Dell Command | Monitor Version 9.0
Benutzerhandbuch

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG liefert wichtige Informationen, mit denen Sie den Computer 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.

2014 - 09

Rev. A00

Inhaltsverzeichnis

1

Einführung

Client Instrumentation bezeichnet Softwareanwendungen, welche die Remote-Verwaltung eines Client-Systems ermöglichen. Die Dell Command | Monitor (Command | Monitor)-Softwareanwendung ermöglicht die Remote-Verwaltung mithilfe von Anwendungsprogrammen für den Zugriff auf Unternehmensinformationen auf dem Client-System, die Überwachung des Status oder die Änderung des Zustands des Systems, z. B. das Remote-Herunterfahren des Systems. Command | Monitor verwendet wesentliche Systemparameter über Standardschnittstellen, sodass Administratoren die Möglichkeit haben, den Bestand zu verwalten, den Funktionszustand des Systems zu überwachen und Informationen von bereitgestellten Unternehmens-Client-Systemen abzurufen. 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.

Dell Command | Monitor Übersicht

Command | Monitor verwaltet Client-Systeme, die das Common Information Model-Standard (CIM) und das Simple Network Management Protocol (SNMP) Management-Protokolle werden. Dies reduziert die Gesamtbetriebskosten, verbessert die Sicherheit und bietet einen ganzheitlichen Ansatz zur Verwaltung sämtlicher Geräte, einschließlich Clients, Server, Speicher-, Netzwerk- und Softwaregeräte.

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

OMCI enthält den zugrunde liegenden Treibersatz, der Systeminformationen von verschiedenen Quellen auf dem Client-System sammelt, einschließlich BIOS, CMOS, Systemverwaltungs-BIOS (SMBIOS), Systemverwaltungsschnittstelle (SMI), Betriebssystem, Anwendungsprogrammierschnittstelle (APIs), dynamische Link-Bibliotheken (DLLs) und Registrierungseinstellungen. Command | Monitor ruft diese Informationen durch die CIM Object Manager (CIMOM)-Schnittstelle der Windows Verwaltungs-Instrumentation (WMI)-Stapel oder durch den SNMP-Agenten ab.

Command | Monitor ermöglicht es IT-Administratoren, Bestandsinformationen zu sammeln, CMOS-Einstellungen zu modifizieren und proaktive Benachrichtigungen für Warnungen über potenzielle Fehlerzustände und Warnungen über Sicherheitslücken zu erhalten. Diese Warnungen sind als Ereignisse im Ereignisprotokoll von CIM Indication oder als SNMP-Traps nach dem Importieren der Management Information Base (MIB) -Datei und Überwachung erhältlich.

Command | Monitor wird verwendet, um durch CIM-Implementierung von SNMP-Agenten eine Bestandsaufnahme der Assets von dem System einzuholen, einschließlich der BIOS-Einstellungen. Es kann in eine Konsole wie z.B. den Microsoft System Center Configuration Manager integriert werden, indem direkt auf die CIM-Informationen zugegriffen wird, oder durch andere Konsolenanbieter, die die

Command | Monitor-Integration implementiert haben. Außerdem können Sie benutzerdefinierte Skripten anwenden, um auf wichtige Bereiche von Interesse zu zielen. Sie können diese Skripts zur Überwachung des Bestands, der BIOS-Einstellungen und des Systemzustands verwenden.

ANMERKUNG: Standard-Installation aktiviert die SNMP-Unterstützung nicht. Weitere Informationen zum Aktivieren der SNMP-Unterstützung finden Sie im *Dell Command | Monitor Installation Guide* (Installationshandbuch) unter **dell.com/clientsystemsmanagement**.

