



強化安全性

數量 **3.5 倍** 的安全性
功能

包括雙因素驗證及 iDRAC9 的外
部金鑰管理



最佳化能源效率

數量多 **6 倍** 的耗電量
報告

Dell OME 有 20 種報告，而
Supermicro SSM 有 3 種



提升作業效率，為系
統管理員節省 **1 小時**
50 分鐘 時間

(每 100 部伺服器)

使用 Dell iDRAC9 自動更新，相
較於 Supermicro IPMI 無自動更
新可用

使用健全的 Dell 伺服器管理工具 提升安全性、可持續性及效率

相較於 Supermicro 管理產品組合

當您為資料中心投資購買新伺服器時，您需要選擇的不僅僅是硬體本身，您還需要選擇一個具有可管理性的解決方案。當系統管理員有高效率且功能豐富的工具可用於部署、監控、維護和保護基礎設施，同時提高其能源效率時，他們便能輕鬆處理日常管理工作，並將更多時間投入推動組織發展的創新工作。選擇向可提供強大管理工具的供應商購買產品，就可以有效節省時間和金錢。

我們評估了 Dell 和 Supermicro® 的伺服器管理產品組合，並將 Dell 的三種工具與 Supermicro 的兩種工具進行了比較。

表 1：我們測試的管理工具。*Dell CloudIQ 是一套雲端式的監控與分析工具；Supermicro 未提供類似工具。資料來源：Principled Technologies。

| | Dell | Supermicro |
|-------------|---|--|
| 嵌入式/遠端伺服器管理 | iDRAC9 (Integrated Dell Remote Access Controller) | Supermicro Intelligent Management (IPMI) |
| 一對多裝置管理主控台 | Dell OpenManage Enterprise (OME) Dell CloudIQ* | Supermicro Server Manager (SSM) |

在可持續性、安全性和日常管理體驗方面，我們發現 Dell 的工具集一直都能提供更加豐富的功能，可讓系統管理員運用更多選項和功能完成工作。

功能更多、更豐富，可自動化及簡化伺服器管理

您的 IT 團隊需要功能豐富的現代化管理工具，這些工具可以節省日常工作時間，並跟上不斷推陳出新的安全性和效率標準。我們評估的 Dell 管理工具擁有許多 Supermicro 管理產品組合欠缺的特色和功能。

永續發展

隨著能源成本的上升和環境法規的加嚴，許多組織都日益重視可持續性的課題。資料中心本身的耗電量很大，但完善的熱管理和電力管理可幫助組織有效減少耗電量。Dell OpenManage Enterprise 內含多種功能，可密切監控和管理耗電量，進而協助您實現可持續性目標。表 2 和表 3 顯示這些功能的關鍵效益，我們會在之後進一步詳細說明。

2 Dell OpenManage Enterprise 與 SSM 在可持續性表現上的差異。資料來源：Principled Technologies。

| 功能 | Dell 管理工具 | Supermicro 管理工具 |
|------------------|-----------|-----------------|
| 碳排放使用量計算機和容量規劃工具 | ✓ | x |
| 碳足跡分析 | ✓ | x |
| 溫度觸發電力管理原則 | ✓ | x |
| 靜態電力管理原則 | ✓ | ✓ |

表 3：Dell OME 與 Supermicro SSM 和 IPMI 的比較摘要。資料來源：Principled Technologies。

| 功能 | Dell 管理工具的主要效益 | Supermicro 管理工具的劣勢 |
|--|--|--|
|  碳排放使用量計算機和容量規劃工具 | 能用自訂數值估算溫室氣體排放，幫助達成可持續性目標 | 無類似功能；導致難以協助您規劃可持續性目標 |
|  碳足跡分析 | 透過 OpenManage Enterprise Power Manager 提供；提供碳排放相關數據，助您達成可持續性目標 | 無類似功能；無法追蹤及監測碳足跡數據，無法助您達成可持續性目標 |
|  自動化電力和熱管理 | 靜態及溫度觸發原則選項，包含可在伺服器耗電量或溫度超過閾值時觸發的選項 | 一種無相關觸發選項的靜態原則類型 |
|  耗電量報告 | 多 6 倍的耗電量報告，包含 20 個內建報告，並提供定時電子郵件發佈和自訂選項 | SSM 中有 2 個內建報告；Supermicro IPMI 中有 1 個報告，但不提供匯出功能 |
|  電力管理指標 | 多達 15 倍的指標，可提供更為精細的耗電量管理深入解析 | 只有 1 個指標，無法有效洞察及控管耗電情況 |



