

Dell Command | Monitor 版本 10.4

使用者指南



備註、提醒及警告

 **備註:**「備註」表示可以幫助您更有效地使用 產品的重要資訊。

 **警告:**「提醒」說明可能會損壞硬件或導致數據遺失，並告訴您如何避免問題。

 **警告:**「警告」表示有可能導致財產損失、人身傷害甚至死亡。

章 1: Dell Command Monitor 10.4 簡介.....	5
Dell Command Monitor 10.4 的最新功能.....	5
Dell Command Monitor 概覽.....	5
章 2: Windows SMM 安全防護功能表格 (WSMT) 規格.....	7
章 3: Dell Command Monitor 10.4 的標準及通訊協定.....	8
章 4: 使用 Dell Command Monitor 10.4 的使用案例情境.....	9
案例 1：資產管理.....	9
SCCM 整合.....	9
案例 2：組態管理.....	9
案例 3：健全狀況監控.....	10
透過作業系統 Event Viewer、Syslog、或 CIM 指示來監控系統.....	10
案例 4：設定檔.....	10
資產設定檔.....	10
電池設定檔.....	11
BIOS 管理設定檔.....	11
開機控制.....	11
基本桌上型行動裝置.....	11
記錄檔記錄.....	11
實體資產.....	11
系統記憶體設定檔.....	12
章 5: 使用 Dell Command Monitor 10.4.....	13
輪詢間隔設定.....	13
RAID 狀態報告.....	13
監控 Dell 用戶端系統.....	13
適用於 Linux 的 Dell Command Monitor 應用程式記錄檔.....	14
偵測進階格式磁碟機.....	14
開機組態.....	14
DCIM_AssetWarrantyInformation.....	14
DCIM_BootConfigSetting.....	15
DCIM_BootSourceSetting.....	15
DCIM_OrderedComponent.....	15
DCIM_Smart 屬性.....	15
DCIM_ThermalInformation.....	16
更改系統設定.....	16
使用 PowerShell 指令在運行 Windows 的系統上設定 BIOS 屬性.....	16
在執行 Linux 的系統設定 BIOS 屬性.....	17
變更開機順序.....	19
遠端關閉並重新啟動 Windows 系統.....	20
遠端取得 Windows 系統上的系統時間值.....	20

章 6: 使用 Dell Command Monitor 10.4 在本機管理 Dell 用戶端系統.....	21
使用 PowerShell 在本機管理 Windows 系統.....	21
使用 OMICLI 在本機管理 Linux 系統.....	22
章 7: 使用 Dell Command Monitor 10.4 遠端管理 Dell 用戶端系統.....	23
使用 PowerShell 透過 Windows 系統遠端管理 Windows 系統.....	23
使用 WinRM 透過 Windows 系統遠端管理 Linux 系統.....	23
使用 WSMAN 透過 Linux 系統遠端管理 Linux 系統.....	24
章 8: Dell Command Monitor 10.4 常見問題.....	25
章 9: 使用 Dell Command Monitor 10.4 的疑難排解步驟.....	27
無法從遠端連線至 Windows Management Instrumentation.....	27
在執行 Windows 的系統上安裝失敗.....	28
BIOS 設定列舉值顯示為 1.....	28
libsmbios 的依存性使 Hapi 安裝失敗.....	28
CIM 資源無法使用.....	28
無法在運行 Ubuntu Core 16 的系統上使用 DCM 執行指令.....	28
章 10: 其他您可能需要的文件.....	29
從 Dell EMC 支援網站存取文件.....	29
章 11: 聯絡 Dell.....	30

Dell Command | Monitor 10.4 簡介

Dell Command | Monitor 軟件應用程式使 IT 管理員可以輕鬆管理車隊庫存、監控系統健全狀況、修改 BIOS 設定及遠端收集已部署 Dell 用戶端系統的資料。

主動系統健全狀況狀態監控可以幫助降低系統總持有成本，並且是管理所有聯網裝置的整體方法一部分。

Dell Command | Monitor 專為 Dell Enterprise 用戶端系統、Dell IoT Gateway 系統以及 Dell Embedded PC 而設。

此文件提供 Dell Command | Monitor 的概覽及其特色。有關支援的 Dell 系統詳情，請參閱可於 dell.com/dellclientcommandsuitemanuals 獲取的發行說明。

主題：

- [Dell Command | Monitor 10.4 的最新功能](#)
- [Dell Command | Monitor 概覽](#)

Dell Command | Monitor 10.4 的最新功能

支援以下新 BIOS 屬性：

- Thermal Management
- Microcode Update Support
- Disable Password Jumper
- Nvme Password Feature
- Allow Non-Admin PSID Revert
- Enable Hybrid Graphics
- PCIe Bifurcation
- HTTP(s) Boot Feature
- HTTP(s) Boot Mode
- Device Configuration Hotkey Access
- Power Button Override
- Disable USB4 PCIe Tunneling
- TME Enable
- Video/Power only on Type-C Ports
- Type-C Dock Override
- Safe Shutter

Dell Command | Monitor 概覽

 **備註：**簡易網絡管理通訊協定 (SNMP) 不支援適用於 Linux 的 Dell Command | Monitor。

Dell Command | Monitor 使用管理通訊協定通用訊息模型 (CIM) 標準和簡易網絡管理通訊協定 (SNMP) 管理用戶端系統。這有助降低系統總持有成本、提高安全性，並提供一種整體方法來管理網絡裝置中的所有裝置。

使用 CIM，您可以透過 Web 服務管理標準 (WSMAN) 存取 Dell Command | Monitor。

Dell Command | Monitor 含有基礎驅動程式集，從不同來源收集用戶端系統資訊，這些來源包括 BIOS、CMOS、System Management BIOS (SMBIOS)、System Management 介面 (SMI)、作業系統和應用程式開發介面 (API)。適用於 Windows 的 Dell Command | Monitor 還從動態連結程式庫 (DLL) 和登錄設定收集用戶端系統資訊。適用於 Windows 的 Dell Command | Monitor 透過 CIM 物件管理員 (CIMOM) 介面、Windows Management Instrumentation (WMI) 堆疊或 SNMP 代理程式來擷取此資訊；而適用於 Linux 的 Dell Command | Monitor 透過開放式管理基礎架構 (OMI) 介面來擷取此資訊。

Dell Command | Monitor 讓 IT 管理員遠端收集資產資訊、修改 BIOS 設定、取得關於潛在故障狀況的主動通知，並取得潛在安全性入侵的警示。在執行 Windows 的系統，這些警示在 NT 事件記錄檔、WMI 事件或 SNMP 設陷 v1 中作為事件提供。在執行 Linux 的系統，這些警示會以 Syslog、OMI 事件或應用程式記錄檔形式接收。

Dell Command | Monitor 可透過直接存取 CIM 資訊整合至主控台，例如 Microsoft System Center Configuration Manager，或透過其他擁有實施適用於 Windows 的 Dell Command | Monitor 整合的主控台廠商。此外，您可以建立自訂指令碼，以針對相關的範圍。指令碼範例可於 Dell 知識庫的 Dell Command | Monitor 頁面獲取。您可以使用這些指令碼來監控資源、BIOS 設定以及系統健康狀況。

i **備註:** 預設安裝並不會啟用 SNMP 支援。如需適用於 Windows 的 Dell Command | Monitor 啟用 SNMP 支援的更多資訊，請參閱 Dell Command | Monitor 安裝指南（載於 dell.com/dellclientcommandsuite/manuals）。

i **備註:** 預設安裝並不會啟用 SNMP 支援。如需適用於 Windows 的 Dell Command | Monitor 啟用 SNMP 支援的更多資訊，請參閱 Dell Command | Monitor 安裝指南。

Windows SMM 安全防護功能表格 (WSMT) 規格

Windows (SMM) 安全防護功能表格規格包含 ACPI 表格的詳細資料，此表格是建立來與支援 Windows 虛擬化安全性 (VBS) 功能的 Windows 作業系統搭配使用。Dell Command | Monitor 兼容 WSMT。在具備支援 WSMT 的 BIOS 的 Dell 用戶端系統上用以組態平台功能。

