Dell Command | Monitor 9.2.1 版
用户指南

注、小心和警告

注:“注”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，并说明如何避免此类问题。

警告:“警告”表示可能会造成财产损失、人身伤害甚至死亡。

2017 - 05

Rev. A00

目录

1

简介

Dell Command | Monitor 软件应用程序利用应用程序访问信息、监测状态或更改系统状态（例如远程关闭系统）来实现远程管理。Dell Command | Monitor 通过标准界面使用关键系统参数，便于管理员管理资源清册、监测系统运行状况和收集部署的 Dell 系统的信息。Dell Command | Monitor 专为 Dell Enterprise 客户端系统、 Dell IoT Gateway 系统以及 Dell 嵌入式 PC 而设计。有关支持的 Dell 系统的更多信息，请参阅 **dell.com/dellclientcommandsuitemanuals** 上的发行说明。本说明文件概述了 Dell Command | Monitor 及其功能。

注: Dell Command | Monitor 即以前的 Dell OpenManage Client Instrumentation (OMCI)。自 OMCI 8.2.1 版以后，OMCI 已更名为 Dell Command | Monitor。

此版本中的新功能

- 支持新的平台：Dell Edge Gateway 3000 系列
- 支持新的操作系统：Ubuntu Core 16
- 支持下列新的 BIOS 设置：
  - 模拟数字接口模式通道 1
  - 模拟数字接口模式通道 2
  - 模拟数字接口模式通道 3
  - 模拟数字接口模式通道 4
  - 模拟数字接口模式通道 5
  - 模拟数字接口模式通道 6
  - 模拟数字接口模式通道 7
  - 模拟数字接口模式通道 8
  - 自动唤醒时间段
  - 清除 BIOS 登录
  - 清除电源日志
  - 清除散热日志
  - MEMS 传感器
  - ZigBee

有关标记的更多信息，请参阅位于 **dell.com/dellclientcommandsuitemanuals** 的 *Dell Command | Monitor Reference Guide*（Dell Command | Monitor 参考指南）。

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 使用公用信息模型 (CIM) 标准和简单网络管理协议 (SNMP) 作为管理协议来管理客户端系统。这会降低总拥有成本、提高安全性并以整体方式管理网络中的所有设备，包括客户端、服务器、存储、网络和软件设备。

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

Dell Command | Monitor 包含基础驱动程序集，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 TechCenter 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/dellclientcommandsuitemanuals 上的 *Dell Command | Monitor Installation Guide*（Dell Command | Monitor 安装指南）。

2

功能

Dell Command | Monitor 的主要功能包括：

- CIM 架构支持
- BIOS 配置
- WMI/OMI 安全性
- 事件报告
- 远程关机
- 使用 WSMAN 协议通过 CIM 架构访问系统信息

  注: 使用 Dell Command | Monitor for Windows，也可以通过 SNMP 访问信息。
- 详细资产信息的编制
- 远程唤醒配置
- 系统设置的远程修改
- 监测系统运行状况和报告状态
- Intel 集成控制器和 LSI 集成控制器的 RAID 监测和警报

  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。
- SNMP 监测和陷阱仅适用于 Dell Command | Monitor for Windows

CIM 架构支持

Dell Command | Monitor for Windows 符合 CIM 2.17 架构，并且包含两个 WMI 提供程序：

- WMI Indication 提供程序或轮询代理
- WMI 实例或方法提供程序

Dell Command | Monitor for Linux 符合 CIM 2.32.0 架构，并且包含两个 WMI 提供程序：

- WMI Indication 提供程序或轮询代理
- WMI 实例或方法提供程序

BIOS 设置配置和枚举

Dell Command | Monitor 提供配置系统 BIOS 的功能。

WMI/OMI 安全性

WMI 在允许用户访问 CIM 数据和方法之前进行用户身份验证。访问权限通过分布式组件对象模型 (DCOM) 安全性和 CIMOM 实施。完整访问权限或受限访问权限基于每个命名空间授予用户。没有类实施或属性级别安全性。默认情况下，管理员组的成员用户具有 WMI 的完整本地和远程访问权限。

