Dell Command | Monitor Version 10.6

Benutzerhandbuch

Oktober 2021
Rev. A01

Hinweise, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und zeigt, wie diese vermieden werden können.

WARNUNG: Mit WARNUNG wird auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen kann.

Inhaltsverzeichnis

1

Einführung in Dell Command | Monitor 10.6

Mithilfe der Dell Command | Monitor-Softwareanwendung können IT-Administratoren problemlos die Flotten-Bestandsaufnahme verwalten, den Systemzustand überwachen, BIOS-Einstellungen ändern und remote Informationen zu bereitgestellten Dell Client-Systemen sammeln.

Die aktive Überwachung des Systemzustands kann dazu beitragen, die Gesamtbetriebskosten für das System zu reduzieren und ist Teil eines ganzheitlichen Ansatzes zur Verwaltung aller vernetzten Geräte.

Dell Command | Monitor ist für Dell Enterprise Client-Systeme, Dell IoT Gateway-Systeme sowie für Dell Embedded PCs ausgelegt.

Dieses Dokument bietet eine Übersicht über Dell Command | Monitor und seine Funktionen. Weitere Informationen zu den unterstützten Dell Systemen finden Sie in den Versionshinweisen, die unter **dell.com/support** verfügbar sind.

Themen:

Was ist neu in dieser Version von Dell Command | Monitor 10.6?

- Support für die folgenden neuen BIOS-Attribute:
  - `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`
- Support der **ResetBIOSDefaults**-Methode.

Dell Command | Monitor Übersicht

ANMERKUNG: Das Simple Network Management Protocol (SNMP) wird für Dell Command | Monitor für Linux nicht unterstützt.

Dell Command | Monitor verwaltet Client-Systeme mithilfe der Managementprotokolle Common Information Model (CIM) und Simple Network Management Protocol (SNMP). Dadurch werden die Gesamtbetriebskosten für das System reduziert und die Sicherheit erhöht. Mit einem ganzheitlichen Ansatz werden alle Geräte im Netzwerk verwaltet.

Mit CIM können Sie auf Dell Command | Monitor über Web Services for Management Standards (WSMAN) zugreifen.

Dell Command | Monitor enthält den zugrunde liegenden Treibersatz, der Systeminformationen von verschiedenen Quellen auf dem Client-System sammelt, darunter BIOS, CMOS, Systemmanagement-BIOS (SMBIOS), Systemmanagementschnittstelle (SMI), Betriebssystem und Anwendungsprogrammierschnittstellen (APIs). Dell Command | Monitor für Windows erfasst außerdem Client-Systeminformationen von DLL- (Dynamic Link Library) und Registrierungseinstellungen. Dell Command | Monitor für Windows ruft diese Informationen über die Schnittstelle CIM Object Manager (CIMOM), den Stack Windows Management Instrumentation (WMI) oder den SNMP-Agent ab. Dell Command | Monitor für Linux ruft die Informationen über die Schnittstelle Open Management Infrastructure (OMI) ab.

Dell Command | Monitor ermöglicht IT-Administratoren auf Remote-Basis Bestandsinformationen zu erfassen, BIOS-Einstellungen zu ändern, proaktive Benachrichtigungen zu potenziellen Fehlerbedingungen und Warnungen zu potenziellen Sicherheitsverletzungen zu empfangen. Auf den Windows-Systemen sind diese Warnungen als Ereignisse im NT-Ereignisprotokoll, WMI-Ereignis oder SNMP traps v1 verfügbar. Linux-Systeme werden diese Warnungen als Syslog, OMI-Ereignis oder im Anwendungsprotokoll ausgegeben.

Dell Command | Monitor für Windows kann in eine Konsole wie Microsoft System Center Configuration Manager integriert werden. Der Zugriff auf die CIM-Informationen ist direkt oder über andere Konsolenanbieter möglich, die die Integration von Dell Command | Monitor implementiert haben. Außerdem können Sie für wichtige Bereiche von Interesse benutzerdefinierte Skripte erstellen. Auf der Seite Dell Command | Monitor in der Dell Knowledge Library finden Sie Beispielskripte. Mit diesen Skripts können Sie Bestand, BIOS-Einstellungen und Systemzustand überwachen.

ANMERKUNG: Standardinstallation aktiviert die SNMP-Unterstützung nicht. Weitere Informationen zum Aktivieren der SNMP-Unterstützung für Dell Command | Monitor für Windows finden Sie im Installationshandbuch für Dell Command | Monitor unter **dell.com/support**.

2

Compliance mit der Windows SMM Security Mitigations Table (WSMT)

Die Windows SMM Security Mitigations Table (WSMT) enthält Informationen zur ACPI-Tabelle, die für das Windows-Betriebssystem, das virtualisierungsbasierte Sicherheitsfunktionen (VBS) unterstützt, erstellt wurde. Dell Command | Monitor ist kompatibel mit WSMT. Dies dient der Konfiguration von Plattformfunktionen auf Dell Client-Systemen mit einem WSMT-fähigen BIOS.

Die folgenden Verhaltensänderungen ergeben sich durch die WSMT-Compliance:

Die Funktionen von Dell Command | Monitor sind auf Dell Client-Plattformen verfügbar, die über eine kompatible BIOS-Version mit Unterstützung für WMI/ACPI verfügen.

ANMERKUNG: Weitere Informationen zu unterstützten Plattformen erhalten Sie unter Unterstützte Plattformen.

3

Standards und Protokolle für Dell Command | Monitor 10.6

Dell Command | Monitor basiert auf den CIM-Standards. Die CIM-Spezifikation führt Zuweisungsmethoden für die verbesserte Kompatibilität mit Verwaltungsprotokollen auf.

Verwaltungsprotokolle wie z. B. WMI, SNMP und WSMAN werden für die Remote-Überwachung verwendet.

ANMERKUNG: Dell Command | Monitor für Windows verwendet Simple Network Management Protocol (SNMP), um verschiedene Systemvariablen zu beschreiben.

Die Desktop Management Task Force (DMTF) ist die branchenweit anerkannte Normungsorganisation, die führend in der Entwicklung, Adaptierung, Vereinheitlichung von Verwaltungsstandards (einschließlich CIM und ASF) und bei Initiativen für Desktop-, Unternehmens- und Internetumgebungen ist.

4

Anwendungsszenarien mit Dell Command | Monitor 10.6

Dieses Kapitel beschreibt verschiedene Nutzerszenarien von Dell Command | Monitor.

Sie können Dell Command | Monitor für folgende Zwecke verwenden:

- Asset Management
- Konfigurationsmanagement
- Überwachung des Akkuzustands
- Profile

Themen:

Szenario 1: Asset Management

Ein Unternehmen, das viele Dell-Systeme verwendet, konnte aufgrund von Veränderungen seiner kaufmännischen und IT-Belegschaft keine präzisen Bestandslisten pflegen. Der Chief Information Officer (CIO) verlangt einen Plan zur Identifizierung der Systeme, die auf die jeweils neueste Version von Windows aktualisiert werden können. Dies erfordert eine Bewertung der bereitgestellten Systeme, um die Größe, die Reichweite und die finanziellen Auswirkungen eines solchen Projekts zu bestimmen. Das Erfassen der Informationen ist ein umfangreiches Unterfangen. Das Bereitstellen von IT-Mitarbeitern für jedes Client-System ist in Hinsicht auf die Unterbrechungen für die Endnutzer kostspielig.

Mithilfe von Dell Command | Monitor auf den einzelnen Dell Systemen, kann der IT-Manager die benötigten Informationen schnell per Remote-Zugriff erfassen. Mit Hilfsprogrammen, wie Microsoft System Center Configuration Manager (SCCM), fragt der IT-Manager jedes Client-System über das Netzwerk ab und erfasst Informationen wie CPU-Typ und -Geschwindigkeit, Speichergröße, Festplattenkapazität, BIOS-Version und Version des derzeitigen Betriebssystems. Sobald die Informationen vorliegen, können Sie analysiert werden, um zu bestimmen, welche Systeme auf die neuesten Windows-Versionen aktualisiert werden können.

Sie können die Bestandsaufnahme der Assets auch über die WSMAN/WinRM-Befehlszeile oder eine beliebige CIM Client-Befehlszeile ermitteln.

SCCM-Integration

Sie können SCCM in Dell Command | Monitor für Windows integrieren, indem Sie wie folgt verfahren:

- Verwenden der MOF-Datei im Dell Command | Monitor-Installationspaket, das alle Dell Command | Monitor-Klassen enthält, und Importieren in den KonfigMgr

  Die MOF befindet sich unter:

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

- Fähigkeiten zum Asset-Report mit Hilfe von Sammlungen ausdehnen

Szenario 2: Konfigurationsmanagement

Ein Unternehmen möchte die Client-Plattform standardisieren und den gesamten Lebenszyklus aller System verwalten. Zu diesem Zweck erwirbt das Unternehmen eine Suite von Tools und plant die Automatisierung der Bereitstellung eines neuen Client-Betriebssystems mit Preboot Execution Environment (PXE).

