

Dell Command | Monitor 10.0 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」表示有可能會導致財產損失、人身傷害甚至死亡。

© 2008 -2018 Dell Inc. 或其子公司。著作權所有，並保留一切權利。Dell、EMC 與其他商標均為 Dell Inc.或其子公司的商標。其他商標可能為其各自擁有者的商標。

1 簡介	6
此版本新特色.....	6
Dell Command Monitor 概觀.....	6
2 Windows SMM 安全性風險降低表格 (WSMT) 相容性	8
3 功能	9
支援 CIM 架構.....	9
BIOS 設定與列舉.....	9
WMI/OMI 安全.....	9
警示報告.....	10
遠端關機.....	10
系統資訊存取.....	10
資產資訊的詳細細節.....	10
遠端喚醒設定.....	10
遠端修改系統 BIOS 設定.....	10
系統健康和狀態.....	10
Intel 和 LSI 控制器的 RAID 監控和警報.....	10
SNMP 監控和設陷.....	10
4 標準和協定	11
5 使用案例	12
案例 1：資產管理.....	12
SCCM 整合.....	12
方案 2：組態管理.....	12
案例 3：健康狀況監視.....	13
透過作業系統事件檢視器、Syslog、或 CIM 指示來監控系統警示.....	13
案例 4：設定檔.....	13
電池設定檔.....	14
BIOS 管理設定檔.....	14
開機控制.....	14
基本桌面行動.....	14
記錄檔記錄.....	14
實體資產.....	15
系統記憶體設定檔.....	15
6 使用 Dell Command Monitor	16
輪詢間隔設定.....	16
RAID 狀態報告.....	16
監控 Dell 用戶端系統.....	16

Linux 適用的 Dell Command Monitor 應用程式記錄.....	17
組態檔案.....	17
偵測進階格式磁碟機.....	17
開機組態.....	17
DCIM_BootConfigSetting.....	18
DCIM_BootSourceSetting.....	18
DCIM_OrderedComponent.....	18
變更系統設定.....	18
使用 PowerShell 命令在執行 Windows 的系統設定 BIOS 屬性.....	18
在執行 Linux 的系統設定 BIOS 屬性.....	19
變更開機順序.....	21
遠端關閉及重新啟動 Windows 系統.....	22
遠端取得 Windows 系統上的系統時間值.....	22
7 在本機管理 Dell 用戶端系統.....	23
使用 PowerShell 在本機管理 Windows 系統.....	23
使用 OMICLI 在本機管理 Linux 系統.....	23
8 遠端管理 Dell 用戶端系統.....	25
使用 PowerShell 透過 Windows 系統遠端管理 Windows 系統.....	25
使用 WinRM 透過 Windows 系統遠端管理 Linux 系統.....	25
使用 WSMAN 透過 Linux 系統遠端管理 Linux 系統.....	26
9 常見問題集.....	27
如何使用 dcim_orderedcomponent.assignedsequence 屬性找到開機組態的開機順序 (順序) ?.....	27
如何變更開機順序 ?.....	27
如何停用開機裝置 ?.....	27
使用 wbemtest 連線到命名空間時出現失敗登入訊息。如何解決 ?.....	27
如何不發生任何問題下執行 TechCenter 指令碼 ?.....	27
如何設定 BIOS 屬性 ?.....	28
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 ?.....	28
Dell Command Monitor 可否與其他應用程式/主控台整合 ?.....	28
可匯入類別至 SCCM 以清查嗎 ?.....	28
SCCM OMCI_SMS_DEF.mof 檔案位於何處 ?.....	28
10 故障排除.....	29
無法從遠端連線至 Windows Management Instrumentation.....	29
在執行 Windows 的系統上安裝失敗.....	30
BIOS 設定列舉值顯示為 1.....	30
libsmbios 的相依性使 Hapi 安裝失敗.....	31
CIM 資源無法使用.....	31
無法在執行 Ubuntu Core 16 的系統上使用 DCM 執行命令.....	31
11 其他您可能需要的文件.....	32

