啟用用戶端。

# 評估用戶端連線能力

每種大量啟用方法都最適合特定的網路設定。若要為組織選取最佳的啟用方法，請評估網路環境，以識別不同群組的電腦連接至網路的方式。企業網路的連線能力、網際網路存取及經常連接至企業網路的電腦數量是需要識別的幾項重要設定特點。由於用戶端電腦連接至網路的方法各不相同，因此大多數的大中型組織會合併使用多種啟用方法。

對於與組織核心網路連接良好或擁有固定連線的電腦而言（例如位於異地的電腦），KMS 是建議的啟用方法。對於位於異地且因為安全考量而連線受限制或無法連接至核心網路的電腦，MAK 是建議的啟用方法。這些包含與核心網路隔離的實驗室和研發環境中的電腦。

表 1 列出常見網路設定與每種設定的建議最佳做法。電腦數量和啟用用戶端的網路連線能力都是每個解決方案的重要因素。

表 1 規劃時的網路基礎結構考量因素

| **網路基礎結構** | **建議事項** | **考量因素** |
| --- | --- | --- |
| **核心網路**  連接良好的區域 網路 (LAN)  最常見的情況 | 如果電腦總數 > KMS 啟S用臨界值：   * 小型（<100 部機器）：KMS 主機數 = 1 * 中型（≥100 部機器）：KMS 主機數 ≥ 1 * 企業：KMS 主機數 > 1   如果電腦總數 ≤ KMS 啟用臨界值：   * MAK（透過電話或網際 網路） * MAK Proxy | * 將 KMS 主機數量降到最少 * 每部 KMS 主機必須持續維持總機器計數 > KMS 啟用臨界值 * KMS 主機為自發 * KMS 主機可透過電話或網際網路啟用 |
| **隔離網路**  分公司、高安全 性網路區段、 周邊網路  連接良好的分區 LAN | 如果可以在 KMS 用戶端和主機間開啟防火牆上的連接埠：   * 在核心網路中使用 KMS  主機   如果政策不允許防火牆修改：   * 在隔離網路中使用區域 KMS 主機 * MAK（透過電話或網際 網路） * MAK Proxy | * 防火牆設定   + 透過 TCP 的 RPC（TCP 連接埠 1688）   + 由用戶端進行初始化 * 變更防火牆規則集的管理 |
| **測試或研發實驗室**  隔離網路 | 如果電腦總數 > KMS 啟用臨界值：   * KMS 主機數 = 1（每個隔離網路）   如果電腦總數 ≤ KMS 啟用臨界值：   * 無啟用（重設限定期限） * MAK（透過電話） * 手動執行的 MAK Proxy | * 變數設定 * 限制的電腦數量 * KMS 主機和透過電話進行的 MAK 啟用；手動執行的 MAK Proxy |
| **個別未連接的電腦**  未連接至網際網路或核心網路  固定連接至核心網路或透過虛擬私人網路 (VPN) 進行連接的漫遊電腦  具有網際網路存取但未連接至核心網路的漫遊電腦 | 固定連接至核心網路的用戶端：   * 在核心網路中使用 KMS  主機   未連接至核心網路或沒有網際網路存取的用戶端：   * MAK（透過電話）   無法連接至核心網路的網路：   * 如果電腦總數 > KMS 啟用臨界值：   + 小型：KMS 主機數 = 1   + 中型：KMS 主機數 ≥ 1   + 企業：KMS 主機數 > 1 * 如果電腦總數 ≤ KMS 啟用臨界值，手動執行 MAK 獨立啟用或 MAK Proxy 啟用   未連接至核心網路但有網際網路存取的用戶端：   * MAK（透過網際網路） | * 無法連接至其他網路的受限環境或網路 * 可以啟用 KMS 主機，並移至中斷連接的網路 * KMS 主機和透過電話進行的 MAK 啟用；手動執行的 MAK Proxy |

以下各節描述需要一種以上啟用方法的異質企業環境中的大量啟用解決方案範例。每個實例都有各自的建議啟用解決方案，但某些環境會有最適用於不同解決方案的基礎結構或原則需求。