Command | Monitor-Architektur

Der Command | Monitor-Datenanbieter sammelt die Systeminformationsdaten und speichert diese Informationen im proprietären XML-Format (Extensible Markup Language). Der Data Manager ist ein Dienst, der diese Anbieter auf Anfrage lädt. Die Command | Monitor CIM-Anbieterschicht abstrahiert die Schnittstelle auf verschiedene CIMOM-Implementierungen. Der Eingangswert ist eine Kombination aus XML- und XSL-Daten (Extensible Stylesheet Language) in proprietärer Form, während der Ausgabewert eine CIM-Objektinstanz ist, die auf Verwaltungsprofilen basiert. Die Daten des CIMOM werden durch WSMAN, welches als Kanalprotokoll dient, angefordert und an die Konsole übertragen.

Die Command | Monitor-Architektur hat mehrere Schichten, die in den Microsoft Windows Management Instrumentation (WMI)-Stapel integriert sind:

- WMI-Anwendungsschicht – Diese Schicht besteht aus Verwaltungsanwendungen, standardbasierten Verwaltungshilfsprogrammen und WMI-Anwendungen, wie z. B. Microsoft SMS, LANDesk und WMI-Tools. Die Anwendungen in dieser Schicht werden von den durch Command | Monitor bereitgestellten Verwaltungsdaten des Systems gespeist. Diese Anwendungen fordern über WSMAN/CIM Object Manager (CIMOM) Client-Informationen an und senden Benachrichtigungen.
- WMI CIM-Anbieter – Ist unterhalb von CIMOM verfügbar und enthält zwei CIM-Anbieter, die am CIMOM angemeldet sind:
  - Der Instanz/Methodenanbieter implementiert eine Schnittstelle, die Hilfsoperationen, wie z.B. Erstellen, Löschen, Ändern und Abfragen ermöglicht.
  - Der Indikationsanbieter implementiert eine Schnittstelle für WMI-Indikationen (oder Ereignisse). Wenn der CIMOM eine Informationsanforderung erhält, leitet er die Anforderung an den entsprechenden Anbieter weiter. Alle Anbieter sind in dieser Schicht vorhanden und geben Auskunft über Systemgeräte. Die Anbieter senden Verwaltungsanwendungs-Aufforderungen vom CIMOM an den Daten-Router.
- Data Manager – Ein Dienst, der basierend auf Anforderungen der oberen Schicht Datenanbieter lädt.
- Datenanbieter – Sammelt Systeminformationen wie Hardware, Treiber und Betriebssystemdaten und speichert diese im proprietären XML-Format.

Die Command | Monitor-Architektur verfügt über mehrere zusätzliche Schichten, die in den SNMP-Stapel integriert sind:

- SNMP-Agent – Zeigt die vom Data Manager empfangenen Daten als SNMP-Tabellen und -Traps an.
- MIB – Die MIB-Dateien enthalten Informationen zu SNMP-Tabellen, deren Attribute und die verfügbaren Traps.

Beispiel: Eine Verwaltungskonsole in der WMI Anwendungsschicht fordert die vorhandenen Prozessorinformationen eines Client-Systems an. Die WMI-Anwendungsschicht stellt die Anforderung über das Netzwerk an die CIMOM des Client-Systems. Der CIMOM gibt die Anforderung an den Command | Monitor CIM-Anbieter und Data Manager weiter. Der Data Manager-Dienst lädt den zugehörigen Datenanbieter, der die Informationen empfängt und in einem proprietären Format speichert.

Die Informationen werden dann (umgekehrt über denselben Pfad) zur Verwaltungskonsole zurückgegeben.

Was ist neu in dieser Version?