Hier muss die schwierige Aufgabe gelöst werden, das BIOS-Kennwort in den einzelnen Client-Computern zu ändern, ohne den Desktop tatsächlich manuell besuchen zu müssen. Wenn Dell Command | Monitor auf den einzelnen Client-Systemen installiert ist, hat die IT-Abteilung des Unternehmens mehrere Möglichkeiten, die Startreihenfolge remote zu ändern. Die Verwaltungskonsole OpenManage Essentials (OME) kann mit Dell Command | Monitor integriert werden und die BIOS-Einstellungen remote auf allen Client-Systemen überwachen. Eine weitere Option besteht darin, ein Skript (CIM, WinRM/WSMAN/PowerShell/WMIC) zu schreiben, das die BIOS-Einstellung ändert. Das Skript kann remote über das Netzwerk an die einzelnen Client-Systeme gesendet und dort ausgeführt werden.

Weitere Informationen zu Dell Command | Monitor finden Sie im Referenzhandbuch zu Dell Command | Monitor unter **dell.com/support**.

Standardisierte Konfigurationen ermöglichen erhebliche Kostenersparnisse für Unternehmen aller Größen. Viele Organisationen stellen standardisierte Client-Systeme bereit, aber nur wenige verwalten die Systemkonfiguration während der gesamten Lebensdauer des Computers. Wenn Dell Command | Monitor auf jedem Client-System installiert ist, kann die IT-Abteilung Legacy-Schnittstellen sperren, um die Verwendung von nicht autorisierten Peripheriegeräten zu verhindern, oder Wake On LAN (WOL) aktivieren, damit das System während der Schwachlastzeit aus dem Ruhezustand geholt wird, um Systemmanagementaufgaben auszuführen.

Szenario 3: Überwachung des Funktionszustands

Ein Nutzer erhält Lesefehlermeldungen, wenn er versucht, auf gewisse Dateien auf der Festplatte des Client-Systems zuzugreifen. Der Nutzer startet das System neu und die Dateien scheinen nun zugreifbar zu sein. Der Nutzer schenkt dem anfänglichen Problem keine Beachtung mehr, da es sich von selbst gelöst zu haben scheint. Inzwischen fragt Dell Command | Monitor die Festplatte mit dem Problem im Hinblick auf einen vorhergesagten Ausfall ab und sendet eine SMART-Warnung (Self-Monitoring, Analysis and Reporting Technology) an die Managementkonsole. Außerdem wird der SMART-Fehler auch dem lokalen Nutzer angezeigt. Die Warnmeldung weist darauf hin, dass auf der Festplatte mehrere Lese-/Schreibfehler aufgetreten sind. Die IT-Abteilung des Unternehmens empfiehlt, dass der Nutzer sofort ein Backup der kritischen Datendateien erstellt. Ein Servicetechniker wird mit einem Ersatzlaufwerk vorbeigeschickt.

Die Festplatte wird ersetzt, bevor sie ausfällt, wodurch Ausfallzeiten für den Benutzer, Anrufe an die Help-Desk und der Besuch eines Technikers beim Desktop zur Problemdiagnose verhindert werden.

Überwachung von Systemwarnungen mit der Ereignisanzeige des Betriebssystems, Syslog oder CIM-Indikation

Dell Command | Monitor unterstützt die Überwachung von Ereignissen durch die folgenden Vorgänge:

- Ziehen des Protokolls durch die CIM-Klasse DCIM_LogEntry.
- Überwachen der CIM-Indikation durch DCIM_AlertIndication-Klasse.
- (nur für Dell Command | Monitor für Windows) Überwachung von Ereignissen mit Simple Network Management Protocol (SNMP) und der Windows-Ereignisanzeige.
- (nur für Dell Command | Monitor für Linux) Überwachung mit Syslog.

Weitere Informationen zu Dell Command | Monitor finden Sie im Referenzhandbuch zu Dell Command | Monitor unter **dell.com/support**.

Szenario 4: Profile

ANMERKUNG: DMTF-Profile werden nur für Dell Command | Monitor für Windows implementiert.

IT-Administratoren werden benötigt, um Clientsysteme in Umgebungen mit Produkten mehrerer Anbieter und verteilten Unternehmensumgebungen zu verwalten. Sie müssen sich mit unterschiedlichsten Tools und Anwendungen auskennen und gleichzeitig verschiedene Desktop- und mobile Clientsysteme in verschiedenen Netzwerken verwalten. Um die Kosten für diese Anforderungen zu reduzieren und die bereitgestellten Managementdaten abzubilden, werden die Branchenstandardprofile Distributed Management Task Force (DMTF) und die Data Center Infrastructure Management (DCIM-OEM) in Dell Command | Monitor implementiert. Einige der DMTF-Profile werden in diesem Handbuch erläutert.

Weitere Informationen zu Dell Command | Monitor finden Sie im Referenzhandbuch zu Dell Command | Monitor unter **dell.com/support**.

Bestandsprofil

Gewährleistungsstatus auf Endpunktgerät:

- Bestimmen Sie den Status der Gewährleistung, indem Sie die Instanz der Klasse **DCIM_AssetWarrantyInformation** aufzählen/ermitteln.

- Überprüfen Sie, ob der Gewährleistungsstatus mithilfe der Eigenschaften **WarrantyStartDate** und **WarrantyEndDate** der Klasse **DCIM_AssetWarrantyInformation** ermittelt werden kann.

  ANMERKUNG: Voraussetzung für DCIM_AssetWarrantyInformation ist, dass Sie über eine funktionierende Internetverbindung verfügen. Wenn Sie Dell Command | Monitor hinter einem Proxyserver ausführen, stellen Sie sicher, dass die Proxyeinstellungen korrekt konfiguriert sind.

  So erhalten Sie weitere Informationen über den Gewährleistungsstatus der Peripheriegeräte:

  1. Rufen Sie die Website Dell.com/support auf.
  2. Überprüfen Sie in der Dropdownliste „Land/Region auswählen“ unten auf der Seite Ihr Land bzw. Ihre Region.
  3. Supportkategorie auswählen – Gewährleistung und Verträge
  4. Zeigt den Service-Tag Ihres Systems an.
- Deaktivieren Sie die Gewährleistungsfunktion und nachfolgende Aktualisierungsaufforderungen.
- Rufen Sie bei Bedarf die Gewährleistungsinformationen ab.

ANMERKUNG: Gewährleistungsinformationen werden automatisch alle 15 Tage aktualisiert. Im Falle eines aktuellen Gewährleistungsstatus sind die aufgezählten Gewährleistungsinformationen möglicherweise nicht mit denen auf der Support-Website von Dell identisch.

Akkuprofil

- Bestimmen Sie den Akkuzustand, indem Sie die Instanz der Klasse **DCIM_Akku** aufzählen/ermitteln.
- Bestimmen Sie die geschätzte Laufzeit und sehen Sie die geschätzte verbleibende Ladung.
- Überprüfen Sie, ob die Informationen zum Akkuzustand unter Verwendung der Eigenschaften „Operational Status“ und „Health State“ der Klasse **DCIM_Battery** bestimmt werden können.
- Weitere Informationen zum Akkuzustand finden Sie unter der Eigenschaft **DCIM_Sensor.CurrentState** oder der Eigenschaft **CIM_NumericSensor.CurrentState**.
- Bestimmen Sie die Position des Akkus und den Akku-ePPID, indem Sie die Eigenschaften **IdentifyingDescriptions** und **OtherIdentifyingInfo** der Klasse **DCIM_Battery** verwenden.

DCIM_Battery

Um die Informationen über den ePPID-Wert des Akkus für ein Akkuelement zu erhalten. Öffnen Sie die Powershell Eingabeaufforderung als Administrator und führen Sie den folgenden Befehl aus: `Get-CimInstance -Namespace root/dcim/sysman -Classname DCIM_Battery |Select ElementName, OtherIdentifyingInfo, IdentifyingDescriptions.`

ANMERKUNG: Der ePPID-Wert des Akkus ist nicht dynamisch und wenn der Akku ausgetauscht wird, müssen Sie das System neu starten, um die Änderungen in der **DCIM_Battery** Instanz zu reflektieren.

BIOS-Verwaltungsprofil

- Bestimmen Sie die BIOS-Version, indem Sie die Instanz der Klasse **DCIM_BIOSElement** aufzählen.
- Überprüfen Sie, ob die BIOS-Attributwerte geändert werden können. Rufen Sie die Instanz der Klasse **DCIM_BIOSEnumeration** ab. Das Attribut kann geändert werden, wenn die Eigenschaft **IsReadOnly** auf FALSE festgelegt ist.
- Legen Sie das Systemkennwort (SystemPwd) fest. Führen Sie die Methode **DCIM_BIOSService.SetBIOSAttributes()** aus und stellen Sie den Parameter „SystemPwd“ auf „AttributeName“ und den Parameter „password value“ auf „AttributeValue“ ein.
- Legen Sie das BIOS- oder Admin-Kennwort (AdminPwd) fest. Führen Sie die Methode **DCIM_BIOSService.SetBIOSAttributes()** aus und stellen Sie den Parameter „AdminPwd“ auf „AttributeName“ und den Parameter „password value“ auf „AttributeValue“ ein.
- Führen Sie die Methode **DCIM_BIOSService.SetBIOSAttribute()** aus und geben Sie die Parameter AttributeName und AttributeValue an.
- Um ein BIOS-Attribut zu ändern, wenn das BIOS/Admin-Kennwort eingestellt ist, führen Sie die Methode **DCIM_BIOSService.SetBIOSAttribute()** aus und geben Sie AttributeName, AttributeValue und das aktuelle BIOS-Kennwort als AuthorizationToken-Eingabeparameter an.

