Dell Command | Monitor 版本 10.6
用户指南

2021 年 10 月
Rev. A01

注意、小心和警告

注： “注意”表示帮助您更好地使用该产品的重要信息。

小心： **“小心”表示可能会损坏硬件或导致数据丢失，并告诉您如何避免此类问题。**

警告： **“警告”表示可能会导致财产损失、人身伤害甚至死亡。**

目录

1

Dell Command | Monitor 10.6 简介

Dell Command | Monitor 软件应用程序使 IT 管理员可以轻松管理队列资源清册、监测系统运行状况、修改 BIOS 设置，以及远程收集已部署 Dell 客户端系统的信息。

活动系统运行状况监视可帮助降低系统的总拥有成本，并且是管理所有联网设备的整体方法的一部分。

Dell Command | Monitor 专为 Dell Enterprise 客户端系统、Dell IoT 网关系统以及 Dell Embedded PC 而设计。

此文档提供了 Dell Command | Monitor 及其功能的概览。有关受支持的 Dell 系统的更多信息，请参阅位于 **dell.com/support** 的发行说明。

主题：

此 Dell Command | Monitor 10.6 发行版的新增功能

- 支持下列新 BIOS 属性：
  - Intel@ GNA Accelerator
  - Multiple Atom Cores
  - USB4 CM Mode
  - Onboard Unmanaged NIC
  - Enable Pre-Boot DMA Support
  - Enable OS Kernel DMA Support
  - PCIe Resizable Base Address Register (BAR)
  - OS Agent Requests
  - Enable Microsoft UEFI CA
  - Legacy Manageability Interface Access
  - Power-on-Self-Test (POST) Automatic Recovery
- 支持 **ResetBIOSDefaults** 方法。

Dell Command | Monitor 概览

注: Dell Command | Monitor for Linux 不支持简单网络管理协议 (SNMP)。

Dell Command | Monitor 使用管理协议公用信息模型 (CIM) 标准和简单网络管理协议 (SNMP) 来管理客户端系统。这有助于降低系统总拥有成本、提高安全性，并以整体的方式管理网络设备内的所有设备。

使用 CIM，您可以通过 Web Services for Management Standards (WSMAN) 访问 Dell Command | Monitor。

Dell Command | Monitor 含有基础驱动程序集，从不同源收集客户端系统信息，这些源包括 BIOS、CMOS、System Management BIOS (SMBIOS)、System Management 接口 (SMI)、操作系统和应用程序编程接口 (API)。Dell Command | Monitor for Windows 还会从动态链接库 (DLL) 和注册表设置中收集客户端系统信息。Dell Command | Monitor for Windows 通过 CIM Object Manager (CIMOM) 接口、Windows Management Instrumentation (WMI) 堆栈或 SNMP 代理程序检索此信息，而 Dell Command | monitor for Linux 通过 Open Management Infrastructure (OMI) 接口检索此信息。

Dell Command | Monitor 支持 IT 管理员远程收集资产信息，修改 BIOS 设置，接收有关潜在故障情况的主动通知，并获得潜在安全漏洞的警报。在运行 Windows 的系统中，这些警报以 NT 事件日志中的事件、WMI 事件或 SNMP 陷阱 v1 形式提供。在运行 Linux 的系统中，这些警报以系统日志、OMI 事件或应用程序日志形式提供。

Dell Command | Monitor for Windows 可以通过直接访问 CIM 信息或已实施 Dell Command | Monitor 集成的其他控制台供应商，集成到 Microsoft System Center Configuration Manager 等控制台。此外，您可以创建自定义脚本以确定感兴趣的关键领域。Dell 知识库的 Dell Command | Monitor 页提供了示例脚本。您可以使用这些脚本监测资源清册、BIOS 设置和系统运行状况。

注: 默认安装不启用 SNMP 支持。有关为 Dell Command | Monitor for Windows 启用 SNMP 支持的更多信息，请参阅 **dell.com/support** 上的 Dell Command | Monitor 安装指南。

2

Windows SMM 安全气候变化表 (WSMT) 合规性

Windows SMM 安全气候变化表包含有关为 Windows 操作系统创建的 ACPI 表的信息，该表支持 Windows 基于虚拟化的安全 (VBS) 功能。Dell Command | Monitor 兼容 WSMT。这是用于配置具有启用 BIOS 的 WSMT 的 Dell 客户端系统上的平台功能。

以下是由 WSMT 合规性产生的行为变更：

在具有支持 WMI/ACPI 的 BIOS 兼容版本的 Dell 客户端平台上可用的 Dell Command | Monitor 功能。

注: 有关支持的平台的更多信息，请参阅受支持的平台。

3

适用于 Dell Command | Monitor 10.6 的标准和协议

Dell Command | Monitor 基于 CIM 标准。CIM 规范详细介绍了用于提高与管理协议兼容性的映射技术。

WMI、SNMP 和 WSMAN 等管理协议用于远程监控。

注: Dell Command | Monitor for Windows 使用简单网络管理协议 (SNMP) 描述系统的几个变量。

桌面管理任务组 (DMTF) 是业界公认的标准机构，负责引领台式机、企业和互联网环境的管理标准（包括 CIM 和 ASF）和计划的开发、采用和统一。

4

使用 Dell Command | Monitor 10.6 的使用案例场景

本章介绍 Dell Command | Monitor 的各种用户方案。

您可将 Dell Command | Monitor 用于：

- 资产管理
- 配置管理
- 运行状况监测
- 配置文件

主题：

方案 1：资产管理

由于业务和 IT 人员的变化，拥有许多 Dell 系统的公司无法维护准确的资源清册信息。首席信息官 (CIO) 请求一项用于确定可以升级到最新版本 Windows 系统的计划。这需要评估部署的系统，以确定此类项目的规模、范围和财务影响。信息收集涉及大量工作。在终端用户中断的情况中，将 IT 员工部署到每个客户端系统的成本很高。

使用各 Dell 系统上的 Dell Command | Monitor，IT 管理员可以远程快速收集信息。使用 Microsoft System Center Configuration Manager (SCCM) 等工具，IT 管理员通过网络查询每个客户端系统，并收集诸如 CPU 类型、速度、内存大小、硬盘驱动器容量、BIOS 版本和当前操作系统版本等信息。收集信息后，可以对其进行分析以确定可升级到最新版本 Windows 的系统。

您还可以通过 WSMAN/WinRM 命令行或使用任何 CIM 客户端命令行来获得资产资源清册。

SCCM 集成

您可以通过以下方法将 SCCM 与 Dell Command | Monitor for Windows 集成：

- 使用 Dell Command | Monitor 安装包内的 MOF 文件（该安装包内包含所有 Dell Command | Monitor 类），并导入 ConfigMgr