- Dell OpenManage Client Instrumentation (OMCI) trägt jetzt den neuen Markennamen Dell Command | Monitor.
- Unterstützung für Überwachung und für Warnmeldungen für LSI-RAID-Controller (Redundant Array of Independent Disks)
- Unterstützung für Überwachung und für Warnmeldungen für alle Sensorensonden
- Legacy-Namespaces **(root/dellomci)** werden nicht unterstützt.
- Unterstützung für neue SNMP-MIB 10909
- Support für die folgenden neuen Token:
  - GPS Radio
  - Tastaturbeleuchtung mit Wechselstrom
  - Kamera auf der Rückseite
  - <Fn>-Lock
  - <Fn>-Lock-Modus
  - Integrierte, nicht verwaltete Netzwerkschnittstellenkarte (NIC)
  - Unmanaged NIC
  - Rear USB Ports (Rückseitige USB-Anschlüsse)
  - Side USB Ports (Seitliche USB-Anschlüsse)
  - Trusted Execution
- Unterstützung für zusätzliche Werte **medium_high** und **medium_high** für **fanspeed**-Token

ANMERKUNG: Legacy-Namespaces und SNMP-MIB 10892 wurden entfernt.

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

Funktionen

Wesentliche Funktionen von Command | Monitor:

- Unterstützung für das CIM 2.17-Schema
- BIOS-Konfiguration
- WMI-Sicherheit
- Ereignismeldung
- Herunterfahren im Remote-Zugriff
- Zugriff auf Systeminformationen unter Verwendung des WMI-CIM Protokolls, WSMAN und SNMP
- Kompilierung von detaillierten Bestandsinformationen
- Remote-Aktivierungs-Konfigurierbarkeit
- Remote-Änderung von Systemeinstellungen
- Überwachen des Systemzustands und Statusbericht
- RAID-Überwachung und Warnmeldungen für Intel- und LSI-Controller

- SNMP-Überwachung und -Traps

Unterstützung für das CIM 2.17-Schema

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

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

BIOS-Konfiguration

Command | Monitor stellt die Möglichkeit zum Durchführen der BIOS-Konfiguration eines Systems bereit, einschließlich der Verwaltung seiner Startreihenfolge.

WMI-Sicherheit

WMI setzt die Benutzerauthentifizierung voraus, bevor der Zugriff auf CIM-Daten und -Methoden gewährt wird. Zugriffsrechte werden von der DCOM-Sicherheit (Distributed Component Object Model) und dem CIMOM erfordert. Zugriff wird Benutzern auf einer Pro-Namespace-Basis entweder uneingeschränkt oder eingeschränkt erteilt. Es ist keine Implementierung von Sicherheit auf Klassen- oder Eigenschaftsebene vorhanden. Standardmäßig besitzen Benutzer, die Mitglied der Administratorengruppe sind, besitzen einen uneingeschränkten lokalen und Remote-Zugriff auf die WMI.

Sie können WMI-Sicherheit mithilfe der WMI-Steuerung konfigurieren, die sich in der Computerverwaltungskonsole im Abschnitt „Dienste und Anwendungen" befindet. Klicken Sie mit der rechten Maustaste auf **WMI-Steuerung**, und klicken Sie anschließend auf **Eigenschaften**. Namespace-spezifische Sicherheit kann im Register **Sicherheit** konfiguriert werden. Sie können die **WMI-Steuerung** auch über das Menü **Start** oder über die **CLI** mithilfe von `wmimgmt.msc` ausführen.

Ereignismeldung

Command | Monitor erkennt Ereignisse auf Dell Systemen und weist den lokalen Benutzer und Netzwerkadministrator auf mögliche Ausfälle, Konfigurationsänderungen und Gehäuseeingriffe hin. Diese Ereignisse werden von einer Systemverwaltungsanwendung, wie z. B. OpenManage Essentials (OME), angezeigt.

Herunterfahren per Remote-Zugriff

Command | Monitor unterstützt das Herunterfahren und Neustarten des Systems per Remote-Zugriff.

Zugriff auf Informationen

Command | Monitor stellt unter Verwendung von CIM den Zugriff auf Systeminformationen bereit, wie z. B. BIOS-Revision und Systemmodell. Das WSMAN-Protokoll kann außerdem für den Zugriff auf diese Informationen durch WMI verwendet werden.

Detaillierte Bestandsinformationen

Command | Monitor stellt den Zugriff auf detaillierte Bestandsinformationen bereit, wie z. B. zu Prozessoren, PCI-Geräten und Akkus.