## 核心網路

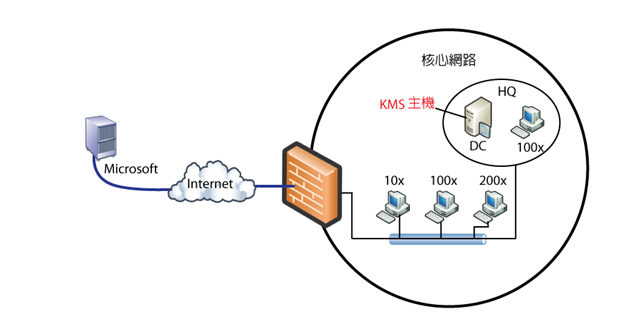
核心網路上的電腦建議使用集中的 KMS 解決方案。此解決方案適合多重網路區段中能夠連接至網際網路的連接良好的電腦所組成的網路。圖 2 顯示具有 KMS 主機的核心網路。

圖 2 核心網路實例

**注：**KMS 主機可以安裝在虛擬機器中，但請選取一個不會移到不同主機電腦的虛擬機器。如果虛擬 KMS 主機移到不同的主機電腦，作業系統會偵測基礎硬體中的變更，且 KMS 主機必須向 Microsoft 進行重新啟用。KMS 主機最多可向 Microsoft 進行 9 次啟用。

## 隔離網路

許多組織擁有可以分隔為多個安全性區域的網路。某些網路因為具有機密資訊而隔離出高安全性區域，而其他網路因處於不同的實體位置（例如分公司位置）而從核心網路中加以分隔。

### 高安全性區域

高安全性區域 是防火牆分隔的網路區段，可限制與其他網路區段進行往來通訊。如果藉由允許 TCP 連接埠 1688 從高安全性區域傳出以及 RPC 回覆傳入來允許高安全性區域中的電腦存取核心網路，則可以使用位於核心網路中的 KMS 主機啟用高安全性區域中的電腦。如此一來，高安全性網路中的用戶端電腦數量就不必達到任何 KMS 啟用臨界值。

如果這些防火牆例外情況未經過授權，而高安全性區域中的電腦總數達到 KMS 啟用臨界值，則可以在高安全性區域新增一部區域 KMS 主機。然後透過電話啟用高安全性區域中的 KMS 主機。

圖 3 顯示企業安全性原則不允許高安全性區域與核心網路中的任何電腦間有流量的環境。由於高安全性區域擁有足夠數目的電腦可達到 KMS 啟用臨界值，因此高安全性區域擁有自身的區域 KMS 主機。KMS 主機可透過電話自行啟用。

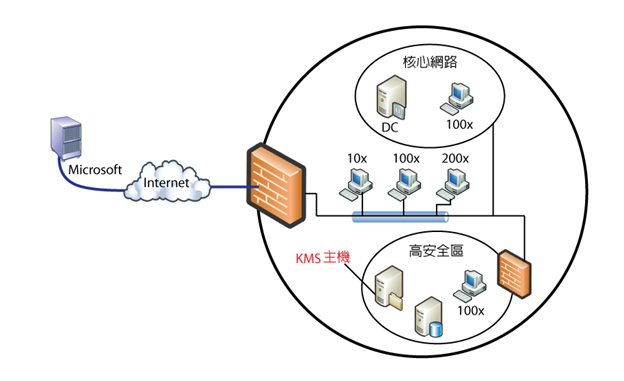


圖 3 高安全性網路實例

如果因為高安全性區域中僅有少數電腦而不適用 KMS 時，建議使用 MAK 獨立啟用。每部電腦都可以透過電話獨立向 Microsoft 進行啟用。

使用 VAMT 的 MAK Proxy 啟用也可能會出現在此實例中。由於在高安全性區域中的電腦無法進行網際網路存取，因此 VAMT 可以使用工作群組中的 AD DS、電腦名稱、IP 位址或成員資格探索這些電腦。VAMT 會使用 Windows Management Instrumentation (WMI) 安裝 MAK 產品金鑰和 CID，並且抓取 MAK 用戶端的狀態。由於不允許此流量通過防火牆，因此必須在高安全性區域中擁有區域 VAMT 主機。

### 分公司位置

圖 4 顯示三家分公司中支援用戶端電腦的企業網路。網站 A 會使用區域 KMS 主機，因為它擁有超過 25 部的用戶端電腦，但是沒有核心網路的安全 TCP/IP 連線能力。網路 B 會使用 MAK 啟用，因為 KMS 不支援少於 25 部 KMS 用戶端電腦的網站，且此網站未透過安全連結連接至核心網路。網站 C 會使用 KMS，因為它會透過私人廣域網路 (WAN) 的安全連線連接至核心網路，並且使用核心網路 KMS 用戶端達到啟用臨界值。

