

# Dell Command | Monitor 10.5 版

## 使用者指南



## 註、警示與警告

 **註:** 「註」表示可以幫助您更有效地使用產品的重要資訊。

 **警示:** 「警示」表示有可能會損壞硬體或導致資料遺失，並告訴您如何避免發生此類問題。

 **警告:** 「警告」表示可能的財產損失、人身傷害或死亡。

<b>章 1: Dell Command   Monitor 10.5 簡介.....</b>	<b>5</b>
Dell Command   Monitor 10.5 版本新功能.....	5
Dell Command   Monitor 概觀.....	5
<b>章 2: Windows SMM 安全性風險降低表格 (WSMT) 相容性.....</b>	<b>7</b>
<b>章 3: Dell Command   Monitor 10.5 適用的標準及通訊協定.....</b>	<b>8</b>
<b>章 4: 使用 Dell Command   Monitor 10.5 的使用案例.....</b>	<b>9</b>
<b>案例 1：資產管理.....</b>	<b>9</b>
SCCM 整合.....	9
<b>方案 2：組態管理.....</b>	<b>9</b>
<b>案例 3：健康狀況監視.....</b>	<b>10</b>
透過作業系統事件檢視器、系統記錄或 CIM 指示來監控系統警示.....	10
<b>案例 4：設定檔.....</b>	<b>10</b>
資產設定檔.....	10
電池設定檔.....	10
BIOS 管理設定檔.....	11
開機控制.....	11
基本桌面行動.....	11
記錄檔記錄.....	11
實體資產.....	11
系統記憶體設定檔.....	12
<b>章 5: 使用 Dell Command   Monitor 10.5.....</b>	<b>13</b>
輪詢間隔設定.....	13
RAID 狀態報告.....	13
監控 Dell 用戶端系統.....	13
Linux 適用的 Dell Command   Monitor 的應用程式記錄檔.....	13
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_智慧屬性.....	15
DCIM_ThermalInformation.....	15
<b>變更系統設定.....</b>	<b>16</b>
使用 PowerShell 命令在執行 Windows 的系統設定 BIOS 屬性.....	16
在執行 Linux 的系統設定 BIOS 屬性.....	16
變更開機順序.....	19
遠端關閉及重新啟動 Windows 系統.....	19
遠端取得 Windows 系統的系統時間值.....	20

<b>章 6: 使用 Dell Command   Monitor 10.5 在本機管理 Dell 用戶端系統.....</b>	<b>21</b>
使用 PowerShell 在本機管理 Windows 系統.....	21
使用 OMICLI 在本機管理 Linux 系統.....	22
<b>章 7: 使用 Dell Command   Monitor 10.5 遠端管理 Dell 用戶端系統.....</b>	<b>23</b>
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
<b>章 8: Dell Command   Monitor 10.5 常見問題集.....</b>	<b>25</b>
<b>章 9: 使用 Dell Command   Monitor 10.5 的故障診斷步驟.....</b>	<b>27</b>
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
由於 libsbios 的相依性，導致 Hapi 安裝失敗.....	28
CIM 資源無法使用.....	28
無法在執行 Ubuntu Core 16 的系統上使用 DCM 執行命令.....	28
<b>章 10: 其他您可能需要的文件.....</b>	<b>29</b>
從 Dell 支援網站存取文件.....	29
<b>章 11: 與 Dell 公司聯絡.....</b>	<b>30</b>

# Dell Command | Monitor 10.5 簡介

Dell Command | Monitor 軟體應用程式可讓 IT 系統管理員輕鬆管理車隊清查、監控系統健全狀況、修改 BIOS 設定，以及遠端收集部署 Dell 用戶端系統所需的資訊。

啟用系統健全狀況狀態監控可協助降低系統總體擁有成本，且屬於管理所有網路裝置的整體分析方法的一部分。

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

本文件概述 Dell Command | Monitor 及其功能。如需有關支援 Dell 系統的更多資訊，請參閱 [dell.com/support](https://dell.com/support) 提供的版本資訊。

## 主題：

- [Dell Command | Monitor 10.5 版本新功能](#)
- [Dell Command | Monitor 概觀](#)

## Dell Command | Monitor 10.5 版本新功能

- 支援以下新 BIOS 屬性：
  - Microsoft UEFI CA
  - Type C Dock Video
  - Type C Dock Audio
  - Type C Dock Lan
  - WLAN Antenna
  - WWAN Antenna
  - GPS Antenna
  - Programmable Button Configuration
  - Button P1 action
  - Button P2 action
  - Button P3 action
  - Camera Vision Sensing
  - TCC Activation Offset
  - RGB Per Key Keyboard Language
  - RGB Per Key Keyboard Color
- 支援 DCIM\_Battery 類別中的電池 ePPID。

## Dell Command | Monitor 概觀

**註：**簡易網路管理通訊協定 (SNMP) 不支援 Linux 適用的 Dell Command | Monitor。


Dell Command | Monitor 使用共用資訊模型 (CIM) 標準與簡易網路管理通訊協定 (SNMP) 等管理通訊協定，來管理用戶端系統。這有助於降低系統總體擁有成本、提高安全性，並提供可管理網路裝置內所有裝置的整體分析方法。