Boot-Steuerung

- Ändern Sie die Reihenfolge von Startelementen in der Legacy- und UEFI-Startliste.
- Aktivieren oder deaktivieren Sie die Startelemente der Legacy- und UEFI-Startliste.

- Suchen Sie die aktuelle Startkonfiguration, indem Sie die Instanzen der Klasse **DCIM_ElementSettingData** aufzählen, deren Eigenschaft **IsCurrent** auf **1** eingestellt ist. Die Instanz **DCIM_BootConfigSetting** repräsentiert die aktuelle Startkonfiguration.

Basis Desktop Mobile

- Bestimmen Sie das Systemmodell, die Service-Tag-Nummer und Seriennummer, indem Sie die Instanz der Klasse **DCIM_ComputerSystem** aufzählen.
- Führen Sie die **DCIM_ComputerSystem.RequestStateChange()**-Methode aus, um den Parameterwert „RequestedState“ auf **3** einzustellen. Der Parameterwert 3 schaltet das System aus.
- Führen Sie die **DCIM_ComputerSystem.RequestStateChange()**-Methode aus und stellen Sie den Parameterwert **RequestedState** auf **11** ein. Der Parameterwert 11 startet das System neu.
- Legen Sie den Stromzustand des Systems fest.
- Legen Sie die Anzahl von Prozessoren im System fest, indem Sie eine Abfrage für Instanzen von **DCIM_Processor** ausführen, die der Zentralinstanz durch die Zuordnung **DCIM_SystemDevice** zugeordnet ist.
- Ermitteln Sie die Systemzeit. Führen Sie die **DCIM_TimeService.ManageTime()**-Methode aus und stellen Sie den Parameterwert **GetRequest** auf **True** ein.
- Überprüfen Sie den Funktionszustand des verwalteten Elements.

Protokolleintrag

- Identifizieren Sie das Protokoll dem Namen nach, indem Sie die Instanz **DCIM_RecordLog** auswählen, in der die Eigenschaft **ElementName** dem Protokollnamen entspricht.
- Suchen Sie die einzelnen Protokolleinträge. Ermitteln Sie alle Instanzen von **DCIM_LogEntry**, die der gegebenen Instanz von **DCIM_RecordLog** durch die Zuordnung **DCIM_LogManagesRecord** zugeordnet sind. Ordnen Sie die Instanzen basierend auf der **RecordID**.
- Überprüfen Sie, ob Eintragsprotokolle aktiviert sind oder nicht, indem Sie die Instanz der Klasse **DCIM_RecordLog** aufzählen, deren Eigenschaft **Enabledstate** auf **2** (steht für Aktiviert) und deren **EnabledState** auf **3** (steht für Deaktiviert) gesetzt ist.
- Ordnen Sie die Protokolldatensätze basierend auf dem Zeitstempel des Protokolleintrags. Ermitteln Sie alle Instanzen von **DCIM_LogEntry**, die der gegebenen Instanz von **DCIM_RecordLog** durch die Zuordnung **DCIM_LogManagesRecord** zugeordnet sind. Ordnen Sie die Instanzen von **DCIM_LogEntry** basierend auf dem Eigenschaftswert **CreationTimeStamp** in der Reihenfolge LIFO (Last in First Out).
- Löschen Sie Protokolle, indem Sie die Methode **ClearLog()** für die angegebene Instanz von **DCIM_RecordLog** ausführen.

Physischer Bestand

- Ermitteln Sie die physische Bestandsaufnahme für alle Geräte in einem System.
- Ermitteln Sie die physische Bestandsaufnahme für ein Systemgehäuse.
- Bestimmen Sie die Teilenummer einer fehlerhaften Komponente.
- Bestimmen Sie, ob der Steckplatz leer ist oder nicht.

Systemspeicherprofil

- Ermitteln Sie die Speicherinformationen des Systems.
- Ermitteln Sie die physischen Speicherinformationen des Systems.
- Überprüfen Sie die Systemspeichergröße.
- Überprüfen Sie die verfügbare Systemspeichergröße.
- Überprüfen Sie die physische Systemspeichergröße.
- Überprüfen Sie den Funktionszustand des Systemspeichers.

5

Verwenden von Dell Command | Monitor 10.6

Hier können Sie die von Dell Command | Monitor bereitgestellten Informationen abrufen: `root\dcim\sysman (standard)`

Dell Command | Monitor stellt die Informationen durch Klassen in diesen Namespaces bereit.

Weitere Informationen zu den Klassen finden Sie im Referenzhandbuch zu Dell Command | Monitor unter **dell.com/support**.

Themen:

Abfrageintervalleinstellungen

Sie können das Abfrageintervall für die Lüftersonde, Temperatursonde, Spannungssonde, Stromsonde, Festplattenkapazitätserhöhung/-verringerung, Speichergrößenerhöhung/-verringerung und Prozessoranzahlerhöhung/-verringerung mithilfe von Dell Command | Monitor ändern.

- Für Windows befinden sich die Dateien `dcsbdy32.ini` oder `dcsbdy64.ini` unter `<Dell Command | Monitor installed location>\omsa\ini`.
- Für Linux befindet sich die Datei `AlertPollingSettings.ini` unter `/opt/dell/dcm/conf`.

ANMERKUNG: Die Zahlen in der INI-Datei sind das Vielfache von **23**. Das Standard-Abfrageintervall für die Festplattenkapazität und die Self-Monitoring, Analysis and Reporting Technology (SMART)-Warnung beträgt **626** Sekunden (die Echtzeit = 626 x 23 Sekunden, was ungefähr drei Stunden entspricht).

RAID-Status-Report

Dell Command | Monitor aktiviert die RAID-Konfigurationsinformationen und überwacht die RAID-Funktionalität für Client-Systeme mit Hardware- und Treibersupport. Sie können RAID-Klassen verwenden, um Details zu RAID-Leveln, Treiberinformationen, die Controller-Konfiguration und den Controller-Status zu erhalten. Nachdem die RAID-Konfiguration aktiviert ist, können Sie Warnmeldungen über Performanceherabsetzungen oder Laufwerks- und Controller-Ausfälle empfangen.

ANMERKUNG: Der RAID-Status-Report wird nur für RAID-Controller unterstützt, die mit CSMI (Common Storage Management Interface) Version 0.81 konformen Treibern arbeiten. Ab OMCI 8.1 wird die Überwachung nur auf dem Intel On-Chip-RAID-Controller und ab OMCI 8.2 die Ausgabe von Warnmeldungen für Intel On-Chip-RAID-Controller unterstützt.

Überwachen der Dell Clientsysteme

- Dell Command | Monitor für Windows unterstützt das Simple Network Management Protocol (SNMP) zur Überwachung und Verwaltung von Client-Systemen wie Laptops, Desktop-PCs und Workstations. Die MIB-Datei (Management Information Base) wird von Dell Command | Monitor und Server Administrator gemeinsam verwendet. Dell Command | Monitorfür Windows verwendet ab Version 9.0 eine spezifische Client-OID (10909), mit der Konsolen Client-Systeme identifizieren können.

Weitere Informationen zu SNMP finden Sie im SNMP-Referenzhandbuch zu Dell Command | Monitor unter **dell.com/support**.

- Dell Command | Monitor für Linux unterstützt die Überwachung mit WinRM- und WSMan-Befehlen.

Anwendungsprotokoll für Dell Command | Monitor für Linux

Dell Command | Monitor für Linux trennt die Anwendungsprotokolle und Warnmeldungen nach Reporting- und Debugging-Zwecken. Der Verlauf der erzeugten Warnmeldungen und Protokolle für Dell Command | Monitor kann in der Datei **dcm_application.log** angezeigt werden, die unter `/opt/dell/dcm/var/log` verfügbar ist.

Konfigurationsdatei

Sie können die Konfigurationsdatei **log.property**, verfügbar unter `/opt/dell/dcm/conf`, aktualisieren, um die gewünschten Einstellungen und DEBUG anzuwenden:

ANMERKUNG: Starten Sie den OMI-Server neu, nachdem Sie Änderungen an der Konfigurationsdatei vorgenommen haben, um die Änderungen zu übernehmen.

- Log_Level – Es gibt drei Protokollebenen, um die Systemmeldungen zu trennen: ERROR, INFO, DEBUG

  Der Nutzer kann die Protokollebene in der Konfigurationsdatei ändern. Wenn die Protokollebene auf DEBUG eingestellt ist, sendet das Anwendungsprotokoll von Dell Command | Monitor alle Informationen an die angegebene Protokolldatei.

  ANMERKUNG: Die standardmäßige Protokollebene ist auf INFO gesetzt.
- File_Size – Der Nutzer kann die maximale Größe der Datei **dcm_application.log** festlegen. Die Standarddateigröße ist 500 MB.

  ANMERKUNG: Der File_Size-Wert muss in Byte ausgedrückt werden.
- BackupIndex – Der Nutzer kann die Rollover-Anzahl der Datei **dcm_application.log** angeben. Wenn die standardmäßige Rollover-Anzahl 2 ist, überschreibt die dritte Backup-Datei die älteste Datei.