1 Dell OME 和 Supermicro SSM 中提供的耗電量報告數量。資料來源：Principled Technologies。



2 Dell OME 和 Supermicro SSM 中提供的電力管理指標數量。資料來源：Principled Technologies。

自動化電力和熱管理

OpenManage Enterprise Power Manager 提供自動化的電力與散熱管理，透過靜態電力和溫度觸發兩種原則選項，讓系統管理員能限制耗電量或溫度上限，以助降低冷卻成本。相比之下，SSM 只有一種原則選項，即對耗電量實施靜態限制，但該限制並不會在伺服器耗電量超出限值時自動觸發，這可能會產生較高的能源成本。

希望能深入瞭解資料中心耗電情況並積極推行最佳化措施的組織，可充分利用 OpenManage Enterprise Power Manager 提供的**20 種不同內建耗電量報告**來達成目標。這些報告對於容量規劃和電力管理非常有用，能協助組織有效提高用電效率。SSM 中的報告選項相當有限。系統管理員只能根據一種服務報告來營運單台主機，或是在監控螢幕中觀察耗電量趨勢。Supermicro IPMI 可讓使用者在 BMC 中查看各元件的耗電圖；但是，他們無法匯出圖中的資料進行分析，只能將其儲存為影像。

OpenManage Enterprise Power Manager 附掛程式可讓系統管理員**查看多達 15 種不同的指標**，包括個別元件用電量、氣流與元件利用率等，而 SSM 僅提供總用電量指標。

碳排放和碳足跡分析

OME 提供碳排放使用量計算機和容量規劃工具，除了能讓您估算自己的溫室氣體排放量外，還有許多其他功能。不僅提供預設的每單位能耗電力成本和碳排放值，還能讓您根據所在區域的電力成本，以及資料中心的耗電模型來自訂這些值。SSM 並未提供類似功能，這可能會令組織難以規劃和監控其可持續發展目標的進展。

安全性

網路犯罪急遽飆升，令公司面臨「資料損毀、資金被盜、生產力損失、智慧財產權盜竊、個人和財務資料盜竊、侵占、欺詐、攻擊後業務中斷、鑑識調查、遭入侵資料和系統的恢復和刪除，以及聲譽損害」等種種威脅。¹ 在此背景下，決策者應將安全性納入選購伺服器的考量因素。我們發現 Dell OpenManage Enterprise 提供了多項有助確保資料安全的功能，而 Supermicro 工具則未提供這些功能 (參見表 4 和表 5)。

3 Dell 管理工具和 Supermicro 管理工具在安全性表現上的差異。資料來源：Principled Technologies。

| 功能 | Dell 管理工具 | Supermicro 管理工具 |
|--------------|-----------|-----------------|
| 多重因素驗證 | ✓ | x |
| 外部金鑰管理 | ✓ | x |
| 範圍型存取控制 | ✓ | x |
| 原則式安全性組態 | ✓ | x |
| 網路安全性公告 | ✓ | x |
| 角色型存取控制 | ✓ | ✓ |
| 動態 USB 連接埠停用 | ✓ | ✓ |

