Dell Command | Monitor Version 9.2
Benutzerhandbuch

Anmerkungen, Vorsichtshinweise und Warnungen

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

VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.

WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

2017 - 01

Rev. A00

Inhaltsverzeichnis

1

Einführung

Die Dell Command | Monitor-Softwareanwendung ermöglicht die Remote-Verwaltung mithilfe von Anwendungsprogrammen für den Zugriff auf die Informationen, die Überwachung des Status oder die Änderung des Zustands des Systems, z. B. das Remote-Herunterfahren des Systems. Dell Command | Monitor verwendet über Standardschnittstellen wichtige Systemparameter, mit denen Administratoren den Bestand verwalten, den Systemzustand überwachen und Informationen zu bereitgestellten Dell-Systemen sammeln. Dell Command | Monitor wurde für Dell Enterprise Client-Systeme, Dell IoT Gateway-Systeme sowie für Dell Embedded PCs entwickelt. Weitere Informationen zu den unterstützten Dell Systemen finden Sie in den Versionshinweisen, die unter **dell.com/dellclientcommandsuitemanuals** verfügbar sind. Dieses Dokument enthält eine Übersicht über Dell Command | Monitor und die zugehörigen Funktionen.

ANMERKUNG: Dell Command | Monitor hieß früher Dell OpenManage Client Instrumentation (OMCI). Ab der OMCI-Version 8.2.1 wird anstelle von OMCI der Markenname Dell Command | Monitor verwendet.

Was ist neu in dieser Version?

- Support für neue Plattformen.
- Unterstützung für neue Betriebssysteme: Embedded Standard 7 Professional (WES7-P), Embedded Standard 7 Enterprise (WES7-E) – Unterstützung nur auf Dell Embedded PCs.
- Unterstützung für Linux-Betriebssysteme: Ubuntu Desktop 16.04 und Red Hat Enterprise Linux 7.0.
- Unterstützung für Anwendungsprotokollfunktion für Systeme, auf denen unterstützte Linux-Betriebssysteme ausgeführt werden.
- Unterstützung für die folgenden neuen BIOS-Einstellungen:
  - Always Allow Dell Docks (Dell Docks immer zulassen)
  - Attempt Legacy Boot (Legacy-Start versuchen)
  - Auto Fan Speed Intensity (Automatische Lüftergeschwindigkeit)
  - Auto OS Recovery Threshold
  - BIOS Auto Recovery (Automatische BIOS-Wiederherstellung)
  - BIOS Connect (BIOS-Verbindung)
  - BIOS Connect Activation (Aktivierung von BIOS-Verbindung)
  - BIOS Integrity Check (BIOS-Integritätsprüfung)
  - CPU RSA (CPU-RSA)
  - dGPU External Display (dGPU – externer Bildschirm)
  - Integrierter Grafikcontroller
  - Fault Tolerant Memory Log Clear (Fehlertolerantes Speicherprotokoll löschen)
  - Full Screen Logo (Vollbildschirmlogo)
  - GPS on WWAN Radio (GPS bei WWAN-Funk)
  - Keyboard Backlight Timeout on AC
  - Keyboard Backlight Timeout on Battery
  - Lid Switch
  - M2 PCIE SSD 0
  - M2 PCIE SSD 1

- Master Password Lockout (Sperrung des Masterkennworts)
- Memory Fault Tolerance Time Limit (Fehlertoleranz-Zeitlimit für Speicher)
- Memory Performance Monitor (Speicherleistungsüberwachung)
- Memory RSA (Speicher – RAS)
- Modern Standby Control (Moderne Standby-Steuerung)
- PCI-Bus
- PCIe RSA (PCIe – RSA)
- Power Off Intel 8260 When Engaging Stealth Mode (Beim Aktivieren des Stealth-Modus Intel 8260 deaktivieren)
- SD Card Boot (SD-Karten-Start)
- Sign of Life Indication (Aktivitätsanzeige)
- Secure Guard Extension (Secure Guard-Erweiterung)
- SFP
- SFP Wake on LAN
- Thunderbolt Boot Support (Thunderbolt-Start-Unterstützung)
- Thunderbolt Pre Boot Module (Thunderbolt-Pre-Boot-Modul)
- Touch Screen (Touchscreen)
- Type-C Battery Overload Protection (Überlastschutz für Typ-C-Akku)
- Uefi Boot Path Security (UEFI-Startpfadsicherheit)
- USB Provision (USB-Bereitstellung)
- Wake on Dock
- XD Card (XD-Karte)

· Unterstützung zusätzlicher Werte für die folgenden unterstützten Attribute:

- CPU Snoop Mode (CPU-Snoop-Modus)
- Secure Guard Extensions (Secure Guard-Erweiterungen)
- Warning And Errors (Warnungen und Fehler)

Weitere Informationen zu Token finden Sie im Referenzhandbuch *Dell Command | Monitor Reference Guide* unter **dell.com/dellclientcommandsuitemanuals**.

Dell Command | Monitor – Überblick

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

Dell Command | Monitor verwaltet Clientsysteme mit dem Standard Common Information Model (CIM) und dem Managementprotokoll Simple Network Management Protocol (SNMP). Dadurch werden die Gesamtbetriebskosten reduziert und die Sicherheit erhöht. Mit einem ganzheitlichen Ansatz werden alle Geräte im Netzwerk verwaltet, einschließlich Clients, Server, Storage-, Netzwerk- und Softwaregeräte.