以下是因要兼容 WSMT 以作出的行為改變：

用戶可於具備兼容 WMI/ACPI 的 BIOS 版本的 Dell 用戶端平台上使用 Dell Command | Monitor 功能。

Dell Command | Monitor 10.4 的標準及通訊協定

Dell Command | Monitor 符合 CIM 標準。CIM 規格詳細介紹了用於提高與管理通訊協定相容性的對應技術。管理通訊協定例如 WMI、SNMP 及 WSMAN 等用於遠端監控。

i | 備註: Dell Command | Monitor for Windows 使用簡易網絡管理通訊協定 (SNMP) 描述系統的幾個變數。

桌面管理任務組 (DMTF) 是業界公認的標準，其領導管理標準 (包括 CIM 和 ASF) 的開發、採用和統一，以及桌面、企業和互聯網環境的計劃。

使用 Dell Command | Monitor 10.4 的使用案例情境

本部分描述以下各種使用 Dell Command | Monitor 的案例情境。

您可以在以下情況使用 Dell Command | Monitor：

- 資產管理
- 組態管理
- 健康狀況監控
- 設定檔

主題：

- 案例 1：資產管理
- 案例 2：組態管理
- 案例 3：健全狀況監控
- 案例 4：設定檔

案例 1：資產管理

因為企業和 IT 人員的變更，一間使用許多 Dell 系統的公司無法維持正確的庫存資訊。資訊總監要求識別可升級至 Windows 最新版本系統的計劃。這需要評估部署的系統，以確定此類計劃的大小、範圍及其在財務上的影響。收集資訊涉及大量心力。就工時和中斷一般使用者而言，要為每個用戶端系統部署 IT 人員費用相當高昂。

在每個 Dell 系統上使用 Dell Command | Monitor，IT 管理員可以快速從遠端收集資訊。使用例如 Microsoft System Center Configuration Manager (SCCM) 的工具，IT 管理員可於網絡上查詢每個用戶端系統並收集資訊，例如 CPU 類型和速度、記憶體大小、硬碟容量、BIOS 版本與目前的作業系統版本。一旦收集資訊，則可對其進行分析，以識別可升級至 Windows 最新版本的系統。

您也可以透過 WSMAN/WinRM 指令列或使用任何 CIM 用戶指令列取得資產庫存。

SCCM 整合

您可以透過以下方法將適用於 Windows 的 Dell Command | Monitor 與 SCCM 整合：

- 使用 Dell Command | Monitor 安裝套件內的 MOF 檔（該安裝套件內包含所有 Dell Command | Monitor 類別），並匯入至 ConfigMgr

MOF 位於：

```
C:\Program Files\Dell\Command_Monitor\ssa\omacim\OMCI_SMS_DEF.mof
```

- 使用集合延伸資產報告功能

案例 2：組態管理

一間公司計劃將用戶端平台標準化，並透過其生命週期管理每個系統。為了在這方面作出努力，該公司取得了一套工具，並計劃使用開機前執行環境 (PXE) 以自動化部署新的用戶端作業系統。

問題在於如何無需手動存取桌上型電腦即可在各個用戶端電腦中修改 BIOS 密碼。在每個用戶端系統安裝了 Dell Command | Monitor 後，該公司的 IT 部門就有多個選項可遠端修改開機順序。OpenManage Essentials (OME) 是可與 Dell Command | Monitor 整合的管理主控台，並用於遠端監控所有用戶端系統的 BIOS 設定。另一個選項是編寫指令碼 (CIM、WinRM/WSMAN/PowerShell/WMIC) 來變更 BIOS 設定。您可以將指令碼在網絡上遠端傳送，並在每個用戶端系統上執行。

有關 Dell Command | Monitor 的更多資訊，請參閱 Dell Command | Monitor 參考指南（載於 dell.com/dellclientcommandsuitemanuals）。

有關 Dell Command | Monitor 的更多資訊，請參閱 Dell Command | Monitor 參考指南。

標準化組態可為各種規模的公司大幅節省成本。許多組織部署了標準化用戶端系統，但很少會以電腦生命週期來管理系統組態。在每個用戶端系統安裝了 Dell Command | Monitor 後，IT 部門可以鎖定傳統連接埠以防止使用未經授權的週邊設備，或啟用 LAN 喚醒 (WOL) 以便系統能夠在非尖峰時間從睡眠狀態喚醒以執行系統管理任務。

案例 3：健全狀況監控

使用者在嘗試存取用戶端系統硬碟上的某些檔案時，收到讀取錯誤訊息。使用者重新啟動系統，檔案現在顯示可供存取。使用者則忽略初始問題，因為它似乎已自動解決。同時，Dell Command | Monitor 以問題查詢硬碟以預測故障問題，並傳送自我監測、分析與報告技術 (SMART) 警示至管理主控台。它也對本機使用者顯示 SMART 錯誤。警示指出硬碟發生數個讀/寫錯誤。公司的 IT 部門建議使用者必須立即進行重要資料的備份，並派遣維修技術人員更換硬碟機。

在硬碟故障之前更換，避免使用者停機時間、省去致電至支援中心並無須技術人員親臨桌上型電腦以診斷問題所在。

透過作業系統 Event Viewer、Syslog、或 CIM 指示來監控系統

Dell Command | Monitor 透過以下程序支援監控事件：

- 透過 CIM 類別 DCIM_LogEntry 提取記錄檔。
- 透過 DCIM_AlertIndication 類別監控 CIM 指示。
- (僅 Windows 適用的 Dell Command | Monitor) 透過簡易網絡管理通訊協定 (SNMP) 與 Windows Event Viewer 監控事件。
- (僅 Linux 適用的 Dell Command | Monitor) 透過 Syslog 監控。

有關 Dell Command | Monitor 的更多資訊，請參閱 Dell Command | Monitor 參考指南 (載於 dell.com/dellclientcommandssuitemanuals)。

有關 Dell Command | Monitor 的更多資訊，請參閱 Dell Command | Monitor 參考指南。

案例 4：設定檔

備註: DMTF 設定檔實施僅針對適用於 Windows 的 Dell Command | Monitor。

IT 管理員需要在多廠商及分散式企業環境內管理用戶端系統。他們必須熟習各式各樣的工具和應用程式，同時管理多種桌上型電腦和各種網絡內的行動用戶端系統，因此面臨挑戰。為了降低上述要求的成本並代表所提供的管理資料，我們在 Dell Command | Monitor 中實施了業界標準的分散式管理任務推動小組 (DMTF) 和資料中心基礎結構管理 (DCIM-OEM) 設定檔。本指南中講解了一些 DMTF 設定檔。

如需更多資訊，請參閱 Dell Command | Monitor 參考指南 (載於 dell.com/dellclientcommandssuitemanuals)。

如需 Dell Command | Monitor 的更多資訊，請參閱 Client Command | Monitor 參考指南。

資產設定檔

端點裝置的保養狀態：

- 透過列舉或獲得 **DCIM_AssetWarrantyInformation** 類別的例項來判斷保養的狀態。
- 檢查是否可以使用 **DCIM_AssetWarrantyInformation** 類別的 **WarrantyStartDate** 和 **WarrantyEndDate** 屬性確定保養狀態。

備註: DCIM_AssetWarrantyInformation 的先決條件是您必須具有有效的互聯網連接。如果您正在 Proxy 伺服器運行 Dell Command | Monitor，確保正確組態 Proxy 設定。

有關更多資訊，請瀏覽 Dell 支援網站：

1. 轉至 Dell.com/support
 2. 在頁面底部的選擇國家/地區下拉清單中確認您的所在國家或地區
 3. 選擇支援類別 — 保養和合約
- 禁用保養功能和隨後的重新整理呼叫。
 - 按需要提取保養資料。

備註: 保養資料每 15 天自動更新一次。如果是最近的保養狀態，則列舉的保養資料可能與 Dell 支援網站的資料不同。

電池設定檔

- 透過列舉或獲得 **DCIM_Battery** 類別的例項來判斷電池的狀態。
- 確定預估運行時間，請參閱預估剩餘電量。
- 檢查是否可使用這些操作狀態與 **DCIM_Battery** 類別的健全狀況屬性來確定電池的健康資訊。
- 利用 **DCIM_Sensor.CurrentState** 屬性或 **CIM_NumericSensor.CurrentState** 屬性取得電池健康之額外資訊。