表 4：Dell 與 Supermicro 管理工具的安全性功能比較摘要。資料來源：Principled Technologies。

| 功能 | Dell 管理工具的主要效益 | Supermicro 管理工具的劣勢 |
|---|---|---------------------------------|
|  多因素驗證 (MFA) | iDRAC 提供電子郵件和 RSA SecurID 雙因素驗證，防止未經授權的使用者存取機密資料 | 無類似功能，存在安全漏洞，可能導致未經授權的使用者存取機密資料 |
|  外部金鑰管理 | iDRAC 中的 Secure Enterprise Key Manager 提供多一道安全防護，利用磁碟機加密和集中管理機制來保護伺服器上的靜態資料 | 無類似功能，存在安全漏洞 |
|  存取控制 | OME 提供角色型存取控制 (RBAC) 和範圍型存取控制 (SBAC)，用於限制裝置管理員能夠存取的裝置群組 | 僅提供 RBAC，系統管理員限制存取的能力受限 |
|  原則式安全性組態 | 透過 CloudIQ 進行原則式安全性組態設定，可在發現差異時向系統管理員發出警示 | 無類似功能，可能造成違規的處置和補救時間延宕 |
|  網路安全性公告 | 透過 Dell CloudIQ 安全功能提供安全性公告報告，內含漏洞詳細資訊和可行的補救建議，以利迅速行動 | 無類似功能，存在安全漏洞，可能遭到不肖分子利用 |

多重因素驗證

多因素驗證 (MFA) 有助於防止未經授權的使用者和不肖分子存取機密資料。經過我們確認，Dell iDRAC 可透過電子郵件和 RSA SecurID (獲眾多行業採用的外部多因素驗證技術) 進行雙因素驗證。² 我們亦確認 Supermicro IPMI 和 SSM 均不提供此功能，因此存在安全漏洞。

金鑰管理

外部金鑰管理系統 (KMS) 可讓 IT 團隊使用單獨的第三方伺服器來管理用於鎖定/解除鎖定伺服器儲存裝置的金鑰，以提供多一層安全防護。iDRAC 還提供適用於所有新型 Dell PowerEdge 伺服器的 Local Key Manager (LKM)。部分授權還提供 Secure Enterprise Key Manager (SEKM)，透過全磁碟加密和外部金鑰管理功能增加安全性。SEKM 支援產業標準的 OASIS KMIP 通訊協定，方便組織選擇使用該標準的任何外部 KMS 供應商。Supermicro 未提供此種安全功能或類似功能。

存取控制

角色式存取控制 (RBAC) 功能會根據使用者的角色決定他們能夠存取哪些系統部分，以及能夠在其中執行哪些任務，是許多伺服器安全策略不可或缺的元素。在 OpenManage Enterprise 中，RBAC 定義了以下三個內建角色的使用者權限：系統管理員、裝置管理器和檢視者。³ 另外，還提供範圍型存取控制 (SBAC)，可讓系統管理員限制裝置管理員能夠存取的裝置群組，⁴ 這樣系統管理員能夠針對某一個裝置的子集來提供存取權限。Supermicro 僅提供 RBAC，未提供 SBAC。

登入資料管理

iDRAC 密碼輪換有幾種用途：根據安全性原則輪換對 OpenManage Enterprise 的存取，預設為每月一次；與外部密碼處理程式搭配使用；支援 CyberArk 管理密碼。^{5,6}

利用 OpenManage Enterprise，系統管理員可以將靜態已知系統管理員帳戶替換為由 OME 管理的服務帳戶，並透過此方式管理 iDRAC 密碼輪換。SSM 沒有此功能。

原則式安全性組態

Dell 在 CloudIQ for PowerEdge AIOps 解決方案中提供原則式網路安全功能。此功能會將已部署 PowerEdge 伺服器的組態，與根據 Dell 最佳實務設定的安全相關組態原則進行比較。如果 CloudIQ 偵測到差異，便會通知系統管理員並提供補救措施。⁷ SSM 未提供類似功能，這可能導致違規偵測延遲。

網路安全性公告

安全性公告旨在向大眾提供安全性問題的相關資訊。根據 Dell 的說法，CloudIQ 中的 Dell Security Advisories 頁面提供了完整的安全性公告清單，同時列出這些安全性問題的影響、受影響的系統數量和發佈日期。⁸ Dell CloudIQ 提供安全性公告報告，其中包含漏洞詳細資訊和補救建議。SSM 未提供類似功能，可能使系統容易遭受攻擊。