  MOF 位于：

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

- 使用集合扩展资产报告功能

方案 2：配置管理

某公司计划实现客户端平台标准化并在系统整个生命周期内对其进行管理。为此，该公司购买了一套工具，并计划使用预引导执行环境 (PXE) 自动部署新的客户端操作系统。

问题在于要在不手动访问台式机的情况下在每个客户端计算机中修改 BIOS 密码。利用每个客户端系统上安装的 Dell Command | Monitor，该公司的 IT 部门可以通过多种方式远程修改引导顺序。OpenManage Essentials (OME) 是一个管理控制台，可与 Dell Command | Monitor 集成并用于远程监控所有客户端系统上的 BIOS 设置。另一种选择是编写可更改 BIOS 设置的脚本（CIM、WinRM/WSMAN/PowerShell/WMIC）。脚本可通过网络远程交付，并在每个客户端系统上运行。

有关 Dell Command | Monitor 的更多信息，请参阅位于 **dell.com/support** 的 Dell Command | Monitor 参考指南。

无论公司的规模如何，标准化配置均可带来显著的成本节省。许多组织都部署了标准化客户端系统，但很少组织能在计算机整个生命周期内管理系统配置。借助安装在每个客户端系统上的 Dell Command | Monitor，IT 部门可以锁定旧端口以防止使用未经授权的外围设备，或启用 LAN 唤醒 (WOL) 以便系统能够在非繁忙时间从睡眠状态唤醒以执行系统管理任务。

方案 3：运行状况监测

用户接收读取错误消息，同时尝试访问客户端系统硬盘驱动器上的特定文件。用户重新引导系统，文件现在已显示并可供访问。用户忽视初始问题，因为该问题似乎已自行解决。同时，Dell Command | Monitor 检查硬盘驱动器是否有问题以预先检测故障，并将自我监测分析与报告技术 (SMART) 警报发送至管理控制台。它还向本地用户显示 SMART 错误。警报指示在硬盘驱动器中存在数个读/写错误。公司的 IT 部门建议用户务必立即备份关键数据文件。已派遣服务技术人员，并带有更换用驱动器。

在硬盘发生故障前进行更换，防止用户停机、技术支持呼叫以及技术人员亲临台式机诊断问题。

通过操作系统事件查看器、系统日志或 CIM 指示监测系统警报

Dell Command | Monitor 通过以下程序支持监测事件：

- 通过 CIM 类 DCIM_LogEntry 提取日志。
- 通过 DCIM_AlertIndication 类监测 CIM 指示。
- （仅适用于 Dell Command | Monitor for Windows）通过简单网络管理协议 (SNMP) 和 Windows 事件查看器监测事件。
- （仅适用于 Dell Command | Monitor for Linux）通过系统日志监测。

有关 Dell Command | Monitor 的更多信息，请参阅位于 **dell.com/support** 的 Dell Command | Monitor 参考指南。

方案 4：配置文件

注: DMTF 配置文件仅针对 Dell Command | Monitor for Windows 实施。

IT 管理员需要管理多供应商和分布式企业环境中的客户端系统。他们面临挑战，因为他们必须掌握各种工具和应用程序，同时管理不同网络中的多个台式机和移动客户端系统。为了降低这些要求的成本和表示所提供的管理数据，在 Dell Command | Monitor 中实施了业界标准的分布式管理综合小组 (DMTF) 和数据中心基础设施管理 (DCIM-OEM) 配置文件。本指南讲解了部分 DMTF 配置文件。

有关更多信息，请参阅位于 **dell.com/support** 的 Dell Command | Monitor 参考指南。

资产配置文件

终端设备的保修状态：

- 通过枚举或获得 **DCIM_AssetWarrantyInformation** 类的实例来确定保修状态。
- 检查是否可以使用类 **DCIM_AssetWarrantyInformation** 的 **WarrantyStartDate** 和 **WarrantyEndDate** 属性来确定保修状态。

  注: DCIM_AssetWarrantyInformation 前提条件是您必须具备有效的互联网连接。如果您在代理服务器后运行 Dell Command | Monitor，请确保已正确配置代理设置。

  要获取有关外围设备保修状态的更多信息，请执行以下操作：

  1. 转至 Dell.com/support
  2. 在页面底部的选择国家/地区下拉列表中，确认您所在的国家/地区。
  3. 选择支持类别 - 保修和合同
  4. 提供相应的系统的服务标签
- 禁用保修功能和后续刷新调用。
- 按需推送保修信息。

注: 保修信息每 15 天自动更新一次。对于最新保修状态，所枚举的保修信息可能与 Dell 支持站点上的信息不同。

电池配置文件

- 通过枚举或获得 **DCIM_Battery** 类的实例来确定电池的状态。
- 确定预计的运行时间并查看预计的剩余电量。

- 检查电池的运行状况信息是否可以通过 **DCIM_Battery** 类的 Operational Status 和 HealthState 属性确定。
- 使用 **DCIM_Sensor.CurrentState** 属性或 **CIM_NumericSensor.CurrentState** 属性获得有关电池运行状况的附加信息。
- 使用类 **DCIM_Battery** 的 **IdentifyingDescriptions** 和 **OtherIdentifyingInfo** 属性确定电池位置和电池 ePPID。

DCIM_Battery

要获取有关电池的电池 ePPID 值的信息，请以管理员身份打开 PowerShell 提示符，然后运行以下命令：`Get-CimInstance -Namespace root/dcim/sysman -Classname DCIM_Battery |Select ElementName, OtherIdentifyingInfo, IdentifyingDescriptions`。

注: 电池 ePPID 值不是动态的，如果更换了电池，则必须重新启动系统才能反映 **DCIM_Battery** 实例中的更改。

BIOS 管理配置文件

- 通过枚举 **DCIM_BIOSElement** 类的实例来确定 BIOS 版本。
- 检查 BIOS 属性值是否可以修改。获取 **DCIM_BIOSEnumeration** 类的实例。如果 **IsReadOnly** 属性设置为 FALSE，则可以修改属性。
- 设置系统密码 (SystemPwd)。运行 **DCIM_BIOSService.SetBIOSAttributes()** 方法，将 SystemPwd 设置为 AttributeName 并将密码值设置为 AttributeValue 参数。
- 设置 BIOS 或管理员密码 (AdminPwd)。运行 **DCIM_BIOSService.SetBIOSAttributes()** 方法，将 AdminPwd 设置为 AttributeName 并将密码值设置为 AttributeValue 参数。
- 运行 **DCIM_BIOSService.SetBIOSAttributes()** 方法，指定 AttributeName 和 AttributeValue 参数。
- 要在 BIOS 或管理员密码已设定时修改 BIOS 属性，请运行 **DCIM_BIOSService.SetBIOSAttributes()** 方法并将 AttributeName、AttributeValue 和当前的 BIOS 密码指定为 AuthorizationToken 输入参数。