Remote-Aktivierungskonfiguration

Command | Monitor unterstützt die Konfiguration von Remote-Aktivierungseinstellungen. Die Remote-Aktivierung ist eine Funktion des Client-Systems und der Netzwerkschnittstellenkarte (NIC).

Remote-Änderung von Systemeinstellungen

Command | Monitor gibt IT-Administratoren die Möglichkeit, von Geschäftskunden BIOS-Einstellungen abzurufen und einzustellen, wie z. B. USB-Schnittstellenkonfiguration, Startreihenfolge und NIC-Einstellungen.

System-Funktionszustand und -status

Command | Monitor überwacht den Systemfunktionszustand, wie z. B. den Lüfterstatus, und meldet diesen über NT-Ereignisprotokolleinträge und CIM-Ereignisse.

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

Überwachung und Warnmeldungen für Intel- und LSI-RAID-Controller für die physischen und logischen Festplatten

SNMP-Überwachung und -Traps

Command | Monitor bestätigt gegenüber SNMP V1 und unterstützt die Überwachung von Systemattributen und Traps.

2

Standards und Protokolle

Command | Monitor verwendet Microsoft Windows Management Instrumentation (WMI) und aktiviert Web Services-Management (WSMAN)-Protokolle. Command | Monitor verwendet Simple Network Management Protocol (SNMP), um verschiedene Systemvariablen zu beschreiben.

CIM-, SNMP-, WMI- und WSMAN-Technologie in der Übersicht

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.

CIM

Das CIM, das von der DMTF als Teil der Internet-basierten Unternehmensverwaltungsinitiative (WBEM) erstellt wurde, bietet eine vereinheitlichte Ansicht von physischen und logischen Objekten in der verwalteten Umgebung.

Im Folgenden finden Sie wichtige Informationen zu CIM:

- CIM ist ein objektorientiertes Datenmodell zur Beschreibung von Verwaltungsinformationen. CIM beschreibt die Art, wie die Daten organisiert werden, jedoch nicht unbedingt das Transportmodell zur Übertragung der Daten. Die vorherrschende Transportmethode ist WMI.
- CIM-fähige Verwaltungsanwendungen sammeln Informationen von einer Vielzahl von CIM-Objekten und -Komponenten, einschließlich Client- und Server-Systemen, Netzwerkinfrastrukturgeräten und Anwendungen.
- Die CIM-Spezifikation führt Zuweisungsmethoden für die verbesserte Kompatibilität mit anderen Verwaltungsprotokollen auf.
- Das CIM-Datenmodell fasst alle Elemente in einer Netzwerkumgebung zusammen und beschreibt sie. Das CIM-Schema liefert Beschreibungen über das Datenmodell und teilt das Netzwerk in eine Reihe verwalteter Objekte ein, die zusammenhängen und allgemein klassifiziert sind.
- Das CIM-Schema wird über eine MOF-Datei (Verwaltetes Objektformat) definiert, die ein standardisiertes Modell zur Beschreibung von Verwaltungsinformationen zwischen Clients in einem Verwaltungssystem bietet. Die MOF-Datei ist nicht an eine spezielle Implementierung gebunden; sie ermöglicht den Austausch von Verwaltungsinformationen zwischen verschiedenen Verwaltungssystemen und Clients.

SNMP

Simple Network Management Protocol (SNMP) ist eine allgemein akzeptierte Lösung zur Verwaltung von Geräten auf IP-Netzwerken. SNMP wurde von der Internet Engineering Task Force (IETF) entwickelt und wird von ihr gepflegt. Command | Monitor greift unter Verwendung von SNMP auf Informationen zu und überwacht Client-Systeme. Geräte, die typischerweise SNMP unterstützen, sind unter anderem Router,

Switches, Server, Workstations sowie die Mehrheit der Hardwarekomponenten. SNMP besteht aus einem Standardsatz für Netzwerkverwaltung, einschließlich eines Anwendungsschichtprotokolls, eines Datenbankschemas und eines Satzes von Datenobjekten. SNMP identifiziert Verwaltungsdaten in der Form von Variablen auf den Verwaltungssystemen, welche die Systemkonfiguration beschreiben. Diese Variablen können dann durch Verwaltungsanwendungen abgefragt werden.