關於 Dell CloudIQ

Dell CloudIQ 是一套雲端式的 AIOps 工具，提供「主動式監控、機器學習與預測分析」，適用於 Dell 的許多產品與服務，包括伺服器、儲存裝置、資料保護裝置及超融合基礎架構。⁹ 在一份 2022 年的 Principled Technologies 研究中，我們發現 CloudIQ 對於網路頻寬的影響小至可以忽略，同時卻讓我們能從單一主控台監控遙測、健全狀況狀態、警示和清查結果。¹⁰

如需瞭解 CloudIQ 的更多資訊，請瀏覽 <https://www.dell.com/en-us/dt/solutions/cloudiq.htm>。

動態 USB 連接埠停用

停用和啟用 USB 連接埠的功能可讓系統管理員控管透過 USB 連接埠存取伺服器的能力，避免 USB 連接埠遭到惡意使用及安裝禁用應用程式或病毒的風險。

Dell iDRAC 提供獨立的動態 USB 連接埠停用功能，不必經歷任何停機時間。雖然 Supermicro 在 BIOS 中提供動態前側 USB (和後側 USB) 停用功能，但需要使用 Supermicro DataCenter 管理套件的節點授權金鑰才能啟用此功能。IT 可以透過系統鎖定命令來觸發此功能，系統鎖定命令可以從 BMC 或 Supermicro IPMI 主控台執行，但它並不是系統鎖定模式之外的獨立功能。¹¹

如圖 3 所示，使用 Dell iDRAC 停用連接埠相當簡單，整個過程只有 4 個步驟且僅需用 41 秒，而 Supermicro IPMI 所用的時間是四倍多，有 6 個步驟，所花時間為 2 分 50 秒。將節省的時間乘以 100 個系統，總共節省的時間可達 3 小時 35 分鐘，這表示系統管理員在使用 Supermicro IPMI 時，需要用將近半個工作天來完成這件事，而使用 Dell iDRAC 時則僅需一個多小時即可完成。

停用正面 USB 連接埠的時間 | 時間(時:分:秒) | 數值越小越好

1 台伺服器

■ Dell iDRAC

■ Supermicro IPMI

0:00:41

0:02:50

100 台伺服器 (推算)

01:08:20

上午 4:43



Dell 可將
停用正面 USB 連接埠所需時間減少 75%
相比於 Supermicro

圖 3：在單一部伺服器停用前置 USB 連接埠所需時間，然後推算在 100 部伺服器停用前置 USB 連接埠所需時間。越少越好。資料來源：Principled Technologies。

關於 Dell OpenManage Enterprise

OpenManage Enterprise 是資料中心的一對多系統管理主控台。其控制台提供現代化的 HTML5 圖形使用者介面，並且可部署為虛擬裝置，適用於 VMware ESXi、Microsoft Hyper-V 及核心型虛擬機器 (KVM) 環境。OpenManage Enterprise 能探索並清查 IPv4 和 IPv6 網路最多 8,000 部裝置，包括 Dell 機架式伺服器、Dell 立式伺服器、Dell 刀鋒和機箱。¹² 在一項近期的 PT 研究中，我們發現部署了 OpenManage Enterprise 與 OpenManage Enterprise Modular (OME-M) 的 Dell 環境，能節省變更 VLAN 所需時間，並可避免在定期韌體更新期間遭到干擾。¹³

如需瞭解 OpenManage Enterprise 的更多資訊，請瀏覽 <https://www.dell.com/en-us/lp/dt/open-manage-enterprise>