对于 Dell Command | Monitor for Windows，您可以使用“Services and Applications”（服务和应用程序）部分下“Computer Management”（计算机管理）控制台中提供的 WMI 控件配置 WMI 安全性。右键单击 **WMI 控件**，然后单击**属性**。您可以从

Security（安全）选项卡配置特定于命名空间的安全性。您也可以从**开始**菜单或从 **CLI** 通过运行 `wmimgmt.msc` 来运行 **WMI 控件**。

警报报告

Dell Command | Monitor 检测 Dell 系统上的事件，并向本地用户和网络管理员发出有关潜在故障、配置更改、组件库存、集成 Intel 和 LSI RAID 控制器、探测器和机箱侵入的警报。这些事件通过 OpenManage Essentials (OME) 等系统管理应用程序显示。

远程关机

Dell Command | Monitor for Windows 支持远程系统关机和重新引导。

系统信息访问

Dell Command | Monitor 使用 CIM 通过 WMI/OMI 提供对以下系统信息的访问权限：BIOS 修订版、BIOS 制造商/供应商、服务标签、系统型号、首次开机日期和系统型号等。WSMAN 协议还可用于通过 WMI/OMI 访问此信息。

详细的资产信息

Dell Command | Monitor 提供对处理器、内存、PCI 设备和电池等详细库存信息的访问权限。

远程唤醒配置

Dell Command | Monitor 支持配置远程唤醒设置。远程唤醒是客户端系统和网络接口卡 (NIC) 的功能。

系统 BIOS 设置的远程修改

Dell Command | Monitor 支持管理员检索和设置商用客户端 BIOS 设置，例如 USB 端口配置和 NIC 设置等。

系统运行状况和状态

Dell Command | Monitor 监测系统运行状况，例如风扇状态、内存、温度、探测器、电池、RAID 控制器和对接站，并报告状态。

Intel 和 LSI 控制器的 RAID 监测和警报

对于 Dell Command | Monitor for Windows，监测 Intel 和 LSI RAID 控制器的物理驱动器和逻辑驱动器并发出警报；对于 Dell Command | Monitor for Linux，仅监测 LSI 控制器并发出警报。

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）

  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。

- 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）

在传感器监测方面，Dell Command | Monitor 支持对电压、温度、安培数、散热设备（风扇）和机箱传感器进行监测和发出警报。

SNMP 监测和陷阱

Dell Command | Monitor for Windows 符合 SNMP v1 并支持监测系统属性和陷阱。

3

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，其引领台式机、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

用户方案

本章介绍 Dell Command | Monitor 的各种用户方案。

您可以将 Dell Command | Monitor 用于：

- 资产管理
- 配置管理
- 运行状况监测
- 配置文件

方案 1：资产管理

一家使用多个 Dell 系统的公司因业务和 IT 员工变动而无法维护准确的资源清册信息。首席信息官 (CIO) 要求制定一个计划，确定可升级到 Microsoft Windows 最新版本的系统。为此需要对部署的系统进行评估，以确定此项目的规模、范围和财务影响。收集信息是一项艰巨的工作。考虑到工时和最终用户中断等因素，将 IT 员工部署到每个客户端系统成本非常高。

通过在每个 Dell 系统上使用 Dell Command | Monitor，IT 经理可以快速地远程收集信息。使用 Microsoft System Center Configuration Manager (SCCM) 等工具，IT 经理可以通过网络查询每个客户端系统，并收集如下信息：CPU 类型和速度、内存大小、硬盘驱动器容量、BIOS 版本和当前操作系统版本等。收集信息后，它可以进行分析，以确定可升级到 Windows 最新版本的系统。