引导控制

- 更改传统和 UEFI 引导列表中引导项的顺序。
- 启用或禁用传统和 UEFI 引导列表中的引导项。
- 通过枚举其 **IsCurrent** 属性设置为 **1** 的 **DCIM_ElementSettingData** 类的实例查找当前的引导配置。**DCIM_BootConfigSetting** 代表当前的引导配置。

基本桌面移动

- 通过枚举 **DCIM_ComputerSystem** 类的实例，确定系统型号、服务标签和序列号。
- 您可以使用 **DCIM_ComputerSystem.RequestStateChange()** 方法将 RequestedState 参数值设置为 **3**。参数值 3，关闭系统。
- 您可以使用 **DCIM_ComputerSystem.RequestStateChange()** 方法将 **RequestedState** 参数值设为 **11**。参数值 11，重新启动系统。
- 确定系统的电源状态。
- 通过查询 **DCIM_Processor**（通过 **DCIM_SystemDevice** 关联与中心实例关联）实例确定系统中的处理器数量。
- 获取系统时间。运行 **DCIM_TimeService.ManageTime()** 方法并将 **GetRequest** 参数设为 **True**。
- 检查托管元素的运行状况。

日志记录

- 通过选择 **DCIM_RecordLog** 实例来确定日志名称，该实例中的 **ElementName** 属性即对应日志名称。
- 查看个别日志条目。获取所有的 **DCIM_LogEntry** 实例，它们通过 **DCIM_LogManagesRecord** 关联与 **DCIM_RecordLog** 的指定实例相关联。根据 **RecordID** 对实例进行排序。
- 通过枚举其属性 **Enabledstate** 设置为 **2**（代表“已启用”）和 **EnabledState** 设置为 **3**（代表“已禁用”）的 **DCIM_RecordLog** 类的实例来检查记录日志启用与否。
- 根据日志条目的时间戳对日志记录进行排序。获取所有的 **DCIM_LogEntry** 实例，它们通过 **DCIM_LogManagesRecord** 关联与 **DCIM_RecordLog** 的指定实例相关联。根据 **CreationTimeStamp** 属性值以后进先出 (LIFO) 顺序对 **DCIM_LogEntry** 实例进行排序。
- 通过对 **DCIM_RecordLog** 的指定实例运行 **ClearLog()** 方法来清除日志。

物理资产

- 获得系统内所有设备的物理资源清册。
- 获得系统机箱的物理资源清册。
- 确定故障组件的部件号。
- 确定插槽是否为空。

系统内存配置文件

- 获取系统的内存信息。
- 获取系统的物理内存信息。
- 检查系统内存大小。
- 检查可用系统内存大小。
- 检查物理系统内存大小。
- 检查系统内存的运行状况。

5

使用 Dell Command | Monitor 10.6

您可以通过访问以下路径来查看 Dell Command | Monitor 提供的信息： `root\dcim\sysman (standard)`

Dell Command | Monitor 通过这些命名空间中的类提供信息。

有关这些类的更多信息，请参阅位于 **dell.com/support** 的 Dell Command | Monitor 参考指南。

主题：

轮询间隔设置

您可以使用 Dell Command | Monitor 更改以下轮询间隔，例如风扇探测器、温度探测器、电压探测器、电流探测器、磁盘容量增加/减少、内存大小增加/减少和处理器数量增加/减少。

- 对于 Windows，`dcsbdy32.ini` 或 `dcsbdy64.ini` 文件位于 `<Dell Command | Monitor installed location>\omsa\ini`。
- 对于 Linux，`AlertPollingSettings.ini` 文件位于 `/opt/dell/dcm/conf`。

注: INI 文件中的数字是 **23** 的倍数。磁盘容量和自我监测分析与报告技术 (SMART) 警报的默认轮询间隔为 **626** 秒（实际时间 = 626 X 23 秒，即大约 3 个小时）。

RAID 状态报告

Dell Command | Monitor 启用 RAID 配置信息并通过硬件和驱动程序支持来监测客户端系统的 RAID 功能。您可以使用 RAID 类获取有关 RAID 级别、驱动程序信息、控制器配置和控制器状态的详细信息。一旦启用了 RAID 配置，即可接收驱动器和控制器降级或故障的警报。

注: RAID 状态报告仅受运行于 Common Storage Management Interface (CSMI) 版本 0.81 兼容驱动程序的 RAID 控制器的支持。OMCI 8.1 及其更高版本仅支持 Intel 片上 RAID 控制器中的监测；而对于 OMCI 8.2 及其更高版本，则支持 Intel 片上 RAID 控制器中的警报功能。

监测 Dell 客户端系统

- Dell Command | Monitor for Windows 支持简单网络管理协议 (SNMP) 用于监测和管理笔记本电脑、台式机和工作站等客户端系统。管理信息库 (MIB) 文件在 Dell Command | Monitor 和服务器管理员之间共享。Dell Command | Monitorfor Windows 从 9.0 版起已修改为使用特定于客户端 OID (10909) 的 OID，以便控制台识别客户端系统。

有关 SNMP 的更多信息，请参阅位于 **dell.com/support** 的 Dell Command | Monitor SNMP 参考指南。

- Dell Command | Monitor for Linux 支持使用 WinRM 和 WSMan 命令进行检测。

适用于 Linux 的 Dell Command | Monitor 应用程序日志

Dell Command | Monitor for Linux 将应用程序日志和警报划分为报告目的和调试目的。为 Dell Command | Monitor 应用程序生成的警报和日志的历史记录可以在 `/opt/dell/dcm/var/log`.中的 **dcm_application.log** 文件中查看。

配置文件

您可以更新 `/opt/dell/dcm/conf` 中的配置文件 **log.property**，以应用所需的设置和调试：

注: 在配置文件中进行任何更改后重新启动 OMI 服务器以应用更改。

- Log_Level — 系统消息划分为三个日志级别：错误、信息、调试

  用户可以从配置文件更改日志级别。如果日志级别设置为调试，Dell Command | Monitor 应用程序日志会将所有信息发送到指定的日志文件。

  注: 默认日志级别设置为信息。
- File_Size — 用户可以指定 **dcm_application.log** 文件的大小上限。默认文件大小为 500 MB。