監控、分析和易用性

各種管理工具在支援系統管理員執行監控和分析活動及其他日常任務 (如排程更新) 的方法上有很大差異。在本節中，我們要來檢視 Dell 和 Supermicro 管理工具在執行這些活動和任務時的方法差異。根據我們在進行可持續性和安全性功能調查時的發現，Dell 管理工具套件提供了許多能有效提升系統管理員工作效率與便利性的功能，而 Supermicro 工具則未具備這些功能。表格 6 比較了這兩款工具在管理效益上的優缺點。

表 4：我們對於 Dell 與 Supermicro 管理工具的比較摘要。資料來源：Principled Technologies。

| 功能 | Dell 管理工具的主要效益 | Supermicro 管理工具的劣勢 |
|--|---|---|
|  遙測串流 | iDRAC9 遙測串流可用於串流遠端 syslog 伺服器；有助於預測故障和最佳化效能；能夠將伺服器指標串流到如 Grafana 和 Splunk 等分析工具 | 無自動遙測串流功能 |
|  行動監控和管理 | 功能豐富且適用於 iOS 和 Android 的 OpenManage Mobile 應用程式，能與 OME 和 iDRAC9 整合 | Supermicro IPMIView 應用程式，不能與 SSM 整合 |
|  第三方裝置和伺服器監控 | OME 支援第三方裝置和伺服器監控，包括對主要競爭對手的支援 | 僅支援使用其代理程式、BMC、支援 IPMI 的舊版工具及支援 Redfish 的裝置的第三方裝置 |
|  資產監控 | 透過 OME 和 CloudIQ 提供；OME 能將授權代管伺服器上的資料傳輸到 CloudIQ，以便同時進行多個資料中心的監控活動 | 未提供雲端入口網站，無法彙總多個資料中心的監控資料 |
|  以警示為基礎的動作 | OME 中的原則能依據警示輸入內容觸發動作 | 未提供以警示為基礎的動作 |
|  更便捷的伺服器部署 (能匯入/匯出系統組態) | 能使用 iDRAC9 匯入/匯出伺服器的所有組態項目，匯入程序只有 5 個步驟，需時 48 秒，匯出程序只有 7 個步驟，需時 1 分 9 秒 | 只能匯入/匯出 Baseboard Management Controller (BMC) 組態，需要對每台伺服器進行大量手動設定 |
|  縮短變更 BIOS 組態設定的時間 | 可直接從 iDRAC 快速變更完整的 BIOS 設定，並能將更新和重新開機作業安排在維護時段執行，節省大量管理時間 | BMC 僅提供有限的 BIOS 變更功能，且伺服器必須重新開機；需要更多手動步驟和管理時間 |
|  做為虛擬裝置執行 | 在 OME 中提供，省卻更新作業系統的步驟 | 無類似功能，必須在代管作業系統中執行。這讓系統管理員多了一個需要修補和更新的部分 |
|  連線檢視 | 在 iDRAC 中提供；使用命令行介面 (LLDP) 的故障診斷工具，可用於診斷如佈線、交換器連接埠損壞等網路連線問題 | 未提供連線檢視，欠缺上游交換器連接埠的實體連線資訊 |
|  可排程韌體與驅動程式更新時間 | 在 OME 和 iDRAC 中提供 | 可排程 BIOS 和 BMC 韌體更新的時間，但無法排程驅動程式更新的時間 |

BIOS 組態項目變更

Dell 直接從 iDRAC 提供完整的 BIOS 組態設定變更功能，並能將這些變更安排在下次重新開機時執行。Supermicro 在其 BMC 中提供有限的 BIOS 設定功能。除了功能有限外，要在 Supermicro 伺服器上為任一組態項目進行 BIOS 組態變更，系統管理員還必須將伺服器重新開機，然後才能從開機畫面存取 BIOS 組態功能表。

圖 4 顯示使用 Dell iDRAC 和 Supermicro IPMI 在單台伺服器上執行 BIOS 組態變更所需的時間。與 iDRAC 中的自動化流程設定作業相比，使用 Supermicro 工具執行手動流程所需的時間多出了 2 分 6 秒，是前者的 4.9 倍。如果推算 100 台相同組態伺服器所需的時間，iDRAC 總共可節省 3.5 小時的時間(如果伺服器的組態不同，將無法節省如此多的時間)。