BIOS 管理設定檔

- 透過列舉 **DCIM_BIOSElement** 的類別例項以判斷 BIOS 版本。
- 檢查 BIOS 屬性值是否可以修改。取得 **DCIM_BIOSEnumeration** 類別的例項。如果屬性 **IsReadOnly** 設定為 **FALSE**，則可以修改屬性。
- 設定系統密碼 (SystemPwd)。運行 **DCIM_BIOSService.SetBIOSAttributes()** 方法，將 SystemPwd 設定為 AttributeName 並將密碼值設定為 AttributeValue 參數。
- 設定 BIOS 或管理員密碼 (AdminPwd)。運行 **DCIM_BIOSService.SetBIOSAttributes()** 方法，將 AdminPwd 設定為 AttributeName 並將密碼值設定為 AttributeValue 參數。
- 運行 **DCIM_BIOSService.SetBIOSAttributes()** 方法，指定 AttributeName 和 AttributeValue 參數。
- 要在 BIOS 或管理員密碼已設定時修改 BIOS 屬性，請運行 **DCIM_BIOSService.SetBIOSAttributes()** 方法並將 AttributeName、AttributeValue 和當前的 BIOS 密碼指定為 AuthorizationToken 輸入參數。

開機控制

- 變更傳統和 UEFI 開機清單中的開機項目順序。
- 啟用或停用傳統和 UEFI 開機清單中的開機項目。
- 透過列舉 **DCIM_ElementSettingData** 類別的例項（其 **IsCurrent** 屬性設為 **1**）可找到目前的開機組態。**DCIM_BootConfigSetting** 代表目前開機組態。

基本桌上型行動裝置

- 透過列舉 **DCIM_ComputerSystem** 類別的例項，判斷系統型號、服務標籤和序號。
- 運行 **DCIM_ComputerSystem.RequestStateChange()** 方法並將 RequestedState 參數值設為 **3**。關閉系統。
- 重新啟動系統。運行 **DCIM_ComputerSystem.RequestStateChange()** 方法並將 RequestedState 參數值設為 **11**。
- 確定系統的電源狀態。
- 透過查詢 **DCIM_Processor** 例項確定系統中的處理器數量，該例項透過 **DCIM_SystemDevice** 關聯與中心例項關聯。
- 取得系統時間。運行 **DCIM_TimeService.ManageTime()** 方法並將 GetRequest 參數設為 **True**。
- 檢查受管元素的健康狀況。

記錄檔記錄

- 選取 **DCIM_RecordLog** 例項以識別記錄檔名稱，該例項的 **ElementName** 屬性對應於記錄檔名稱。
- 尋找各個記錄檔項目。透過關聯的 **DCIM_LogManagesRecord** 獲取與 **DCIM_RecordLog** 指定例項關聯的所有 **DCIM_LogEntry** 例項。根據 **RecordID** 排序例項。
- 透過列舉類別 **DCIM_RecordLog**（其屬性 **Enabledstate** 設定為 **2**，代表啟用，而 **EnabledState** 設定為 **3**，代表停用）的例項來檢查記錄檔是否已啟用。
- 根據記錄檔項目的時間戳排序記錄檔記錄。透過關聯的 **DCIM_LogManagesRecord** 獲取與 **DCIM_RecordLog** 指定例項關聯的所有 **DCIM_LogEntry** 例項。根據後進先出法 (LIFO) 順序的 **CreationTimeStamp** 屬性值排序 **DCIM_LogEntry** 例項。
- 運行 **ClearLog()** 方法以清除 **DCIM_RecordLog** 提供的例項記錄。

實體資產

- 取得系統中所有裝置的實體清單。
- 取得系統機箱的實體清單。
- 判斷失敗元件的零件號碼。

- 判斷插槽是否是空的。

系統記憶體設定檔

- 取得系統的記憶體資訊。
- 取得系統的實體記憶體資訊。
- 檢查系統的記憶體大小。
- 檢查可用的系統記憶體大小。
- 檢查實體系統記憶體大小。
- 檢查系統記憶體的 health 狀況。

使用 Dell Command | Monitor 10.4

您可存取下列連結，瀏覽由 Dell Command | Monitor 提供的資訊：`root\dcim\sysman (standard)`

Dell Command | Monitor 透過這些命名空間中的類別提供資訊。

有關這些類別的更多資訊，請參閱 Dell Command | Monitor 參考指南（載於 dell.com/dellclientcommandssuitemanuals）。

主題：

- 輪詢間隔設定
- RAID 狀態報告
- 監控 Dell 用戶端系統
- 適用於 Linux 的 Dell Command | Monitor 應用程式記錄檔
- 偵測進階格式磁碟機
- 開機組態
- 更改系統設定

輪詢間隔設定

可以使用 Dell Command | Monitor 更改以下輪詢間隔，例如風扇探查、溫度探查、電壓探查、電流探查、磁碟容量增加/減少、記憶體大小增加/減少和處理器數量增加/減少。

- Windows 的 `dcsbdy32.ini` 或 `dcsbdy64.ini` 檔案載於 `<Dell Command | Monitor installed location>\omsa\ini`。
- Linux 的 `AlertPollingSettings.ini` 檔案載於 `/opt/dell/dcm/conf`。

備註：INI 檔案中的數字是 **23** 的倍數。磁碟容量和自我監控分析，與報告技術 (SMART) 警示的預設輪詢間隔為 **626** 秒（實際時間 = 626×23 秒，即大約 3 個小時）。

RAID 狀態報告

Dell Command | Monitor 啟用 RAID 組態資訊並透過硬體和驅動程式支援來監控用戶端系統的 RAID 功能。您可以使用 RAID 類別以取得有關 RAID 層級、驅動程式資訊、控制器組態和控制器狀態的詳細資訊。一旦啟用了 RAID 組態，即可接收磁碟機和控制器降級或故障的警示。

備註：RAID 狀態報告僅受運行於 Common Storage Management Interface (CSMI) 版本 0.81 相容驅動程式的 RAID 控制器支援。OMCI 8.1 及其更高版本僅支援 Intel 晶片上 RAID 控制器中的監控；而對於 OMCI 8.2 及其更高版本，則支援 Intel 晶片上 RAID 控制器中的警示功能。

監控 Dell 用戶端系統

- Dell Command | Monitor 適用於 Windows，可支援簡易網絡管理通訊協定 (SNMP) 以監控及管理用戶端系統，例如筆記型電腦、桌上型電腦和工作站。管理資訊庫 (MIB) 檔案在 Dell Command | Monitor 和 Server Administrator 之間共用。Dell Command | Monitor 適用於 Windows，從版本 9.0 已經過修改，使用用戶端特定的 OID (10909)，使得主控台可識別用戶端系統。

如需 SNMP 的更多資訊，請參閱 Dell Command | Monitor SNMP 參考指南（載於 dell.com/dellclientcommandssuitemanuals）。

如需 SNMP 的更多資訊，請參閱 Dell Command | Monitor SNMP 參考指南。

- Dell Command | Monitor 適用於 Linux，可支援使用 WinRM 和 WSMAN 指令進行監控。

適用於 Linux 的 Dell Command | Monitor 應用程式記錄檔

適用於 Linux 的 Dell Command | Monitor 將應用程式記錄檔和警示分為報告和偵錯用途。您可以在 `dcm_application.log` 檔案（載於 `/opt/dell/dcm/var/log`）檢視 Dell Command | Monitor 應用程式產生的警示和記錄檔歷史。

組態檔案

您可以更新 `log.property` 組態檔案（載於 `/opt/dell/dcm/conf`），以套用所需的設定並除錯：

備註： 對組態檔案作任何變更後，需要重新啟動 OMI 伺服器，才能套用這些變更。

- Log_Level - 設有三個記錄檔層級以分隔系統訊息：錯誤 (ERROR)、資訊 (INFO)、除錯 (DEBUG)。

使用者可以在組態檔案變更記錄檔層級。如果記錄檔層級設定為除錯 (DEBUG)，Dell Command | Monitor 應用程式記錄檔會將所有資訊傳送至指定的記錄檔。

備註： 預設記錄檔層級設定為資訊。

- File_Size — 使用者可以指定 `dcm_application.log` 檔案的大小上限。預設檔案大小為 500 MB。

備註： File_Size 的值必需以位元表示。

- BackupIndex — 使用者可以指定 `dcm_application.log` 檔案的變換計數。如果預設變換計數為 2，第三個備份檔案將會覆寫最舊的檔案。