  注: File_Size 值必须以字节表示。
- BackupIndex — 用户可以指定 **dcm_application.log** 文件的翻转计数。如果默认翻转计数为 2，则第三个备份文件将覆盖最旧的文件。

检测高级格式驱动器

客户端系统转换为高级格式 (AF) 驱动器以获得更大储存容量，并解决 512 字节扇区硬盘驱动器 (HDD) 的限制。硬盘驱动器转换为 4KB 扇区可以保持向后兼容性，而最新的 AF 硬盘驱动器（也叫作 512e 硬盘驱动器）匹配 512 字节 SATA 并在 4KB 下操作。在转换过程中，您可能会遇到性能问题，如客户端系统中分区未对齐的硬盘导致基于扇区的加密软件包（处理 512e 硬盘驱动器）发生故障。Dell Command | Monitor 可让您确定系统中的硬盘驱动器是否为 4KB AF 驱动器，从而有助于防止这些问题。

引导配置

注: Dell Command | Monitor for Linux 不提供引导配置功能。因此该部分不适用于 Dell Command | Monitor for Linux。

客户端系统可以有两种类型的引导配置之一：

- 传统 (BIOS)
- UEFI

在 Dell Command | Monitor 中，引导配置（传统或 UEFI）使用下面的类建模：

- DCIM_ElementSettingData
- DCIM_BootConfigSetting
- DCIM_OrderedComponent
- DCIM_BootSourceSetting
- DCIM_SmartAttributeInfo

注: 术语引导配置和引导列表类型可互换使用，且传达了代表传统或 UEFI 的相同含义。

DCIM_AssetWarrantyInformation

- 要查询终端设备上的保修状态，请在 PowerShell 提示符处运行以下命令：

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

- 要按 `WarrantyEndDate` 的时间顺序列出保修权利，请在 PowerShell 提示符处运行以下命令：

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

- 要禁用保修功能和后续刷新调用，请在 PowerShell 提示符处运行以下命令：

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

- 要按需推送保修信息，请在 PowerShell 提示符处运行以下命令：

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

注: 设置代理配置 -

- 默认代理 – Dell Command | Monitor 并选择默认系统代理（在 IE 中设置）
- 自定义代理

  DCIM_ApplicationProxySetting 类用于根据代理环境修改 Dell Command | Monitor 的代理设置。

DCIM_BootConfigSetting

DCIM_BootConfigSetting 的一个实例代表在引导过程中使用的一种引导配置。例如，在客户端系统上，存在两类引导配置：传统和 UEFI。因此，**DCIM_BootConfigSetting** 最多可代表两个实例，传统和 UEFI 各一个。

使用以下属性，用户可以决定是否 **DCIM_BootConfigSetting** 代表传统：

- InstanceID = "DCIM:BootConfigSetting:Next:1"
- ElementName = "Next Boot Configuration Setting : Boot List Type 1"

使用以下属性，用户可以决定是否 **DCIM_BootConfigSetting** 代表 UEFI：

- InstanceID = "DCIM:BootConfigSetting:Next:2"
- ElementName = "Next Boot Configuration Setting : Boot List Type 2"

DCIM_BootSourceSetting

此类代表引导设备或源。**ElementName**、**BIOSBootString** 和 **StructuredBootString** 属性包含标识引导设备的字符串。例如，floppy、hard disk、CD/DVD、network、Personal Computer Memory Card International Association (PCMCIA)、Battery Electric Vehicle (BEV) 或 USB。根据设备的引导列表类型，**DCIM_BootSourceSetting** 的一个实例关联 **DCIM_BootConfigSetting** 的一个实例。

DCIM_OrderedComponent

DCIM_OrderedComponent 关联类用于将 **DCIM_BootConfigSetting** 实例与代表引导设备所属引导列表类型（传统或 UEFI）之一的 **DCIM_BootSourceSetting** 实例相关联。**DCIM_OrderedComponent** 的 **GroupComponent** 属性引用 **DCIM_BootConfigSetting** 实例，**PartComponent** 属性引用 **DCIM_BootSourceSetting** 实例。

DCIM_Smart 属性

要读取 smart 属性值，请运行以下命令：

例如：

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

要设置自定义阈值，请运行以下命令：

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 管理散热配置设置，例如散热模式、AAC 模式和风扇故障模式。

- 要查询有关设备的散热信息，请运行以下命令：

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

- 要设置散热模式的值，请运行以下命令：

```
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")}
```

更改系统设置

在 Dell Command | Monitor 中，使用以下方法更改本地或远程系统的系统设置和状态：

- SetBIOSAttributes - 更改 BIOS 设置

  注: Dell Command |Monitor for Linux 目前仅支持 SetBIOSAttributes 方法。
- ChangeBootOrder - 更改引导配置
- RequestStateChange - 关闭和重新启动系统
- ManageTime — 显示系统时间

在 Dell Command | Monitor for Windows 中，您可以使用 winrm、VB 脚本、PowerShell 命令、wmic 和 WMI wbemtest 来运行这些方法。

对于在 Windows 或 Linux 上运行的系统，将 BIOS 重置为默认值

ResetBIOSDefaults（方法）

PowerShell (WMI) 命令：`Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod -MethodName ResetBIOSDefaults -Arguments @{ DefaultType=<one of the possible values>}`

OMI 命令：`/omicli iv root/dcim/sysman { DCIM_BIOSService Name DCIM:BiosService SystemCreationClassName DCIM_ComputerSystem SystemName <ServiceTag> CreationClassName DCIM_BIOSService } ResetBIOSDefaults { DefaultType <one of the possible values> }`

可能的值：

- 0-内置安全默认配置 — 这称为 BIOS 默认配置。此配置支持任何平台，因此不能更改配置。
- 1-最近一次的正确配置 — 这由 BIOS 在成功完成开机自检后自动生成。此选项可将 BIOS 恢复为良好的配置。如果**内置安全默认配置**已损坏，则可以使用**最近一次的正确配置**来恢复 BIOS。
- 2-出厂默认值配置 — 出厂默认配置在系统发货之前生成。此配置针对硬件配置进行了优化，或根据您在购买或维修时的要求进行自定义。
- 3-用户配置 1 — 这是在用户需要时配置的。您必须在 BIOS 设置或 F2 屏幕中**保存当前配置**，才能通过 Dell Command | Monitor 应用程序重置配置。
- 4-用户配置 2 — 这是在用户需要时配置的。您必须在 BIOS 设置或 F2 屏幕中**保存当前配置**，才能通过 Dell Command | Monitor 应用程序重置配置。