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，可從不同來源收集用戶端系統資訊，這些來源包括 BIOS、CMOS、系統管理 BIOS (SMBIOS)、系統管理介面 (SMI)、作業系統，以及應用程式設計介面 (API)。Windows 適用的 Dell Command | Monitor 也會從動態連結程式庫 (DLL) 和登錄檔設定收集用戶端系統資訊。Windows 適用的 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 Linux 適用的 Dell Command | Monitor 則是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 管理員能遠端收集資產資訊、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、WMI 事件或 SNMP 設陷 v1 中作為事件提供。在執行 Linux 的系統，這些警示會以系統記錄、OMI 事件或應用程式記錄形式接收。

Dell Command | Monitor 適用於 Windows，可整合至主控台 (例如 Microsoft System Center Configuration Manager)，方法是透過直接存取 CIM 資訊，或透過其他已實作過 Dell Command | Monitor 整合的主控台廠商來進行整合。您也可以建立自訂指令檔，以鎖定相關的範圍。範例指令檔可在 Dell Knowledge Library Dell Command | Monitor 頁面取得。您可以使用這些指令檔來監控清查、BIOS 設定以及系統健康狀況。


 **註:** 預設安裝並不會啟用 SNMP 支援。如需為 Windows 適用的 Dell Command | Monitor 啟用 SNMP 支援的更多資訊，請參閱位於 [dell.com/support](https://dell.com/support) 的 Dell Command | Monitor 安裝指南。

# Windows SMM 安全性風險降低表格 (WSMT) 相容性

Windows (SMM) 安全性風險降低表格包含有關專為 Windows 作業系統建立之 ACPI 表格的資訊，支援 Windows 虛擬化安全性 (VBS) 功能。Dell Command | Monitor 與 WSMT 相容。這是用來設定具有支援 WSMT 的 BIOS 之 Dell 用戶端系統上的平台功能。

以下是 WSMT 相容性造成的運作方式變更：

Dell Command | Monitor 功能在具有支援 WMI/ACPI 之相容版本 BIOS 的 Dell 用戶端平台上提供使用。

 註：如需有關支援的平台的更多資訊，請參閱[支援的平台](#)。

# Dell Command | Monitor 10.5 適用的標準及通訊協定

Dell Command | Monitor 主要根據 CIM 標準。CIM 規範詳細介紹了用於提高與管理通訊協定相容性的對應技術。遠端監控使用如 WMI、SNMP 和 WSMAN 等管理通訊協定。

**註：**適用於 Windows 的 Dell Command | Monitor 使用簡易網路管理通訊協定 (SNMP) 描述系統的幾個變數。

桌面管理任務推動小組 (DMTF) 是業界公認的標準機構，其引領桌上型電腦、企業和網路環境在管理標準 (包括 CIM 和 ASF) 的發展、採用和統一。

# 使用 Dell Command | Monitor 10.5 的使用案例

本節說明 Dell Command | Monitor 的各種使用案例。

您可以使用 Dell Command | Monitor 來進行下列操作：

- 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
- 方案 2：組態管理
- 案例 3：健康狀況監視
- 案例 4：設定檔

## 案例 1：資產管理

擁有許多 Dell 系統的公司，因其業務和 IT 人員有所變動，而無法維持準確的清查資訊。資訊長 (CIO) 需求的計畫要能識別可升級至最新版本 Windows 的系統。這需要評量已部署的系統，以決定此類專案的大小、範圍和財務影響。資訊集合涉及大量工作。在每個用戶端系統部署 IT 人員及導致最終使用者中斷都所費不貲。

在每個 Dell 系統上使用 Dell Command | Monitor，可以讓 IT 管理員透過遠端方式快速收集資訊。IT 管理員使用如 Microsoft System Center Configuration Manager (SCCM) 之類的工具，即能透過網路查詢每個用戶端系統，並收集 CPU 類型和速度、記憶體大小、硬碟容量、BIOS 版本和目前作業系統版本等資訊。收集資訊後，即可進行分析，以識別可升級至最新版本 Windows 的系統。

您也可以透過 WSMAN/WinRM 命令列或使用任何 CIM 用戶端命令列取得資產清查。

## SCCM 整合

您可以透過以下方法，將 SCCM 與 Windows 適用的 Dell Command | Monitor 整合：

- 使用 Dell Command | Monitor 安裝套裝內的 MOF 檔 (該安裝套裝內包含所有 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

## 方案 2：組態管理

一間公司計劃將用戶端平台標準化，並在完整生命週期中管理每個系統。為了在這方面作出努力，該公司取得了一套工具，並計畫使用開機前執行環境 (PXE) 以自動化方式部署新的用戶端作業系統。

問題在於如何無需手動存取每一台桌上型電腦，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 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檔 (CIM、WinRM/WSMAN/PowerShell/WMIC) 來變更 BIOS 設定。指令檔可以透過網路遠端傳送，並在每個用戶端系統上執行。

有關 Dell Command | Monitor 的更多資訊，請參閱位於 [dell.com/support](http://dell.com/support) 的 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，但在整個電腦生命週期中很少會管理系統組態。在每個用戶端系統安裝 Dell Command | Monitor 後，IT 部門可以鎖定舊式連接埠以防止使用未經授權的週邊設備，或啟用網路喚醒 (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：健康狀況監視