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

Dell Command | Monitor enthält den zugrunde liegenden Treibersatz, der Clientsystem-Informationen von verschiedenen Quellen sammelt, darunter BIOS, CMOS, System Management BIOS (SMBIOS), System Management Interface (SMI), Betriebssystem und Anwendungsprogrammierschnittstellen (APIs). Dell Command Monitor für Windows sammelt auch Informationen zu Clientsystemen aus der Dynamic Link Library (DLL) 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.

IT-Administratoren können mit Dell Command | Monitor Bestandsinformationen remote erfassen, BIOS-Einstellung ändern, proaktive Benachrichtigungen zu potenziellen Fehlerbedingungen empfangen und Warnungen zu potenziellen Sicherheitsverletzungen erhalten. Auf den Windows-Systemen sind diese Warnungen als Ereignisse im NT-Ereignisprotokoll, WMI-Ereignis oder SNMP traps v1 verfügbar. Auf den 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. Darüber hinaus können Sie für wichtige Bereiche von Interesse benutzerdefinierte Skripte erstellen. Auf der Seite Dell Command | Monitor im Dell TechCenter 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 *Dell Command | Monitor Installationshandbuch* unter dell.com/dellclientcommandsuitemanuals.

2

Funktionen

Wichtigste Funktionen von Dell Command | Monitor:

- Unterstützung des CIM-Schemas
- BIOS-Konfiguration
- WMI/OMI-Sicherheit
- Ereignismeldung
- Herunterfahren im Remote-Zugriff
- Zugriff auf Systeminformationen über das CIM-Schema mit dem WSMAN-Protokoll

  ANMERKUNG: Mit Dell Command | Monitor für Windows ist der Zugriff auf Informationen auch über SNMP möglich.
- Kompilierung von detaillierten Bestandsinformationen
- Remote-Aktivierungs-Konfigurierbarkeit
- Remote-Änderung von Systemeinstellungen
- Überwachen des Systemzustands und Statusbericht
- RAID-Überwachung und -Warnungen für Intel- und LSI-integrierte Controller

  ANMERKUNG: Überwachung von Intel-integrierten Controllern wird für Systeme unter Linux nicht unterstützt.
- SNMP-Überwachung und -Traps nur über Dell Command | Monitor für Windows

Unterstützung des CIM-Schemas

Dell Command | Monitor für Windows entspricht dem CIM 2.17-Schema und umfasst zwei WMI-Anbieter:

- WMI-Indikationsanbieter oder Abfrageagent
- WMI-Instanzen- oder Methodenanbieter

Dell Command | Monitor für Linux entspricht dem CIM 2.32.0-Schema und umfasst zwei WMI-Anbieter:

- WMI-Indikationsanbieter oder Abfrageagent
- WMI-Instanzen- oder Methodenanbieter

Konfiguration und Enumeration von BIOS-Einstellungen

Dell Command | Monitor bietet die Möglichkeit, ein System-BIOS zu konfigurieren.

WMI/OMI-Sicherheit

WMI schützt den Zugriff auf CIM-Daten und -Methoden mithilfe von Benutzerauthentifizierung. Zugriffsrechte werden von DCOM-Sicherheit (Distributed Component Object Model) und CIMOM durchgesetzt. Benutzern werden auf einer Namespace-Basis uneingeschränkte oder eingeschränkte Zugriffsrechte gewährt. Es gibt keine Klassenimplementierung oder Sicherheit auf Eigenschaftsebene. Standardmäßig verfügen Benutzer, die Mitglied der Administratorengruppe sind, über den uneingeschränkten lokalen und Remote-Zugriff auf WMI.

Für Dell Command | Monitor für Windows können Sie WMI-Sicherheit mithilfe der WMI-Steuerung konfigurieren, die in der Verwaltungskonsole des Computers im Abschnitt „Dienste und Anwendungen“ verfügbar sind. Klicken Sie mit der rechten Maustaste

auf **WMI-Steuerung** und dann auf **Eigenschaften**. Auf der Registerkarte **Sicherheit** können Sie Namespace-spezifische Sicherheit konfigurieren. Sie können die **WMI-Steuerung** auch im Menü **Start** oder in der **CLI** aufrufen, indem Sie `wmimgmt.msc` ausführen.

Warnmeldungen

Dell Command | Monitor erkennt Ereignisse auf Dell-Systemen und warnt und informiert den lokalen Benutzer und Netzwerkadministrator über mögliche Ausfälle, Konfigurationsänderungen, Komponentenbestand, integrierte Intel- und LSI-RAID-Controller, Probleme und Gehäuseeingriffe. Diese Ereignisse werden über eine Anwendung zur Systemverwaltung wie OpenManage Essentials (OME) angezeigt.

Herunterfahren im Remote-Zugriff

Dell Command | Monitor für Windows unterstützt das Herunterfahren und Neustarten von Systemen im Remote-Modus.

Zugriff auf Systeminformationen

Dell Command | Monitor ermöglicht den Zugriff auf Systeminformationen wie BIOS-Version, BIOS-Hersteller/-Anbieter, Service-Tag, Systemmodell, Datum des ersten Hochfahrens und Systemmodell über WMI/OMI mit CIM. Zum Zugriff auf diese Informationen über WMI/OMI kann auch das WSMAN-Protokoll verwendet werden.

Detaillierte Bestandsinformationen

Dell Command | Monitor bietet Zugriff auf detaillierte Bestandsinformationen zu Prozessoren, Speicher, PCI-Geräten und Akkus.

Remote-Aktivierungskonfiguration

Dell Command | Monitor unterstützt die Konfiguration von Aktivierungseinstellungen im Remote-Modus. Die Remote-Aktivierung ist eine Funktion des Clientsystems und der Netzwerkkarte (NIC).