偵測進階格式磁碟機

用戶端系統轉換為進階格式 (AF) 磁碟機，以獲得更大的儲存容量，並解決 512 位元組磁區硬碟 (HDD) 的限制。硬碟轉換為 4KB 磁區可以保持回溯相容性，而最新的 AF 硬碟（也稱為 512e 硬碟）匹配 512 位元組 SATA 並在 4KB 下操作。在轉換過程中，您可能會遇到性能問題，如用戶端系統中磁碟分割未對齊的硬碟導致基於磁區的加密軟體套件（處理 512e 硬碟）發生故障。Dell Command | Monitor 可讓您確定系統中的硬碟是否為 4KB AF 磁碟機，從而有助於防止這些問題。

開機組態

備註： Dell Command | Monitor for Linux 不提供開機組態功能。因此本部分不適用於 Dell Command | Monitor for Linux。

用戶端系統可以有兩種類型的開機組態之一：

- 傳統 (BIOS)
- UEFI

在 Dell Command | Monitor 中，開機組態（傳統或 UEFI）使用下面的類別模型化：

- DCIM_ElementSettingData
- DCIM_BootConfigSetting
- DCIM_OrderedComponent
- DCIM_BootSourceSetting
- DCIM_SmartAttributeInfo

備註： 字詞開機組態和開機清單類型可互換使用，且傳達了代表傳統或 UEFI 的相同含義。

DCIM_AssetWarrantyInformation

- 要查詢端點裝置的保養狀態，請運行以下指令：

```
Get-CimInstance -Namespace root/DCIM/SYSMAN -ClassName DCIM_AssetWarrantyInformation
```

- 按 WarrantyEndDate 的時間順序列出保養使用權利，請運行以下指令：

```
Get-CimInstance -Namespace root/dcim/sysman -ClassName DCIM_AssetWarrantyInformation |
Sort-Object -Property WarrantyEndDate | Select Name, WarrantyEndDate, WarrantyStartDate
```

- 要禁用保養功能和隨後的重新整理呼叫，請運行以下指令：

```
Get-CimInstance -Namespace root/DCIM/SYSMAN -ClassName DCIM_AssetWarrantyInformation |
Where-Object{$_ .InstanceID -eq "Root/MainSystemChassis/COOObject/COOWarranty:0"} | Invoke-
CimMethod -MethodName DisableWarranty
```

- 按需要提取保養資料，請運行以下指令：

```
Get-CimInstance -Namespace root/DCIM/SYSMAN -ClassName DCIM_AssetWarrantyInformation |
Where-Object{$_ .InstanceID -eq "Root/MainSystemChassis/COOObject/COOWarranty:0"} | Invoke-
CimMethod -MethodName RefreshWarranty
```

i 備註: 設定 Proxy 組態 —

- 預設 proxy — Dell Command | Monitor 選擇預設的系統 proxy (在 IE 中設定)
- 自訂 proxy

DCIM_ApplicationProxySetting 類別用於根據 proxy 環境修改 Dell Command | Monitor 的 proxy 設定。

DCIM_BootConfigSetting

DCIM_BootConfigSetting 的例項代表開機組態，在開機程序期間使用。例如，在用戶端系統上，有兩種類型的開機組態 — Legacy (傳統) 和 UEFI。因此，**DCIM_BootConfigSetting** 有兩個例項的最大值，分別代表 Legacy (傳統) 和 UEFI。

您可以使用下列屬性判斷 **DCIM_BootConfigSetting** 是否代表傳統：

- InstanceID = 「DCIM:BootConfigSetting:Next:1」
- ElementName = 「下一個開機組態設定：開機清單類型 1」

您可以使用下列屬性判斷 **DCIM_BootConfigSetting** 是否代表 UEFI：

- InstanceID = 「DCIM:BootConfigSetting:Next:2」
- ElementName = 「下一個開機組態設定：開機清單類型 2」

DCIM_BootSourceSetting

此類別代表開機裝置或來源。**ElementName**、**BIOSBootString** 及 **StructuredBootString** 屬性包含用於識別開機裝置的字串。例如：軟碟機、硬碟、CD/DVD 光碟機、網絡、個人電腦記憶卡國際協會 (PCMCIA)、電池電動車 (BEV) 或 USB。根據裝置的開機清單類型，**DCIM_BootSourceSetting** 的例項與其中一個 **DCIM_BootConfigSetting** 的例項相關聯。

DCIM_OrderedComponent

DCIM_OrderedComponent 關聯類別用於將 **DCIM_BootConfigSetting** 例項與代表開機裝置所屬之開機清單類型 (傳統或 UEFI) 之一的 **DCIM_BootSourceSetting** 例項相關聯。**DCIM_OrderedComponent** 的 **GroupComponent** 屬性泛指 **DCIM_BootConfigSetting** 例項，而 **PartComponent** 屬性泛指 **DCIM_BootSourceSetting** 例項。

DCIM_Smart 屬性

如要讀取 smart 屬性值，運行以下指令：

例如：

- Get-CimInstance -Namespace root\dcim\sysman DCIM_SmartAttributeInfo | Format-Table
- Get-CimInstance -Namespace root\dcim\sysman DCIM_SmartAttributeInfo -Filter "AttributeID like '< Attribute ID Value >'"

如要設定自訂閾值，執行以下指令：

例如：

- `Get-CimInstance -Namespace root\dcim\sysman DCIM_SmartAttributeInfo -Filter "AttributeID like '<Attribute ID Value>'" | Invoke-CimMethod -MethodName "SetCustomThreshold" -Arguments @{CustomThresholdValue="<custom threshold value to be set>"}`

DCIM_ThermalInformation

DCIM_ThermalInformation 管理散熱組態設定，例如熱模式、AAC 模式和風扇故障模式。

- 要查詢裝置的散熱資料，請運行以下指令：

```
Get-CimInstance -Namespace root/DCIM/SYSMAN -ClassName DCIM_ThermalInformation
```

- 要設定熱模式的值，請運行以下指令：

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ThermalInformation | Where-Object {$_.AttributeName -eq "Thermal Mode"} | Invoke-CimMethod -MethodName ChangeThermalMode -Arguments @{AttributeName=@"Thermal Mode";AttributeValue=@"2"}
```

更改系統設定

在 Dell Command | Monitor 中，使用以下方法來更改系統設定和本機或遠端系統的狀態：

- SetBIOSAttributes — 變更 BIOS 設定
 - ⓘ **備註：**適用於 Linux 的 Dell Command | Monitor 目前僅支援 SetBIOSAttributes 方法。
- ChangeBootOrder — 變更開機的組態
- RequestStateChange — 關閉及重新啟動系統
- ManageTime — 顯示系統時間

在適用於 Windows 的 Dell Command | Monitor 中，您可以使用 `winrm`、VB 指令碼、PowerShell 指令、`wmic` 和 WMI `wbemtest` 以運行這些方法。

使用 PowerShell 指令在運行 Windows 的系統上設定 BIOS 屬性

使用 SetBIOSAttributes 方式來設定 BIOS 屬性：下面說明使用啟用可信平台模組 (Trusted Platform Module, TPM) 的程序為範例。

ⓘ **備註：**按照下列程序啟用 TPM 之前，請確定 TPM 選項已在 BIOS 中清除。

ⓘ **備註：**使用具有管理員權限的 PowerShell。

啟用 TPM，

1. 設定系統的 BIOS 密碼。若尚未設定，使用下列的 PowerShell 指令：

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod -MethodName SetBIOSAttributes -Arguments @{AttributeName=@"AdminPwd";AttributeValue=@"<Admin password>"}
```

2. 使用以下指令確保 TPM 安全：

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod -MethodName SetBIOSAttributes -Arguments @{AttributeName=@"Trusted Platform Module";AttributeValue=@"1";AuthorizationToken="<Admin password>"}
```

3. 重新啟動系統。

4. 使用以下指令啟用 TPM：

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod -MethodName SetBIOSAttributes -Arguments @{AttributeName=@"Trusted Platform Module Activation";AttributeValue=@"2";AuthorizationToken="<Admin password>"}
```