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。使用者重新開機系統後，檔案即顯示為可存取。使用者忽略最初的問題，因為此問題似乎已自行解決。與此同時，Dell Command | Monitor 會向硬碟查詢此問題以預測故障，並將自我監控、分析與報告技術 (SMART) 警示傳送至管理主控台。它也會向本機使用者顯示 SMART 錯誤。此警示指出硬碟發生幾個讀取/寫入錯誤。公司的 IT 部門建議使用者必須立即備份關鍵資料檔案。派遣維修技術人員帶著替換磁碟機前往現場。

在硬碟機故障之前更換，避免使用者停機時間、省去致電至服務台並無須技術人員親臨桌上型電腦以診斷問題所在。

## 透過作業系統事件檢視器、系統記錄或 CIM 指示來監控系統警示

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。
- 透過 `DCIM_AlertIndication` 類別監控 CIM 指示。
- (僅 Windows 適用的 Dell Command | Monitor) 透過簡易網路管理通訊協定 (SNMP) 與 Windows 事件檢視器監控事件。
- (僅 Linux 適用的 Dell Command | Monitor) 透過系統記錄監控。

有關 Dell Command | Monitor 的更多資訊，請參閱位於 [dell.com/support](https://dell.com/support) 的 Dell Command | Monitor 參考指南。

## 案例 4：設定檔


 註：DMTF 設定檔實作僅限 Windows 適用的 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。他們所面臨的挑戰是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路內的行動用戶端系統。為了降低上述需求的成本並展現所提供的管理資料，我們在 Dell Command | Monitor 中實作了業界標準的分散式管理任務推動小組 (DMTF) 和資料中心基礎架構管理 (DCIM-OEM) 設定檔。本指南中說明了部分 DMTF 設定檔。

有關 Dell Command | Monitor 的更多資訊，請參閱位於 [dell.com/support](https://dell.com/support) 的 Dell Command | Monitor 參考指南。


## 資產設定檔

端點裝置上的保固狀態：

- 透過列舉或獲得 `DCIM_AssetWarrantyInformation` 類別的例項來判斷保固的狀態。
- 檢查是否可使用類別 `DCIM_AssetWarrantyInformation` 的屬性 `WarrantyStartDate` 和 `WarrantyEndDate` 來判斷保固狀態。  
 註：DCIM\_AssetWarrantyInformation 的必要條件為您必須具備有效的網際網路連線。如果您在代理伺服器後面執行 Dell Command | Monitor，請確定已正確配置代理設定。

若要取得週邊設備保固狀態的詳細資料：

1. 前往 [Dell.com/support](https://Dell.com/support)
  2. 在網頁底部的「選擇國家/地區」下拉式清單中確認您所在的國家或地區
  3. 選取支援類別 - 保固與合約
  4. 提供適合您系統的產品服務編號。
- 停用保固功能和後續的重新整理呼叫。
  - 依需求提取保固資訊。


 註：保固資訊會每 15 天自動更新一次。若為最新的保固狀態，列舉的保固資訊可能與 Dell 支援網站上的不同。

## 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。
- 判斷預計的執行時間並查看預計的剩餘電量。
- 使用 `DCIM_Battery` 類別的 `OperationalStatus` 和 `HealthState` 屬性，檢查是否能判定電池的健全狀況資訊。
- 使用 `DCIM_Sensor.CurrentState` 屬性或 `CIM_NumericSensor.CurrentState` 屬性獲得有關電池執行狀況的更多資訊。
- 使用 `DCIM_Battery` 類別的 `IdentifyingDescriptions` 和 `OtherIdentifyingInfo` 屬性，判斷電池位置和電池 ePPID。

## DCIM\_Battery

取得有關電池元素的電池 ePPID 值資訊。以系統管理員身份開啟 PowerShell 提示字元，並執行下列命令：`Get-CimInstance -Namespace root/dcim/sysman -Classname DCIM_Battery |Select ElementName, OtherIdentifyingInfo, IdentifyingDescriptions.`

 註：電池 ePPID 值並非動態，且若更換了電池，您必須重新啟動系統，以反映 DCIM\_Battery 例項內的變更。

## BIOS 管理設定檔

- 透過列舉 **DCIM\_BIOSElement** 的類別例項判斷 BIOS 版本。
- 請檢查 BIOS 屬性值是否可修改。取得 **DCIM\_BIOSEnumeration** 類別的例項。如果屬性 **IsReadOnly** 設為 FALSE，則可修改屬性。
- 設定系統密碼 (SystemPwd)。執行 **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)。執行 **DCIM\_BIOSService.SetBIOSAttributes()** 方法，將 AdminPwd 設定為 AttributeName，並將密碼值設定為 AttributeValue 參數。
- 執行 **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，請執行 **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** 代表目前的開機組態。

## 基本桌面行動

- 透過列舉 **DCIM\_ComputerSystem** 類別的例項，判斷系統型號、產品服務編號和序號。
- 您可以使用 **DCIM\_ComputerSystem.RequestStateChange()** 方法，並將 RequestedState 參數值設定為 3。參數值 3 會關閉系統。
- 您可以使用 **DCIM\_ComputerSystem.RequestStateChange()** 方法，並將 RequestedState 參數值設定為 11。參數值 11 會重新開機系統。
- 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。執行 **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。
- 尋找個別的記錄項目。取得透過 **DCIM\_LogManagesRecord** 關聯，與 **DCIM\_RecordLog** 的給定例項關聯的所有 **DCIM\_LogEntry** 例項。根據 **RecordID** 為例項排序。
- 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。
- 根據記錄項目的時間戳記為記錄檔記錄排序。取得透過 **DCIM\_LogManagesRecord** 關聯，與 **DCIM\_RecordLog** 的給定例項關聯的所有 **DCIM\_LogEntry** 例項。根據 **CreationTimeStamp** 屬性值，以後進先出 (LIFO) 順序為 **DCIM\_LogEntry** 的例項排序。
- 執行 **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編號。
- 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 10.5