12 與 Dell 公司聯絡	33
其他您可能需要的文件.....	33
從 Dell EMC 支援網站存取文件.....	33

簡介

Dell Command | Monitor 軟體應用程式可讓遠端管理使用應用程式以存取資訊、監視電腦狀態或變更系統狀態，如從遠端關閉系統。Dell Command | Monitor 透過標準介面使用金鑰系統參數，可讓系統管理員管理清查、監控系統健全狀況和收集已部署的 Dell 系統資訊。Dell Command | Monitor 專為 Dell 企業用戶端系統、Dell IoT 閘道系統，以及 Dell Embedded 個人電腦打造。如需支援的 Dell 系統之更多資訊，請參閱在 Dell.com/dellclientcommandssuitemanuals 的版本說明。此文件概述 Dell Command | Monitor 及其功能。

註: Dell Command | Monitor 即以前的 Dell OpenManage Client Instrumentation (OMCI)。自 OMCI 8.2.1 版以後，OMCI 已更名為 Dell Command | Monitor。

主題：

- 此版本新特色
- Dell Command | Monitor 概觀

此版本新特色

支援 WSMT 相容性。如需 WSMT 相容性的更多資訊，請參閱《Dell Command | Monitor 使用者指南》中的「Windows SMM 安全性風險降低表格 (WSMT) 相容性」一節。

支援下列 BIOS 功能：

- Auto Switch、Battery Slice Charge Configuration、BIOS Enumeration Mode、Broadcom TruManage、Dust Filter Maintenance、eMMC、Enable Block SID、Enable Tablet Button LED Sign of Life、Fan Speed Auto Level on Cpu Zone、Fan Speed Auto Level on Psu Zone、GraphicSpecMode、HDD0 Fan Enable、HDD4 Fan Enable、Intel Speed Shift Technology、PCIE0、PCIE1、PCIE0_CPU1、PCIE1_CPU1、PPI Bypass for Block SID Command、PPI Bypass for TPM Clear、Report Logo Type、SATA-8、Secure Boot Mode、SMM Security Mitigation、Slice Battery Custom Charge Limit 及 Wake on 2nd LAN (RJ-45/SFP)。

有關 BIOS 屬性的更多資訊，請參閱位於 dell.com/dellclientcommandssuitemanuals 的 Dell Command | Monitor 參考指南。

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 使用管理協定：說明共同資訊模型 (CIM) 標準及簡易網路管理通訊協定 (SNMP) 來管理用戶端系統。這樣能降低總持有成本、提升安全性，並且提供一種在網路中管理所有裝置的整體方法，包括用戶端、伺服器、儲存裝置、網路以及軟體裝置。

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，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，以及應用程式開發介面 (API)。Windows 適用的 Dell Command | Monitor 也會從動態連結程式庫 (DLL) 和登錄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 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，這些警報在 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，這些警報會以 Syslog、OMI 事件或應用程式記錄形式接收。

Windows 適用的 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，或透過其他擁有實作 Dell Command | Monitor 整合的主控台廠商。此外，您可以建立自訂指令碼，以鎖定相關的範圍。範例指令碼在 Dell TechCenter Dell Command | Monitor 頁面提供。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。

- ① **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/dellclientcommandssuitemanuals](https://dell.com/dellclientcommandssuitemanuals) 的 *Dell Command | Monitor 安裝指南*。
- ① **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 *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。

以下是因為 WSMT 相容性的運作方式變更：

- 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。如需有關平台清單的更多資訊，請參閱[支援的平台](#)。

Dell Command | Monitor 的主要功能：

- 支援 CIM 架構
- BIOS 設定
- WMI/OMI 安全
- 事件報告
- 遠端關機
- 使用 WSMAN 通訊協定，透過 CIM 架構存取系統資訊
- 詳細資產資訊的編譯
- 遠端喚醒組態
- 系統設定的遠端修改
- 監控系統健康狀況和報告狀態
- Intel 整合式控制器和 LSI 整合式控制器的 RAID 監控和警示。
- SNMP 監控和設陷只能透過 Windows 適用的 Dell Command | Monitor 進行