5. 重新啟動系統。

在執行 Linux 的系統設定 BIOS 屬性

使用下列其中一種方式來設定 BIOS 屬性：

- 使用 OMICLI
- 使用 WinRM
- 使用 WSMAN

 **備註:** 確保 OMI 伺服器已啟動並正在運行。

使用 OMICLI 設定 BIOS 屬性

使用 SetBIOSAttributes 方式來設定 BIOS 屬性：下面說明使用啟用可信平台模組 (Trusted Platform Module, TPM) 的程序為範例。

 **備註:** 按照下列程序啟用 TPM 之前，請確定 TPM 選項已在 BIOS 中清除。

使用 OMICLI 指令設定 BIOS 屬性：

1. 設定系統的 BIOS 密碼。若尚未設定，運行

```
./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService
SystemCreationClassName DCIM_ComputerSystem SystemName <system name displayed in
DCIM_BIOSService class> CreationClassName DCIM_BIOSService } SetBIOSAttributes
{ AttributeName "AdminPwd" AttributeValue "<new Admin Password>" }
```

2. 使用以下指令確保 TPM 安全，運行

```
./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService
SystemCreationClassName DCIM_ComputerSystem SystemName <system name displayed in
DCIM_BIOSService class> CreationClassName DCIM_BIOSService } SetBIOSAttributes
{ AttributeName "Trusted Platform Module" AttributeValue "1" AuthorizationToken
"<password>" }
```

3. 重新啟動系統。
4. 要啟用 TPM，運行

```
./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService
SystemCreationClassName DCIM_ComputerSystem SystemName <system name displayed in
DCIM_BIOSService class> CreationClassName DCIM_BIOSService } SetBIOSAttributes
{ AttributeName "Trusted Platform Module Activation" AttributeValue "2"
AuthorizationToken "<password>" }
```

5. 重新啟動系統。
6. 要重設 BIOS 密碼，運行

```
./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService
SystemCreationClassName DCIM_ComputerSystem SystemName <system name displayed in
DCIM_BIOSService class> CreationClassName DCIM_BIOSService } SetBIOSAttributes
{ AttributeName "AdminPwd" AttributeValue "" AuthorizationToken "<password>" }
```

使用 WinRM 設定 BIOS 屬性

使用 SetBIOSAttributes 方式來設定 BIOS 屬性：下面說明使用啟用可信平台模組 (Trusted Platform Module, TPM) 的程序為範例。

 **備註:** 按照下列程序啟用 TPM 之前，請確定 TPM 選項已在 BIOS 中清除。

使用 WinRM 指令設定 BIOS 屬性：

1. 透過列舉 DCIM_BIOSService 類別來獲取選擇器集。運行：

```
winrm e wsman/DCIM_BIOSService?__cimnamespace=root/dcim/sysman -auth:basic -r:https://
<system IP or system name>:<Port Number (5985/5986)> -username:<user name> -
password:<password> -skipCAcheck -skipCNcheck -encoding:utf-8 -returnType:epr
```

備註: 選擇器設定值 (SystemName=<system name from DCIM_BIOSService class>winrm i SetBIOSAttributes wsman/DCIM_BIOSService?SystemName=dt: +SystemCreationClassName=DCIM_ComputerSystem+Name=DCIM:BiosService +CreationClassName=DCIM_BIOSService+) 在此例子中用於設定操作。

2. 設定系統的 BIOS 密碼。若尚未設定，使用下列的指令：

```
winrm i SetBIOSAttributes http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_BIOSService?__cimnamespace=root/dcim/sysman+Name=DCIM:BiosService+SystemCreationClassName=DCIM_ComputerSystem+SystemName=<system name from DCIM_BIOSService class>+CreationClassName=DCIM_BIOSService -r:https://<system IP or system name>:5986 -u:<user name> -password:<password> -auth:basic -skipCAcheck -skipCNcheck -encoding:utf-8 @{@AttributeName="AdminPwd";AttributeValue="<Password>"}
```

3. 運行以下指令確保 TPM 安全：

```
winrm i SetBIOSAttributes "http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_BIOSService?__cimnamespace=root/dcim/sysman+Name=DCIM:BiosService+SystemCreationClassName=DCIM_ComputerSystem+SystemName=<system name from DCIM_BIOSService class>+CreationClassName=DCIM_BIOSService -r:https://<system IP or system name>:5986 -u:<user name> -password:<password> -auth:basic -skipCAcheck -skipCNcheck -encoding:utf-8 @{@AttributeName="Trusted Platform Module";AttributeValue="1";AuthorizationToken="<Admin password>"}
```

4. 重新啟動系統。

5. 使用以下指令啟用 TPM：

```
winrm i SetBIOSAttributes "http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_BIOSService?__cimnamespace=root/dcim/sysman+Name=DCIM:BiosService+SystemCreationClassName=DCIM_ComputerSystem+SystemName=<system name from DCIM_BIOSService class>+CreationClassName=DCIM_BIOSService -r:https://<system IP or system name>:5986 -u:<user name> -password:<password> -auth:basic -skipCAcheck -skipCNcheck -encoding:utf-8 @{@AttributeName=("Trusted Platform Module Activation");AttributeValue=("2");AuthorizationToken="<Admin password>"}
```

使用 WSMAN 設定 BIOS 屬性

您可以使用 WSMAN 在運行 Linux 的系統上設定 BIOS 屬性。下面說明使用啟用可信平台模組 (Trusted Platform Module, TPM) 的程序為範例。

備註: 按照下列程序啟用 TPM 之前，請確定 TPM 選項已在 BIOS 中清除。

1. 透過列舉 DCIM_BIOSService 類別來獲取選擇器集。運行：

```
wsman invoke -a "SetBIOSAttributes" http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_BIOSService?Name="DCIM:BIOSService", SystemCreationClassName="DCIM_ComputerSystem", SystemName="<system name from DCIM_BIOSService class>", CreationClassName="DCIM_BIOSService" -N root/dcim/sysman -h <system IP/name> -P 5985 -u <user name> -p <password> -y basic -v -V -k "AttributeName=AdminPwd" -k "AttributeValue=<password>"
```

2. 設定系統的 BIOS 密碼。若尚未設定，使用下列的指令：

```
wsman invoke -a "SetBIOSAttributes" http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_BIOSService?Name="DCIM:BIOSService", SystemCreationClassName="DCIM_ComputerSystem", SystemName="<system name from DCIM_BIOSService class>", CreationClassName="DCIM_BIOSService" -N root/dcim/sysman -h <system IP or system name> -P 5985 -u <user name> -p <password> -y basic -v -V -k "AttributeName=Trusted Platform Module" -k "AttributeValue=1" -k "AuthorizationToken=<password>"
```

3. 使用以下指令確保 TPM 安全：

```
wsman invoke -a "SetBIOSAttributes" http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_BIOSService?Name="DCIM:BIOSService", SystemCreationClassName="DCIM_ComputerSystem", SystemName="<system name from DCIM_BIOSService class>", CreationClassName="DCIM_BIOSService" -N root/dcim/sysman -h <system IP or system name> -P 5985 -u <user name> -p <password> -y basic -v -V -k "AttributeName=Trusted Platform Module Activation" -k "AttributeValue=2" -k "AuthorizationToken=<password>"
```

4. 重新啟動系統。
5. 使用以下指令啟用 TPM：

```
wsman invoke -a "SetBIOSAttributes" http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/DCIM_BIOSService?Name="DCIM:BIOSService", SystemCreationClassName="DCIM_ComputerSystem", SystemName="<system name from DCIM_BIOSService class>", CreationClassName="DCIM_BIOSService" -N root/dcim/sysman -h <system IP/name> -P 5985 -u <user name> -p <password> -y basic -v -V -k "AttributeName=AdminPwd" -k "AttributeValue=" -k "AuthorizationToken=<password>"
```

變更開機順序

如欲變更開機順序，遵循下列步驟：

1. 使用以下指令檢查開機順序類型（傳統或 UEFI）：

- WMI 指令：`wmic /namespace:\\root\dcim\sysman path dcim_BootConfigSetting get ElementName/ format:list。`
- PowerShell 指令：`gwmi -namespace root\dcim\sysman -class dcim_BootConfigSetting -Property ElementName。`

2. 使用以下指令檢查目前開機順序類型（傳統或 UEFI）：

- WMI 指令：`wmic /namespace:\\root\dcim\sysman path dcim_ElementSettingData.IsCurrent=1 get SettingData /format:list。`
- PowerShell 指令：`gwmi -namespace root\dcim\sysman -class dcim_elementSettingData -Filter "IsCurrent=1" -Property SettingData。`