若要檢視 Dell Command | Monitor 所提供的資訊，請存取：`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，請參閱位於 [dell.com/support](http://dell.com/support) 的 Dell Command | Monitor 參考指南。

## 主題：

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

## 輪詢間隔設定

您可以使用 Dell Command | Monitor 來變更下列項目的輪詢間隔：風扇警報、溫度警報、電壓警報、電流警報、磁碟容量增加/減少、記憶體大小增加/減少，以及處理器數量增加/減少。

- 在 Windows 方面，`dcsbdy32.ini` 或 `dcsbdy64.ini` 檔案位於 `<Dell Command | Monitor installed location>\omsa\ini`。
- 在 Linux 方面，`AlertPollingSettings.ini` 檔案位於 `/opt/dell/dcm/conf`。

**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 =  $626 \times 23$  秒，大約 3 個小時)。

## RAID 狀態報告

Dell Command | Monitor 為具備硬體和驅動程式支援的用戶端系統，啟用 RAID 組態資訊並監控 RAID 功能。您可以使用 RAID 類別來接收有關 RAID 層級、驅動程式資訊、控制器組態和控制器狀態的詳細資料。啟用 RAID 組態後，即可收到磁碟機和控制器降級或故障的警示。

**註：**只有在通用儲存裝置管理介面 (CSMI) 版本 0.81 相容驅動程式上運作的 RAID 控制器才支援 RAID 狀態報告。OMCI 8.1 及更新版本僅支援 Intel 晶片上 RAID 控制器的監控功能，而從 OMCI 8.2 及更新版本，則支援 Intel 晶片上 RAID 控制器的警示功能。

## 監控 Dell 用戶端系統

- Dell Command | Monitor 適用於 Windows，支援簡易網路管理通訊協定 (SNMP)，以監控和管理用戶端系統，例如筆記型電腦、桌上型電腦和工作站。Dell Command | Monitor 和伺服器管理員之間會共用管理資訊庫 (MIB) 檔案。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，請參閱位於 [dell.com/support](http://dell.com/support) 的 Dell Command | Monitor SNMP 參考指南。

- Dell Command | Monitor Linux 適用的 Dell Command | Monitor 支援使用 WinRM 和 WSMAN 命令進行監控。

## Linux 適用的 Dell Command | Monitor 的應用程式記錄檔

Linux 適用的 Dell Command | Monitor 基於報告和偵錯目的區隔應用程式記錄和警示。您可以在 `/opt/dell/dcm/var/log` 的 `dcm_application.log` 檔案中，檢視 Dell Command | Monitor 應用程式產生的警示和記錄檔歷程記錄。

## 組態檔案

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

**i** 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 — 設有三個記錄層級以區隔系統訊息：ERROR (錯誤)、INFO (資訊)、DEBUG (除錯)

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

**i** 註：預設記錄層級設定為 INFO。

- 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。

**i** 註：File\_Size 值必需以位元表示。

- BackupIndex — 使用者可以指定 **dcm\_application.log** 檔案的換用計數。如果預設換用計數為 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

用戶端系統會轉換為 Advanced Format (AF) 磁碟機，以提供更大的儲存容量，並解決 512 位元組磁區硬碟機 (HDD) 的限制。轉換為 4KB 磁區的硬碟維持回溯相容性，而目前的 AF 硬碟 (稱為 512e 硬碟) 符合 512 位元組 SATA，並以 4KB 運作。在轉換過程中，您可能遇到效能問題，例如用戶端系統中磁碟分割錯位的磁碟機，導致負責處理 512e 磁碟機的磁區式加密軟體套裝失敗。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

**i** 註：適用於 Linux 的 Dell Command | Monitor 不提供開機組態功能。因此，對於適用於 Linux 的 Dell Command | Monitor，本節並不適用。

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 (舊版或 UEFI) 使用下面的類別模型化：

- DCIM\_ElementSettingData
- DCIM\_BootConfigSetting
- DCIM\_OrderedComponent
- DCIM\_BootSourceSetting
- DCIM\_SmartAttributeInfo

**i** 註：開機組態和開機清單類型兩詞可交替使用，分別代表傳統或 UEFI 之相同意義。

## DCIM\_AssetWarrantyInformation

- 若要查詢端點裝置的保固狀態，請在 PowerShell 提示字元內執行下列命令：

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

- 若要依照 WarrantyEndDate 的時間順序列出保固權益，請在 PowerShell 提示字元內執行下列命令：

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

- 若要停用保固功能和後續的重新整理呼叫，請在 PowerShell 提示字元內執行下列命令：

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

- 若要依需求提取保固資訊，請在 PowerShell 提示字元內執行下列命令：

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

**i** 註：設定代理組態 -

- 預設代理 – Dell Command | Monitor 會選取預設的系統代理 (在 IE 中設定)
- 自訂代理

**DCIM\_ApplicationProxySetting** 類別是用來根據代理環境修改 Dell Command | Monitor。

## DCIM\_BootConfigSetting

**DCIM\_BootConfigSetting** 的例項，代表開機過程中使用的開機組態。例如，在用戶端系統上，有兩種類型的開機組態：舊版和 UEFI。因此，**DCIM\_BootConfigSetting** 最多有兩個例項，分別代表舊版和 UEFI。