Remote-Änderung von System-BIOS-Einstellungen

Dell Command | Monitor bietet Administratoren die Möglichkeit, BIOS-Einstellungen von Business Clients abzurufen und einzustellen, u. a. die USB-Portkonfiguration, und die NIC-Einstellungen.

System-Funktionszustand und -status

Dell Command | Monitor überwacht und meldet den Systemzustand (u. a. Lüfterstatus, Speicher, Temperatur, Probleme, Akku, RAID-Controller, Dockingstation).

RAID-Überwachung und Warnmeldungen für Intel- und LSI-Controller

Bei Dell Command | Monitor für Windows – Überwachung und Warnmeldungen zu den physischen und logischen Laufwerken für Intel- und LSI-RAID-Controller; bei Dell Command | Monitor für Linux – Überwachung und Warnmeldungen nur für LSI-Controller

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

- Intel-integrierte Controller (kompatibel mit CSMI v0.81 oder höher)

  ANMERKUNG: Überwachung von Intel-integrierten Controllern wird für Systeme unter Linux nicht unterstützt.

- LSI-integrierten RAID-Controllern; und 9217, 9271, 9341, 9361 und den zugehörigen Treibern (physischen und logischen)

Im Rahmen der Sensorüberwachung unterstützt Dell Command | Monitor Überwachung und Warnmeldungen für Spannung, Temperatur, Stromstärke, Kühlgeräte (Lüfter) und Gehäusesensoren.

SNMP-Überwachung und -Traps

Dell Command | Monitor für Windows unterstützt mit SNMP v1 die Überwachung von Systemattributen und Traps.

3

Standards und Protokolle

Dell Command | Monitor basiert auf den CIM-Standards. Die CIM-Spezifikation gibt Zuordnungsverfahren für verbesserte Kompatibilität mit Managementprotokollen an.

Für die Remote-Überwachung werden Managementprotokolle wie WMI, SNMP und WSMAN verwendet.

ANMERKUNG: Dell Command | Monitor für Windows nutzt das Simple Network Management Protocol (SNMP) zur Beschreibung verschiedener Systemvariablen.

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 Initiativen für Desktop-, Unternehmens- und Internetumgebungen ist.

4

Benutzerszenarien

Dieses Kapitel beschreibt verschiedene Benutzerszenarien von Dell Command | Monitor.

Sie können Dell Command | Monitor für folgende Zwecke einsetzen:

- Bestandsverwaltung
- Konfigurationsverwaltung
- Überwachung des Akkuzustands
- Profile

Szenario 1: Bestandsverwaltung

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 Microsoft 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 Sammeln der Informationen ist ein umfangreiches Unterfangen. Das Bereitstellen von IT-Mitarbeitern für jedes Clientsystem ist in Hinsicht auf die Arbeitsstunden und Unterbrechungen für die Endbenutzer kostspielig.

Ist Dell Command | Monitor auf allen Dell-Systemen installiert, kann der IT-Manager schnell Informationen per Remote-Zugriff erfassen. Mit Tools wie Microsoft System Center Configuration Manager (SCCM) fragt der IT-Manager jedes Clientsystem über das Netzwerk ab und sammelt Informationen wie CPU-Typ und -Geschwindigkeit, Speichergröße, Festplattenkapazität, BIOS-Version und aktuelle Betriebssystemversion. Die gesammelten Informationen können dann analysiert werden, und zeigen an, welche Systeme auf die neuesten Windows-Versionen aktualisiert werden können.

Über die WSMAN/WinRM-Befehlszeile oder eine beliebige CIM-Clientbefehlszeile können Sie auch Bestandsinformationen abrufen.

SCCM-Integration

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

- Mit der MOF-Datei im Installationspaket von Dell Command | Monitor, das alle Klassen von Dell Command | Monitor enthält und in ConfigMgr importiert

  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: Konfigurationsverwaltung

Ein Unternehmen möchte die Clientplattform 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 im BIOS der einzelnen Client-Computer zu ändern, ohne den Desktop tatsächlich manuell besuchen zu müssen. Wenn Dell Command | Monitor auf den einzelnen Clientsystemen installiert ist, hat

die IT-Abteilung des Unternehmens mehrere Möglichkeiten, die Startreihenfolge im Remote-Modus zu ändern. Die Verwaltungskonsole OpenManage Essentials (OME) kann mit Dell Command | Monitor integriert werden und die BIOS-Einstellungen im Remote-Zugriff auf allen Enterprise-Clientsystemen überwachen. Die IT-Abteilung kann ein Skript (CIM, WinRM/WSMAN/ PowerShell/WMIC) schreiben, das die BIOS-Einstellung ändert. Das Skript kann remote über das Netzwerk an die einzelnen Clientsysteme gesendet und dort ausgeführt werden.

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

Standardisierte Konfigurationen ermöglichen erhebliche Kostenersparnisse für Unternehmen aller Größen. Viele Organisationen stellen standardisierte Clientsysteme bereit, aber nur wenige verwalten die Systemkonfiguration während der gesamten Lebensdauer des Computers. Wenn Dell Command | Monitor auf jedem Clientsystem installiert ist, kann die IT-Abteilung durch Sperren von Legacy-Ports die Nutzung nicht autorisierter Peripheriegeräte verhindern, oder Wake On LAN (WOL) aktivieren, um das System zur Ausführung von Systemverwaltungsaufgaben aus dem Ruhezustand zu holen.