① | 註：使用 **Windows** 適用的 **Dell Command | Monitor**，也可透過 **SNMP** 存取資訊。

① | 註：執行 **Linux** 作業系統的系統不支援監控 **Intel** 整合式控制器。

支援 CIM 架構

Windows 適用的 Dell Command | Monitor 符合 CIM 2.17 架構，並包含兩個 WMI 提供者：

- WMI 指示提供者或輪詢代理程式
- WMI 例項或方法提供者

Linux 適用的 Dell Command | Monitor 符合 CIM 2.32.0 架構，並包含兩個 WMI 提供者：

- WMI 指示提供者或輪詢代理程式
- WMI 例項或方法提供者

BIOS 設定與列舉

Dell Command | Monitor 提供設定系統 BIOS 的能力。

WMI/OMI 安全

WMI 提供在將存取權限授予 CIM 資料和方法前先進行使用者驗證。存取權限由分散式元件物件模型 (DCOM) 安全性與 CIMOM 強制執行。完整或有限的存取權限會按照每個命名空間授予使用者。這之中不涉及類別實作或屬性層級安全性。根據預設，管理員群組內的成員都具有完整的本機及遠端 WMI 存取權。

針對 Windows 適用的 Dell Command | Monitor，您可以在 [服務與應用程式] 區段下的電腦管理主控台中使用 [WMI 控制] 來設定 WMI 安全性。以滑鼠右鍵按一下 **WMI 控制**，然後按一下 **Properties (內容)**。您可以從**安全性**標籤設定命名空間的特定安全性。您也可以從**開始**功能表執行 **WMI 控制**或從 **CLI** 執行 `wimgmt.msc`。

警示報告

Dell Command | Monitor 會偵測 Dell 系統上的事件，並向本機使用者和網路管理員報告潛在故障、組態變更、元件清查、整合式 Intel 和 LSI RAID 控制器、Probs 以及機箱入侵。這些事件會由系統管理應用程式顯示，例如 OpenManage Essentials (OME)。

遠端關機

Windows 適用的 Dell Command | Monitor 支援遠端系統關機與重新啟動。

系統資訊存取

Dell Command | Monitor 提供系統資訊存取，例如 BIOS 版本、BIOS 製造商/廠商、服務標籤、系統型號、首次開機日期，以及使用 CIM 透過 WMI / OMI 存取系統型號。您也可使用 WSMAN 通訊協定透過 WMI/OMI 來存取此資訊。

資產資訊的詳細細節

Dell Command | Monitor 提供對詳細的清查資訊 (例如處理器、記憶體、PCI 設備和電池) 的存取。

遠端喚醒設定

Dell Command | Monitor 支援遠端喚醒設定的組態。遠端喚醒是用戶端系統和網路介面卡 (NIC) 的功能。

遠端修改系統 BIOS 設定

Dell Command | Monitor 允許管理員擷取和設定企業用戶端 BIOS 設定，例如 USB 連接埠組態和 NIC 設定等。

系統健康和狀態

Dell Command | Monitor 會監控系統健康狀況，例如風扇狀態、記憶體、溫度、探查、電池、RAID 控制器、擴充座，並報告其狀態。

Intel 和 LSI 控制器的 RAID 監控和警報

針對 Windows 適用的 Dell Command | Monitor，Intel 和 LSI RAID 控制器的監控與警示適用於實體和邏輯磁碟機；針對 Linux 適用的 Dell Command | Monitor，監控與警報僅適用於 LSI 控制器。

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

- Intel 整合式控制器 (與 CSMI v0.81 或更新版本相容)
- LSI 整合式 RAID 控制器；和 9217、9271、9341、9361、9440、9460 及其相關的驅動程式 (實體和邏輯)

① | 註：執行 Linux 作業系統的系統不支援監控 Intel 整合式控制器。

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

SNMP 監控和設陷

Windows 適用的 Dell Command | Monitor 符合 SNMP v1 並支援監控系統屬性和設陷。

標準和協定

Dell Command | Monitor 是依據 CIM 標準而建立。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。

管理通訊協定如 WMI、SNMP 和 WSMAN 等均用於遠端監控。

註: Windows 適用的 Dell Command | Monitor 使用簡易網路管理通訊協定 (SNMP) 描述幾個系統變數。

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。

使用案例

本章介紹 Dell Command | Monitor 的各種使用案例。

您可以使用 Dell Command | Monitor 進行：

- 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

一間使用大量 Dell 系統的公司，因為業務和 IT 人員的變換，而無法精確維護清查資訊。資訊長 (CIO) 要求制定一個計劃，以識別可升級至 Microsoft Windows 最新版本的系統。此動作需要評估已部署的系統，從而判定某個專案所造成的規模、範圍及財務影響。而資訊收集方面將耗費龐大資源。就工作時數和對使用者的干擾而言，為每個用戶端系統部署 IT 員工的成本很高。