表. 1: ResetBIOSDefaults 的可能值

说明	错误代码（SetResult 值）
成功	0
输入值无效/输入值超出范围	1
验证错误	2

表. 1: ResetBIOSDefaults 的可能值 （续）

说明	错误代码（SetResult 值）
不支持的配置	3
空配置	4
一般故障/失败/服务未运行时	4294967295

注: **ResetBIOSDefaults** 操作后需要重新启动系统，才能成功实现更改。

DCM 窗口具有通过以下 API 关闭或重新启动系统的功能：

- 重启系统 —`Get-CimInstance -Namespace ROOT\DCIM\SYSMAN -ClassName DCIM_ComputerSystem |Where-Object {$_.Dedicated -ne 28} | Invoke-CimMethod -MethodName RequestStateChange -Arguments @{RequestedState ='11'}`
- 关闭系统 —`Get-CimInstance -Namespace ROOT\DCIM\SYSMAN -ClassName DCIM_ComputerSystem |Where-Object {$_.Dedicated -ne 28} | Invoke-CimMethod -MethodName RequestStateChange -Arguments @{RequestedState ='3'}`

以下 API 可在 GNU 或 Linux 操作系统中使用：

- shutdown -r +5
- sudo reboot

注: 在重置操作期间，一部分选项不会重置为默认值。这可能是由于安全原因（例如，密码）或启动功能（例如，启动列表和传统选项 ROM）。

BIOS 事件日志不会重置以存储系统硬件的历史记录。

下表枚举了不重置为默认值的功能的完整列表。

表. 2: 不重置为默认值的功能的完整列表

部分	子部分	项目
常规	系统信息	服务编号
	系统信息	Asset Tag 资产标签
	系统信息	Ownership Tag 所有权标签
	引导顺序	引导列表
	高级引导选项	启用传统 OROMS
	日期/时间	日期/时间
	集成 NIC	集成 NIC
	集成 NIC	启用 UEFI 网络堆栈
	SATA 操作	SATA 操作
安全性	不适用	管理员密码
	不适用	系统密码
	不适用	内部 HDD-x 密码
	不适用	主密码锁定
	SMM 安全缓解	SMM 安全缓解
	英特尔 SGX 启用	英特尔 SGX 启用
安全启动	安全启动	安全启动
	专业密钥管理	密钥数据库

使用 PowerShell 命令在运行 Windows 的系统中设置 BIOS 属性

您可以使用 SetBIOSAttributes 方法设置 BIOS 属性。通过使用启用受信任的平台模块 (TPM) 作为示例的任务，该过程阐述如下。

注: 确保清除 BIOS 中的 TPM 选项，然后再执行以下步骤来启用 TPM。

注: 使用管理员权限运行 PowerShell。

要启用 TPM，

1. 如果尚未设定系统的 BIOS 密码，请使用以下 PowerShell 命令设置该密码：

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

2. 使用以下命令启用 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. 重新启动系统。
4. 使用以下命令激活 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. 重新启动系统。

   通用免责声明

   Powershell PSReadline 保存您输入到文本文件的每个控制台命令。因此建议您使用 “Get-Credential” commandlet 安全地处理密码。

   a. $cred = Get-Credential

   b. 在显示对话框时，输入您的用户名和密码，例如 AdminPWD 和 Dell_123$。

   c. $BSTR = [System.Runtime.InteropServices.Marshal]::SecureStringToBSTR($cred.Password)

   d. $plainpwd=[System.Runtime.InteropServices.Marshal]::PtrToStringAuto($BSTR)

   e. Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod MethodName SetBIOSAttributes -Arguments @{AttributeName=@("AdminPwd");AttributeValue=@(" $plainpwd ")}

在运行 Linux 的系统中设置 BIOS 属性

您可以使用以下任何方法设置 BIOS 属性。

- 使用 OMICLI
- 使用 WinRM
- 使用 WSMan

注: 确保 OMI 服务器已启动且正在运行。

使用 OMICLI 设置 BIOS 属性

您可以使用 SetBIOSAttributes 方法设置 BIOS 属性。通过使用启用受信任的平台模块 (TPM) 作为示例的任务，该过程阐述如下。

注: 确保清除 BIOS 中的 TPM 选项，然后再执行以下步骤来启用 TPM。

要使用 OMICLI 命令设置 BIOS 属性：

1. 要在尚未设置的情况下在系统上设置 BIOS 密码，请运行

   ```
   ./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. 要使用以下命令启用 TPM 安全性，请运行

```
./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. 重新启动系统。
4. 要激活 TPM，请运行

```
./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. 重新启动系统。
6. 要重设 BIOS 密码，请运行

```
./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 设置 BIOS 属性

您可以使用 SetBIOSAttributes 方法设置 BIOS 属性。通过使用启用受信任的平台模块 (TPM) 作为示例的任务，该过程阐述如下。

注: 确保清除 BIOS 中的 TPM 选项，然后再执行以下步骤来启用 TPM。

使用 WinRM 命令设置 BIOS 属性：

1. 通过枚举 DCIM_BIOSService 类来获取选择器集。运行：

```
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
```

注: 本例中，设置操作使用选择器集值（SystemName=<来自 DCIM_BIOSService 类的系统名称>winrm i SetBIOSAttributes wsman/DCIM_BIOSService?SystemName=dt:+SystemCreationClassName=DCIM_ComputerSystem+Name=DCIM:BiosService+CreationClassName=DCIM_BIOSService+）。

2. 如果尚未设定系统的 BIOS 密码，请使用以下命令设置该密码：

```
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. 运行以下命令，启用 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. 重新启动系统。
5. 使用以下命令激活 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 设置 BIOS 属性

您可以使用 WSMan 在运行 Linux 的系统上设置 BIOS 属性。通过使用启用受信任的平台模块 (TPM) 作为示例的任务，该过程阐述如下。

注: 确保清除 BIOS 中的 TPM 选项，然后再执行以下步骤来启用 TPM。

1. 通过枚举 DCIM_BIOSService 类来获取选择器集。运行：

```
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. 如果尚未设定系统的 BIOS 密码，请使用以下命令设置该密码：

```
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. 使用以下命令启用 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. 重新启动系统。
5. 使用以下命令激活 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>"
```

更改引导顺序

要更改引导顺序，请执行以下步骤：

1. 使用以下命令检查引导顺序类型（传统或 UEFI）：
   - WMIC 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. 使用以下命令检查当前引导顺序类型（传统或 UEFI）：
   - WMIC 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. 使用以下命令更改引导顺序：
   - WMIC 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")` 。