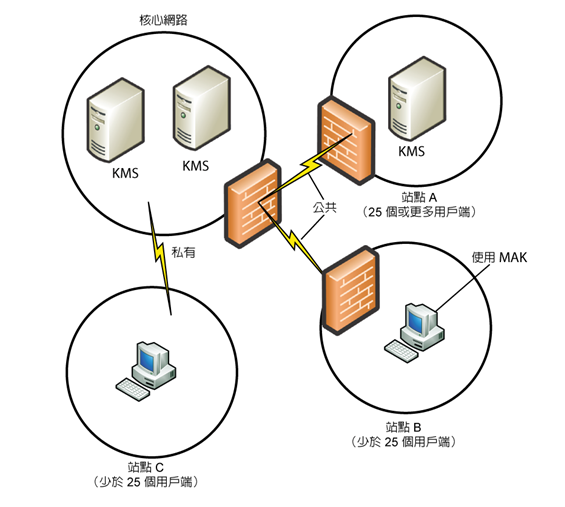


圖 4 分公司實例

## 未連接的個別電腦

組織中的某些使用者或許身在遠端位置，也或許外出至許多不同的位置。對於漫遊用戶端（例如銷售人員所用電腦或其他身處異地而不在分公司的使用者所用電腦）來說，這個實例很常見。這個實例也適用於未連接至核心網路或暫時連接至核心網路的遠端分公司位置。

視電腦連接至核心網路的頻率而定，未連接的電腦可以使用 KMS 或 MAK。對於至少每 180 天直接或透過 VPN 連接一次核心網路，而且核心網路使用 KMS 啟用的電腦，可使用 KMS 啟用。對於很少或從未連接至核心網路的電腦，可透過電話或網際網路使用 MAK 獨立啟用。圖 5 顯示透過網際網路及電話使用 MAK 獨立啟用的未連接用戶端。

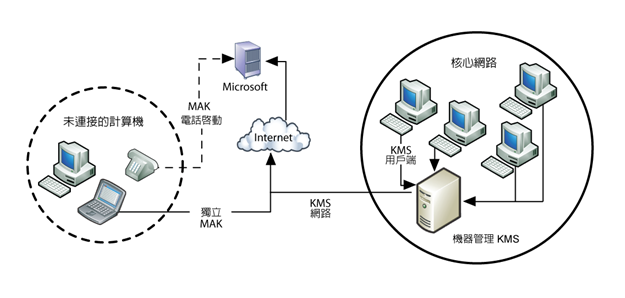


圖 5 未連接電腦實例

## 測試和研發實驗室

實驗室環境通常有大量的虛擬機器，同時實驗室中的電腦經常重新設定。判斷測試及研發實驗室中的電腦是否需要啟用。對於執行 Windows 7 或 Windows Server 2008 R2 的電腦，其 30 天初始限定期限可以重設 3 次，而不需啟用電腦。因此，如果您會在 120 天內重新建立實驗室電腦，則這些電腦不需要被啟用。

如果實驗室電腦需要啟用，可以使用 KMS 或 MAK 啟用。如果電腦能夠連接至使用 KMS 的核心網路，請使用 KMS 啟用。如果實驗室中的電腦數量達到 KMS 啟用臨界值，可以部署區域 KMS 主機。

在電腦更換率高而 KMS 用戶端少的實驗室中，務必監控 KMS 啟用計數，以便使 KMS 主機上快取的 CMID 數量保持充足。KMS 主機會快取電腦啟用要求長達 30 天。（請參閱本指南前面所述的[最低電腦需求](#_Minimum_Computer_Requirements)一節，以取得 CMID 如何影響啟用的詳細資訊）如果需要啟用實驗室環境但未達到 KMS 啟用條件，請使用 MAK 啟用。MAK 用戶端可透過電話或網際網路啟用，視實驗室可使用者為何。