Szenario 3: Überwachung des Funktionszustands

Ein Benutzer erhält Lesefehlermeldungen, wenn er versucht, auf gewisse Dateien auf der Festplatte des Clientsystems zuzugreifen. Der Benutzer startet das System neu, und die Dateien scheinen nun zugreifbar zu sein. Der Benutzer schenkt dem anfänglichen Problem keine Beachtung mehr, da es sich von selbst gelöst zu haben scheint. In der Zwischenzeit fragt Dell Command | Monitor die Festplatte bezüglich des Problems mit dem möglichen Ausfall ab und sendet eine Selbstdiagnose-, Analyse- und Berichtstechnologie (SMART)-Warnung an die Verwaltungskonsole. Zudem wird dem lokalen Benutzer der SMART-Fehler angezeigt. Die Warnmeldung gibt an, dass mehrere Lese-/Schreibfehler auf der Festplatte aufgetreten sind. Die IT-Abteilung des Unternehmens empfiehlt, dass der Benutzer ein Backup der kritischen Datendateien erstellt. Anschließend wird ein Servicetechniker 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 oder CIM-Indikation

Dell Command | Monitor unterstützt die Überwachung von Ereignissen mit den folgenden Verfahren:

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

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

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 schwierigen Anforderungen zu reduzieren und die bereitgestellten Verwaltungsdaten 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/dellclientcommandsuitemanuals**.

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 *Betriebsstatus* und *Akkuzustand* der Klasse **DCIM_Akku** bestimmt werden können.
- Weitere Informationen zum Akkuzustand finden Sie unter der Eigenschaft **DCIM_Sensor.CurrentState** oder der Eigenschaft **CIM_NumericSensor.CurrentState**.

BIOS-Verwaltungsprofil

- Legen Sie die BIOS-Version fest, indem Sie die Instanz der Klasse **DCIM_BIOSElement.** aufzählen.
- Überprüfen Sie, ob der BIOS-Attributwert geändert werden kann oder nicht. Ermitteln Sie die Instanz der Klasse **DCIM_BIOSEnumeration**. Das Attribut kann geändert werden, wenn die Eigenschaft **IsReadOnly** auf FALSCH eingestellt ist.
- Stellen Sie das Systemkennwort (SystemPwd) ein. Führen Sie die Methode **DCIM_BIOSService.SetBIOSAttribute()** aus, und stellen Sie den Parameter „SystemPwd“ auf „AttributeName“ und den Parameter „password value“ auf „AttributeValue“ ein.
- Stellen Sie das BIOS- oder Admin-Kennwort (AdminPwd) ein. Führen Sie die Methode **DCIM_BIOSService.SetBIOSAttribute()** 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.

Startsteuerung

- 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, und stellen Sie den Parameterwert „RequestedState“ auf **3** ein. Schalten Sie das System aus.
- Starten Sie das System neu. Führen Sie die **DCIM_ComputerSystem.RequestStateChange()**-Methode aus, und stellen Sie den Parameterwert **RequestedState** auf **11**.
- 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 **Methode DCIM_TimeService.ManageTime()** 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. Sortieren Sie die Instanzen basierend auf **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.
- Sortieren Sie die Protokolleinträge 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. Sortieren 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

Sie können die Informationen anzeigen von Dell Command | Monitor , indem Sie auf Folgendes zugreifen:

- 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 *Dell Command | Monitor Reference Guide* unter **dell.com/dellclientcommandsuitemanuals**.

Abfrageintervalleinstellungen

Mit Dell Command | Monitor können Sie die folgenden Parameter ändern: Abfrageintervall für Lüftersonde, Temperatursonde, Spannungssonde, Stromsonde, Erhöhung/Verringerung der Festplattenkapazität, Erhöhung/Verringerung der Speichergröße und Erhöhung/Verringerung der Prozessoranzahl.

- Bei Windows-Systemen ist die Datei dcsbdy32.ini oder dcsbdy64.ini unter <Verzeichnis von Dell Command | Monitor>\omsa\ini gespeichert.
- Bei Linux-Systemen ist die Datei AlertPollingSettings.ini unter /opt/dell/dcm/conf gespeichert.

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

RAID-Status-Report

Dell Command | Monitor zeigt RAID-Konfigurationsinformationen und überwacht die RAID-Funktionalität für Clientsysteme mit Hardware- und Treiberunterstützung. Mit RAID-Klassen erhalten Sie detaillierte Informationen zu RAID-Stufen, Treibern, Controllerkonfigurationen und Controllerstatus. Nach der Aktivierung der RAID-Konfiguration können Sie den Empfang von Warnmeldungen konfigurieren, die über Leistungseinbußen oder Laufwerks- und Controllerausfälle informieren.

ANMERKUNG: Die Meldung des RAID-Status wird nur für die RAID-Controller unterstützt, deren Treiber mit CSMI (Common Storage Management Interface), Version 0.81 kompatibel sind. OMCI 8.1 und neuere Versionen unterstützen nur die Überwachung auf dem Intel On-Chip-RAID-Controller; ab der Version OMCI 8.2 werden 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 Clientsystemen wie Notebooks, Desktops und Workstations. Die MIB-Datei (Management Information Base) wird von Dell Command | Monitor und Server Administrator gemeinsam verwendet. Dell Command | Monitor für Windows verwendet ab Version 9.0 eine spezifische Client-OID (10909), mit der Konsolen Clientsysteme identifizieren können.

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

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

Anwendungsprotokoll für Dell Command | Monitor für Linux

Dell Command | Monitor für Linux trennt die Anwendungsprotokolle und Warnungen für Berichterstellungs- und Fehlerbehebungszwecke. Der Verlauf der für die Dell Command | Monitor-Anwendung generierten Warnungen und Protokolle kann in der Datei **dcm_application.log** im Pfad **/opt/dell/dcm/var/log** angezeigt werden.