     注: `dcim_BootConfigSetting` 实例必须代表您要更改的引导配置 – 类型 1（传统）或类型 2 (UEFI)。
   - 参数：
     - `Authorization Token` — 这是管理员或引导密码。
     - `Source` – 这是取自 `dcim_OrderedComponent.PartComponent` 属性的引导顺序列表。新的引导顺序由源数组中的引导设备顺序确定。
4. 使用 PowerShell 更改类型 1 引导列表的引导顺序：
   a. 通过运行以下命令获取类型 1 引导列表的当前引导顺序入：`$boLegacy = Get-WmiObject -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-1'} | select -expand partcomponent.`
   b. 定义一个 PowerShell 变量以指定引导顺序设置 `$newboLegacy`. 将新引导顺序分配至它。例如，当前引导顺序类型将被保留。
   c. $newboLegacy = $boLegacy
   d. 通过运行以下命令获取类型 1 引导列表对应的 `dcim_bootconfigsetting` 实例：`$bcsLegacy = Get-WmiObject -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 1'}.`
   e. 运行以下命令，调用方法：`$ bcsLegacy.changebootorder($newboLegacy, $AuthorizationToken)`。`$AuthorizationToken` 变量用于传递 BIOS 密码。
5. 使用 PowerShell 更改类型 2 引导列表的引导顺序：
   a. 通过运行以下命令获取类型 2 引导列表的当前引导顺序入：`$boUefi = Get-WmiObject -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-2'} | select -expand partcomponent.`
   b. 定义一个 PowerShell 变量以指定引导顺序设置 `$newboUefi`。将新引导顺序分配至它。例如，当前引导顺序类型将被保留。
   c. 通过运行以下命令获取类型 2 引导列表对应的 `dcim_bootconfigsetting` 实例：`$bcsUefi = Get-WmiObject -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 2'}`。
   d. 运行以下命令，调用方法：`$ bcsUefi.changebootorder($newboUefi, $AuthorizationToken)`。`$AuthorizationToken` 变量用于传递 BIOS 密码。

远程关闭和重新启动 Windows 系统

您可以使用 RequestStateChange 方法远程关闭或重新启动 Windows 系统。

1. 使用以下命令远程关闭 Windows 系统：

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

2. 使用以下命令远程重新启动 Windows 系统：

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

远程获取 Windows 系统上的系统时间值

您可以使用 ManageTime 方法远程获取 Windows 系统的系统时间值。例如：

在命令行界面中，运行以下命令：

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"}`

6

使用 Dell Command | Monitor 10.6 本地管理 Dell 客户端系统

您可以使用以下方法本地管理 Dell 客户端系统：

- 对于运行 Windows 的系统，使用 PowerShell
- 对于运行 Linux 的系统，使用 OMICLI

主题：

使用 PowerShell 在本地管理 Windows 系统

您可以使用 PowerShell 命令管理在本地运行 Windows 的 Dell 客户端系统。

- 枚举 DCIM 类的实例
  - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSEnumeration`
  - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSPassword`
- 获取 BIOS 设置的属性

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

- 更改 BIOS 设置

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

- 修改非严重值

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

- 订阅警报

```
$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)
```

- 从 WMI 获取用户同意的命令：

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

- 从 WMI 设置用户同意的命令：

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

注： Dell Command | Monitor 10.5 和 10.6 x64 位版本提供改进计划。

- 从 WMI 获取代理的命令：

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

- 从 WMI 设置代理的命令：

```
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 在本地管理 Linux 系统

您可以使用 OMICLI 命令在本地管理 Linux 系统。在运行 Linux 的系统上，OMICLI 的安装位置为 `/opt/omi/bin`。

- 枚举 DCIM 类的实例
  - `./omicli ei root/dcim/sysman DCIM_BIOSEnumeration`
  - `./omicli ei root/dcim/sysman DCIM_BIOSPassword`
- 获取 BIOS 设置的属性

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

- 设置管理员密码

```
./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 BIOS 设置
  - `./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> }
```

- 订阅警报

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

7

使用 Dell Command | Monitor 10.6 远程管理 Dell 客户端系统

您可以使用以下任意方法对 Dell 客户端系统进行远程管理：

- 对于运行 Windows 的系统， 使用 PowerShell 通过 Windows 系统远程管理 Windows 系统 页面上的 25
- 对于运行 Linux 的系统， 使用 WinRM 通过 Windows 系统远程管理 Linux 系统 页面上的 25

主题：

使用 PowerShell 通过 Windows 系统远程管理 Windows 系统

您可以使用 PowerShell 通过 Windows 系统远程访问和监控 Windows 系统。

管理 Windows 系统的前提条件：

- Windows PowerShell 3.0
- 配置用于运行远程脚本的 PowerShell

受管 Windows 系统的前提条件：

- Dell Command | Monitor
- Windows PowerShell 3.0
- 配置用于运行远程脚本的 PowerShell
- 应启用 PowerShell-remoting 功能

注：

如需远程使用 Windows PowerShell，必须配置远程计算机以进行远程管理。有关详细信息（包括说明），请运行 PowerShell 命令 - `Get-Help about_remote_requirements`。

使用 WinRM 通过 Windows 系统远程管理 Linux 系统

您可以使用 WinRM 命令通过运行 Windows 的系统访问和监测运行 Linux 的系统。

Windows 系统的前提条件

- 支持的 Windows 操作系统
- 为远程管理运行和配置的 WinRM 服务

Linux 系统的前提条件

- Root 权限
- Dell Command | Monitor
- 支持的 Linux 操作系统
- 在 WMI 服务器上启用 5985 和 5986 端口
- 为您的环境配置的系统

在命令行界面中，运行

```
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 通过 Linux 系统远程管理 Linux 系统

您可以使用 WSMan 命令通过运行系统访问和监测运行 Linux 的系统。

管理 Linux 系统的前提条件：

- 已安装支持的 Linux 操作系统软件包
- 已安装 wsmancli 软件包

受管 Linux 系统的前提条件：

- Root 访问权限
- 支持的 Linux 操作系统
- Dell Command | Monitor

启动终端并运行

```
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
```

8

有关 Dell Command | Monitor 10.6 的常见问题

- 我如何使用 DCIM_OrderedComponent.AssignedSequence 属性找到“引导配置”的引导次序（顺序）？

  当 **DCIM_BootConfigSetting** 实例（传统或 UEFI）通过 **DCIM_OrderedComponent** 关联的实例有多个与其相关联的 **DCIM_BootSourceSetting** 实例（引导设备）时，**DCIM_OrderedComponent.AssignedSequence** 属性的值用于确定在引导过程中使用关联的 **DCIM_BootSourceSetting** 实例（引导设备）的顺序。如果 **DCIM_BootSourceSetting** 的关联 **CIM_OrderedComponent.AssignedSequence** 属性等于 **0**，则会将其忽略，不会将其视为引导顺序的一部分。

- 我如何更改引导次序?