在此實例中也可以使用透過 VAMT 進行的 MAK Proxy 啟用。在隔離的實驗室網路以及能夠存取網際網路的網路中安裝 VAMT。在隔離實驗室中，VAMT 會執行探索、取得狀態、安裝 MAK 產品金鑰，並且取得實驗室中每部電腦的 IID。資訊可以從 VAMT 匯出，並儲存至卸除式媒體，然後檔案可以匯入執行 VAMT 同時有網際網路存取的電腦。VAMT 會將 IID 傳送至 Microsoft，並取得完成啟用所需的相對應 CID。將此資料匯出至卸除式媒體後，可以將該資料攜帶至隔離實驗室以匯入 CID，如此一來 VAMT 即可完成啟用。

**注：**在高安全性模式中，VAMT 會在其匯出的檔案中移除所有可辨識個人的資訊 (PII)。此檔案為可讀取的可延伸標記語言 (XML) 檔，可以任何 XML 或文字編輯器檢視。

# 將電腦對應至啟用方法

在評估建議的啟用實例後，下一步就是使用大量啟用將電腦對應至啟用方法。目標是確認所有電腦都與啟用選項產生關聯。表 2 提供簡易的工作協助，以確認所有的電腦都已對應至啟用方法。完成此工作協助時，請確認所有使用 KMS 的電腦都位在達到 KMS 啟用臨界值的網路。

表 2 啟用方法工作表

|  |  |  |
| --- | --- | --- |
| 條件 | 啟用方法 | 電腦數量 |
| 要啟用的電腦總數 | |  |
| 至少每 180 天（直接或透過 VPN）連接一次網路且達到 KMS 啟用臨界值的電腦數量 | KMS |  |
| 至少每 180 天都未連接一次網路的電腦數量 | MAK |  |
| 達到 KMS 啟用臨界值的隔離網路中的電腦數量 | KMS |  |
| 未達到 KMS 啟用臨界值的隔離網路中的電腦數量 | MAK |  |
| 測試/研發實驗室中不會啟用的電腦數量 | 無 |  |
| 漫遊電腦計數應該為零 | |  |

# 決定產品金鑰的需求

Windows 7 和 Windows Server 2008 R2 作業系統都擁有不同的版本。為了簡化大量啟用和組織所需的產品金鑰數量，Microsoft 建立了*產品金鑰群組*。KMS 和 MAK 的產品金鑰會套用至產品群組而非個別的版本，但是 KMS 和 MAK 使用產品金鑰群組的方法不同：

* MAK 啟用會將產品金鑰群組用作個別群組。MAK 啟用產品金鑰會直接與單一產品群組產生關聯，但只能啟用特定產品群組中的 Windows 版本。
* 使用 KMS 時，產品金鑰會以階層式方式與產品群組一同運作。KMS 啟用的產品金鑰會與產品群組產生關聯，同時可以啟用該特定產品群組中的版本以及在產品階層中較低的其他版本。

Windows 7 與 Windows Server 2008 R2 的產品群組如表 3 所示。

表 3 產品群組

| 大量授權產品金鑰群組 | Windows 作業系統版本 |
| --- | --- |
| 用戶端 VL | * Windows 7 Professional * Windows 7 Enterprise |
| 伺服器群組 A | * Windows Server 2008 R2 HPC Edition * Windows Web Server 2008 R2 |
| 伺服器群組 B | * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise |
| 伺服器群組 C | * Windows Server 2008 R2 Datacenter * Itanium 型系統適用的 Windows Server 2008 R2 |

## 選擇 MAK 產品金鑰群組

由於 MAK 產品金鑰與單一產品群組產生關聯，它只能啟用該群組中的作業系統版本，因此請在群組中選擇符合要安裝之 Windows 版本的 MAK 金鑰。例如，如果您要安裝 Windows 7 Enterprise，可安裝映像中的用戶端 VL MAK 金鑰或直接從目標系統中安裝。

## 選擇 KMS 金鑰

KMS 的產品金鑰會與產品群組產生關聯，同時可以啟用該特定產品群組中的 Windows 版本以及在產品階層中低於它的任何版本。階層中第一個且具有最小涵蓋範圍的群組是「用戶端大量授權」產品群組；而伺服器群組 C 是 KMS 階層中具有最大涵蓋範圍的群組。

此階層延伸至 Windows Vista 和 Windows Server 2008 大量授權版本和產品金鑰群組。個別產品金鑰群組會發給不同的 KMS 金鑰，這表示客戶會有一個 KMS 金鑰可存取用戶端 VL 的 Windows 7 和 Windows Vista。較新 Windows 產品的 KMS 金鑰同時能夠啟用較早世代的產品，這表示客戶可以使用單一 KMS 金鑰啟用多個 Windows 版本和世代。表 4 顯示產品群組的相互關聯。