3. 使用以下指令更改開機順序：

- WMI 指令：`wmic /namespace:\\root\dcim\sysman path dcim_bootconfigsetting call ChangeBootOrder /?:full。`
- PowerShell 指令：`(gwmi -namespace root\dcim\sysman -class dcim_bootconfigsetting).getmethodparameters("ChangeBootOrder")。`
- ① 備註：`dcim_BootConfigSetting` 例項必須代表您想變更的開機組態 — 無論是類型 1（傳統）或類型 2（UEFI）。

- 引數為：
 - Authorization Token — 這是系統管理員或開機密碼。
 - Source — 這是取自 `dcim_OrderedComponent.PartComponent` 屬性的開機順序清單。新的開機順序由來源陣列中的開機裝置順序所決定。

4. 使用 PowerShell 變更類型 1 開機清單的開機順序：

- a. 執行以下指令獲取類型 1 開機清單的目前開機順序：`$boLegacy = gwmi -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-1'} | select -expand partcomponent。`
- b. 定義 PowerShell 變數來指定開機順序，以設定 `$newboLegacy`。為其分配新的開機順序。例如，保留目前的開機順序類型。
- c. `$newboLegacy = $boLegacy`
- d. 執行以下指令獲取對應類型 1 開機清單的 `dcim_bootconfigsetting` 例項：`$bcsLegacy = Gwmi -Namespace root \dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 1'}。`
- e. 執行以下指令調用方法：`$ bcsLegacy.changebootorder($newboLegacy, $AuthorizationToken)。`
`$AuthorizationToken` 變數用於通過 BIOS 密碼。

5. 使用 PowerShell 變更類型 2 開機清單的開機順序：

- a. 執行以下指令獲取類型 2 開機清單的目前開機順序：`$boUefi = gwmi -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-2'} | select -expand partcomponent。`
- b. 定義 PowerShell 變數來指定開機順序，以設定 `$newboUefi`。為其分配新的開機順序。例如，保留目前的開機順序類型。
- c. 執行以下指令獲取對應類型 2 開機清單的 `dcim_bootconfigsetting` 例項：`$bcsUefi = Gwmi -Namespace root \dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 2'}。`
- d. 執行以下指令調用方法：`$ bcsUefi.changebootorder($newboUefi, $AuthorizationToken)。`
`$AuthorizationToken` 變數用於通過 BIOS 密碼。

遠端關閉並重新啟動 Windows 系統

您可以使用 RequestStateChange 方法遠端關閉或重新啟動 Windows 系統。

1. 使用以下指令遠端關閉 Windows 系統：

```
(gwmi -ComputerName "SYSNAME" -Namespace root\dcim\sysman DCIM_ComputerSystem | Where-Object {$_.Dedicated -ne 28}).RequestStateChange(3)
```

2. 使用以下指令遠端重新啟動 Windows 系統：

```
(gwmi -ComputerName "SYSNAME" -Namespace root\dcim\sysman DCIM_ComputerSystem | Where-Object {$_.Dedicated -ne 28}).RequestStateChange(11)
```

遠端取得 Windows 系統上的系統時間值

您可以使用 ManageTime 方法遠端取得 Windows 系統的系統時間值。例如：

在指令列介面中，執行以下操作：

- a. \$cred = Get-Credential
- b. \$session = New-CimSession -ComputerName "Server01" -Credential \$cred
- c. Get-CimInstance -CimSession \$session -Namespace root\dcim\sysman -ClassName DCIM_TimeService | Invoke-CimMethod -MethodName ManageTime -Arguments @{GetRequest="TRUE"}

使用 Dell Command | Monitor 10.4 在本機管理 Dell 用戶端系統

您可使用任何下列方法在本機管理 Dell 用戶端系統：

- 對於執行 Windows 的系統，使用 PowerShell。
- 對於執行 Linux 的系統，使用 OMICLI。

主題：

- 使用 PowerShell 在本機管理 Windows 系統
- 使用 OMICLI 在本機管理 Linux 系統

使用 PowerShell 在本機管理 Windows 系統

您可以使用 PowerShell 指令管理在本機運行 Windows 的 Dell 用戶端系統。

- 列舉 DCIM 類別例項
 - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSEnumeration`
 - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSPassword`
- 獲取 BIOS 設定的屬性

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSEnumeration | Where-Object
{$_ .AttributeName -eq "Num Lock"}
```

- 更改 BIOS 設定

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod
-MethodName SetBIOSAttributes -Arguments @{AttributeName=@"Num
Lock"};AttributeValue=@"1"}
```

- 修改非關鍵值

```
Get-CimInstance -Namespace root\dcim\sysman DCIM_NumericSensor | Where-Object {$_ .DeviceID
-like "Root/MainSystemChassis/TemperatureObj:3"} | Set-CimInstance -Property
@{UpperThresholdNonCritical="10"}
```

- 訂閱警示

```
$a = 0
$timespan = New-Object System.TimeSpan(0, 0, 1)
$scope = New-Object System.Management.ManagementScope("\\.\root\dcim\sysman")
$query = New-Object System.Management.WQLEventQuery("Select * from DCIM_AlertIndication")
$watcher = New-Object System.Management.ManagementEventWatcher($scope,$query)
[array]$alerts=@()
do{ $watcher.WaitForNextEvent() }
while ($a -ne 1)
```

- 從 WMI 獲取使用者同意的指令：

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ImprovementProgramConsent
```

- 從 WMI 設定使用者同意的指令：

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ImprovementProgramConsent |
Invoke-CimMethod -MethodName OverrideImprovementProgramConsent -Arguments @{NewValue="1"}
```

 **備註：** 改進程式僅適用於 DCM 10.4 x64 位元版本。

- 從 WMI 獲取 Proxy 的指令：

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting
```

- 從 WMI 設定 Proxy 的指令：

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting |
Invoke-CimMethod -MethodName Change
ProxySetting -Arguments @{NewAddress="10.0.0.223"; NewPort="8080"}
```

使用 OMICLI 在本機管理 Linux 系統

您可以使用 OMICLI 指令在本機管理 Linux 系統。在運行 Linux 的系統上，OMICLI 安裝在 /opt/omi/bin。

- 列舉 DCIM 類別例項
 - ./omicli ei root/dcim/sysman DCIM_BIOSEnumeration
 - ./omicli ei root/dcim/sysman DCIM_BIOSPassword
- 獲取 BIOS 設定的屬性

```
./omicli gi root/dcim/sysman { DCIM_BIOSPassword InstanceID DCIM:BIOSSetupPassword }
```

- 設定管理員密碼

```
./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService
SystemCreationClassName DCIM_ComputerSystem SystemName <system name from DCIM_BIOSService
class> CreationClassName DCIM_BIOSService } SetBIOSAttributes { AttributeName "AdminPwd"
AttributeValue dell }
```

- 更改此 BIOS 設定

- ./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM_BiosService
SystemCreationClassName DCIM_ComputerSystem SystemName <system name in DCIM_BIOSService
class> CreationClassName DCIM_BIOSService } SetBIOSAttributes { AttributeName "Num Lock"
AttributeValue "1" AuthorizationToken "" }
- ./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService
SystemCreationClassName DCIM_ComputerSystem SystemName <system name from DCIM_BIOSService
class> CreationClassName DCIM_BIOSService } SetBIOSAttributes { AttributeName "AdminPwd"
AttributeValue <password> }

```
./omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService
SystemCreationClassName DCIM_ComputerSystem SystemName <system name from DCIM_BIOSService
class> CreationClassName DCIM_BIOSService } SetBIOSAttributes { AttributeName "AdminPwd"
AttributeValue <password> }
```

- 訂閱警示

```
./omicli sub root/dcim/sysman --queryexpr "select * from DCIM_AlertIndication"
```

使用 Dell Command | Monitor 10.4 遠端管理 Dell 用戶端系統

您可使用任何下列方法遙距管理 Dell 用戶端系統：

- 運行 Windows 的系統方面，使用 PowerShell 透過 Windows 系統遠端管理 Windows 系統 於第 頁 23
- 運行 Linux 的系統方面，使用 WinRM 透過 Windows 系統遠端管理 Linux 系統 於第 頁 23