  可以使用 **DCIM_BootConfigSetting.ChangeBootOrder()** 方法更改引导顺序。**ChangeBootOrder()** 方法可设置 **DCIM_BootSourceSetting** 实例与 **DCIM_BootConfigSetting** 实例关联的顺序。该方法有一个输入参数：**Source**。**Source** 参数是 **DCIM_OrderedComponent** 类中 **PartComponent** 属性的有序阵列，表示 **DCIM_BootSourceSetting** 实例（引导设备）与 **DCIM_BootConfigSetting** 实例（引导列表类型：传统或 UEFI）之间的关联。

- 我如何禁用引导设备?

  更改引导次序时，每一个将目标 **DCIM_BootConfigSetting** 实例与未存在于 **Source** 参数输入数组中的 **DCIM_BootSourceSetting** 实例相关联的 **DCIM_OrderedComponent** 实例的 **AssignedSequence** 属性值被设为 **0**，表明该设备被禁用。

- 当 <要尝试连接的内容>尝试使用 wbemtest 连接到命名空间时，显示登录失败消息。

  使用管理员权限级别启动 **wbemtest** 可以阻止任何登录消息。从**所有程序**列表中找到 Internet Explorer，右键单击并选择**以管理员身份运行**，启动 **wbemtest** 并避免命名空间错误。

- 我该如何在保证不出现任何问题的情况下运行知识库脚本?

  以下是运行 Dell Command | Monitor 知识库链接中提供的 VBS 脚本的步骤：

  1. 使用命令 `winrm quickconfig` 在系统上配置 **winrm**。
  2. 检查系统上是否存在标记支持，方法是观察：
     - BIOS 设置中的 **F2 屏幕**。
     - 使用 wbemtest 之类的工具检查脚本中定义的键值是否存在于系统上。

     注: Dell 建议使用最新 BIOS（可从 **dell.com/support** 获取）。有关更多信息，请参阅位于 **dell.com/support** 的 Dell Command | Monitor 参考指南。

- 如何设置 BIOS 属性?

  可以使用 **DCIM_BIOSService.SetBIOSAttributes()** 方法更改 BIOS 属性。**SetBIOSAttributes()** 方法可设置 **DCIM_BIOSEnumeration** 类中定义的实例的值。该方法有七个输入参数。前两个参数可以为空或 NULL。第三个参数 **AttributeName** 必须将输入映射到 **DCIM_BIOSEnumeration** 类的属性名称实例的值。第四个参数或 **AttributeValue** 可以是 **DCIM_BIOSEnumeration** 类中定义的任意可能的属性名称值。第五个参数 AuthorizationToken 是可选的，第五个参数的输入是 BIOS 密码。只有在系统中已经设置 BIOS 密码的情况下才应使用第五个参数，否则应将此参数留空。第六个参数和第七个参数也可以为空或 NULL。

- 对于 Windows 和 Linux 操作系统，Dell Command | Monitor 是否支持存储和传感器监测?

  是的。对于支持的 Windows 和 Linux 操作系统，Dell Command | Monitor 支持存储和传感器监测。

  在存储监测方面，Dell Command | Monitor 支持对以下设备进行监测和发出警报：

  - Intel 集成控制器（兼容 CSMI v0.81 或更高版本）
  - LSI 集成的 RAID 控制器；以及 9217、9271、9341、9361 及其关联的驱动程序（物理和逻辑）

  注: 运行 Linux 操作系统的系统不支持对 Intel 集成控制器进行监测。

  在传感器监测方面，Dell Command | Monitor 支持电压、温度、安培数、散热设备（风扇）和机箱传感器的监测和警报。

  有关类和警报的更多信息，请参阅 **dell.com/support** 上的 Dell Command | Monitor 参考指南。

- Dell Command | Monitor 和其他应用程序/控制台集成吗?

  可以。Dell Command | Monitor 可与满足行业标准的领先企业管理控制台交互。它可以与以下现有企业管理工具集成：

  - Dell Client Integration Suite for System Center 2012

- Dell OpenManage Essentials
- Dell Client Management Pack for System Center Operation Manager

- 我是否可将类导入 SCCM 以用于资源清册?

  是，各个 MOF 或 OMCI_SMS_DEF.mof 文件可在 SCCM 控制台中导入以用于资源清册。

- SCCM OMCI_SMS_DEF.mof 文件位于何处?

  OMCI_SMS_DEF.mof 文件的位置是：C:\Program Files\Dell\Command_Monitor\ssa\omacim\OMCI_SMS_DEF.mof。

- 如何为 DCM 10.2.1 配置代理?
- DCM 10.2.1 无法获取保修信息。
- 使用 DCIM_ApplicationProxySetting 类检查应用程序代理设置是否已正确配置。

  我如何为 Dell Command | Monitor 配置代理凭据。

  如果您通过 Dell Command | Monitor 登录，则可以使用相同的凭据进行代理身份验证。

- Dell Command | Monitor 未显示保修信息。
  - 轮询期间客户端系统未连接到互联网。

    通过运行以下命令，连接互联网并推送保修信息：`Get-CimInstance -Namespace root/DCIM/SYSMAN -ClassName DCIM_AssetWarrantyInformation| Where-Object{$_.InstanceID -eq "Root/MainSystemChassis/COOObject/COOWarranty:0"} | Invoke-CimMethod -MethodName RefreshWarranty`

  - 客户端系统未配置代理服务器。

    通过运行以下命令，在 Dell Command | Monitor 中配置代理设置：

    - 要从 WMI 获取代理，请运行以下命令：`Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting`。
    - 要从 WMI 设置代理，请运行以下命令：`Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting | Invoke-CimMethod -MethodName Change ProxySetting -Arguments @{NewAddress="10.0.0.223"; NewPort="8080"}`

      您必须根据代理环境替换 **NewAddress** 和 **NewPort**（如果适用）。

9

使用 Dell Command | Monitor 10.6 的故障处理步骤

主题：

无法远程连接至 Windows Management Instrumentation

如果管理应用程序无法获得远程客户端系统的公用信息模型 (CIM) 信息，或者使用分布式组件对象模型 (DCOM) 的远程 BIOS 更新失败，则会显示以下错误消息：

- **访问被拒**
- **Win32: RPC 服务器不可用**

1. 确认客户端系统是否已连接到网络。在服务器的命令提示符下键入以下内容：
   `ping <Host Name or IP Address>` 并按下 `<Enter>`。
2. 如果服务器和客户端系统属于同一个域，请执行以下步骤：
   - 验证该域管理员帐户是否同时具备对这两个系统的管理员权限。