SNMP definiert nicht, welche Informationen (welche Variablen) ein Verwaltungssystem bieten sollte. Stattdessen verwendet SNMP ein erweiterbares Design, bei dem die Liste der verfügbaren Infromationen durch Verwaltungsinformationsbasen (MIBs) definiert wird. MIBs beschreiben die Struktur der verwalteten Daten eines Geräts und dessen Untersysteme. MIBs verwenden einen hierarchischen Namespace, der Objektbezeichner (OID) enhält. Jeder OID identifiziert eine Variable, die über SNMP gelesen werden kann.

WMI

WMI ist die Microsoft-Methode zur Implementierung von Webbasierter Unternehmensverwaltung (WBEM). Die WMI ist in Microsoft Windows-Plattformen integriert. WMI unterstützt CIM- und Microsoft-spezifische CIM-Erweiterungen.

WMI enthält:

- Einen leistungsstarken Satz nativer Dienste, wie z.B. das abfragebasierte Einholen von Informationen und Ereignisbenachrichtigung
- Umfassende Scripting-Möglichkeiten über WSH (Windows Scripting Host)
- Den CIMOM, der die Schnittstelle und der Bearbeitungspunkt für CIM-Objekte und -Informationen ist
- Das Repository, in dem CIMOM die Verwaltungsdaten speichert

In der Command | Monitor-Architektur werden CIMOM und das Repository durch den Microsoft WMI Object Manager (WMI-Objektverwaltung) repräsentiert. Der CIMOM ist die Schnittstelle und der Bearbeitungspunkt für CIM-Objekte und -Informationen. Er fungiert als Vermittler, indem er Informationen sammelt und Objekteigenschaften verändert. Microsoft hat diese Komponente als Windows-Verwaltungsdienst (winmgmt) implementiert. Bei CIMOM handelt sich um eine Software-Mittelschicht, die Interaktionen zwischen Verwaltungsanwendungen der höheren Ebene und der Instrumentierung niedrigerer Ebene vermittelt, wie z. B. Command | Monitor und anderer Anbieter ermöglicht. Der CIMOM stellt sicher, dass die vom Anbieter bereitgestellten Daten den Verwaltungsanwendungen auf eine einheitliche und anbieterunabhängige Weise zur Verfügung gestellt werden. Der CIMOM führt diese Aufgaben durch die Verwendung der COM-API (Komponenten-Objektmodell-Anwendungs-Programmierschnittstelle) aus.

Das Repository ist eine binäre Datei, in der CIMOM Verwaltungsdaten speichert. Die Daten enthalten Informationen aus den kompilierten MOF-Dateien (Verwaltetes Objektformat), einschließlich der Definitionen der CIM-Klasse, Eigenschaften, Kennzeichnungen und hierarchischen Beziehungen. Instanzdaten werden, sobald diese verfügbar sind, ebenfalls im Repository gespeichert.

WMI stellt eine Scripting-Schnittstelle zur Verfügung. Unter Verwendung von VBScript oder JScript können Sie Skripts verfassen, lokal oder im Remote-Zugriff eine Verbindung zu WMI-Diensten herstellen, Informationen abrufen oder Methoden ausführen. Sie können die meisten Command | Monitor-Aufgaben als Skripts verfassen, da Command | Monitor über WMI implementiert ist.

Weitere Informationen zu VBScript und Beispiele für Skripts finden Sie im Referenzhandbuch *Dell Command | Monitor Reference Guide* unter **dell.com/clientsystemsmanagement**.

Weitere Informationen zur WMI finden Sie unter **technet.microsoft.com**.