您可以使用下列屬性判斷 **DCIM\_BootConfigSetting** 是否代表舊版：

- 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** 和 **StructuredBootString** 屬性包含可識別開機裝置的字串。例如：軟碟、硬碟機、CD/DVD、網路、個人電腦記憶卡國際協會 (PCMCIA)、電動車 (BEV) 或 USB。根據裝置的開機清單類型，**DCIM\_BootSourceSetting** 的例項會與 **DCIM\_BootConfigSetting** 的一個例項建立關聯。

## DCIM\_OrderedComponent

**DCIM\_OrderedComponent** 關聯類別用於將 **DCIM\_BootConfigSetting** 的例項，與 **DCIM\_BootSourceSetting** 的例項相關聯，後者代表開機裝置所屬的其中一種開機清單類型 (舊版或 UEFI)。**DCIM\_OrderedComponent** 的 **GroupComponent** 屬性指的是 **DCIM\_BootConfigSetting** 例項，而 **PartComponent** 屬性指的是 **DCIM\_BootSourceSetting** 例項。

## DCIM\_智慧屬性

若要讀取智慧屬性值，請執行下列命令：

例如：

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

若要設定自訂閾值，請執行下列命令：

例如：

- `Get-CimInstance -Namespace root\dcim\sysman DCIM_SmartAttributeInfo -Filter "AttributeID like '<屬性 ID 值>'" | Invoke-CimMethod -MethodName "SetCustomThreshold" -Arguments @{CustomThresholdValue="<要設定的自訂閾值>"}`

## DCIM\_ThermalInformation

**DCIM\_ThermalInformation** 管理散熱組態設定，例如散熱模式、AAC 模式和風扇故障模式。

- 若要查詢裝置的散熱資訊，請執行下列命令：

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

- 若要設定散熱模式的值，請執行下列命令：

```
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")}
```

## 變更系統設定

在 Dell Command | Monitor 中，使用下列方法來變更系統設定和本機或遠端系統的狀態：

- SetBIOSAttributes — 變更 BIOS 設定
  - ⓘ 註: Linux 適用的 Dell Command | Monitor 目前僅支援 SetBIOSAttributes 方法。
- ChangeBootOrder — 變更開機組態
- RequestStateChange — 關閉系統並重新開機
- ManageTime — 顯示系統時間

在 Windows 適用的 Dell Command | Monitor 中，您可以使用 winrm、VB 指令檔、PowerShell 命令、wmic 和 WMI wbemtest 執行這些方法。

## 使用 PowerShell 命令在執行 Windows 的系統設定 BIOS 屬性

您可以使用 SetBIOSAttributes 方法設定 BIOS 屬性。以下程序針對使用啟用可信賴平台模組 (TPM) 的工作作為範例做解說。

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

ⓘ 註: 使用具有管理員權限的 Powershell。

若要啟用 TPM，

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

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

2. 使用下列命令啟用 TPM 安全性：

```
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. 使用下列命令啟動 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

您可以使用下列任一方法設定 BIOS 屬性：

- 使用 OMICLI
- 使用 WinRM
- 使用 WSMAN

ⓘ 註: 請確定 OMI 伺服器已啟動且執行中。

## 使用 OMICLI 設定 BIOS 屬性

您可以使用 SetBIOSAttributes 方法設定 BIOS 屬性。以下程序針對使用啟用可信賴平台模組 (TPM) 的工作作為範例做解說。

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

若要使用 OMICLI 命令設定 BIOS 屬性：

1. 若要在尚未設定 BIOS 密碼的系統上設定此密碼，請執行

```
./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. 若要使用下列命令啟用 TPM 安全性，請執行

```
./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. 若要啟用 TPM，請執行

```
./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. 若要重設 BIOS 密碼，請執行

```
./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

您可以使用 SetBIOSAttributes 方法設定 BIOS 屬性。以下程序針對使用啟用可信賴平台模組 (TPM) 的工作作為範例做解說。

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

若要使用 WinRM 命令設定 BIOS 屬性：

1. 列舉 DCIM\_BIOSService 類別以取得選擇器集。執行：

```
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
```

**註:** 在此範例中將選擇器集的值 (SystemName=<system name from DCIM\_BIOSService class>winrm i SetBIOSAttributes wsman/DCIM\_BIOSService?SystemName=dt:+SystemCreationClassName=DCIM\_ComputerSystem+Name=DCIM:BiosService+CreationClassName=DCIM\_BIOSService+) 用來進行設定操作。

2. 設定系統的 BIOS 密碼。若尚未設定，使用下列命令：

```
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. 執行下列命令啟用 TPM 安全性：

```
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. 使用下列命令啟動 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 在執行 Linux 的系統上設定 BIOS 屬性。以下程序針對使用啟用可信賴平台模組 (TPM) 的工作作為範例做解說。

 **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. 列舉 DCIM\_BIOSService 類別以取得選擇器集。執行：

```
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，使用下列命令：

```
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. 使用下列命令啟用 TPM 安全性：

```
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. 使用下列命令啟動 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. 使用下列命令檢查開機順序類型 (傳統或 UEFI)：