在每個 Dell 系統上使用 Dell Command | Monitor，IT 經理就能從遠端快速收集資訊。使用例如 Microsoft System Center Configuration Manager (SCCM) 的工具，IT 經理可在網路上查詢每個用戶端系統，並收集例如 CPU 類型和速度、記憶體大小、硬碟機容量、BIOS 版本、和目前的作業系統版本等資訊。收集資訊後即可進行分析，從而識別出可升級至 Windows 最新版本的系統。

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

SCCM 整合

您可以透過以下方式整合 SCCM 與 Windows 適用的 Dell Command | Monitor：

- 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\OMCL_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，並計劃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桌上型電腦即可在各個用戶端電腦的 BIOS 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企業用戶端系統的 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。指令碼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/dellclientcommandssuitemanuals 的 *Dell Command | Monitor 參考指南*。

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，但在整個電腦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：健康狀況監視

在嘗試存取特定用戶端系統硬碟機上的檔案時，使用者收到讀取錯誤訊息。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。將派遣服務技術人員更換硬碟機。

在硬碟機故障之前更換，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。

透過作業系統事件檢視器、Syslog、或 CIM 指示來監控系統警示

Dell Command | Monitor 支援透過下列程序監控事件：

- 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 Syslog 監控。

有關 Dell Command | Monitor 的更多資訊，請參閱位於 dell.com/dellclientcommandssuitemanuals 的 *Dell Command | Monitor 參考指南*。

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

① | 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，因此而面臨挑戰。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) 和資料中心基礎結構管理 (DCIM-OEM) 設定檔。本指南中說明了一些 DMTF 設定檔。

有關 Dell Command | Monitor 的更多資訊，請參閱位於 dell.com/dellclientcommandssuitemanuals 的 *Dell Command | Monitor 參考指南*。

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

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。
- 檢查電池的執行狀況資訊是否可以透過 **DCIM_Battery** 類別的 *Operational Status* 和 *HealthState* 屬性判斷。
- 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。

BIOS 管理設定檔

- 透過列舉 **dcim_bioselement** 的類別例項以判斷 BIOS 版本。
- 請檢查 BIOS 屬性值是否可以修改。取得類別的例項，**dcim_biosenumeration**。如果屬性 **isreadonly** 設定為 **FALSE**，您可以修改屬性。
- 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、服務標籤和序號。
- 執行 **DCIM_ComputerSystem.RequestStateChange()** 方法並將 RequestedState 參數值設定為 **3**。關閉系統。
- 重新開機系統。執行 **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。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。
- 找到個別記錄項目。取得所有透過 **DCIM_LogManagesRecord** 關聯與 **DCIM_RecordLog** 所提供的例項相關聯的 **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。

- 根據記錄項目的時間戳記排序記錄檔記錄。取得所有透過 **DCIM_LogManagesRecord** 關聯與 **DCIM_RecordLog** 所提供的例項相關聯的 **DCIM_LogEntry** 例項。根據於後進先出法 (LIFO) 中順序中 **CreationTimeStamp** 的屬性排序 **DCIM_LogEntry** 例項。
- 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。
- 檢查系統記憶體的健康狀況。

使用 Dell Command | Monitor

您可以透過存取以下位置，檢視由 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。

有關類別的更多資訊，請參閱 *Dell Command | Monitor 參考指南*，網址為 dell.com/dellclientcommandssuite/manuals。

如需有關類別的更多資訊，請參閱 *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 應用程式記錄
- 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 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。

- 針對 Windows，`dcscopy32.ini` 或 `dcscopy64.ini` 檔案位於 `<Dell Command | Monitor installed location>\omsa\ini`。
- 針對 Linux，`AlertPollingSettings.ini` 檔案位於 `/opt/dell/dcm/conf`。

① **註：**INI 檔中的數字是 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 X 23 秒，即大約 3 個小時)。

RAID 狀態報告

Dell Command | Monitor 透過硬體和驅動程式支援為用戶端系統啟用 RAID 組態資訊並監控 RAID 功能。您可以使用 RAID 類別取得關於 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。在 RAID 組態啟用後，您會收到效能降低或磁碟機及控制器故障的警示。