您也可以通过 WSMAN/WinRM 命令行或使用任何 CIM 客户端命令行获取资产资源清册。

SCCM 集成

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

- 使用 Dell Command | Monitor 安装软件包中的 MOF 文件（其中包含所有 Dell Command | Monitor 类）并导入到 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的 BIOS 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企业客户端系统上的 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 **dell.com/dellclientcommandsuitemanuals** 上的 *Dell Command | Monitor Reference Guide*（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。利用每个客户端系统上安装的 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) 以便能够在非繁忙时间将系统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 支持通过以下步骤监测事件：

- 通过 CIM 类 **DCIM_LogEntry** 提取日志。
- 通过 **DCIM_AlertIndication** 类监测 CIM 指示。
- （仅面向适用于 Windows 的 Dell Command | Monitor）通过简单网络管理协议 (SNMP) 和 Windows 事件查看器监测事件。
- （仅面向适用于 Linux 的 Dell Command | Monitor）通过系统日志进行监测。

有关 Dell Command | Monitor 的更多信息，请参阅 **dell.com/dellclientcommandsuitemanuals** 上的 *Dell Command | Monitor Reference Guide*（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 Dell Command | Monitor 的更多信息，请参阅 **dell.com/dellclientcommandsuitemanuals** 上的 *Dell Command | Monitor Reference Guide*（Dell Command | Monitor 参考指南）。

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。

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。
- 运行 **DCIM_ComputerSystem.RequestStateChange()** 方法并将 RequestedState 参数值设置为 **3**。关闭系统。
- 重新引导系统。运行 **DCIM_ComputerSystem.RequestStateChange()** 方法并将 **RequestedState** 参数值设为 **11**。
- 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。
- 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。获取所有通过 **DCIM_LogManagesRecord** 关联与 **DCIM_RecordLog** 的给定实例相关联的 **DCIM_LogEntry** 实例。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

您可以查看 Dell Command | Monitor 提供的信息，方法是访问：

- 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/dellclientcommandsuitemanuals** 的 *Dell Command | Monitor Reference Guide*（Dell Command | Monitor 参考指南）。

轮询间隔设置

您可以使用 Dell Command | Monitor 更改以下轮询间隔：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 **安装位置**>\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 小时）。

RAID 状态报告

Dell Command | Monitor 为具有硬件和驱动程序支持的客户端系统启用 RAID 配置信息并监测 RAID 功能。您可以使用 RAID 类接收有关 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。启用 RAID 配置后，您可以接收驱动器和控制器降级或发生故障的警报。

注: 仅在 Common Storage Management Interface (CSMI) 版本 0.81 兼容驱动程序上运行的 RAID 控制器支持 RAID 状态报告。OMCI 8.1 和更高版本在 Intel 芯片 RAID 控制器上仅支持监测；从 OMCI 8.2 和更高版本起，支持 Intel 芯片 RAID 控制器警报。

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 | Monitor for 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 **dell.com/dellclientcommandsuitemanuals** 上的 *Dell Command | Monitor SNMP Reference Guide*（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。

Dell Command | Monitor for Linux 的应用程序日志

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 DEBUG（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：ERROR（错误）、INFO（信息）、DEBUG（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 DEBUG（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 INFO（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，此部分不适用于 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**

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_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。

更改系统设置

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

- **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 运行上述方法。

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。下面以启用受信任的平台模块 (TPM) 任务为例，说明了步骤。

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 安全保护：
   ```
   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。

在运行 Linux 的系统中设置 BIOS 属性

您可以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 服务器已启动并且正在运行。

使用 OMICLI 设置 BIOS 属性

您可以使用 SetBIOSAttributes 方法设置 BIOS 属性。下面以启用受信任的平台模块 (TPM) 任务为例，说明了步骤。

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，请执行以下操作：

1. 要在系统上设置 BIOS 密码（如果尚未设置），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 安全保护，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。下面以启用受信任的平台模块 (TPM) 任务为例，说明了步骤。有关详情，请参阅 远程管理 Dell 客户端系统。

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 WinRM 命令设置 BIOS 属性，请执行以下操作：

1. 通过枚举 DCIM_BIOSService 类获取选择器设置。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: 在本例中，选择器设置值 (SystemName=<system name from DCIM_BIOSService class>winrm i SetBIOSAttributes wsman/DCIM_BIOSService?SystemName=dt: +SystemCreationClassName=DCIM_ComputerSystem+Name=DCIM:BiosService +CreationClassName=DCIM_BIOSService+) 将用于设置操作。

2. 如果尚未在系统上设置 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. 通过运行以下命令启用 TPM 安全保护：