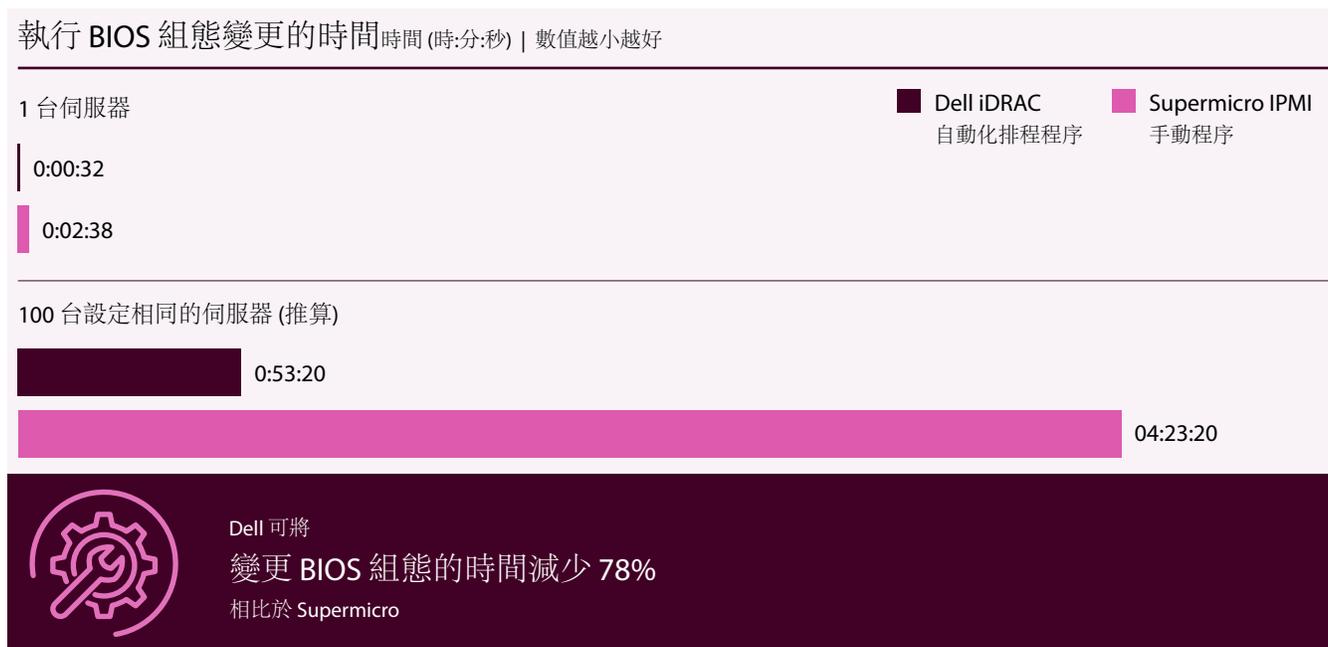


圖 4：在單台伺服器和 100 台組態相同的伺服器上執行 BIOS 組態變更所需的時間 (推算)。越少越好。資料來源：Principled Technologies。

關於 iDRAC9

Dell PowerEdge™ 伺服器隨附 Integrated Dell Remote Access Controller 9 並配備 Dell Lifecycle Controller，提供各種系統管理功能，包括系統警示和遠端管理功能。Dell 表示，iDRAC9 的主要效益包括：

- 能夠使用 API 和指令碼工具來管理數以千計伺服器的功能
- 可檢視伺服器健全狀況並監控數千種狀態參數的嵌入式支援
- 強大的安全性功能與選項¹⁴

如需瞭解 iDRAC9 提供功能的更多資訊，請瀏覽 <https://www.dell.com/en-us/lp/dt/open-manage-idrac>。

自動化韌體和驅動程式更新

iDRAC

與 Supermicro IPMI 不同，Dell iDRAC 可讓您排程自動韌體更新時間。也就是說，排程自動更新的設定工作只需要做一次，可免除每次更新週期重複設定的麻煩。圖 5 顯示使用 Dell iDRAC 和 Supermicro IPMI 初次為 100 台伺服器排程自動韌體更新的推算時間。與 iDRAC 中的自動化流程設定作業相比，使用 Supermicro 工具執行手動流程所需的時間多出了 13 分鐘。