① **註：**RAID 狀態報告僅支援使用 Common Storage Management Interface (CSMI) 版本 0.81 相容驅動程式的 RAID 控制器。OMCI 8.1 及更新版本僅支援在 Intel 晶片上的 RAID 控制器使用監控功能，而 OMCI 8.2 及更新版本支援在 Intel 晶片上的 RAID 控制器使用警示功能。

監控 Dell 用戶端系統

- Windows 適用的 Dell Command | Monitor 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。管理資訊庫 (MIB) 檔案在 Dell Command | Monitor 和伺服器管理員之間共用。Windows 適用的 Dell Command | Monitor 從版本 9.0 已經過修改，採用用戶端特定的 OID (10909)，使得主控台可識別用戶端系統。

如需 SNMP 更多的資訊，請參閱 *Dell Command | Monitor SNMP 參考指南*，網址為 dell.com/dellclientcommandssuitemanuals。

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

- 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 應用程式記錄

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歷史。

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：

① 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。

① 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。

① 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 (也叫作 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 驅動器，從而有助於防止這些問題。

開機組態

① 註：Linux 適用的 Dell Command | Monitor 不提供開機組態功能。因此，本節不適用於 Linux 適用的 Dell Command | Monitor。

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) 使用以下類別來模型化：

- DCIM_ElementSettingData**
- DCIM_BootConfigSetting**
- DCIM_OrderedComponent**
- DCIM_BootSourceSetting**

① 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_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** 屬性包含用於識別開機裝置的字串。例如：軟碟機、硬碟、CD/DVD 光碟機、網路、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** 的例項之一相關聯。

DCIM_OrderedComponent

DCIM_OrderedComponent 關聯類別用於將 **DCIM_BootConfigSetting** 例項與代表開機設備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** 屬性指的是 **DCIM_BootConfigSetting** 例項，**PartComponent** 屬性指的是 **DCIM_BootSourceSetting** 例項。

變更系統設定

在 Dell Command | Monitor，使用下列方法可變更系統設定以及本機或遠端系統上的狀態：

- **SetBIOSAttributes** — 變更 BIOS 設定
 - ① 註: Linux 適用的 Dell Command | Monitor 目前僅支援 **SetBIOSAttributes** 方法。
- **ChangeBootOrder** — 變更開機組態
- **RequestStateChange** — 關閉及重新啟動系統
- **ManageTime** — 顯示系統時間

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

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

您可以使用 **SetBIOSAttributes** 方法來設定 BIOS 屬性。此程序接下來會以啟用信賴平台模組 (TPM) 工作為例子說明。

① 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 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

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：確定 OMI 伺服器已啟動並正在執行。

使用 OMICLI 設定 BIOS 屬性

您可以使用 SetBIOSAttributes 方法來設定 BIOS 屬性。此程序接下來會以啟用信賴平台模組 (TPM) 工作為例子說明。

❗ 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 若要設定系統的 BIOS 密碼。若尚未設定，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 若要使用以下命令啟用 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

```
./omiccli 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 方法來設定 BIOS 屬性。此程序接下來會以啟用信賴平台模組 (TPM) 工作為例子說明。如需詳細資訊，請參閱[遠端管理 Dell 用戶端系統](#)。

① 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 透過列舉設定 DCIM_BIOSService 類別取得選取器設定。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
```

① 註：在此例子中，會使用選取器設定值 (SystemName=<system name from DCIM_BIOSService class>winrm i SetBIOSAttributes wsman/DCIM_BIOSService?SystemName=dt: +SystemCreationClassName=DCIM_ComputerSystem +Name=DCIM:BiosService+CreationClassName=DCIM_BIOSService+) 進行設定操作。

- 2 設定系統的 BIOS 密碼。若尚未設定，請使用下列命令：

```
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，以啟用 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 在執行 Linux 的系統上設定 BIOS 屬性。此程序接下來會以啟用信賴平台模組 (TPM) 工作為例子說明。如需詳細資訊，請參閱[遠端管理 Dell 用戶端系統](#)。

① 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 透過列舉設定 DCIM_BIOSService 類別取得選取器設定。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，請使用下列命令：

```
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 使用下列命令檢查開機順序類型 (傳統或 UEFI)：