```
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。下面以启用受信任的平台模块 (TPM) 任务为例，说明了步骤。有关详情，请参阅 远程管理 Dell 客户端系统。

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 类获取选择器设置。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. 如果尚未在系统上设置 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 安全保护：

```
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. 使用以下方法检查引导列表类型：
   - **WMIC 命令：** `wmic /namespace:\\root\dcim\sysman path dcim_BootConfigSetting get ElementName/format:list`
   - **PowerShell 命令：** `Get-CimInstace -Namespace root\dcim\sysman -ClassName DCIM_BootConfigSetting -Property ElementName`
2. 使用以下方法检查引导顺序类型（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-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ElementSettingData -Filter "IsCurrent=1" -Property SettingData`
3. 使用以下方法更改引导顺序：
   - **WMIC 命令：** `wmic /namespace:\\root\dcim\sysman path dcim_bootconfigsetting call ChangeBootOrder /?:full`
   - **PowerShell 命令：** `(Get-CimClass -namespace root\dcim\sysman -ClassName DCIM_Bootconfigsetting).CimClassMethods["ChangeBootOrder"].Parameters`

   ChangeBootOrder 方法所需的参数包括：
   - 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 **source** 阵列中的引导设备的顺序决定。

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

在本地管理 Dell 客户端系统

您可以使用以下方法在本地管理 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。

使用 PowerShell 在本地管理 Windows 系统

您可以使用 PowerShell 命令在本地管理运行 Windows 的 Dell 客户端系统。

- **枚举 DCIM 类实例**
  - `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")}
```

- **修改非临界值**

```
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)
```

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 安装在 **/opt/omi/bin**。

- **枚举 DCIM 类实例**
  - `./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

远程管理 Dell 客户端系统

您可以使用以下任一方法远程管理 Dell 客户端系统：

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

使用 PowerShell 通过 Windows 系统远程管理 Windows 系统

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

管理 Windows 系统的前提条件：

- 已安装支持的 Windows 操作系统软件包
- 系统已针对您的环境进行配置

受管理 Windows 系统的前提条件：

- 管理员权限
- Dell Command | Monitor
- 已安装支持的 Windows 操作系统软件包
- 已启用 PowerShell 远程功能
- 系统已针对您的环境进行配置

1. 通过打开命令行界面并运行以下命令，创建一个会话：

   ```
   $session=New-CimSession -ComputerName "<managed system IP or system name>" -Credential
   <Administartor Credentials>
   ```

2. 提供密码。
3. 通过运行以下命令，访问和监测 Windows 系统：

   ```
   Get-CimInstance -CimSession $session -Namespace root\dcim\sysman -ClassName <class name>
   ```

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 Microsoft 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
- WinRM 服务正在运行
- 系统已针对您的环境进行配置

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

- 系统已针对您的环境进行配置

  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 Linux 的系统远程访问和监测运行 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

受管理 Linux 系统的前提条件：

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

  启动一个终端，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

常见问题

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）通过关联 **DCIM_OrderedComponent** 的实例具备多个 **DCIM_BootSourceSetting** 实例（引导设备）与其相关联时，**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。

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。

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。

使用 wbemtest 连接到命名空间时，显示登录失败消息。如何解决该问题？

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** 并避免任何命名空间导致的错误。

我该如何运行 TechCenter 脚本而不出现任何问题？

以下是执行在 Dell Command | Monitor Techcenter 链接中提供的 VBS 脚本的前提条件：

1. 请使用命令 `winrm quickconfig` 在系统上配置 **winrm**。
2. 检查系统上是否存在标记支持，方法是参考：
   - 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 dell.com/dellclientcommandsuitemanuals 上的 Dell Command | Monitor（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** 需要将输入映射到 **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。如果在系统上设置了 BIOS 密码，则必须在第五个参数中提供相同的密码。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）