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

2. 使用下列命令檢查目前的開機順序類型 (傳統或 UEFI)：

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

3. 使用下列命令變更開機順序：

- WMI 命令：`wmic /namespace:\\root\dcim\sysman path dcim_bootconfigsetting call ChangeBootOrder /?:full。`
- PowerShell 命令：`(Get-WmiObject -namespace root\dcim\sysman -class dcim_bootconfigsetting).getmethodparameters("ChangeBootOrder")。`  
**i** 註：dcim\_BootConfigSetting 例項必須呈現您要變更的開機組態：類型 1 (舊版) 或類型 2 (UEFI)。
- 引數為：
  - Authorization Token — 這是系統管理員或開機密碼。
  - Source — 這是從 dcim\_OrderedComponent.PartComponent 屬性取得的開機順序清單。新的開機順序是由來源陣列中的開機裝置順序決定。

4. 使用 PowerShell 變更類型 1 開機清單的開機順序：

- a. 執行下列命令，取得類型 1 開機清單目前的開機順序：`$boLegacy = Get-WmiObject -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-1'} | select -expand partcomponent。`
- b. 定義 PowerShell 變數以指定開機順序，設定 `$newboLegacy`。指派新的開機順序至該變數。例如保留目前的開機順序類型。
- c. `$newboLegacy = $boLegacy`
- d. 執行下列命令，取得對應於類型 1 開機清單的 dcim\_bootconfigsetting 例項：`$bcsLegacy = Get-WmiObject -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 1'}。`
- e. 執行下列命令，叫用方法：`$ bcsLegacy.changebootorder($newboLegacy, $AuthorizationToken)。`  
`$AuthorizationToken` 變數是用於傳送 BIOS 密碼。

5. 使用 PowerShell 變更類型 2 開機清單的開機順序：

- a. 執行下列命令，取得類型 2 開機清單目前的開機順序：`$boUefi = Get-WmiObject -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-2'} | select -expand partcomponent。`
- b. 定義 PowerShell 變數以指定開機順序，設定 `$newboUefi`。指派新的開機順序至該變數。例如保留目前的開機順序類型。
- c. 執行下列命令，取得對應於類型 2 開機清單的 dcim\_bootconfigsetting 例項：`$bcsUefi = Get-WmiObject -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 2'}。`
- d. 執行下列命令，叫用方法：`$ bcsUefi.changebootorder($newboUefi, $AuthorizationToken)。`  
`$AuthorizationToken` 變數是用於傳送 BIOS 密碼。

## 遠端關閉及重新啟動 Windows 系統

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

1. 使用下列命令，遠端關閉 Windows 系統：

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

2. 使用下列命令，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：

在命令行介面中，執行下列步驟：

- 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 10.5 在本機管理 Dell 用戶端系統

您可以請使用下列方法在本機管理 Dell 用戶端系統：

- 若為執行 Windows 的系統，請使用 PowerShell
- 若為執行 Linux 的系統，則使用 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 命令，來管理在本機執行 Windows 的 Dell 用戶端系統。

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

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

- 變更 BIOS 設定

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

- 修改非重大值

```
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 取得使用者同意的命令：

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

- 從 WMI 設定使用者同意的命令：

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

 **註：**改善方案僅適用於 DCM 10.5 x64 位元版本。

- 從 WMI 取得代理的命令：

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

- 從 WMI 設定代理的命令：

```
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 命令在本機上管理 Linux 系統。在執行 Linux 的系統上，OMICLI 已安裝在 /opt/omi/bin。

- 列舉 DCIM 類別的例項
  - ./omicli ei root/dcim/sysman DCIM\_BIOSEnumeration
  - ./omicli ei root/dcim/sysman DCIM\_BIOSPassword
- 取得 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 }
```

- 變更 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 10.5 遠端管理 Dell 用戶端系統

您可以使用下列任一方法遠端管理 Dell 用戶端系統：

- 若為執行 Windows 的系統，使用 PowerShell 透過 Windows 系統遠端管理 Windows 系統 第頁的 23
- 若為執行 Linux 的系統，使用 WinRM 透過 Windows 系統遠端管理 Linux 系統 第頁的 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 系統遠端存取和監控 Windows 系統。

管理 Windows 系統的先決條件：

- Windows PowerShell 3.0
- 經配置可執行遠端指令檔的 PowerShell

受管理 Windows 系統的先決條件：

- Dell Command | Monitor
- Windows PowerShell 3.0
- 經配置可執行遠端指令檔的 PowerShell
- 應啟用 PowerShell-remoting 功能

### 註：

若要以遠端方式使用 Windows PowerShell，必須對遠端電腦進行配置，使其能進行遠端管理。如需詳細資訊 (包括指示)，請執行 PowerShell 命令 - 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 命令，透過執行 Windows 的系統，存取和監控執行 Linux 的系統。

Windows 系統的先決條件

- 支援的 Windows 作業系統
- 為遠端管理執行及設定的 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
- 為您的環境設定的系統

在命令行介面中，執行

```
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 命令，透過執行 Linux 的系統，遠端存取和監控執行 Linux 的系統。