   如果服务器和客户端系统属于同一个工作组（不在同一个域），请执行以下步骤：
   - 确保服务器正在运行最新的 Windows Server。

   注: 在更改注册表前备份系统数据文件。错误编辑注册表可能会导致操作系统无法使用。
3. 在客户端系统上编辑注册表更改。单击**开始** > **运行**，键入 **regedit**，然后单击**确定**。在**注册表编辑器**窗口中，浏览至 `My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`。
4. 将 **forceguest** 值设置为 0（默认值为 1）。除非修改该值，否则即使提供的凭据具备管理员权限，远程连接至系统的用户也将仅具有访客权限。
   a. 在客户端系统上创建一个帐户，该帐户的用户名和密码与运行 WMI 管理应用程序的系统上的管理员帐户的用户名和密码相同。
   b. 如果您使用的是 IT Assistant，请运行 IT Assistant ConfigServices 公用程序（IT Assistant 安装目录下 `/bin` 目录中的 `configservices.exe`）。将 IT Assistant 配置为在本地管理员帐户（现在也是远程客户端的管理员）下运行。此外，请验证已启用 DCOM 和 CIM。
   c. 如果您使用的是 IT Assistant，请使用管理员帐户为客户端系统配置子网发现。输入 <客户端计算机名称>\<帐户名称> 形式的用户名。如果已发现该系统，请从已发现系统的列表中将其删除，为其配置子网发现，然后重新进行发现。

   注: Dell 建议使用 Dell OpenManage Essentials 来替代 IT Assistant。有关 Dell OpenManage Essentials 的更多信息，请参阅 **dell.com/support**。
5. 执行以下步骤以修改用于远程连接到系统 WMI 的用户权限级别：
   a. 单击**开始** > **运行**，键入 `compmgmt.msc`，然后单击**确定**。
   b. 浏览至**服务和应用程序**下的 **WMI 控件**。
   c. 右键单击 **WMI 控件**，然后单击**属性**。
   d. 单击**安全**选项卡，然后选择 **Root** 树下的 **DCIM/SYSMAN**。
   e. 单击**安全**。
   f. 选择要控制访问权限的特定组或用户，然后使用**允许**或**拒绝**复选框来配置权限。
6. 执行以下步骤，以使用 WMI CIM Studio 从远程系统连接至系统上的 WMI (`root\DCIM\SYSMAN`)：

a. 在本地系统上安装 WMI 工具以及 wbemtest，然后在远程系统上安装 Dell Command | Monitor。
b. 为 WMI 远程连接在系统上配置防火墙。例如，在 Windows 防火墙中打开 TCP 端口 135 和 445。
c. 在本地安全策略中，将**本地安全**设置设定为**典型 - 本地用户以自己的身份验证网络访问：本地帐户的共享和安全模式。**
d. 使用 WMI wbemtest 从远程系统连接至本地系统上的 WMI (`root\DCIM\SYSMAN`)。例如，\\[目标远程系统的 IP 地址]\root\DCIM\SYSMAN
e. 如有提示，输入目标远程系统的管理员凭据。

有关 WMI 的更多信息，请参阅 msdn.microsoft.com 上适用的 Microsoft 说明文件。

在运行 Windows 的系统上安装失败

如果您无法完成用于 Windows 的 Dell Command | Monitor 安装，请确保：

- 您对目标系统具有管理员权限。
- 目标系统为装有 SMBIOS 2.3 版或更高版本的 Dell 系统。
- 不能打开 PowerShell 控制台。

注: 要查看系统的 SMBIOS 版本，请转至**开始** > **运行**，然后运行 `msinfo32.exe` 文件。在“系统摘要”页面可查看 SMBIOS 版本。

注: 系统必须运行受支持的 Windows 操作系统。

注: 系统必须升级到 .NET 4.0 或更高版本。

BIOS 设置枚举值显示为 1

1. 验证是否使用 root 用户权限安装了以下软件包；
   - omi-1.0.8.ssl_100.x64.rpm
   - srvadmin-hapi-8.3.0-1908.9058.el7.x86_64
   - command_monitor-linux-<版本号>-<内部版本号>.x86_64.rpm
2. 如果安装了以上软件包，请验证是否已加载驱动程序模块。
   a. 通过运行以下命令，验证是否已加载驱动程序模块 `lsmod | grep dcdbas`。
   b. 如果驱动程序模块不可用，则通过运行以下命令检索驱动程序的详细信息 `modinfo dcdbus`。
   c. 通过运行以下命令 `insmod <filename>` 加载驱动程序模块。

由于 libsmbios 的相关性，Hapi 安装失败

如果由于相关性问题导致安装失败，

通过运行 `apt-get -f install` 命令以强制安装所有相关软件包。

CIM 资源不可用

在枚举时，如果您收到错误 "CIM 资源不可用"，

验证命令是否以 root 权限执行。

无法使用 DCM 在运行 Ubuntu Core 16 的系统上执行命令

确保系统上的快照版本为 2.23 或更高版本。

10

您可能需要的其他说明文件

除了本用户指南以外，您还可以访问位于 **dell.com/support** 上的以下文档。单击 Dell Command | Monitor（之前称为 OpenManage Client Instrumentation），然后单击**常规支持**部分中相应的产品版本链接。

除了本用户指南以外，您还可以访问以下指南。

- Dell Command | Monitor 参考指南提供了关于所有类、属性及说明的详细信息。
- Dell Command | Monitor 安装指南提供有关安装的信息。
- Dell Command | Monitor SNMP 参考指南提供了适用于 Dell Command | Monitor 的简单网络管理协议 (SNMP) 管理信息库 (MIB)。

主题：

从 Dell 支持站点访问文档

您可以通过选择您的产品访问说明文件。

1. 转至 www.dell.com/manuals。
2. 单击**浏览所有产品**，单击**软件**，然后单击**客户端系统管理**。
3. 要查看所需说明文件，请单击所需的产品名称和版本号。

11

联系戴尔

注: 如果您不能连接至 Internet，您可以在您的购买发票、装箱单、账单或戴尔产品目录中找到联系信息。

戴尔提供多种联机和基于电话的支持和服务选项。具体的服务随您所在国家/地区以及产品的不同而不同，某些服务在您所在的地区可能不提供。如要联系戴尔解决有关销售、技术支持或客户服务问题：

1. 访问 **Dell.com/support**。
2. 选择您的支持类别。
3. 在页面底部的**选择国家/地区**下拉列表中，确认您所在的国家或地区。
4. 根据您的需要选择相应的服务或支持链接