  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。

- 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）

在传感器监测方面，Dell Command | Monitor 支持对电压、温度、安培数、散热设备（风扇）和机箱传感器进行监测和发出警报。

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

Dell Command | Monitor 能否与其他应用程序/控制台集成？

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 文件位于 C:\Program Files\Dell\Command_Monitor\ssa\omacim\OMCI_SMS_DEF.mof。

9

故障排除

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：

- **Access Denied（访问被拒）**
- **Win32:RPC server is unavailable（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，浏览到 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/dellclientcommandsuitemanuals。
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 从远程系统连接到本地系统上的 WMI (**root\DCIM\SYSMAN**)。例如，\\[目标远程系统 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 Dell Command | Monitor for Windows 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 制造的系统。
- PowerShell 控制台不得打开。

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”页面查看 SMBIOS 版本。

注: 系统必须运行受支持的 Microsoft 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. 验证是否已使用根用户权限安装以下软件包；
   - 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. 如果已安装上述软件包，请验证是否已加载驱动程序模块。
   a. 通过运行以下命令 `lsmod | grep dcdbas` 验证是否已加载驱动程序模块。
   b. 如果驱动程序模块不可用，请通过运行以下命令 `modinfo dcdbus` 检索驱动程序详细信息。
   c. 通过运行以下命令 `insmod <filename>` 加载驱动程序模块。

由于 libsmbios 的相关性问题导致 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` 强制安装所有相关软件包。

CIM 资源不可用

枚举时，如果收到错误消息“CIM resource not available”（CIM 资源不可用），

请验证是否使用根权限执行命令。

无法使用 DCM 在运行 Ubuntu Core 16 的系统上执行命令

确保系统上 Snap 的版本为 2.23 或更高版本。

10

联系 Dell

注: 如果没有活动的 Internet 连接，您可以在购货发票、装箱单、帐单或 Dell 产品目录上查找联系信息。

Dell 提供了若干联机及电话支持和服务选项。服务会因所在国家和地区以及产品的不同而有所差异，您所在的地区可能不提供某些服务。如要联系 Dell 解决有关销售、技术支持或客户服务问题：

1. 请转至 **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。

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/dellclientcommandsuitemanuals** 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。

- *Dell Command | Monitor Reference Guide*（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 Installation Guide*（Dell Command | Monitor 安装指南）提供有关安装的信息。
- *Dell Command | MonitorSNMP Reference Guide*（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)。

访问 Dell 支持站点上的文档

您可以使用以下链接访问所需的文档：

- Dell EMC 企业系统管理说明文档 — Dell.com/SoftwareSecurityManuals
- OpenManage 说明文档 — Dell.com/OpenManageManuals
- Dell EMC 远程企业系统管理说明文档 — Dell.com/esmmanuals
- iDRAC 和 Dell EMC 生命周期控制器说明文档 — Dell.com/idracmanuals
- Dell EMC OpenManage 连接企业系统管理说明文档 — Dell.com/OMConnectionsEnterpriseSystemsManagement
- Dell EMC 可维护性工具说明文档 — Dell.com/ServiceabilityTools
- 客户端命令套件系统管理说明文件 — Dell.com/DellClientCommandSuiteManuals
- a. 转至 Dell.com/Support/Home。
  b. 单击**从所有产品中选择**。
  c. 从**所有产品**部分，单击**软件和安全**，然后单击以下部分中的所需链接：
  - **企业系统管理**
  - **远程企业系统管理**
  - **维护工具**
  - **Dell 客户端命令套件**

- **Connections 客户端系统管理**

d. 要查看说明文件，请单击所需的产品版本。

- 使用搜索引擎：
  - 在搜索框中键入说明文件的名称和版本。