主題：

- 使用 PowerShell 透過 Windows 系統遠端管理 Windows 系統
- 使用 WinRM 透過 Windows 系統遠端管理 Linux 系統
- 使用 WSMAN 透過 Linux 系統遠端管理 Linux 系統

使用 PowerShell 透過 Windows 系統遠端管理 Windows 系統

您可以使用 PowerShell 透過 Windows 系統遠端存取及監控 Windows 系統。

管理 Windows 系統的先決條件：

- Windows PowerShell 3.0
- 為運行遠端指令碼組態 PowerShell

受管理 Windows 系統的先決條件：

- Dell Command | Monitor
- Windows PowerShell 3.0
- 為運行遠端指令碼組態 PowerShell
- 應啟用 PowerShell 遠端功能

備註：

要遠端使用 Windows PowerShell，必須將遠端電腦組態為遠端管理。有關遠端要求的更多資訊（包括指示操作），請運行 PowerShell 指令 - Get-Help about_remote_requirements。

使用 WinRM 透過 Windows 系統遠端管理 Linux 系統

您可以使用 WinRM 指令在運行 Windows 的系統存取及監控運行 Linux 的系統。

Windows 系統的先決條件

- 支援的 Windows 作業系統
- 為遠端管理運行並組態 WinRM 服務

Linux 系統的先決條件

- 根權限
- Dell Command | Monitor
- 支援的 Linux 作業系統
- 在 WMI 伺服器上啟用 5985 和 5986 連接埠
- 為您的環境組態系統

在指令列介面中，運行

```
winrm enumerate wsman/<DCM class name>?_cimnamespace=root/dcim/sysman -auth:basic -r:http://<system IP or system name:5985> -username:<user name> -password:<password> -skipCAcheck -skipCNcheck -encoding:utf-8
```

使用 WSMAN 透過 Linux 系統遠端管理 Linux 系統

您可以使用 WSMAN 指令運行 Linux 的系統遠端存取及監控運行 Linux 的系統。

管理 Linux 系統的先決條件：

- 已安裝支援的 Linux 作業系統套件
- 已安裝 wsmancli 套件

受管理 Linux 系統的先決條件：

- 根目錄存取權限
- 支援的 Linux 作業系統
- Dell Command | Monitor

啟動終端，並運行

```
wsman enumerate http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/sysman/ <class name> -N root/dcim/sysman -h <system ip/name> -u <user name> -p <password> -P 5985 -y basic -v -V
```

Dell Command | Monitor 10.4 常見問題

如何使用 `DCIM_OrderedComponent.AssignedSequence` 屬性找到開機組態的開機順序？

當 `DCIM_BootConfigSetting` 例項 (舊版或 UEFI) 透過 `DCIM_OrderedComponent` 關聯的例項擁有多個與其相關聯的 `DCIM_BootSourceSetting` 例項 (開機裝置) 時，會使用 `DCIM_OrderedComponent.AssignedSequence` 屬性的值用來判斷順序，相關的 `DCIM_BootSourceSetting` 例項 (開機裝置) 會用來判斷開機順序。當 `DCIM_BootSourceSetting` 其相關的 `CIM_OrderedComponent.AssignedSequence` 屬性等於 0 時，會被忽略且不會被視為開機順序的一部分。

我如何變更開機順序？

您可以使用 `DCIM_BootConfigSetting.ChangeBootOrder()` 方法將開機順序變更。`ChangeBootOrder()` 方法以 `DCIM_BootSourceSetting` 的例項與 `DCIM_BootConfigSetting` 例項相關聯來設定順序。此方法有一種輸入參數，即 `Source`。`Source` 參數是 `DCIM_OrderedComponent` 類別 `PartComponent` 屬性的順序陣列，代表 `DCIM_BootSourceSetting` 例項 (開機裝置) 與 `DCIM_BootConfigSetting` 例項 (開機清單類型 — 傳統或 UEFI) 之間的關聯。

我如何停用開機裝置？

變更開機順序時，每個 `DCIM_OrderedComponent` 例項上的 `AssignedSequence` 屬性值 (此值將 `DCIM_BootConfigSetting` 例項目標與未出現在 `Source` 參數輸入陣列的 `DCIM_BootSourceSetting` 例項互相關聯) 設定為 0，表示該裝置已停用。

當 <what is trying to connect> 嘗試使用 `wbemtest` 連接至命名空間時，將顯示失敗登入訊息。

以管理員權限層級啟動 `wbemtest` 來解決任何登入訊息。從所有程式清單移至 Internet Explorer，然後以右鍵按一下以系統管理員身份執行啟動 `wbemtest` 並避免任何命名空間可產生的錯誤。

如何不發生任何問題下執行知識庫指令碼？

以下是運行於 Dell Command | Monitor 知識庫連結提供的 VBS 指令碼時的步驟：

1. 使用指令 `winrm quickconfig` 於系統上組態 `winrm`。
2. 檢查權杖支援是否存在於系統上，請參閱：
 - 在 BIOS 設定中的 **F2 螢幕**。
 - 使用如 `wbemtest` 的工具，檢查指令碼定義的金鑰值是否存在於系統中。

備註： Dell 建議您使用最新的 BIOS，您可於 dell.com/support 獲取。如需更多資訊，請參閱 Dell Command | Monitor 參考指南 (載於 dell.com/dellclientcommandssuitemanuals)。

備註： 使用最新的 BIOS。

如何設定 BIOS 屬性？

BIOS 屬性可使用 `DCIM_BIOSService.SetBIOSAttributes()` 方法來變更。`SetBIOSAttributes()` 方法會設定在 `DCIM_BIOSEnumeration` 類別中定義的例項的值。此方法有七個輸入參數。首兩個參數可空白或為零。第三個參數 `AttributeName` 必須將輸入對應 `DCIM_BIOSEnumeration` 類別屬性名稱例項的值。第四個參數或 `AttributeValue` 可以在 `DCIM_BIOSEnumeration` 類別中定義的屬性名稱的任何可能的值。第五個參數 `AuthorizationToken` 為可選，第五個參數的輸入為 BIOS 密碼。第五個參數僅在系統上設定 BIOS 密碼時使用，否則為空白。第六個和第七個引數可再次空白或為零。

Dell Command | Monitor 是否支援 Windows 與 Linux 作業系統的儲存和感測器監控？

是，Dell Command | Monitor 可支援受支援 Windows 與 Linux 作業系統的儲存和感測器監控。

在儲存監控中，Dell Command | Monitor 支援以下監控與警示：

- Intel 整合式控制器 (與 CSMI v0.81 或較後版本相容)
- LSI 整合式 RAID 控制器；和 9217、9271、9341、9361 及其相關的驅動程式 (實體和邏輯)

備註： 執行 Linux 作業系統的系統不支援監控 Intel 整合式控制器。

在感測器監控中，Dell Command | Monitor 支援電壓、溫度、安培、散熱裝置 (風扇) 和機箱感測器的監控與警示。

有關類別和警示的更多資訊，請參閱 Dell Command | Monitor 參考指南 (載於 dell.com/dellclientcommandssuitemanuals)。

Dell Command | Monitor 可以與其他應用程式/主控台整合嗎？

可以，Dell Command | Monitor 能與支援業界標準的領先企業管理主控台接合。它可以使用下列現有的企業管理工具進行整合：

- 適用 System Center 2012 的 Dell 用戶端整合套件

- Dell OpenManage Essentials
- 適用 System Center 作業管理員的 Dell 用戶端管理套件

可匯入類別至 SCCM 以清查嗎？

是的，個別 MOF 或 OMCI_SMS_DEF.mof 檔案可匯入 SCCM 主控台做為清查用。

SCCM OMCI_SMS_DEF.mof 檔案位於何處？

OMCI_SMS_DEF.mof 檔案位於 C:\Program Files\Dell\Command_Monitor\ssa\omacim\OMCI_SMS_DEF.mof。