- WMIC 命令：wmic /namespace:\\root\dcim\sysman path dcim_BootConfigSetting get ElementName/format:list。
- PowerShell 命令：gwmi -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)：

- WMIC 命令：wmic /namespace:\\root\dcim\sysman path dcim_ElementSettingData.IsCurrent=1 get SettingData /format:list。
- PowerShell 命令：gwmi -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：

- WMIC 命令：wmic /namespace:\\root\dcim\sysman path dcim_bootconfigsetting call ChangeBootOrder /?:full。
- PowerShell 命令：(gwmi -namespace root\dcim\sysman -class dcim_bootconfigsetting).getmethodparameters("ChangeBootOrder")。

① 註: dcim_BootConfigSetting 例項必須呈現您要變更的開機組態：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：

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

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

在命令列介面中，執行下列命令：

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

在本機管理 Dell 用戶端系統

您可以使用下列任一方法在本機管理 Dell 用戶端系統：

- 若為執行 Windows 的系統，使用 [PowerShell](#)。
- 若為執行 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 命令在本機管理執行 Windows 的 Dell 用戶端系統。

- **DCIM 類別的列舉例項**

```
- 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)
```

使用 OMICLI 在本機管理 Linux 系統

您可以使用 OMICLI 命令在本機管理 Linux 系統。在執行 Linux 的系統中，OMICLI 安裝於 `/opt/omi/bin`。

- **DCIM 類別的列舉例項**

```
- ./omicli ei root/dcim/sysman DCIM_BIOSEnumeration
- ./omicli ei root/dcim/sysman DCIM_BIOSPassword
```

- **取得 BIOS 設定屬性**

```
./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"
```

遠端管理 Dell 用戶端系統

您可以使用下列任一方法來遠端管理 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
- 若為執行 Linux 的系統，使用 WinRM 透過 Windows 系統遠端管理 Linux 系統

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 系統遠端存取與監控 Windows 系統。
管理 **Windows** 系統的先決條件：

- Windows PowerShell 3.0
- PowerShell 已針對執行遠端指令碼加以設定

受管理 **Windows** 系統的先決條件：

- Dell Command | Monitor
- Windows PowerShell 3.0
- PowerShell 已針對執行遠端指令碼加以設定
- 已啟用 PowerShell 遠端功能

① 註：

若要遠端使用 Windows PowerShell，必須設定遠端電腦以便進行遠端管理。如需更多資訊 (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 Microsoft Windows 的系統存取與監控執行 Linux 的系統。

Windows 系統的先決條件

- 受支援的 Windows 作業系統
- WinRM 服務執行中且已針對遠端管理進行設定

Linux 系統的先決條件：

- Root 權限
- Dell Command | Monitor
- 受支援的 Linux 作業系統

- 在 WMI 伺服器上啟用 5985 和 5986 連接埠
- 為您的環境設定系統

在命令列介面，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 的系統遠端存取與監控執行 Linux 的系統。