Erkennen von Advanced Format-Laufwerken

Client-Systeme werden zunehmend auf Advanced Format (AF)-Laufwerke umgestellt, damit eine größere Storage-Kapazität zur Verfügung steht und die Einschränkungen von Festplatten (HDDs) mit 512-Byte-Sektoren aufgehoben werden. Festplatten, die in 4-kB-Sektoren umgewandelt werden, bleiben abwärts kompatibel, während die aktuellen AF-Festplatten, die auch als 512e-Festplatten bekannt sind, mit 512-Byte-SATA übereinstimmen und mit 4 kB betrieben werden. Während des Übergangs stellen Sie möglicherweise Performanceprobleme fest, z. B. in Verbindung mit Laufwerken mit falsch zugeordneten Partitionen in den Client-Systemen, was dazu führt, dass sektorbasierte Verschlüsselungssoftwarepakete, die 512e-Festplatten handhaben, ausfallen. Dell Command | Monitor ermöglicht es Ihnen festzustellen, ob die Festplatte auf einem System eine 4-kB-AF-Festplatte ist, wodurch sich diese Probleme vermeiden lassen.

Startkonfigurationen

ANMERKUNG: Dell Command | Monitor für Linux bietet keine Start-Konfigurationsfunktionen. Dieser Abschnitt gilt also nicht für Dell Command | Monitor für Linux.

Ein Clientsystem kann eine von zwei Arten von Startkonfigurationen aufweisen:

- Legacy (BIOS)
- UEFI (UEFI-Modus)

In Dell Command | Monitor wird die Startkonfiguration (Legacy oder UEFI) mithilfe der folgenden Klassen modelliert:

- DCIM_ElementSettingData
- DCIM_BootConfigSetting
- DCIM_OrderedComponent
- DCIM_BootSourceSetting
- DCIM_SmartAttributeInfo

ANMERKUNG: Die Begriffe Startkonfiguration und Startlistentyp werden synonym verwendet und vermitteln dieselbe Bedeutung: Legacy oder UEFI.

DCIM_AssetWarrantyInformation

- Führen Sie den folgenden Befehl in der Powershell Aufforderung aus, um den Garantiestatus auf dem Endgerät abzufragen:

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

- Um die Gewährleistungsansprüche in chronologischer Reihenfolge von `WarrantyEndDate` aufzulisten, führen Sie den folgenden Befehl in der Powershell Aufforderung aus:

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

- Um die Gewährleistungsfunktion und nachfolgende Aktualisierungsaufforderungen zu deaktivieren, führen Sie den folgenden Befehl in der Powershell Aufforderung aus:

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

- Um bei Bedarf Gewährleistungsinformationen abzurufen, führen Sie den folgenden Befehl in der Powershell Aufforderung aus:

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

ANMERKUNG: Für die Proxy-Konfiguration einrichten:

- Standard-Proxy – Dell Command | Monitor wählt den Standard-System-Proxy aus (im IE festgelegt)
- Benutzerdefinierter Proxy

  Die Klasse **DCIM_ApplicationProxySetting** wird verwendet, um die Proxy-Einstellungen für Dell Command | Monitor gemäß der Proxy-Umgebung zu ändern.

DCIM_BootConfigSetting

Eine Instanz von **DCIM_BootConfigSetting** repräsentiert eine Startkonfiguration, die beim Startvorgang verwendet wird. Auf Client-Systemen gibt es beispielsweise zwei Arten von Startkonfigurationen: Legacy und UEFI. **DCIM_BootConfigSetting** muss daher maximal zwei Instanzen repräsentieren, eine für Legacy und eine für UEFI.

Sie können festlegen, ob **DCIM_BootConfigSetting** Legacy repräsentiert, indem Sie die folgenden Eigenschaften verwenden:

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

Sie können festlegen, ob **DCIM_BootConfigSetting** UEFI repräsentiert, indem Sie die folgenden Eigenschaften verwenden:

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

DCIM_BootSourceSetting

Diese Klasse repräsentiert die Startgeräte oder -quellen. Die Eigenschaften **ElementName**, **BIOSBootString** und **StructuredBootString** enthalten eine Zeichenfolge, die die Startgeräte identifiziert. Zum Beispiel Diskette, Festplatte, CD/DVD, Netzwerk, Personal Computer Memory Card International Association (PCMCIA), Battery Electric Vehicle (BEV) oder USB. Basierend auf dem Startlistentyp des Geräts ist eine Instanz von **DCIM_BootSourceSetting** einer der Instanzen von **DCIM_BootConfigSetting** zugeordnet.

DCIM_OrderedComponent

Die **DCIM_OrderedComponent**-Zuordnungsklasse wird dazu verwendet, Instanzen von **DCIM_BootConfigSetting** Instanzen von **DCIM_BootSourceSetting** zuzuordnen, was einen Startlistentyp (Legacy oder UEFI) repräsentiert, zu dem die Startgeräte gehören. Die **GroupComponent**-Eigenschaft von **DCIM_OrderedComponent** verweist auf die **DCIM_BootConfigSetting**-Instanz und die **PartComponent**-Eigenschaft verweist auf die **DCIM_BootSourceSetting**-Instanz.

DCIM_Smart-Attribut

Zum Lesen des Smart-Attributwerts führen Sie die folgenden Befehle aus:

Zum Beispiel:

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

Zum Einrichten der benutzerdefinierten Schwellenwerte führen Sie die folgenden Befehle aus:

Zum Beispiel:

- Get-CimInstance -Namespace root\dcim\sysman DCIM_SmartAttributeInfo -Filter "AttributeID like '<Attribut-ID-Wert>'" | Invoke-CimMethod -MethodName "SetCustomThreshold" -Arguments @{CustomThresholdValue="<einzustellender benutzerdefinierter Schwellenwert>"}

DCIM_ThermalInformation

DCIM_ThermalInformation verwaltet die thermischen Konfigurationseinstellungen, wie z. B. den thermischen Modus, den AAC-Modusund den Lüfter-Fehlermodus.

- Führen Sie den folgenden Befehl aus, um die Systeminformationen über die Wärmeentwicklung abzufragen:

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

- Um den Wert für den thermischen Modus festzulegen, führen Sie den folgenden Befehl aus:

```
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")}
```

Ändern der Systemeinstellungen

In Dell Command | Monitor können die folgenden Methoden verwendet werden, um die Systemeinstellungen und den Zustand der lokalen oder Remote-Systeme zu ändern:

- SetBIOSAttributes – Zum Ändern der BIOS-Einstellung

  ANMERKUNG: Dell Command | Monitor für Linux unterstützt derzeit nur die SetBIOSAttributes-Methode.
- ChangeBootOrder – Zum Ändern der Startkonfiguration
- RequestStateChange – Zum Herunterfahren und Neustarten des Systems
- ManageTime – Zum Anzeigen der Systemzeit

In Dell Command | Monitor für Windows können Sie diese Methoden mithilfe von winrm, VB-Skript, PowerShell-Befehlen, wmic und WMI wbemtest ausführen.

Zurücksetzen des BIOS auf Standardeinstellungen auf Systemen, die unter Windows oder Linux ausgeführt werden

ResetBIOSDefaults (Methode)

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

OMI-Befehl:`/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> }`

Mögliche Werte:

- 0 – Integrierte sichere Standardeinstellungen – auch als BIOS-Standardeinstellung bezeichnet. Diese Konfiguration unterstützt alle Plattformen und kann daher nicht geändert werden.

- 1 – Zuletzt als funktionierend bekannte Einstellungen – werden automatisch vom BIOS nach erfolgreichem Abschluss des POST generiert. Mit dieser Option wird BIOS auf eine als funktionierend bekannte Konfiguration zurückgesetzt. Wenn die **integrierten sicheren Standardeinstellungen** beschädigt sind, können Sie die **zuletzt als funktionierend bekannte Einstellungen** verwenden, um BIOS wiederherzustellen.
- 2 – Werkseinstellungen – Werkseinstellungen, die vor dem Versand des Systems generiert werden. Diese Konfiguration ist für die Hardwarekonfiguration optimiert oder wird gemäß Ihren Anforderungen beim Kauf oder Service angepasst.
- 3-Nutzerkonfiguration 1 – wird auf Nutzeraufforderung konfiguriert. Wählen Sie im BIOS-Setup- oder F2-Bildschirm **aktuelle Konfiguration speichern** aus, um die Konfiguration über die Anwendung Dell Command | Monitor die Konfiguration zurückzusetzen.
- 4-Nutzerkonfiguration 2 – wird auf Nutzeraufforderung konfiguriert. Wählen Sie im BIOS-Setup- oder F2-Bildschirm **aktuelle Konfiguration speichern** aus, um die Konfiguration über die Anwendung Dell Command | Monitor die Konfiguration zurückzusetzen.

Tabelle 1. Mögliche Werte für ResetBIOSDefaults

Beschreibung	Fehlercode (SetResult-Wert)
Erfolg	0
Ungültiger Eingabewert/Eingabewert außerhalb des zulässigen Bereichs	1
Authentifizierungsfehler	2
Nicht unterstützte Konfiguration	3
Leere Konfiguration	4
Allgemeiner Fehler/Nicht erfolgreich/wenn Dienst nicht ausgeführt wird	4294967295

ANMERKUNG: Nach dem Vorgang **ResetBIOSDefaults** ist ein Neustart des Systems erforderlich, damit die Änderungen erfolgreich wiedergegeben werden.