Konfigurationsdatei

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

ANMERKUNG: Starten Sie den OMI-Server nach den Änderungen in der Konfigurationsdatei neu, um die Änderungen zu übernehmen.

- **Log_Level**: Die Systemmeldungen werden in drei Protokollebenen unterteilt: ERROR, INFO, DEBUG

  Benutzer können die Protokollebene in der Konfigurationsdatei ändern. Ist die Protokollebene DEBUG eingestellt, sendet das Dell Command | Monitor-Anwendungsprotokoll alle Informationen in die angegebene Protokolldatei.

  ANMERKUNG: Die Standardprotokollebene ist INFO.
- **File_Size**: Benutzer können die maximale Größe der Datei **dcm_application.log** festlegen. Die Standarddateigröße ist 500 MB.

  ANMERKUNG: Der Wert für File_Size wird in Byte angegeben.
- **BackupIndex**: Benutzer können die Rollover-Anzahl der Datei **dcm_application.log** festlegen. Bei einer Standardanzahl von 2 überschreibt die dritte Sicherungsdatei die älteste Datei.

Erkennen von Advanced Format-Laufwerken

Clientsysteme werden momentan auf Advanced Format (AF)-Laufwerke umgestellt, damit sie eine größere Speicherkapazität haben und die Einschränkungen mit Festplatten mit 512-Byte-Sektoren (HDDs) behoben werden. Festplatten, die in 4KB-Sektoren umgewandelt werden, bleiben rückwärts kompatibel, während die aktuellen AF-Festplatten, die auch als 512e-Festplatten bekannt sind, mit dem 512-Byte-SATA übereinstimmen und mit 4KB betrieben werden. Während des Übergangs stellen Sie möglicherweise Leistungsprobleme fest, z. B. in Verbindung mit Festplatten mit falsch zugeordneten Partitionen in den Clientsystemen, 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 4KB-AF-Festplatte ist, was es wiederum ermöglicht, diese Probleme zu vermeiden.

Startkonfigurationen

ANMERKUNG: Dell Command | Monitor für Linux bietet keine Startkonfigurationsfunktionen. Daher ist dieser Abschnitt für Dell Command | Monitor für Linux nicht relevant.

Ein Clientsystem kann eine von zwei Arten von Startkonfigurationen aufweisen:

- Legacy (BIOS)
- UEFI

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

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

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

DCIM_BootConfigSetting

Eine Instanz von **DCIM_BootConfigSetting** repräsentiert eine Startkonfiguration, die während des Startvorgangs verwendet wird. Beispiel: Auf Client-Systemen gibt es zwei Typen von Startkonfigurationen – Legacy und UEFI. Daher muss **DCIM_BootConfigSetting** 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 stellt die Startgeräte (oder Quellen) dar. Die Eigenschaften **ElementName**, **BIOSBootString** und **StructuredBootString** enthalten eine Zeichenkette, die die Startgeräte identifizieren. Zum Beispiel: Floppy, Festplatte, CD/DVD, Netzwerk, Personal Computer Memory Card International Association (PCMCIA), Battery Electric Vehicle (BEV) oder USB. Je nach Startlistentyp des Geräts ist eine Instanz von **DCIM_BootSourceSetting** einer der Instanzen von **DCIM_BootConfigSetting** zugewiesen.

DCIM_OrderedComponent

Die **DCIM_OrderedComponent**-Zuordnungsklasse wird dazu verwendet, Instanzen von **DCIM_BootConfigSetting** Instanzen von **DCIM_BootSourceSetting** zuzuordnen, wodurch ein Startlistentyp (Legacy oder UEFI) repräsentiert wird, 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.

Ändern der Systemeinstellungen

Ändern Sie in Dell Command | Monitor mit den folgenden Methoden die Systemeinstellungen und den Zustand der lokalen oder Remote-Systeme:

- **SetBIOSAttributes**: Ändert die BIOS-Einstellung

  ANMERKUNG: Dell Command | Monitor für Linux unterstützt derzeit nur die Methode SetBIOSAttributes.
- **ChangeBootOrder**: Ändert die Startkonfiguration
- **RequestStateChange**: Fährt das System herunter und startet es erneut
- **ManageTime**: Zeigt die Systemzeit an

In Dell Command | Monitor für Windows können Sie diese Methoden mit winrm, dem VB-Skript, Powershell-Befehlen , wmic, und WMI wbemtest ausführen.

Einstellen von BIOS-Attributen auf Windows-Systemen mit Power Shell-Befehlen

Sie können BIOS-Attribute mit der Methode SetBIOSAttributes einstellen. Der Vorgang wird im Folgenden anhand der Beispielaufgabe der Aktivierung des Trusted Platform Module (TPM) erläutert.

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 die TPM-Sicherheit, indem Sie den folgenden Befehl ausführen:

```
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.

Festlegen von BIOS-Attributen auf Linux-Systemen

Sie können die BIOS-Attribute mit einer der folgenden Methoden festlegen:

- OMICLI verwenden
- WinRM verwenden
- WSMan verwenden

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

Festlegen von BIOS-Attributen mit OMICLI

Sie können BIOS-Attribute mit der Methode SetBIOSAttributes einstellen. Der Vorgang wird im Folgenden anhand der Beispielaufgabe der Aktivierung des Trusted Platform Module (TPM) erläutert.
So legen Sie die BIOS-Attribute mit OMICLI-Befehlen fest:

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

So aktivieren Sie das TPM:

1. Um das BIOS-Kennwort festzulegen, 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 "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 aktiveren, 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 Activation" AttributeValue "2"
AuthorizationToken "<password>" }
```