管理 Linux 系統的先決條件：

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

受管理 Linux 系統的先決條件：

- 根存取權限
- 受支援的 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
```

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 · 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 `dcim_orderedcomponent.assignedsequence` 屬性等於 0 時 · 其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 ?

變更啟動順序時 · 每個 `DCIM_OrderedComponent` 例項上的 `AssignedSequence` 屬性的值 (建立 `DCIM_BootConfigSetting` 例項目標與未出現在來源參數輸入陣列的 `DCIM_BootSourceSetting` 例項關聯) · 設定為 0, 表示該裝置已停用。

使用 `wbemtest` 連線到命名空間時出現失敗登入訊息。如何解決 ?

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可能產生的錯誤。

如何不發生任何問題下執行 TechCenter 指令碼 ?

以下是執行 Dell Command | Monitor Techcenter 連結中提供的 VBS 指令碼時的先決條件 :

- 1 請使用命令 `winrm quickconfig` 於系統上設定 `winrm`。
- 2 檢查權杖支援是否存在於系統上 · 參照 :
 - 在 BIOS 設定中的 **F2** 螢幕。
 - 使用例如 `wbemtest` 的工具檢查指令碼定義的金鑰值是否存在於系統中。

① 註: Dell 建議您使用最新的 BIOS · 您可於 dell.com/support 取得。如需更多資訊 · 請參閱 dell.com/dellclientcommandsuitemanuals 的 Dell Command | Monitor 參考指南。

① 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` 需要將輸入對應 `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。如果系統中已設定 BIOS 密碼，您則必須在第五個引數中輸入相同密碼。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 Windows 與 Linux 作業系統支援儲存裝置和感應器監控。

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

- Intel 整合式控制器 (與 CSM v0.81 或更新版本相容)
- 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)

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

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

有關類別和警示的更多資訊，請參閱位於 dell.com/dellclientcommandsuite/manuals 的 Dell Command | Monitor 參考指南。

Dell Command | Monitor 可否與其他應用程式/主控台整合？

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 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`。

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 的相依性使 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：

- 請確定您的伺服器執行於最新的 Windows 伺服器上。

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。

- 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。
- 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。
- 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。

註：Dell 建議使用 Dell OpenManage Essentials 替代 IT Assistant。如需深入瞭解 Dell OpenManage Essentials，請參閱 dell.com/dellclientcommandssuitemanuals。

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 在本機系統上安裝 **WMI 工具**與 **wbemtest**，然後在遠端系統上安裝 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 將**本機安全性**設定設為 **傳統 - 本機使用者以自身身分驗證的網路存取：共用和安全性模式**用於本機安全性原則的本機帳戶中。
 - 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。
- PowerShell 主控台必須為關閉。

① **註：**若要檢查系統的 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。

① **註：**系統必須執行支援的 **Microsoft Windows** 作業系統。

① **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 確認下列套件均以根使用者權限安裝；
 - `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 如果已安裝上述套件，請確認已載入驅動程式模組。
 - a 執行以下命令 `lsmod | grep dcdbas` 以確認已載入驅動程式模組。
 - b 如果驅動程式模組無法使用，請執行以下命令 `modinfo dcdbus` 以擷取驅動程式詳細資料。
 - c 透過執行以下命令 `insmod <filename>` 載入驅動程式模組。

libsmbios 的相依性使 Hapi 安裝失敗

如因相依性問題使安裝失敗，

透過執行 `apt-get -f install` 來強制安裝所有相依套件。

CIM 資源無法使用

在列舉時，如果您收到「CIM 資源無法使用」的錯誤訊息，

請確認已使用根權限執行命令。

無法在執行 Ubuntu Core 16 的系統上使用 DCM 執行命令

確定系統上的 Snap 版本為 2.23 版或更新版本。

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/dellclientcommandssuitemanuals 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)。

與 Dell 公司聯絡

① | 註: 如果無法連線網際網路，則可以在購買發票、包裝單、帳單或 Dell 產品目錄中找到聯絡資訊。

Dell 提供多項線上和電話支援與服務選擇。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 Dell 聯絡：

- 1 移至 **Dell.com/support**。
- 2 選取您的支援類別。
- 3 在網頁底部的 **Choose A Country/Region (選擇國家/地區)** 下拉式選單中確認您所在的國家或地區。
- 4 根據您的需求選取適當的服務或支援連結。

主題：

- 其他您可能需要的文件
- 從 Dell EMC 支援網站存取文件

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/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)。

從 Dell EMC 支援網站存取文件

您可以用下列連結存取所需文件：

- Dell EMC 企業系統管理文件 — Dell.com/SoftwareSecurityManuals
- Dell EMC OpenManage 文件 — Dell.com/OpenManageManuals
- Dell EMC 遠端企業系統管理文件 — Dell.com/esmanuals
- iDRAC 和 Dell EMC Lifecycle Controller 文件 — Dell.com/idracmanuals
- Dell EMC OpenManage Connections 企業系統管理文件 — Dell.com/OMConnectionsEnterpriseSystemsManagement
- Dell EMC 服務性工具文件 — Dell.com/ServiceabilityTools
- a 前往 Dell.com/Support/Home。
- b 按一下從所有產品選擇。
- c 從所有產品區段中，按一下軟體和安全性，然後按一下以下所需的連結：
 - 企業系統管理

- 遠端企業系統管理
 - 服務性工具
 - **Dell** 用戶端命令套件
 - **Connections** 用戶端系統管理
- d 若要檢視文件，按一下所需的產品版本。
- 使用搜尋引擎：
 - 在搜尋方塊輸入文件名稱和版本。