DCM-Windows verfügt über Funktionen zum Herunterfahren oder Neustarten des Systems über die folgenden APIs:

- System neu starten `–Get-CimInstance -Namespace ROOT\DCIM\SYSMAN -ClassName DCIM_ComputerSystem |Where-Object {$_.Dedicated -ne 28} | Invoke-CimMethod -MethodName RequestStateChange -Arguments @{RequestedState ='11'}`
- System herunterfahren `–Get-CimInstance -Namespace ROOT\DCIM\SYSMAN -ClassName DCIM_ComputerSystem |Where-Object {$_.Dedicated -ne 28} | Invoke-CimMethod -MethodName RequestStateChange -Arguments @{RequestedState ='3'}`

Im GNU- oder Linux-Betriebssystem können folgende APIs verwendet werden:

- shutdown -r +5
- sudo reboot

ANMERKUNG: Während des Reset-Vorgangs wird ein Teilbereich der Optionen nicht auf die Standardeinstellungen zurückgesetzt. Dem können entweder Sicherheitsgründe (z. B. Kennwörter) oder die Boot-Fähigkeit (z. B. Startliste und Legacy Option ROMs) zugrunde liegen.

Die BIOS-Ereignisprotokolle werden nicht zurückgesetzt, um die Historie der Systemhardware zu speichern.

In der folgenden Tabelle wird die umfassende Liste der Funktionen aufgelistet, die nicht auf die Standardeinstellungen zurückgesetzt werden.

Tabelle 2. Umfassende Liste der Funktionen, die nicht auf die Standardeinstellungen zurückgesetzt werden

Abschnitt	Unterabschnitt	Objekt
Allgemein	Systeminformationen	Service-Tag-Nummer
	Systeminformationen	Bestands-Tag
	Systeminformationen	Ownership Tag
	Startreihenfolge	Startliste
	Advanced Boot Options	Enable Legacy OROMs (ROMs der Legacy-Option aktivieren)
	Date/Time	Date/Time

Tabelle 2. Umfassende Liste der Funktionen, die nicht auf die Standardeinstellungen zurückgesetzt werden (fortgesetzt)

Abschnitt	Unterabschnitt	Objekt
	Integrated NIC	Integrated NIC
	Integrated NIC	Enable UEFI Network Stack
	SATA Operation (SATA-Betrieb)	SATA Operation (SATA-Betrieb)
Sicherheit	NA	Admin Password
	NA	Systemkennwort
	NA	Interne HDD-x-Kennwörter
	NA	Master Password Lockout
	SMM Security Mitigation	SMM Security Mitigation
	Intel SGX Enable	Intel SGX Enable
Secure Boot	Secure Boot Enable	Secure Boot Enable
	Expert Key Management	Wichtige Datenbanken

Festlegen von BIOS-Attributen in einem Windows-System mithilfe von PowerShell-Befehlen

Sie können BIOS-Attribute mithilfe der Methode SetBIOSAttributes festlegen. Der Vorgang wird im Folgenden erklärt, indem das Trusted Platform Module (TPM) als Beispiel aktiviert wird.

ANMERKUNG: Stellen Sie sicher, dass die TPM-Option im BIOS deaktiviert ist, bevor Sie das Verfahren zum Aktivieren des TPM anwenden.

ANMERKUNG: Verwenden Sie PowerShell mit Administratorrechten.

So aktivieren Sie das TPM:

1. Stellen Sie das BIOS-Kennwort mithilfe des folgenden PowerShell-Befehls ein, falls noch nicht geschehen:

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

2. Aktivieren Sie TPM-Sicherheit mit dem folgenden Befehl:

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

3. Starten Sie das System neu.
4. Aktivieren Sie das TPM mit dem folgenden Befehl:

   ```
   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. Starten Sie das System neu.

   Allgemeiner Haftungsausschluss

   Das Modul PowerShell PSReadline speichert jeden von Ihnen eingegebenen Konsolenbefehl in eine Textdatei. Es wird daher empfohlen, das Comandlet „Get-Credential“ zum sicheren Umgang mit dem Kennwort zu verwenden.

   a. $cred = Get-Credential

   b. Geben Sie Ihren Nutzernamen und Ihr Kennwort ein, z. B. AdminPWD und Dell_123$, wenn das Dialogfeld angezeigt wird.

   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 ")}

Festlegen von BIOS-Attributen auf Linux-Systemen

Sie können BIOS-Attribute mithilfe einer der folgenden Methoden festlegen:

- Verwenden von OMICLI
- Verwenden von WinRM
- Verwenden von WSMan

ANMERKUNG: Stellen Sie sicher, dass der OMI-Server ausgeführt wird.

Festlegen von BIOS-Attributen mit OMICLI

Sie können BIOS-Attribute mithilfe der Methode SetBIOSAttributes festlegen. Der Vorgang wird im Folgenden erklärt, indem das Trusted Platform Module (TPM) als Beispiel aktiviert wird.

ANMERKUNG: Stellen Sie sicher, dass die TPM-Option im BIOS deaktiviert ist, bevor Sie das Verfahren zum Aktivieren des TPM anwenden.

So legen Sie BIOS-Attribute mit OMICLI-Befehlen fest:

1. Um das BIOS-Kennwort auf dem System festzulegen, wenn es nicht bereits festgelegt wurde, führen Sie Folgendes aus:

```
./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. Um die TPM-Sicherheit zu aktivieren, führen Sie den folgenden Befehl aus:

```
./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. Starten Sie das System neu.
4. Um das TPM zu aktivieren, führen Sie Folgendes aus:

```
./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. Starten Sie das System neu.
6. Um das BIOS-Kennwort zurückzusetzen, führen Sie Folgendes aus:

```
./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>"  }
```

Festlegen von BIOS-Attributen mit WinRM

Sie können BIOS-Attribute mithilfe der Methode SetBIOSAttributes festlegen. Der Vorgang wird im Folgenden erklärt, indem das Trusted Platform Module (TPM) als Beispiel aktiviert wird.

ANMERKUNG: Stellen Sie sicher, dass die TPM-Option im BIOS deaktiviert ist, bevor Sie das Verfahren zum Aktivieren des TPM anwenden.

So legen Sie BIOS-Attribute mit WinRM-Befehlen fest:

1. Rufen Sie den festgelegten Selektor ab, indem Sie die Klasse DCIM_BIOSService aufzählen. Ausführen:

```
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
```

ANMERKUNG: Die festgelegten Selektor-Werte (SystemName=<Systemname von DCIM_BIOSService class>winrm i SetBIOSAttributes wsman/DCIM_BIOSService?SystemName=dt: +SystemCreationClassName=DCIM_ComputerSystem+Name=DCIM:BiosService+CreationClassName=DCIM_BIOSService+) werden in diesem Beispiel für den festgelegten Betrieb verwendet.

2. Stellen Sie das BIOS-Kennwort mithilfe des folgenden Befehls ein, falls noch nicht geschehen:

```
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. Aktivieren Sie TPM-Sicherheit, indem sie folgenden Befehl ausführen:

```
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. Starten Sie das System neu.
5. Aktivieren Sie das TPM mit dem folgenden Befehl:

```
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>"}
```

Festlegen von BIOS-Attributen mit WSMan

Sie können BIOS-Attribute auf Systemen festlegen, die Linux unter Verwendung des WSMan ausführen. Der Vorgang wird im Folgenden erklärt, indem das Trusted Platform Module (TPM) als Beispiel aktiviert wird.

ANMERKUNG: Stellen Sie sicher, dass die TPM-Option im BIOS deaktiviert ist, bevor Sie das Verfahren zum Aktivieren des TPM anwenden.

1. Rufen Sie den festgelegten Selektor ab, indem Sie die Klasse DCIM_BIOSService aufzählen. Ausführen:

```
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. Stellen Sie das BIOS-Kennwort mithilfe des folgenden Befehls ein, falls noch nicht geschehen:

```
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. Aktivieren Sie TPM-Sicherheit mit dem folgenden Befehl:

```
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. Starten Sie das System neu.
5. Aktivieren Sie das TPM mit dem folgenden Befehl:

```
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>"
```

Ändern der Startreihenfolge

Um die Startreihenfolge zu ändern, führen Sie die folgenden Schritte aus:

1. Überprüfen Sie den Startreihenfolgetyp (Legacy oder UEFI) mithilfe des folgenden Befehls:
   - WMIC-Befehl: `wmic /namespace:\\root\dcim\sysman path dcim_BootConfigSetting get ElementName/ format:list`.
   - Power Shell-Befehl: `Get-WmiObject -namespace root\dcim\sysman -class dcim_BootConfigSetting -Property ElementName`.
2. Überprüfen Sie den aktuellen Startreihenfolgetyp (Legacy oder UEFI) mithilfe des folgenden Befehls:
   - WMIC-Befehl: `wmic /namespace:\\root\dcim\sysman path dcim_ElementSettingData.IsCurrent=1 get SettingData /format:list .`
   - Power Shell-Befehl: `Get-WmiObject -namespace root\dcim\sysman -class dcim_elementSettingData -Filter "IsCurrent=1" -Property SettingData`.
3. Ändern der Startreihenfolge mithilfe des folgenden Befehls:
   - WMIC-Befehl: `wmic /namespace:\\root\dcim\sysman path dcim_bootconfigsetting call ChangeBootOrder /?:full .`
   - Power Shell-Befehl: `(Get-WmiObject -namespace root\dcim\sysman -class dcim_bootconfigsetting).getmethodparameters("ChangeBootOrder") .`

     ANMERKUNG: Die Instanz `dcim_BootConfigSetting` muss die Startkonfiguration darstellen, die Sie ändern möchten – entweder Typ 1 (Legacy) oder Typ 2 (UEFI).
   - Die Argumente lauten:
     - `Authorization Token` – Dies ist das Administrator- oder Startkennwort.
     - `Source` – Dies ist die Startreihenfolgenliste aus der Eigenschaft `dcim_OrderedComponent.PartComponent`. Die neue Startreihenfolge richtet sich nach der Reihenfolge der Startgeräte im Quellarray.
4. Ändern der Startreihenfolge für Startliste Typ 1 mithilfe von PowerShell:
   a. Rufen Sie die aktuelle Startreihenfolge für die Startliste Typ 1 ab, indem Sie den folgenden Befehl ausführen: `$boLegacy = Get-WmiObject -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-1'} | select -expand partcomponent.`
   b. Definieren Sie zum Bestimmen einer neuen Startreihenfolge eine neue PowerShell-Variable, um `$newboLegacy.` festzulegen. Weisen Sie die neue Startreihenfolge zu. Zum Beispiel: Aktueller Startreihenfolgentyp wird beibehalten.
   c. $newboLegacy = $boLegacy
   d. Rufen Sie die Instanz `dcim_bootconfigsetting` ab, die der Startliste Typ 1 entspricht, indem Sie den folgenden Befehl ausführen: `$bcsLegacy = Get-WmiObject -Namespace root\dcim\sysman -ClassName`

`dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 1'}.`

e. Rufen Sie die Methode auf, indem Sie den folgenden Befehl ausführen: `$ bcsLegacy.changebootorder($newboLegacy, $AuthorizationToken)`. Die Variable `$AuthorizationToken` wird verwendet, um das BIOS-Kennwort weiterzugeben.

5. Ändern der Startreihenfolge für Startliste Typ 2 mithilfe von PowerShell:
   a. Rufen Sie die aktuelle Startreihenfolge für die Startliste Typ 2 ab, indem Sie den folgenden Befehl ausführen: `$boUefi = Get-WmiObject -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-2'} | select -expand partcomponent.`
   b. Definieren Sie zum Bestimmen der Startreihenfolge eine PowerShell-Variable, um `$newboUefi` festzulegen. Weisen Sie die neue Startreihenfolge zu. Zum Beispiel: Aktueller Startreihenfolgentyp wird beibehalten.
   c. Rufen Sie die Instanz `dcim_bootconfigsetting` ab, die der Startliste Typ 2 entspricht, indem Sie den folgenden Befehl ausführen: `$bcsUefi = Get-WmiObject -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 2'}.`
   d. Rufen Sie die Methode auf, indem Sie den folgenden Befehl ausführen: `$ bcsUefi.changebootorder($newboUefi, $AuthorizationToken)`. Die Variable `$AuthorizationToken` wird verwendet, um das BIOS-Kennwort weiterzugeben.

Herunterfahren und Neustarten des Windows-Systems per Remote-Zugriff

Sie können das Windows-System mithilfe der RequestStateChange-Methode per Remote-Zugriff herunterfahren oder neu starten.

1. Fahren Sie das Windows-System per Remote-Zugriff mithilfe des folgenden Befehls herunter:

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

2. Starten Sie das Windows-System per Remote-Zugriff mithilfe des folgenden Befehls neu:

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

Remote-Abruf der Systemzeit auf Windows-System

Sie können die Systemzeit für das Windows-System unter Verwendung der ManageTime-Methode per Remote-Zugriff abrufen. Zum Beispiel:

Führen Sie in der Befehlszeilenschnittstelle Folgendes aus:

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

Managen von Dell Clientsystemen im lokalen Modus unter Verwendung von Dell Command | Monitor 10.6

Sie können Dell Clientsysteme mit einer der folgenden Methoden lokal verwalten:

- Für Systeme, die Windows ausführen, Verwendung von PowerShell.
- Für Systeme, die Linux ausführen, Verwendung von OMICLI.

Themen:

Lokale Verwaltung von Windows-Systemen mit PowerShell

Sie können Dell Client-Systeme, die Windows lokal ausführen, mit PowerShell-Befehlen verwalten.

- Aufzählen von Instanzen einer DCIM-Klasse
  - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSEnumeration`
  - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSPassword`
- Aufrufen von Eigenschaften für eine BIOS-Einstellung

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

- Ändern von BIOS-Einstellungen

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

- Ändern von nicht-kritischen Werten

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

- Abonnieren von Warnungen

```
$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)
```

- Befehle zum Beziehen der Nutzerzustimmung von WMI:

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

- Befehle zum Festlegen der Nutzerzustimmung von WMI:

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

ANMERKUNG: Verbesserungsprogramm für Dell Command | Monitor 10.5 und 10.6 in der x64-Bit-Version.

- Befehle zum Beziehen des Proxys von WMI:

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

- Befehle zum Festlegen des Proxys von WMI:

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

Lokale Verwaltung von Linux-Systemen mit OMICLI

Sie können Linux-Systeme lokal mithilfe von OMICLI-Befehlen managen. Bei Systemen, auf denen Linux ausgeführt wird, ist OMICLI unter `/opt/omi/bin` installiert.

- Aufzählen von Instanzen einer DCIM-Klasse
  - `./omicli ei root/dcim/sysman DCIM_BIOSEnumeration`
  - `./omicli ei root/dcim/sysman DCIM_BIOSPassword`
- Aufrufen von Eigenschaften für eine BIOS-Einstellung

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

- Festlegen des Admin-Kennworts

```
./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 }
```

- Ändern der BIOS-Einstellungen
  - `./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> }
```

- Abonnieren von Warnungen

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

7

Managen von Dell Client-Systemen im Remote-Modus unter Verwendung von Dell Command | Monitor 10.6

Sie können Dell Clientsysteme mit einer der folgenden Methoden per Remotezugriff verwalten:

- Für Systeme, die Windows ausführen, Remote-Management eines Windows-Systems von einem Windows-System mithilfe von PowerShell auf Seite 25
- Für Systeme, die Linux ausführen, Verwalten von Linux-Systemen per Remote-Zugriff mit WinRM vom Windows-System auf Seite 25

Themen:

Remote-Management eines Windows-Systems von einem Windows-System mithilfe von PowerShell

Sie können mithilfe von PowerShell von einem Windows-System remote auf ein Windows-System zugreifen und es überwachen.

Voraussetzungen für das Management-Windows-System:
- Windows PowerShell 3.0
- PowerShell konfiguriert für die Ausführung von Remote-Skripten

Voraussetzungen für das Managed-Windows-System:
- Dell Command | Monitor
- Windows PowerShell 3.0
- PowerShell konfiguriert für die Ausführung von Remote-Skripten
- PowerShell mit aktivierter Remote-Funktion

ANMERKUNG:

Um Windows PowerShell remote zu verwenden, muss der Remote-Computer für das Remote-Management konfiguriert sein. Für weitere Informationen, einschließlich Anweisungen, führen Sie den PowerShell-Befehl `– Get-Help` about_remote_requirements aus.

Verwalten von Linux-Systemen per Remote-Zugriff mit WinRM vom Windows-System

Der Zugriff auf das Linux-System und dessen Überwachung erfolgt durch WinRM-Befehle vom Windows-System.

Voraussetzungen für das Windows-System
- Unterstütztes Windows-Betriebssystem
- Ausgeführte WinRM-Services, die für die Remote-Verwaltung konfiguriert sind

Voraussetzungen für das Linux-System
- Root-Berechtigungen
- Dell Command | Monitor
- Unterstütztes Linux-Betriebssystem

- Aktivieren Sie die Ports 5985 und 5986 auf dem WMI-Server.
- Für Ihre Umgebung konfiguriertes System

Führen Sie folgenden Befehl in der Befehlszeilenschnittstelle aus

```
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
```

Remote-Management eines Linux-Systems von einem Linux-System mithilfe von WSMan

Sie können mithilfe von WSMan-Befehlen von einem Linux-System remote auf ein Linux-System zugreifen und es überwachen.

Voraussetzungen für das Management-Linux-System:
- Unterstütztes Linux-Betriebssystempaket ist installiert.
- wsmancli-Paket ist installiert.

Voraussetzungen für das Managed-Linux-System:
- Root-Zugriffsberechtigungen
- Unterstütztes Linux-Betriebssystem
- Dell Command | Monitor