表 4 產品群組的相互關聯

| 大量授權產品金鑰群組 | Windows 版本  （Windows 7 與 Windows Server 2008 R2） | Windows 版本  （Windows Vista 與 Windows Server 2008） |
| --- | --- | --- |
| 用戶端 VL | * Windows 7 Professional * Windows 7 Enterprise | * Windows Vista Business * Windows Vista Enterprise |
| 伺服器群組 A | * Windows Web Server 2008 R2 * Windows Server 2008 R2 HPC Edition * Windows HPC Server 2008 R2 | * Windows Web Server 2008 * Windows Compute Cluster Server 2008 |
| 伺服器群組 B | * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise | * Windows Server 2008 Standard * Windows Server 2008 Enterprise * 包括無 Hyper-V™ 的版本 |

|  |  |  |
| --- | --- | --- |
| 伺服器群組 C | * Windows Server 2008 R2 Datacenter * Itanium 型系統適用的 Windows Server 2008 R2 | * Windows Server 2008 Datacenter * Itanium 型系統適用的 Windows Server 2008 * 包括無 Hyper-V™ 的版本 |

## 選擇 KMS 主機

在本指南前面提過，KMS 可以裝載於實體電腦或虛擬機器上的用戶端或伺服器作業系統。選擇 KMS 主機系統時，考慮要透過 KMS 啟用的作業系統版本。裝載於 Windows 7 的 KMS 只能啟用用戶端作業系統，但裝載於 Windows Server 2008 R2 的 KMS 則可以啟用用戶端和伺服器電腦。請參閱表 5 以取得此階層的說明。

表 5 KMS 階層

| 產品金鑰群組 | 可裝載的 KMS（KMS 金鑰啟用 KMS 主機） | 由此 KMS 主機所啟用的 Windows 產品版本 |
| --- | --- | --- |
| 適用於 Windows 7 的用戶端 VL | * Windows Vista * Windows 7 * 適用於 Windows Server 2003 v1.2 的 KMS | * Windows 7 Professional * Windows 7 Enterprise * Windows Vista Business * Windows Vista Enterprise |
| 適用於 Windows Server 2008 R2 的伺服器群組 A | * 適用於 Windows Server 2003 v1.2 的 KMS * Windows Web Server 2008 * Windows Web Server 2008 R2 * Windows HPC Server 2008 * Windows HPC Server 2008 R2 | 包括前述，外加：   * Windows Web Server 2008 R2 * Windows Web Server 2008 * Windows HPC Server 2008 R2 * Windows HPC Server 2008 |
| 適用於 Windows Server 2008 R2 的伺服器群組 B | 包括前述，外加：   * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise * Windows Server 2008 Standard * Windows Server 2008 Enterprise | 包括前述，外加：   * Windows Server 2008 R2 Standard * Windows Server 2008 R2 Enterprise * Windows Server 2008 Standard * Windows Server 2008 Enterprise |

|  |  |  |
| --- | --- | --- |
| 伺服器群組 C | 包括前述，外加：   * Windows Server 2008 R2 Datacenter * Windows Server 2008 Datacenter * Itanium 型系統適用的 Windows Server 2008 | 包括前述，外加：   * Windows Server 2008 R2 Datacenter * Windows Server 2008 Datacenter * Itanium 型系統適用的 Windows Server 2008 |

# 決定監控與報告的需求

使用大量啟用的組織需要追蹤產品金鑰使用狀況與已啟用電腦的授權狀態。客戶可以在大量授權服務中心 <http://go.microsoft.com/fwlink/?LinkId=107544> 上檢視 KMS 金鑰的資訊以及 MAK 金鑰的剩餘啟用次數。

此外，有許多工具可以協助大量授權客戶管理啟用及產品金鑰使用狀況。以下各節描述可用的工具，以及各種工具如何協助大量授權客戶：

## Windows Management Instrumentation

啟用期間收集的資料可使用 WMI 進行存取。事實上，多種可用的工具會使用 WMI 存取大量啟用資料。請參閱[大量啟用技術參考指南](http://go.microsoft.com/fwlink/?LinkId=152550)，以取得所有 WMI 方法、內容、登錄機碼及大量啟用事件識別碼的清單。