假設系統管理員排定於每個月第一個星期六的晚上執行更新，則使用 iDRAC 時，每台伺服器的一次性時間投資為 58 秒。100 台伺服器的一次性設定時間總共為 1 小時 36 分 40 秒。相比之下，使用 Supermicro IPMI 時，100 台伺服器在每個維護時段的時間投資為 1 小時 50 分鐘。如果我們將 iDRAC 的一次性設定與 Supermicro IPMI 多次重覆設定的第一次進行比較，Dell 管理工具可節省約 13 分 20 秒(請參閱圖 5)。

但是，第二次和以後的每一次，**Dell 都可省下 110 分鐘的時間，因為系統管理員不需要重新執行設定**(請參閱圖 6)。即使 100 台伺服器的組態不相同，也能節省大量時間。請注意，這些時間僅包含將韌體上傳到 BMC 的時間，不包含 Supermicro 韌體的下載和解壓縮時間。

OME

Dell OME 支援**所有元件韌體更新**及 Windows 驅動程式更新。SSM 支援 BIOS 和 BMC 韌體更新，**但不支援驅動程式更新或其他元件的更新。**

初次排程自動韌體更新的推算時間 (100 台伺服器) 時間 (時:分:秒) | 數值越小越好

Dell iDRAC 自動化排程程序

01:36:40

Supermicro IPMI 手動程序

01:50:00



為 100 台伺服器進行首次韌體自動更新排程可節省多達 13 分鐘的時間

圖 5：初次更新 100 台伺服器韌體的推算時間。越少越好。資料來源：Principled Technologies。

排程每次後續自動韌體更新的推算時間 (100 台伺服器) 時間 (時:分:秒) | 數值越小越好

Dell iDRAC 自動化排程程序

無額外時間

Supermicro IPMI 手動程序

01:50:00



透過自動更新程序節省管理時間，完成初次設定後便不需要再花時間進行更新

圖 6：更新 100 台伺服器韌體隨後每次的推斷時間。越少越好。資料來源：Principled Technologies。

結論

在採購伺服器時，供應商的選擇要考慮的不僅僅是硬體平台的效能。決策者還必須考慮影響更長遠的因素，包括系統/資料安全性、能源效率和易管理性。考量這些因素，供應商提供的系統管理工具與硬體一樣重要。

我們研究了 Dell 和 Supermicro 伺服器管理工具的特色和功能，並對 Dell iDRAC9 與 Supermicro IPMI 進行了嵌入式伺服器管理功能比較，以及對 Dell OpenManage Enterprise 和 CloudIQ 與 Supermicro Server Manager 進行了一對多裝置和主控台管理和監控功能的比較。我們發現，與 Supermicro 伺服器相比，Dell 管理工具提供了更完善的安全性、可持續性和管理/監控功能。此外，Dell 工具還能自動執行更多任務，藉此簡化伺服器管理作業，與需要手動執行相同任務的 Supermicro 工具相比，Dell 工具可為系統管理員節省大量時間。

在選購伺服器時，供應商提供的相關管理產品，對於保護資料、支援環境永續和簡化系統維護至關重要。我們的測試和研究顯示，與同類 Supermicro 管理產品相比，適用於 PowerEdge 伺服器的 Dell 管理產品組合提供了更多功能來協助組織達成這些目標。