管理 Linux 系統的先決條件：

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

管理 Linux 系統的先決條件：

- 根存取權限
- 支援的 Linux 作業系統
- Dell Command | Monitor

啟動終端機，然後執行

```
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 10.5 常見問題集

- 如何使用 `DCIM_OrderedComponent.AssignedSequence` 屬性找到開機組態的開機順序 (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，`DCIM_OrderedComponent.AssignedSequence` 屬性的值用來判斷開機程序時，相關的 `DCIM_BootSourceSetting` 例項順序 (開機裝置)。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份。
- 如何變更開機順序?  
您可以使用 `DCIM_BootConfigSetting.ChangeBootOrder()` 方法變更開機順序。`ChangeBootOrder()` 方法以 `DCIM_BootSourceSetting` 的例項與 `DCIM_BootConfigSetting` 例項相關聯來設定順序。此方法有一個輸入參數，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。
- 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 (建立 `DCIM_BootConfigSetting` 例項目標與未出現在 `Source` 參數輸入陣列的 `DCIM_BootSourceSetting` 例項關聯) 設定為 0，表示該裝置已停用。
- 當 <要連接的內容> 嘗試使用 `wbemtest` 連線到命名空間時，會顯示登入失敗訊息。  
以管理員權限層級啟動 `wbemtest` 來解決任何登入訊息問題。從所有程式清單移至 Internet Explorer，按右鍵，然後以系統管理員身分執行啟動 `wbemtest`，並避免任何命名空間的錯誤。
- 如何不發生任何問題下執行 Knowledge Library 指令檔?  
以下步驟可用以執行 Dell Command | Monitor Knowledge Library 連結中提供的 VBS 指令檔：
  1. 請使用命令 `winrm quickconfig`，在系統上設定 `winrm`。
  2. 檢查權杖支援是否存在於系統上，查看：
    - 在 BIOS 設定中的 **F2** 螢幕。
    - 使用如 `wbemtest` 的工具檢查指令檔定義的金鑰值是否存在於系統中。

**i** 註：Dell 建議您使用最新的 BIOS，您可於 [dell.com/support](http://dell.com/support) 取得。如需更多資訊，請參閱位於 [dell.com/support](http://dell.com/support) 的 Dell Command | Monitor 參考指南。
- 我該如何設定 BIOS 屬性?  
BIOS 屬性可使用 `DCIM_BIOSService.SetBIOSAttributes()` 方法來變更。`SetBIOSAttributes()` 方法可設定定義在 `DCIM_BIOSEnumeration` 類別中的例項值。此方法有七個輸入參數。首兩個參數可為空白或為 `null`。第三個參數 `AttributeName` 必須將輸入對應至 `DCIM_BIOSEnumeration` 類別的屬性名稱例項值。第四個參數或 `AttributeValue` 可以是定義於 `DCIM_BIOSEnumeration` 類別中任何可能的屬性名稱值。第五個參數 `AuthorizationToken` 是可選的，第五個參數的輸入是 BIOS 密碼。只有已在系統上設定 BIOS 密碼時才使用第五個參數，否則它是空的。第六個和第七個引數可再次為空白或 `null`。
- Dell Command | Monitor 是否支援 Windows 與 Linux 作業系統的儲存裝置和感應器監控?  
是，Dell Command | Monitor 可針對受支援的 Windows 與 Linux 作業系統支援儲存裝置和感應器監控。  
在儲存裝置監控方面，Dell Command | Monitor 支援以下監控與警示：
  - Intel 整合式控制器 (符合 CSMI v0.81 或更新版本)
  - 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)

**i** 註：執行 Linux 作業系統的系統不支援 Intel 整合式控制器監控。

在感應器監控方面，Dell Command | Monitor 支援電壓、溫度、安培、冷卻裝置 (風扇) 和機箱感應器的監控與警示。如需有關類別和警示的更多資訊，請參閱位於 [dell.com/support](http://dell.com/support) 的 Dell Command | Monitor 參考指南。
- Dell Command | Monitor 可以和其他應用程式/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連接。它可以與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 Client Management Pack

- 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。
- 如何設定 DCM 10.2.1 的代理？
- DCM 10.2.1 無法擷取保固資訊。
- 檢查應用程式代理設定是否已使用 DCIM\_ApplicationProxySetting 類別正確配置。  
我要如何設定 Dell Command | Monitor 的代理登入資料。  
如果您已透過 Dell Command | Monitor 登入，您可以使用相同的認證來進行代理驗證。
- Dell Command | Monitor 並未顯示保固資訊。
  - 用戶端系統並未在輪詢時連線至網際網路。  
連線至網際網路，並執行下列命令以提取保固資訊：  
`Get-CimInstance -Namespace root/DCIM/SYSMAN -ClassName DCIM_AssetWarrantyInformation | Where-Object{$_.InstanceID -eq "Root/MainSystemChassis/COOObject/COOWarranty:0"} | Invoke-CimMethod -MethodName RefreshWarranty`
  - 用戶端系統並未設定代理伺服器。  
執行下列命令，在 Dell Command | Monitor 中設定代理設定：
    - 若要從 WMI 取得代理，請執行下列命令：  
`Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting。`
    - 若要從 WMI 設定代理，請執行下列命令：  
`Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting | Invoke-CimMethod -MethodName Change ProxySetting -Arguments @{NewAddress="10.0.0.223"; NewPort="8080"}`