## System Center Configuration Manager

客戶可以使用 Microsoft Systems Management Server (SMS) 2003 SP3 或 Microsoft System Center Configuration Manager 2007 來監控組織中電腦的授權狀態。如需可用授權狀態的詳細描述，請參閱本指南後面的附錄 B：[授權狀態](#_附錄_B：授權狀態)。

Systems Management Server SP3 和 System Center Configuration Manager 會使用內建的 Asset Intelligence 報告和 WMI 來產生執行 Windows 7 或 Windows Server 2008 R2 之電腦的詳細啟用報告。此資訊也可用作組織從授權角度進行追蹤及報告軟體資產管理的起點。此外，System Center Operations Manager 2007 可用來監控金鑰管理服務的狀態和活動訊號。

## 事件記錄檔

KMS 服務會記錄 KMS 用戶端與主機應用程式記錄檔中的每個動作。KMS 用戶端會使用 Windows 安全性授權 (SLC) 事件識別碼 12288 和 12289，記錄 KMS 用戶端本機應用程式記錄檔中的啟用要求、更新和回應。KMS 主機會將從 KMS 用戶端接收的每個要求的個別項目記錄為 SLC 事件識別碼 12290。這些項目會儲存至「應用程式及服務記錄檔」資料夾中的「金鑰管理服務」記錄檔。每個 KMS 主機會保留個別的啟用記錄檔。KMS 主機之間不會進行記錄檔複寫，雖然可以使用記錄檔轉送功能將多部 KMS 主機的記錄檔複寫到中心位置以進行監控。如需 KMS 事件的詳細資訊，請參閱[大量啟用技術參考指南](http://go.microsoft.com/fwlink/?LinkId=152550)。

## KMS 管理組件

KMS 事件記錄檔可以手動封存或檢視。或者使用 Microsoft System Center Operations   
Manager 2007 時，IT 專業人員可以使用 System Center Operations Manager 的 Windows 金鑰管理服務管理組件。KMS 管理組件可以監控 KMS 服務的狀態和活動訊號。若要下載管理組件和指南，請參閱 <http://go.microsoft.com/fwlink/?LinkID=110332> 中的 **System Center Pack Catalog（系統中心組件目錄）**。

## 大量啟用管理工具

組織可以使用 VAMT 在其網路上管理 KMS 和 MAK 啟用。此外，還可以使用它來監控 MAK 的剩餘啟用次數。它會報告所有使用大量啟用之電腦的授權狀態，並且追蹤 MAK 啟用計數。

# 附錄 A：傳送至 Microsoft 的資訊

Microsoft 會使用在啟用期間收集的資訊來確認該軟體版本已授權，然後會將資訊彙總以進行統計分析。Microsoft 不會使用這些資訊來識別或連絡組織。如需啟用期間所擷取資訊以及 Microsoft 如何使用這些資料的詳細資訊，請參閱 <http://go.microsoft.com/fwlink/?LinkID=52526>http://go.microsoft.com/fwlink/?LinkId=52526。

在 MAK 啟用和 KMS 主機啟用期間，會將下列資訊傳送至 Microsoft：

* 產品金鑰
* 作業系統版本以及取得的管道
* 目前日期
* 授權及啟用狀態
* 硬體識別碼雜湊（無法進行反向工程的非唯一號碼）
* 語言設定
* 僅用來驗證要求位置的 IP 位址

# 附錄 B：授權狀態

軟體授權架構可以管理執行 Windows 作業系統之電腦的授權狀態。此架構擁有以多項核心 Windows 安全性技術建立的原則引擎。此架構的設計目的是防止程式碼及相關授權狀態遭到竄改或其他惡意行為的破壞。

原則引擎會從一組經過密碼編譯而簽署的可延伸權限標記語言 (XrML) 授權檔案中取得資料。XrML 是許多 Windows 元件使用的業界標準權限表述語言。授權檔案會定義 Windows 已安裝版本的權限與狀態。原則引擎使用的所有授權檔案和其他資料都會使用鏈結至 Microsoft 信任之安全根目錄的金鑰進行數位簽署或加密。

Windows 7 與 Windows Server 2008 R2 可能處於下列四種軟體授權狀態的其中一種：已啟用、限定期限、正版 或通知。以下各節描述這些狀態，它能夠反映電腦的啟用及正版狀態，這些狀態會決定使用者經驗。圖 6 說明這些狀態。