5. Starten Sie das System neu.
6. Um das BIOS-Kennwort zurückzusetzen, 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 "AdminPwd" AttributeValue "" AuthorizationToken "<password>"  }
```

Festlegen von BIOS-Attributen mit WinRM

Sie können BIOS-Attribute mit der Methode SetBIOSAttributes einstellen. Der Vorgang wird im Folgenden anhand der Beispielaufgabe der Aktivierung des Trusted Platform Module (TPM) erläutert.

So stellen Sie BIOS-Attribute mit WinRM-Befehlen ein:

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

1. Rufen Sie das Selector-Set ab, indem Sie die Klasse DCIM_BIOSService enumerieren. Führen Sie den folgenden Befehl aus:

   ```
   winrm e wsman/DCIM_BIOSService?__cimnamespace=root/dcim/sysman -auth:basic -r:https://
   <system IP or system name>:5986 -username:<user name> -password:<password> -skipCAcheck
   -skipCNcheck -encoding:utf-8 -returnType:epr
   ```

   ANMERKUNG: Die Selector-Set-Werte (SystemName=<system name from 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 Set-Vorgang verwendet.

2. Legen Sie das BIOS-Kennwort mithilfe des folgenden Befehls fest, 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 die TPM-Sicherheit, indem Sie den 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

Mithilfe von WSMan können Sie BIOS-Attribute auf den Linux-Systemen festlegen. Der Vorgang wird im Folgenden anhand der Beispielaufgabe der Aktivierung des Trusted Platform Module (TPM) erläutert.
So legen Sie die BIOS-Attribute mit OMICLI-Befehlen in einer PowerShell-Konsole fest:

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

1. Rufen Sie das Selector-Set ab, indem Sie die Klasse DCIM_BIOSService enumerieren. Führen Sie den folgenden Befehl aus:

   ```
   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. Legen Sie das BIOS-Kennwort mithilfe des folgenden Befehls fest, 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 die TPM-Sicherheit, indem Sie den folgenden Befehl 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 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 Startlistentyp unter Verwendung folgender Befehle:
   - **WMIC-Befehl:** `wmic /namespace:\\root\dcim\sysman path dcim_BootConfigSetting get ElementName/format:list`
   - **Power Shell-Befehl:** `Get-CimInstace -Namespace root\dcim\sysman -ClassName DCIM_BootConfigSetting -Property ElementName`
2. Überprüfen Sie den Startreihenfolgetyp (Legacy oder UEFI) unter Verwendung folgender Befehle:
   - **WMIC-Befehl:** `wmic /namespace:\\root\dcim\sysman path dcim_ElementSettingData.IsCurrent=1 get SettingData /format:list`
   - **Power Shell-Befehl:** `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ElementSettingData -Filter "IsCurrent=1" -Property SettingData`
3. Ändern Sie die Startreihenfolge unter Verwendung folgender Befehle:
   - **WMIC-Befehl:** `wmic /namespace:\\root\dcim\sysman path dcim_bootconfigsetting call ChangeBootOrder /?:full`
   - **Power Shell-Befehl:** `Equivalent Command - (Get-CimClass -namespace root\dcim\sysman -ClassName DCIM_Bootconfigsetting).CimClassMethods["ChangeBootOrder"].Parameters`

   Folgende Argumente sind für die ChangeBootOrder-Methode erforderlich:
   - Autorisierungs-Token – Dies ist das Administrator- oder Startkennwort.
   - Source – Dies ist die Startreihenfolgeliste aus der Eigenschaft DCIM_OrderedComponent.PartComponent. Die neue Startreihenfolge richtet sich nach der Reihenfolge der Startgeräte im Array **source**.

Herunterfahren und Neustarten des Windows Systems im Remote-Zugriff

Sie können das Windows-System mit der Methode RequestStateChange remote herunterfahren oder neu starten.

1. Fahren Sie das Windows-System mit dem folgenden Befehl remote herunter:

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

2. Starten Sie das Windows-System mit dem folgenden Befehl remote:

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

Remote-Abruf der Systemzeit auf Windows-Systemen

Mit der Methode ManageTime können Sie den Systemzeitwert für das Windows-System remote abrufen.

Führen Sie an der Befehlsschnittstelle folgenden Befehl aus:

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

6

Lokale Verwaltung von Dell-Clientsystemen

Mit den folgenden Methoden können Sie Dell-Clientsysteme lokal verwalten:

- Für Systeme unter Windows: Verwenden von PowerShell.
- Für Systeme unter Linux: Verwenden von OMICLI.

Lokale Verwaltung von Windows-Systemen mit PowerShell

Mit PowerShell-Befehlen können Sie Dell-Clientsysteme unter Windows lokal verwalten.

- **Enumerieren von Instanzen der Klasse DCIM**
  - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSEnumeration`
  - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSPassword`
- **Abrufen 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 unkritischer Werte**

```
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)
```

Lokale Verwaltung von Linux-Systemen mit OMICLI

Sie können Linux-Systeme lokal mit OMICLI-Befehlen verwalten. Auf den Linux-Systemen ist OMICLI unter **/opt/OMI-/bin** installiert.