如何為 DCM 10.2.1 組態 proxy ？

DCM 10.2.1 無法獲取保養資料。

使用 DCIM_ApplicationProxySetting 類別檢查是否正確組態應用程式 proxy 設定。

我如何為 Dell Command | Monitor 組態 proxy 憑證？

如果您通過 Dell Command | Monitor 登入，您可以使用相同的憑證進行 proxy 驗證。

使用 Dell Command | Monitor 10.4 的疑難排解 步驟

主題：

- 無法從遠端連線至 Windows Management Instrumentation
- 在執行 Windows 的系統上安裝失敗
- BIOS 設定列舉值顯示為 1
- libsbios 的依存性使 Hapi 安裝失敗
- CIM 資源無法使用
- 無法在運行 Ubuntu Core 16 的系統上使用 DCM 執行指令

無法從遠端連線至 Windows Management Instrumentation

如果遠端客戶端電腦系統的 Common Information Model (CIM, 通用訊息模型) 資訊無法為管理應用程式使用, 或如果使用分散式元件物件模型 (DCOM) 的遠端 BIOS 更新失敗, 會顯示下列錯誤訊息：

- 存取遭拒
 - Win32：無法使用 RPC 伺服器
1. 確認用戶端系統已連接至網絡。在伺服器指令提示輸入下列內容：
ping <Host Name or IP Address> 並按下 <Enter>。
 2. 如果伺服器和用戶端系統都在同一個網域中運行下列步驟：
 - 請確認網域管理員帳戶在兩個系統都有管理員權限。

如果伺服器和用戶端系統都在同一個工作群組中 (不在同一個網域), 運行下列步驟：

- 確保您的伺服器運行於最新的 Windows 伺服器上。

i 備註: 變更登錄前請先備份系統資料檔案。不正確編輯登錄可能會使作業系統無法使用。

3. 在用戶端系統編輯登錄變更。按一下**開始 > 執行**, 輸入 **regedit**, 然後按一下**確定**。在**登錄編輯程式**視窗中, 瀏覽至 `My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`。
4. 將 **forceguest** 值設為 0 (預設值為 1)。除非您修改此值, 從遠端連接至系統的使用者會有「來賓」的權限, 即使提供的憑證提供系統管理員權限亦是如此。
 - a. 以相同的使用者名稱和密碼在用戶端系統上建立帳戶, 以在 WMI 管理應用程式的系統上, 做為管理員帳戶。
 - b. 如果您使用 IT Assistant, 請執行 IT Assistant ConfigServices 公用程式 (在 IT Assistant 安裝目錄下的 `configservices.exe`, 位於 `/bin` 目錄中)。設定 IT Assistant 在本機系統管理員帳戶下執行, 亦即是現在遠端用戶端的管理員。此外, 確認 DCOM 和 CIM 已啟用。
 - c. 如果您使用 IT Assistant, 使用系統管理員帳戶來為用戶端系統設定子網絡探索。輸入使用者名稱為 `<client machine name>\<account name>`。如果已探索到系統, 請從已探索系統清單中移除系統, 為其設定子網絡探索, 然後再重新探索。

i 備註: Dell 建議使用 Dell OpenManage Essentials 替代 IT Assistant。如需更多 Dell OpenManage Essentials 的資訊, 請參閱 dell.com/dellclientcommandsuitemanuals。

i 備註: 使用 Dell OpenManage Essentials 以替代 IT Assistant。

5. 修改遠端連線到系統的 WMI 的使用者權限層級, 請運行以下步驟：
 - a. 按一下**開始 > 執行**, 輸入 `compmgmt.msc`, 然後按一下**確定**。
 - b. 瀏覽至**服務和應用程式**下的 **WMI 控制**。
 - c. 以滑鼠右鍵按一下 **WMI 控制**, 然後按一下**內容**。
 - d. 按一下**安全性**索引標籤, 然後選取在 **根目錄樹狀圖**下的 **DCIM/SYSMAN**。
 - e. 按一下**安全性**。

- f. 選取所要控制存取的特定群組或使用者，並使用**允許**或**拒絕**核取方塊組態權限。
6. 執行下列步驟，以從使用 WMI CIM Studio 的遠端系統連線至 WMI (root\DCIM\SYSMAN)：
 - a. 將 WMI 工具連同 wbemtest 安裝至本機系統上，然後在遠端系統安裝 Dell Command | Monitor。
 - b. 組態 WMI 遠端連線系統上的防火牆。例如，在 Windows 防火牆開啟 TCP 連接埠 135 和 445。
 - c. 在**本機安全性原則**中，將本機安全性設定為**傳統 — 本機使用者以自身身份驗證的網絡存取：用於本機帳戶的共用和安全性模式**。
 - d. 使用 WMI wbemtest 從遠端系統連線到本機系統上的 WMI (root\DCIM\SYSMAN)。例如，\\[Target remote system IP Address]\root\DCIM\SYSMAN
 - e. 提示時，請輸入目標遠端系統管理員認證。如需更多有關 WMI 的資訊，請參閱位於 msdn.microsoft.com 適當的 Microsoft 說明文件。

在執行 Windows 的系統上安裝失敗

如果您無法完成 Windows 的 Dell Command | Monitor 安裝，請確定：

- 您在目標系統上具有管理員權限。
 - 目標系統為搭載 SMBIOS 2.3 版或更新版本的 Dell 製造系統。
 - 必須關閉 PowerShell 主控台。
- i** **備註:** 要檢查系統的 SMBIOS 版本，請前往**開始 > 執行**，然後執行 `msinfo32.exe` 檔案，並在系統摘要頁面中檢查 SMBIOS 的版本。
- i** **備註:** 系統必須執行支援的 Windows 作業系統。
- i** **備註:** 系統必須升級至 .NET 4.0 或更新的版本。

BIOS 設定列舉值顯示為 1

1. 驗證是否使用根使用者權限安裝了以下套件；
 - `omi-1.0.8.ssl_100.x64.rpm`
 - `srvadmin-hapi-8.3.0-1908.9058.el7.x86_64`
 - `command_monitor-linux-<version number>-<buid number>.x86_64.rpm`
2. 如果安裝了以上套件，請確認已加載驅動程式模組。
 - a. 運行以下指令 `lsmod | grep dcdbas` 驗證已加載驅動程式模組。
 - b. 如果驅動程式模組無法使用，請運行以下指令 `modinfo dcdbus` 以取得驅動程式詳細資料。
 - c. 運行以下指令 `insmod <filename>` 加載驅動程式模組。

libsmbios 的依存性使 Hapi 安裝失敗

如果安裝因依存性問題而失敗，

運行 `apt-get -f install` 以強制安裝所有依存性套件。

CIM 資源無法使用

列舉時，如果收到錯誤消息「CIM 資源無法使用」，

驗證指令是否使用根權限執行。

無法在運行 Ubuntu Core 16 的系統上使用 DCM 執行指令

確保系統上的 snap 版本為 2.23 或更新版本。

其他您可能需要的文件

除了本使用者指南外，您還可以存取位於 dell.com/dellclientcommandsuitemanuals 上的以下說明文件。按一下 Dell Command | Monitor (之前稱為 OpenManage Client Instrumentation) ，然後按一下**一般支援**部分中適當的產品版本連結。

除了本使用者指南外，您還可以存取以下指南。

- Dell Command | Monitor 參考指南提供關於所有類別、屬性及說明的詳細資訊。
- Dell Command | Monitor 安裝指南提供有關安裝的資訊。
- Dell Command | Monitor SNMP 參考指南提供適用於 Dell Command | Monitor 的簡易網絡管理通訊協定 (SNMP) 管理資訊庫 (MIB)。

主題：

- [從 Dell EMC 支援網站存取文件](#)

從 Dell EMC 支援網站存取文件

您亦可透過選擇產品來存取所需文件。

1. 前往 www.dell.com/manuals。
2. 按一下「**瀏覽所有產品**」，按一下「**軟件**」，然後按一下「**用戶端系統管理**」。
3. 要檢視所需文件，請按一下所需產品，然後再按一下所需版本。

聯絡 Dell

 **備註:** 如果您沒有有效的互聯網連線，則您可以在購機發票、裝箱單、賬單或 Dell 產品目錄中找到聯絡資料。

Dell 提供幾種網上和電話支援及服務選項。服務供應情況視乎國家/地區和產品而定；某些服務可能無法在您的所在地區提供。要聯絡 Dell 查詢銷售、技術支援或客戶服務問題：

1. 轉至 **Dell.com/support**。
2. 選擇您的支援類別。
3. 在頁面底部的**選擇國家/地區**下拉清單中確認您所在國家或地區。
4. 根據您的需求選擇相應服務或支援連結。