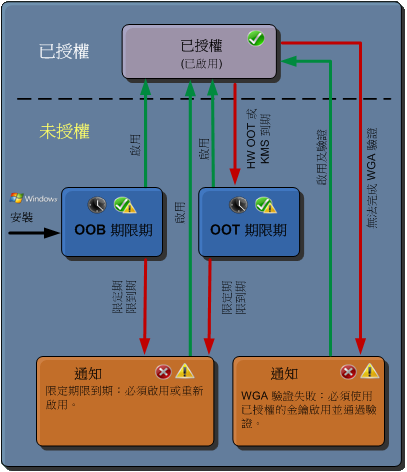


圖 6 授權狀態

## 已啟用

電腦啟用後，使用者就可以存取作業系統的完整功能。啟用程序完成後所授予的授權檔案與一組原則（權限）的組合會定義 Windows 版本的功能。個別的 Windows 元件會呼叫軟體授權應用程式設計介面 (API)，以決定授予哪些權限並根據回應調整功能。

## 限定期限

安裝 Windows 7 或 Windows Server 2008 R2 作業系統後，在完成啟用前，使用者可以在限定的時間內（限定期限 ）存取作業系統的完整功能。用戶端或伺服器作業系統的限定期限長度為 30 天。在初始限定期限中，作業系統會定期通知使用者需要啟用電腦。此外，當硬體有重大變更時，Windows 可能會處於有效的容許限定期限外。通知會盡可能減少干擾，而且可能不會在限定期限一開始就出現，但愈接近限定期限截止日，出現的頻率就愈高。

## 正版

正版狀態與啟用程序並無關聯。這其實是由線上正版驗證服務所決定的狀態。當使用者嘗試要下載或使用僅限正版的功能時，線上驗證服務會檢查提出要求之電腦所使用的作業系統。

作業系統可能會有下列三種正版狀態中的其中一種：

* **非正版**。電腦已從線上驗證服務取得票證，指出它為非正版。
* **本機正版**。電腦尚未取得驗證票證。
* **正版**。電腦已從線上驗證服務取得 Microsoft 簽署的票證，指出它為正版。

正版授權狀態只適用於 Windows 作業系統的用戶端版本。在限定期限的開始，執行這些 Windows 版本的電腦會一直處於本機正版的狀態。在電腦未通過線上驗證服務的驗證且收到非正版票證前，電腦不會被標示為非正版。同樣地，在電腦具有非正版狀態後，必須透過線上驗證服務成功完成驗證，才能收到正版票證。

雖然要啟用的電腦必須為正版，但啟用程序並不會重設或清除先前的非正版狀態。因此，若要將電腦回復到功能完整的已啟用狀態，就必須進行啟用，並透過線上驗證服務進行驗證。如需詳細資訊，請參閱 Microsoft 網站上的 **Genuine Microsoft Software（正版 Microsoft 軟體）**<http://go.microsoft.com/fwlink/?LinkId=151993>。

## 通知

通知型經驗的目的是為了區別正版並已啟用 Windows 作業系統的版本，以及非正版或沒有以維持電腦功能（例如登入、存取常用桌面等）的方式進行啟用的版本。Windows 7 或 Windows Server 2008 R2 中不包含精簡功能模式 (RFM)。兩套作業系統都以通知型經驗代替。此一全新的通知使用者經驗表示未在限定期限中啟用（初始啟用及因硬體變更的啟用）或未能通過驗證的電腦都可能提供以下使用者經驗：

* 登入電腦後，使用者會看到一個對話方塊，提醒他們必須啟用 Windows，並提供立即啟用或稍後啟用的選項。如果使用者在兩分鐘內未與對話方塊互動，登入程序會正常繼續。
* 處於通知狀態時，Windows 的桌面底色圖案會變成全黑色的背景，在通知區域中顯示表示啟用狀態的通知，並出現對話方塊顯示使用者必須採取的動作。
* 處於通知狀態時，使用者可以存取已安裝之 Windows 版本的完整功能，但以下功能停用：
* 設定為 KMS 主機的電腦會以 KMS 未被啟用的錯誤訊息回應 KMS 用戶端的要求。
* Windows Update 下載安全性和重大更新（選用的更新除外）。
* 無法使用需要線上驗證服務的選用下載，亦稱為正版守護的 下載。

必須啟用電腦，才能讓它結束通知狀態。