- **Enumerieren von Instanzen der Klasse DCIM**
  - `./omicli ei root/dcim/sysman DCIM_BIOSEnumeration`
  - `./omicli ei root/dcim/sysman DCIM_BIOSPassword`
- **Abrufen von Eigenschaften für eine BIOS-Einstellung**

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

- **Einstellen des Administratorkennworts**

```
./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

Remote-Verwaltung von Dell-Clientsystemen

Mit den folgenden Methoden können Sie Dell-Clientsysteme remote verwalten:

- Für Systeme unter Windows: Verwalten von Windows-Systemen per Remote-Zugriff mit PowerShell auf Windows-System
- Für Systeme unter Linux: Verwalten von Linux-Systemen per Remote-Zugriff mit WinRM vom Windows-System

Verwalten von Windows-Systemen per Remote-Zugriff mit PowerShell auf Windows-System

Mit PowerShell können Sie im Remote-Modus von einem Windows-System auf Windows-Systeme zugreifen und sie überwachen.
Voraussetzungen für das Management Windows-System:

- Administratorrechte
- Unterstütztes Windows-Betriebssystempaket ist installiert.
- Konfiguration des Systems ist an Ihre Umgebung angepasst.

Voraussetzungen für das Managed Windows-System:

- Administratorrechte
- Dell Command | Monitor
- Unterstütztes Windows-Betriebssystempaket ist installiert.
- PowerShell-Remote-Funktion ist aktiviert.
- Konfiguration des Systems ist an Ihre Umgebung angepasst.

1. Erstellen Sie eine Sitzung, indem Sie die Befehlsschnittstelle öffnen und den folgenden Befehl ausführen:
   ```
   $session=New-CimSession -ComputerName "<managed system IP or system name>" -Credential <user name>
   ```
2. Geben Sie das Kennwort an.
3. Greifen Sie auf das zu überwachende Windows-System zu, indem Sie folgenden Befehl ausführen:
   ```
   Get-CimInstance -CimSession $session -Namespace root\dcim\sysman -ClassName <class name>
   ```

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

Mithilfe von WinRM-Befehlen können Sie von Microsoft Windows-Systemen auf Linux-Systeme zugreifen und sie überwachen.
Voraussetzungen für das Windows-System

- Root-Zugriffsberechtigungen
- Windows-Betriebssystem wird unterstützt.
- WinRM-Dienste werden ausgeführt.
- Konfiguration des Systems ist an Ihre Umgebung angepasst.

Voraussetzungen für das Linux-System

- Administratorrechte
- Dell Command | Monitor
- Linux-Betriebssystem wird unterstützt.

- Ports 5985 und 5986 sind auf dem PMI-Server aktiviert.
- Konfiguration des Systems ist an Ihre Umgebung angepasst.

Führen Sie an der Befehlsschnittstelle folgenden Befehl 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-Verwaltung von Linux-Systemen über ein Linux-System mit WSMan

Mit WSMan-Befehlen können Sie remote von Linux-Systemen auf Linux-Systeme zugreifen und sie überwachen.
Voraussetzungen für das Management Linux-System:

- Root-Zugriffsberechtigungen
- Unterstütztes Linux-Betriebssystempaket ist installiert.
- wsmancli-Paket ist installiert.

Voraussetzungen für das Managed Linux-System:

- Root-Zugriffsberechtigungen
- Linux-Betriebssystem wird unterstützt.
- Dell Command | Monitor 9.2

Starten Sie einen Terminal, und führen Sie die folgenden Befehle 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

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 Verbindung zum Namespace mit wbemtest wird die Meldung „Anmeldung fehlgeschlagen“ angezeigt. Wie kann ich das Problem verhindern?

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

Wie kann ich TechCenter-Skripts fehlerfrei ausführen?

Die folgenden Voraussetzungen gelten für die Ausführung von VBS-Skripts, die im Techcenter-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 Dell Command | Monitor unter dell.com/dellclientcommandsuitemanuals.

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. Wurde im System ein BIOS-Kennwort festgelegt, wird es im fünften Argument eingegeben. 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)

  ANMERKUNG: Überwachung von Intel-integrierten Controllern wird für Systeme unter Linux nicht unterstützt.
- LSI-integrierten RAID-Controllern; und 9217, 9271, 9341, 9361 und den zugehörigen Treibern (physischen und logischen)

Im Rahmen der Sensorüberwachung unterstützt Dell Command | Monitor Überwachung und Warnmeldungen für Spannung, Temperatur, Stromstärke, Kühlgeräte (Lüfter) und Gehäusesensoren.

Weitere Informationen zu Klasse und Warnfunktion finden Sie im Dell Command | Monitor unter **dell.com/dellclientcommandsuitemanuals**.

Kann Dell Command | Monitor mit anderen Anwendungen/Konsolen integriert werden?

Ja, Dell Command | Monitor verfügt über Schnittstellen mit führenden Unternehmensverwaltungskonsolen, 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.

9

Fehlerbehebung

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. Überprüfen Sie, ob das Clientsystem mit dem Netzwerk verbunden ist. Geben Sie an der Eingabeaufforderung des Servers den folgenden Befehl ein:

   `ping <Host Name or IP Address>` und drücken Sie `<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 folgendenSchritt durch:
   - Stellen Sie sicher, dass auf dem Server die neueste Version von Windows Server ausgeführt wird.

   ANMERKUNG: Sichern Sie Ihre Systemdatendateien, bevor Sie an 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 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** ein (Standardwert ist **1**). Wenn Sie diesen Wert nicht ändern, besitzt der Benutzer, der eine Remote-Verbindung zum System herstellt, nur Gastrechte, selbst wenn aufgrund der gegebenen Anmeldeinformationen Administratorrechte erteilt werden sollten.