 您必須根據每個代理環境取代 **NewAddress** 和 **Newport** (若適用)。

# 使用 Dell Command | Monitor 10.5 的故障診斷步驟

## 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
- 由於 libsbios 的相依性，導致 Hapi 安裝失敗
- CIM 資源無法使用
- 無法在執行 Ubuntu Core 16 的系統上使用 DCM 執行命令

## 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線至網路。在伺服器上，於命令提示字元中輸入下列內容：  
ping <Host Name or IP Address> 然後按下 <Enter>。
  2. 如果伺服器和用戶端系統都在同一個網域中執行下列步驟：
    - 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)，執行下列步驟：

    - 請確定伺服器執行於最新的 Windows 伺服器上。

**i** 註：變更登錄前先備份系統資料檔案。若不正確地編輯登錄，可能會造成您的作業系統無法使用。
  3. 在用戶端系統上編輯登錄變更。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，瀏覽至電腦 \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，否則從遠端連線至系統的使用者將會有「來賓」權限，即使提供的認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，以在執行 WMI 管理應用程式的系統上，做為管理員帳戶。
    - b. 如果您使用的是 IT Assistant，請執行 IT Assistant ConfigServices 公用程式 (configservices.exe，位於 IT Assistant 安裝目錄下的 /bin 目錄)。設定 IT Assistant 以本機系統管理員帳戶執行 (該帳戶現在也是遠端用戶端上的系統管理員)。此外，請確認 DCOM 和 CIM 已啟用。
    - c. 如果您使用的是 IT Assistant，請使用系統管理員帳戶為用戶端系統設定子網路探索。以下列格式輸入使用者名稱：<用戶端機器名稱>\<帳戶名稱>。如果已探索到系統，請從已探索到的系統清單中移除系統、為其設定子網路探索，然後再重新探索。

**i** 註：Dell 建議使用 Dell OpenManage Essentials 替代 IT Assistant。如需 Dell OpenManage Essentials 的更多資訊，請參閱 [dell.com/support](http://dell.com/support)。
  5. 修改遠端連線到系統的 WMI 的使用者權限層級，請執行以下步驟：
    - 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**核取方塊設定權限。

6. 執行下列步驟，使用 WMI CIM Studio 從遠端系統連線至系統上的 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. 設定系統上的防火牆，以允許 WMI 遠端連線。例如，在 Windows 防火牆中開啟 TCP 連接埠 135 和 445。
  - c. 在本機安全性原則中，將本機安全性設定設為舊版 - 本機使用者以自身身分驗證網路存取：適用於本機帳戶的共用和安全性模型。
  - 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 \\[目標遠端系統 IP 位址]\root\DCIM\SYSMAN
  - e. 提示時，請輸入目標遠端系統管理員認證。如需有關 WMI 的更多資訊，請參閱 [msdn.microsoft.com](https://msdn.microsoft.com) 適用的 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 適用的 Dell Command | Monitor 安裝，請確定下列事項：

- 您在目標系統上具有管理員權限。
  - 目標系統是由 Dell 以 SMBIOS 版本 2.3 或更新版本所製造。
  - PowerShell 主控台不得開啟。
- i** 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** 註：系統必須執行支援的 Windows 作業系統。
- i** 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. 確認下列套裝已透過根使用者權限安裝；
  - `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. 如果已安裝上述套裝，則請確認已載入驅動程式模組。
  - a. 請執行下列命令，確認驅動程式模組是否已載入：`lsmod | grep dcdbas`。
  - b. 如果驅動程式模組無法使用，請執行下列命令，以取得驅動程式詳細資料：`modinfo dcdbus`。
  - c. 請執行下列命令，以載入驅動程式模組：`insmod <filename>`。

## 由於 libsbios 的相依性，導致 Hapi 安裝失敗

如果因相依性問題而導致安裝失敗，

執行 `apt-get -f install` 以強制安裝所有相依套裝。

## CIM 資源無法使用

若您在列舉時，收到「CIM 資源無法使用」的錯誤，

請確認命令是以根權限執行的。

## 無法在執行 Ubuntu Core 16 的系統上使用 DCM 執行命令

請確定系統上的 snap 版本是 2.23 或更新版本。

## 其他您可能需要的文件

除了本使用者指南以外，您還可以存取位於 [dell.com/support](https://dell.com/support) 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。

除了本使用者指南以外，您還可以存取以下指南。

- Dell Command | Monitor 參考指南提供了關於所有類別、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 參考指南提供了適用於 Dell Command | Monitor 的簡易網路管理通訊協定 (SNMP) 管理資訊庫 (MIB)。

### 主題：


- [從 Dell 支援網站存取文件](#)

## 從 Dell 支援網站存取文件

您可以透過選取產品來存取所需文件。

1. 請前往 [www.dell.com/manuals](https://www.dell.com/manuals)。
2. 按一下**瀏覽所有產品**，按一下**軟體**，然後按一下**用戶端系統管理**。
3. 若要檢視所需文件，請按一下所需的產品名稱和版本編號。

## 與 Dell 公司聯絡

 **註:** 若您無可用的網際網路連線，您可在購買發票、包裝單、帳單或 Dell 產品目錄上找出聯絡資訊。

Dell 提供數種線上及電話的支援及服務選項。服務的提供因國家/地區和產品而異，某些服務可能在您所在地區並不提供。若因銷售、技術支援或客戶服務問題要與聯絡 Dell 公司：

1. 前往 **Dell.com/support**。
2. 選取您的支援類別。
3. 在網頁底部的**選擇國家/地區**下拉式選單中確認您所在的國家或地區。
4. 選取您所需要的適當服務或支援連結。