1. Steve Morgan, "Cybercrime To Cost The World \$10.5 Trillion Annually By 2025" (到 2025 年，網路犯罪每年將使世界損失 10.5 萬億美元)，2024 年 2 月 15 日存取，<https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>。
2. Dell, "Using iDRAC9 RSA SecurID 2FA" (使用 iDRAC9 RSA SecurID 2FA)，2024 年 2 月 15 日存取，<https://dl.dell.com/Manuals/Common/dellemc-idrac9-rsa-securid-2fa.pdf>。
3. Dell, "Dell EMC OpenManage Enterprise SupportAssist Version 1.1 User's Guide" (Dell EMC OpenManage Enterprise SupportAssist 1.1 版使用者指南)，2024 年 2 月 15 日存取，<https://www.dell.com/support/manuals/en-us/openmanage-enterprise-supportassist/omesapuserguide11/role-and-scope-based-access-control-in-openmanage-enterprise?>。
4. Dell, "Dell EMC OpenManage Enterprise SupportAssist Version 1.1 User's Guide" (Dell EMC OpenManage Enterprise SupportAssist 1.1 版使用者指南)
5. Dell, "OpenManage Enterprise 4.0: iDRAC Password Management and Rotation" (OpenManage Enterprise 4.0: iDRAC 密碼管理和輪換)，2024 年 2 月 15 日存取，<https://www.dell.com/support/kbdoc/en-us/000219279/openmanage-enterprise-4-0-idrac-password-management-and-rotation>。
6. Dell, "OpenManage Portfolio Software Licensing Guide" (OpenManage 產品組合軟體授權指南)，2024 年 4 月 3 日存取，<https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/openmanage-portfolio-software-licensing-guide.pdf>。
7. Mark Maclean 和 Kyle Shannon, "Dell CloudIQ Cybersecurity For PowerEdge: The Benefits Of Automation" (適用於 PowerEdge 的 Dell CloudIQ 網路安全性：自動化的優勢)，2024 年 2 月 15 日存取，<https://infohub.delltechnologies.com/en-US/p/dell-cloudiq-cybersecurity-for-poweredge-the-benefits-of-automation/>。
8. Dell, "Security Advisories" (安全性公告)，2024 年 2 月 15 日存取，<https://infohub.delltechnologies.com/en-US/l/cloudiq-a-detailed-review/security-advisories/>。
9. Dell, "Dell CloudIQ - AIOps for Intelligent IT Infrastructure Insights" (Dell CloudIQ IJ 適用於智慧型 IT 基礎結構深入分析的 AIOps)，2024 年 2 月 15 日存取，<https://www.dell.com/en-us/dt/solutions/cloudiq.htm>。
10. Principled Technologies, "Dell CloudIQ provides a single console for proactive monitoring and had negligible impact on network bandwidth in our tests" (Dell CloudIQ 提供單一主控台支援主動監控，經測試證實對網路頻寬影響可忽略不計)，2024 年 1 月 17 日存取 <https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf>。
11. Supermicro, "X13DEM User's Manual" (X13DEM 使用手冊)，2024 年 2 月 16 日存取，<https://www.supermicro.com/manuals/motherboard/X13/MNL-2407.pdf>。
12. Dell, "OpenManage Enterprise"，2023 年 12 月 20 日存取，<https://www.dell.com/en-us/work/learn/openmanage-enterprise>。
13. Principled Technologies, "A Dell PowerEdge MX environment using OpenManage Enterprise and OpenManage Enterprise Modular can make life easier for administrators" (Dell PowerEdge MX 環境使用 OpenManage Enterprise 與 OpenManage Enterprise Modular 能讓系統管理員工作變更輕鬆)，2024 年 1 月 17 日存取，<https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf>。
14. "Integrated Dell Remote Access Controller (iDRAC)"，2024 年 1 月 16 日存取，<https://www.dell.com/en-us/lp/dt/open-manage-idrac>。

閱讀本報告背後的科學依據 ▶



Facts matter.®

Principled Technologies 為 Principled Technologies, Inc. 的註冊商標。
所有其他產品名稱皆為各自所有人之商標。
如需更多資訊，請閱讀本報告背後的科學依據。

此專案是由 Dell Technologies 委託執行。