   a. Erstellen Sie ein Konto auf dem Client-System mit dem gleichen Benutzernamen 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 (Datei **configservices.exe** im Verzeichnis **/bin** im Installationsverzeichnis des IT Assistant). Konfigurieren Sie IT Assistant so, dass er unter einem lokalen Administratorkonto ausgeführt wird, das nun ebenfalls ein Administrator auf dem Remote-Client ist. Prüfen Sie, ob DCOM und CIM aktiviert sind.
   c. Konfigurieren Sie mit dem Administratorkonto die Subnetzermittlung für das Clientsystem. Geben Sie den Benutzernamen in der Form <*Client-Computername*> \<*Kontoname*> ein. Wurde das System bereits erkannt, entfernen Sie es aus der Liste der erkannten Systeme, konfigurieren Sie die Subnetzermittlung und ermitteln Sie das System 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/dellclientcommandsuitemanuals.
5. Führen Sie die folgenden Schritte durch, um Benutzerzugriffsstufen 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 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 Benutzer 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 von einem Remote-System mit WMI CIM Studio eine Verbindung zu einer WMI (root \DCIM/SYSMAN) auf einem System herzustellen:
   a. Installieren Sie **WMI-Hilfsprogramme** 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 beispielsweise die TCP-Ports 135 und 445 in der Windows-Firewall.
   c. Stellen Sie die Einstellung **Lokale Sicherheit** auf **Klassisch – Lokale Benutzer authentifizieren sich als sie selbst für Netzwerkzugriff: Freigabe und Sicherheitsmodell für lokale Konten** (in **Lokale Sicherheitsrichtlinie**).
   d. Stellen Sie von einem Remote-System mit WMI CIM Studio eine Verbindung mit dem WMI (root/DCIM/SYSMAN) auf dem lokalen System her. Beispielsweise \\ [IP-Adresse Ziel-Remote-System]\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 Systemen unter Windows

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

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

ANMERKUNG: Um die SMBIOS-Version des Systems zu prüfen, navigieren 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 das unterstützte Microsoft Windows-Betriebssystem verwenden.

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

Als Enumerationswert der BIOS-Einstellung wird „1“ angezeigt

1. Prüfen Sie, ob die folgenden Pakete mit Root-Benutzerberechtigungen 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>-<buid number>.x86_64.rpm
2. Sind die obigen Pakete installiert, stellen Sie sicher, dass das Treibermodul geladen ist.
   a. Prüfen Sie, ob das Treibermodul geladen ist, indem Sie den Befehl `lsmod | grep dcdbas` ausführen.
   b. Wenn das Treibermodul nicht verfügbar ist, rufen Sie die Treiberdetails mit dem Befehl `modinfo dcdbus` ab.
   c. Laden Sie das Modul, indem Sie den folgenden Befehl ausführen: `insmod <filename>`.

Fehler bei der Hapi-Installation aufgrund der Abhängigkeit von libsmbios

Falls die Installation aufgrund von Abhängigkeitsproblemen fehlschlägt,

Installieren Sie alle abhängigen Pakete mit force-install: `apt-get –f install`.

CIM-Ressourcen nicht verfügbar

Gehen Sie wie folgt vor, wenn Sie die Fehlermeldung „CIM-Ressource nicht verfügbar“ erhalten:

Stellen Sie sicher, dass die Befehle mit Root-Berechtigungen ausgeführt werden.

10

Kontaktaufnahme mit Dell

ANMERKUNG: Wenn Sie nicht über eine aktive Internetverbindung verfügen, können Sie Kontaktinformationen auch auf Ihrer Auftragsbestätigung, dem Lieferschein, der Rechnung oder im Dell-Produktkatalog finden.

Dell stellt verschiedene onlinebasierte und telefonische Support- und Serviceoptionen bereit. Da die Verfügbarkeit dieser Optionen je nach Land und Produkt variiert, stehen einige Services in Ihrer Region möglicherweise nicht zur Verfügung. 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.

Weitere nützliche Dokumente

Zusätzlich zu diesem Benutzerhandbuch können Sie auf die folgenden Dokumente unter **dell.com/dellclientcommandsuitemanuals** 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**.

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

Zugriff auf Dokumente der Dell Support-Website

Sie können auf eine der folgenden Arten auf die folgenden Dokumente zugreifen:

- Verwendung der folgenden Links:
  - Für alle Enterprise-System-Verwaltungsdokumente – **Dell.com/SoftwareSecurityManuals**
  - Für OpenManage-Dokumente – **Dell.com/OpenManageManuals**
  - Für Remote-Enterprise-System-Verwaltungsdokumente – **Dell.com/esmmanuals**
  - Für Dokumente zu iDRAC und Lifecycle Controller – **Dell.com/idracmanuals**
  - Für OpenManage Connections Enterprise-System-Verwaltungsdokumente – **Dell.com/OMConnectionsEnterpriseSystemsManagement**
  - Für Betriebsfähigkeits-Tools-Dokumente – **Dell.com/ServiceabilityTools**
  - Für Client Command Suite-System-Verwaltungsdokumente – **Dell.com/DellClientCommandSuiteManuals**
- Gehen Sie auf der Dell Support-Website folgendermaßen vor:
  a. Rufen Sie die Website **Dell.com/Support/Home** auf.
  b. Klicken Sie unter **Wählen Sie ein Produkt** auf **Software und Sicherheit**.
  c. Klicken Sie im Gruppenfeld **Software & Sicherheit** auf einen der folgenden Links:

- **Enterprise-Systemverwaltung**
- **Remote Enterprise-Systemverwaltung**
- **Tools für die Betriebsfähigkeit**
- **Dell Client Command Suite**
- **Connections Client-Systemverwaltung**

d. Um ein Dokument anzuzeigen, klicken Sie auf die jeweilige Produktversion.

- Verwendung von Suchmaschinen:
  - Geben Sie den Namen und die Version des Dokuments in das Kästchen „Suchen“ ein.