Starten Sie ein Terminal und führen Sie Folgendes aus

```
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

Häufig gestellte Fragen zu Dell Command | Monitor 10.6

- Wie finde ich die Startreihenfolge (Sequenz) der Startkonfiguration mit Hilfe der Eigenschaft DCIM_OrderedComponent.AssignedSequence?

  Sind einer **DCIM_BootConfigSetting**-Instanz (Legacy oder UEFI) über Instanzen der **DCIM_OrderedComponent**-Zuordnung mehrere **DCIM_BootSourceSetting**-Instanzen (Startgeräte) zugeordnet, kann mit dem Wert der Eigenschaft **DCIM_OrderedComponent.AssignedSequence** die Reihenfolge der zugeordneten **DCIM_BootSourceSetting**-Instanzen (Startgeräte) im Startvorgang festgelegt werden. Eine **DCIM_BootSourceSetting**-Instanz, deren zugeordnete Eigenschaft **CIM_OrderedComponent.Assigned Sequence** gleich **0** ist, wird ignoriert und nicht als Teil der Startreihenfolge betrachtet.

- Wie ändere ich die Startreihenfolge?

  Die Startreihenfolge kann mit der Methode **DCIM_BootConfigSetting.ChangeBootOrder()** geändert werden. Mit der Methode **ChangeBootOrder()** wird die Reihenfolge festgelegt, in der die Instanzen von **DCIM_BootSourceSetting** mit einer **DCIM_BootConfigSetting**-Instanz verknüpft werden. Die Methode hat einen Eingabeparameter: **Source**. Der Parameter **Source** ist ein geordnetes Array der Eigenschaft **PartComponent** der Klasse **DCIM_OrderedComponent**, die die Zuordnung zwischen **DCIM_BootSource Setting**-Instanzen (Startgeräten) und der **DCIM_BootConfigSetting**-Instanz (Startlistentyp Legacy oder UEFI) repräsentiert.

- Wie deaktiviere ich die Startreihenfolge?

  Beim Ändern der Startreihenfolge wird der Wert der Eigenschaft **AssignedSequence** auf jeder Instanz von **DCIM_OrderedComponent**, die die Zielinstanz **DCIM_BootConfigSetting** einer nicht im Eingabe-Array des Parameters **Source** vorhandenen **DCIM_BootSourceSetting**-Instanz zuordnet, auf **0** eingestellt, was angibt, dass das Gerät deaktiviert ist.

- Bei der Verbindung zum Namespace über wbemtest wird die Meldung „Anmeldung fehlgeschlagen" angezeigt.

  Starten Sie **wbemtest** mit Administratorrechten, um Meldungen zur Anmeldung zu umgehen. Öffnen Sie Internet Explorer über die Liste **Alle Programme**. Klicken Sie mit der rechten Maustaste auf **Als Administrator ausführen**, um **wbemtest** zu starten und Namespace-Fehler zu vermeiden.

- Wie kann ich Knowledge Library-Skripts fehlerfrei ausführen?

  Nachfolgend sind die Schritte zur Ausführung von VBS-Skripten aufgeführt, die im Knowledge Library-Link von Dell Command | Monitor verfügbar sind:

  1. Konfigurieren Sie **winrm** mit dem Befehl `winrm quickconfig` auf dem System.
  2. Überprüfen Sie folgendermaßen, ob der Token-Support auf dem System besteht:
     - Überprüfen Sie den **F2-Bildschirm** im BIOS-Setup.
     - Verwenden Sie ein Hilfsprogramm wie wbemtest, um sicherzustellen, dass „keyValue define“ im Skript auf dem System vorhanden ist.

     ANMERKUNG: Dell empfiehlt, das neueste BIOS zu verwenden, das unter **dell.com/support** verfügbar ist. Weitere Informationen finden Sie im Referenzhandbuch zu Dell Command | Monitor unter **dell.com/support**.

- Wie stelle ich die BIOS-Attribute ein?

  BIOS-Attribute können mit der Methode **DCIM_BIOSService.SetBIOSAttributes()** geändert werden. Die Methode **SetBIOSAttributes()** stellt den Wert der in der Klasse **DCIM_BIOSEnumeration** definierten Instanz ein. Die Methode nimmt sieben Eingabeparameter an. Die ersten beiden Parameter können leer oder NULL sein. Der dritte Parameter **AttributeName** ist die Eingabezuordnung zum Wert der Attributnameninstanz der Klasse **DCIM_BIOSEnumeration**. Der vierte Parameter oder **AttributeValue** kann einer der Werte des Attributnamens sein wie in der Klasse **DCIM_BIOSEnumeration** definiert. Der fünfte Parameter AuthorizationToken ist optional, die Eingabe für den fünften Parameter ist das BIOS-Kennwort. Der fünfte Parameter wird nur verwendet, wenn das BIOS-Kennwort auf dem System eingestellt ist. Andernfalls ist er leer. Das sechste und siebte Argument können wieder leer oder null sein.

- Unterstützt Dell Command | Monitor Storage- und Sensorüberwachung für Windows- und Linux-Betriebssysteme?

  Ja, Dell Command | Monitor unterstützt Storage- und Sensorüberwachung für unterstützte Windows- und Linux-Betriebssysteme.

  Im Rahmen der Storage-Überwachung unterstützt Dell Command | Monitor Überwachung und Warnmeldungen für:

- Intel-integrierte Controller (kompatibel mit CSMI v0.81 oder höher)
- LSI-integrierte RAID-Controller; und 9217, 9271, 9341, 9361 und die zugehörigen Treiber (physische und logische)

ANMERKUNG: Das Monitoring von Intel-integrierten Controllern wird für Linux-Betriebssysteme nicht unterstützt.

Im Rahmen der Sensorüberwachung unterstützt Dell Command | Monitor die Überwachung und Ausgabe von Warnmeldungen für Spannungs-, Temperatur-, Stromstärke- Kühlgeräte- (Lüfter-) und Gehäusesensoren.

Weitere Informationen zu Klasse und Warnfunktionen finden Sie im Referenzhandbuch zu Dell Command | Monitor unter **dell.com/support**.

- Kann Dell Command | Monitor in andere Anwendungen/Konsolen integriert werden?

  Ja, Dell Command | Monitor verfügt über Schnittstellen mit führenden Unternehmensmanagementkonsolen, die Industriestandards unterstützen. Das Programm lässt sich mit den folgenden bestehenden Enterprise Management Tools integrieren:

  - Dell Client Integration Suite für System Center 2012
  - Dell OpenManage Essentials
  - Dell Client Management Pack für System Center Operation Manager
- Kann ich in SCCM Klassen für die Bestandsliste importieren?

  Ja, einzelne MOFs oder OMCI_SMS_DEF.mof-Dateien können für die Bestandsliste in die SCCM-Konsole importiert werden.

- Wo befindet sich die SCCM OMCI_SMS_DEF.mof-Datei?

  Die OMCI_SMS_DEF.mof-Datei befindet sich im Verzeichnis C:\Program Files\Dell\Command_Monitor\ssa\omacim\OMCI_SMS_DEF.mof.

- Wie wird der Proxy für DCM 10.2.1 konfiguriert?
- DCM 10.2.1 ist nicht in der Lage, Gewährleistungsinformationen abzurufen.
- Überprüfen Sie mit der Klasse DCIM_ApplicationProxySetting, ob die Anwendungs-Proxy-Einstellungen ordnungsgemäß konfiguriert wurden.

  Wie kann ich eine Proxy-Anmeldeinformation für Dell Command | Monitor konfigurieren?

  Wenn Sie sich über Dell Command | Monitor angemeldet haben, können Sie dieselben Zugangsdaten für die Proxy-Authentifizierung verwenden.

- Dell Command | Monitor zeigt die Gewährleistungsinformationen nicht an.
  - Das Client-System ist während der Abfrage nicht mit dem Internet verbunden.

    Stellen Sie eine Internetverbindung her und rufen Sie die Gewährleistungsinformationen ab, indem Sie den folgenden Befehl ausführen: `Get-CimInstance -Namespace root/DCIM/SYSMAN -ClassName DCIM_AssetWarrantyInformation| Where-Object{$_.InstanceID -eq "Root/MainSystemChassis/COOObject/COOWarranty:0"} | Invoke-CimMethod -MethodName RefreshWarranty`
  - Das Client-System ist nicht mit dem Proxyserver konfiguriert.

    Konfigurieren Sie die Proxyeinstellungen in Dell Command | Monitor, indem Sie die folgenden Befehle ausführen:

    - Um Proxy von der WMI abzurufen, führen Sie den Befehl `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting` aus:
    - Um den Proxy über die WMI einzustellen, führen Sie den folgenden Befehl aus: `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ApplicationProxySetting | Invoke-CimMethod -MethodName Change ProxySetting -Arguments @{NewAddress="10.0.0.223"; NewPort="8080"}`

      Sie müssen **NewAddress** und **NewPort** gemäß der Prox-Umgebung ersetzen (falls zutreffend).

9

Schritte zum Troubleshooting bei der Verwendung von Dell Command | Monitor 10.6

Themen:

Remote-Verbindung zu Windows Management Instrumentation kann nicht hergestellt werden

Wenn CIM-Informationen (Gemeinsames Informationsmodell) für ein Remote-Client-Computersystem für die Verwaltungsanwendung nicht zur Verfügung stehen oder wenn eine Remote-BIOS-Erweiterung, die das DCOM (Verteiltes Komponenten-Objektmodell) verwendet, fehlschlägt, werden die folgenden Fehlermeldungen angezeigt:

- **Zugriff verweigert.**
- **Win32: Der RPC-Server ist nicht verfügbar**

1. Stellen Sie sicher, dass das Client-System mit dem Netzwerk verbunden ist. Geben Sie in der Befehlsaufforderung des Servers Folgendes ein:
   `ping <Host Name or IP Address>` und drücken Sie die Eingabetaste `<Enter>`.
2. Wenn sich der Server und das Client-System auf derselben Domäne befinden, führen Sie den folgenden Schritt durch:
   - Überprüfen Sie, ob das Domänenadministratorkonto über Administratorrechte für beide Systeme verfügt.

   Wenn sich der Server und das Client-System in einer Arbeitsgruppe (nicht in derselben Domäne) befinden, führen Sie den folgenden Schritt durch:
   - Stellen Sie sicher, dass auf dem Server die neueste Version von Windows Server ausgeführt wird.

   ANMERKUNG: Sichern Sie Ihre Systemdatendateien, bevor Sie in der Registrierung Änderungen vornehmen. Eine unsachgemäße Bearbeitung der Registrierung, kann dazu führen, dass das Betriebssystem nicht mehr ausgeführt werden kann.
3. Weitere Informationen über die Lizenzierung von Lifecycle Controller-Remote Services finden Sie unter Lizenzierung. Klicken Sie auf **Start** > **Ausführen**, geben Sie anschließend **regedit** ein, und klicken Sie dann auf **OK**. Navigieren Sie im Fenster **Registrierungs-Editor** zu My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.
4. Stellen Sie den Wert **forceguest** auf 0 (Standardwert ist 1). Solange keine Änderung an diesem Wert vorgenommen wird, besitzt der Nutzer, der eine Remote-Verbindung zum System herstellt, nur Gastrechte, selbst wenn die gegebenen Anmeldeinformationen Administratorrechte erteilen.
   a. Erstellen Sie ein Konto auf dem Client-System mit dem gleichen Nutzernamen und Kennwort wie bei einem Administratorkonto auf dem System, auf dem die WMI-Verwaltungsanwendung ausgeführt wird.
   b. Wenn Sie IT Assistant verwenden, führen Sie das Dienstprogramm IT Assistant ConfigServices aus (die Datei configservices.exe im Verzeichnis /bin im Installationsverzeichnis von IT Assistant). Konfigurieren Sie IT Assistant so, dass das Programm unter einem lokalen Administratorkonto ausgeführt wird, das nun ebenfalls ein Administrator auf dem Remote-Client ist. Überprüfen Sie außerdem, ob DCOM und CIM aktiviert sind.
   c. Wenn Sie IT Assistant verwenden, verwenden Sie das Administratorkonto, um die Subnetzermittlung für das Client-System zu konfigurieren. Geben Sie den Nutzernamen im Format <Name Client-Rechner>\<Kontoname> ein. Wenn das System bereits ermittelt wurde, entfernen Sie es aus der Liste der ermittelten Systeme, konfigurieren Sie die Subnetzermittlung für das System und ermitteln Sie es dann erneut.

ANMERKUNG: Dell empfiehlt die Verwendung von Dell OpenManage Essentials als Ersatz für IT Assistant. Weitere Informationen zu Dell OpenManage Essentials finden Sie unter **Dell.com/support**.

5. Führen Sie die folgenden Schritte durch, um Nutzerzugriffsstufen zu ändern, damit eine Remote-Verbindung zur WMI eines Systems hergestellt werden kann:
   a. Klicken Sie auf **Start** > **Ausführen**, geben Sie `compmgmt.msc` ein, und klicken Sie dann auf **OK**.
   b. Wechseln Sie zu **WMI-Steuerung** unter **Dienste und Anwendungen**.
   c. Klicken Sie mit der rechten Maustaste auf **WMI-Steuerung** und dann auf **Eigenschaften**.
   d. Klicken Sie auf das Register **Sicherheit**, und wählen Sie dann **DCIM/SYSMAN** in der **Stamm**struktur aus.
   e. Klicken Sie auf **Sicherheit**.
   f. Wählen Sie die spezifische Gruppe oder den Nutzer aus, bei der/dem Sie den Zugriff steuern möchten, und verwenden Sie das Kästchen **Zulassen** oder **Ablehnen**, um Berechtigungen zu konfigurieren.
6. Führen Sie die folgenden Schritte aus, um eine Verbindung zu einer WMI (root\DCIM\SYSMAN) auf einem System von einem Remote-System mithilfe von WMI CIM Studio herzustellen:
   a. Installieren Sie WMI-Tools zusammen mit wbemtest auf dem lokalen System und installieren Sie dann Dell Command | Monitor auf dem Remote-System.
   b. Konfigurieren Sie die Firewall auf dem System für die WMI-Remote-Konnektivität. Öffnen Sie zum Beispiel die TCP-Ports 135 und 445 in der Windows-Firewall.
   c. Stellen Sie die Einstellung Lokale Sicherheit auf **Klassisch – Lokale Nutzer authentifizieren sich als sie selbst für Netzwerkzugriff: Freigabe und Sicherheitsmodell für lokale Konten** in **Lokale Sicherheitsrichtlinie**.
   d. Verbinden Sie sich mit dem WMI (root\DCIM\SYSMAN) auf dem lokalen System von einem Remote-System mithilfe von WMI wbemtest. Beispiel: \\ Ziel-Remote-System-IP-Adresse]\root\DCIM\SYSMAN
   e. Geben Sie bei Aufforderung die Anmeldeinformationen des Administrators des Ziel-Remote-Systems ein.

   Weitere Informationen zur WMI erhalten Sie in der entsprechenden Microsoft-Dokumentation unter msdn.microsoft.com.

Installationsfehler auf Windows-Systemen

Wenn Sie die Installation von Dell Command | Monitor für Windows nicht abschließen können, stellen Sie Folgendes sicher:

- Sie verfügen über Administratorrechte auf dem Zielsystem.
- Das Zielsystem ist ein von Dell hergestelltes System mit der SMBIOS-Version 2.3 oder höher.
- PowerShell Console darf nicht geöffnet sein.

ANMERKUNG: Zum Prüfen der SMBIOS-Version auf dem Systems gehen Sie zu **Start** > **Ausführen** und führen Sie die Datei `msinfo32.exe` aus. Überprüfen Sie die SMBIOS-Version auf der Seite Systemübersicht.

ANMERKUNG: Das System muss ein unterstütztes Windows-Betriebssystem ausführen.

ANMERKUNG: Das System muss auf die Version .NET 4.0 oder höher aktualisiert werden.

Aufzählwert der BIOS-Einstellung wird als 1 angezeigt

1. Überprüfen Sie, ob die folgenden Pakete mit root-Nutzerberechtigungen installiert sind:
   - omi-1.0.8.ssl_100.x64.rpm
   - srvadmin-hapi-8.3.0-1908.9058.el7.x86_64
   - command_monitor-linux-<version number>-<build number>.x86_64.rpm
2. Wenn die oben genannten Pakete installiert sind, überprüfen Sie, ob das Treibermodul geladen ist.
   a. Zum Überprüfen, ob das Treibermodul geladen ist, führen Sie den folgenden Befehl aus `lsmod | grep dcdbas`.
   b. Wenn das Treibermodul nicht verfügbar ist, rufen Sie die Treiberdetails ab, indem Sie den folgenden Befehl ausführen `modinfo dcdbus`.
   c. Laden Sie das Treibermodul, indem Sie den folgenden Befehl ausführen: `insmod <filename>`.

HAPI-Installation schlägt aufgrund der Abhängigkeit von libsmbios fehl

Wenn die Installation aufgrund von Abhängigkeitsproblemen fehlschlägt,
erzwingen Sie die Installation aller abhängigen Pakete durch Ausführen von `apt-get -f install`.

CIM-Ressourcen nicht verfügbar

Wenn Sie beim Aufzählen eine Fehlermeldung wie „CIM-Ressource nicht verfügbar“ erhalten,
überprüfen Sie, ob die Befehle mit Root-Berechtigungen ausgeführt werden.

Befehle können nicht über DCM auf Systemen mit Ubuntu Core 16 ausgeführt werden

Stellen Sie sicher, dass die Snap-Version auf dem System 2.23 oder höher ist.

10

Weitere nützliche Dokumente

Zusätzlich zu diesem Benutzerhandbuch können Sie auf die folgenden Dokumente unter **dell.com/support** zugreifen. Klicken Sie auf Dell Command | Monitor (vormals OpenManage Client Instrumentation) und klicken Sie anschließend auf die Verknüpfung der jeweiligen Produktversion im Abschnitt **Allgemeiner Support**.

Zusätzlich zu diesem Benutzerhandbuch können Sie auf die folgenden Handbücher zugreifen.

- Das Referenzhandbuch zu Dell Command | Monitor enthält detaillierte Informationen zu allen Klassen, Eigenschaften und deren Beschreibungen.
- Das Installationshandbuch zu Dell Command | Monitor enthält Informationen zur Installation.
- Das SNMP-Referenzhandbuch zu Dell Command | Monitor enthält die SNMP-MIB (Simple Network Management Protocol Management Information Base) für Dell Command | Monitor.

Themen:

Zugriff auf Dokumente der Dell Support Website

Sie können auf Dokumente zugreifen, indem Sie Ihr Produkt auswählen.

1. Rufen Sie die Website www.dell.com/manuals auf.
2. Klicken Sie auf **Alle Produkte Durchsuchen**, klicken Sie auf **Software**und klicken Sie dann auf **Client-Systemverwaltung**.
3. Um die erforderlichen Dokumente anzuzeigen, klicken Sie auf den benötigten Produktnamen und die Versionsnummer.

11

Kontaktaufnahme mit Dell

ANMERKUNG: Wenn Sie über keine aktive Internetverbindung verfügen, so finden Sie Kontaktinformationen auf der Eingangsrechnung, dem Lieferschein, der Rechnung oder im Dell Produktkatalog.

Dell bietet verschiedene Optionen für Online- und Telefonsupport an. Die Verfügbarkeit ist abhängig von Land und Produkt und einige Dienste sind in Ihrem Gebiet möglicherweise nicht verfügbar. So erreichen Sie den Vertrieb, den Technischen Support und den Kundendienst von Dell:

1. Rufen Sie die Website **Dell.com/support** auf.
2. Wählen Sie Ihre Supportkategorie.
3. Wählen Sie das Land bzw. die Region in der Drop-Down-Liste **Land oder Region auswählen** am unteren Seitenrand aus.
4. Klicken Sie je nach Bedarf auf den entsprechenden Service- oder Support-Link.