ANMERKUNG: Um eine Remote-Verbindung zu WMI-Diensten herstellen zu können, müssen Sie sowohl auf dem lokalen als auch auf dem Remote-System über Administratorrechte verfügen.

WSMAN

Das WSMAN Protokoll ist ein offener DMTF-Standard, der ein SOAP (Simple Object Access Protocol)-basiertes Protokoll für die Verwaltung von Servern, Geräten, Anwendungen und Webdiensten definiert. Es verwendet Daten des CIMOM, um die Verwaltung zu vereinfachen.

WSMAN ist ein Protokoll, das eine Abstrahierungsschicht für den Zugriff auf die CIM-Informationen zur Verfügung stellt. Hintergrund ist, dass die Konsole WSMAN verwenden kann, um mit bandinternen und bandexternen Systemen zu kommunizieren und Bestandsinformationen zu sammeln, Informationen festzulegen oder Methoden auszuführen. In bandinternen Systemen abstrahiert die WSMAN-Schicht außerdem das unterhalb vorhandene Betriebssystem. Command | Monitor benötigt jedoch WSMAN nicht und Command | Monitor aktiviert WSMAN nicht direkt, da es sich hierbei nur um ein Protokoll handelt.

Weitere Informationen über die Verwaltung von WSMAN über DMTF finden Sie unter **dmtf.org/standards/wsman/**.

Weitere Informationen zum Aktivieren der WSMAN-basierten Verwaltung von WMI auf einem Windows-System finden Sie im Dokument **msdn.microsoft.com/en-us/library/aa384426%28v=VS.85%29.aspx**.

Weitere Informationen zu den DMTF-Profilen, die in Command | Monitor verwendet werden, finden Sie im Referenzhandbuch *Dell Command | Monitor Reference Guide* unter **dell.com/clientsystemsmanagement**.

PowerShell

Windows PowerShell ist ein Microsoft-Framework für die Task-Automatisierung und Konfigurationsverwaltung. PowerShell umfasst eine Befehlszeilen-Shell und eine entsprechende Scripting-Sprache, die auf.NET Framework aufbaut. PowerShell stellt einen uneingeschränkten Zugriff auf COM und WMI bereit und ermöglicht Administratoren dadurch mithilfe der Command | Monitor-Dienste die Ausführung administrativer Tasks, wie z. B. die Konfiguration und Überwachung auf lokalen und auf Remote-Systemen, auf denen das Windows-Betriebssystem ausgeführt wird.

Administratoren können benutzerdefinierte PowerShell-Skripts (Dateien mit der Erweiterung **.ps1**) erstellen, die eine Verbindung zum DCIM-Namespace herstellen und die Überwachung benutzerdefinierter Maßnahmen auf dem System ermöglichen.

3

Systemanforderungen

Dieses Kapitel enthält Informationen zu den Hardware- und Softwareanforderungen für Command | Monitor.

Hardwareanforderungen

Anforderung	Einzelheiten
System	Enterprise Client-System mit SMBIOS 2.3 oder höher.

Softwareanforderungen

Anforderung	Einzelheiten
Unterstütztes Betriebssystem	• Microsoft Windows 8.1 • Microsoft Windows 8 • Microsoft Windows 7 • Microsoft Windows Vista
Unterstütztes Framework	• Microsoft .NET 4.0

4

Benutzerszenarien

Dieses Kapitel beschreibt verschiedene Benutzerszenarien von Command | Monitor.

Sie können Command | Monitor für folgende Zwecke einsetzen:

- Bestandsverwaltung
- Konfigurationsverwaltung
- Überwachung des Funktionszustands
- Profile

Szenario 1: Bestandsverwaltung

Ein Unternehmen, das viele Dell Systeme verwendet, konnte wegen Veränderungen seiner geschäftlichen und IT-Belegschaft keine genauen Bestandsaufnahmendaten führen. 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 den finanziellen Impakt eines solchen Projekts zu bestimmen. Die Sammlung der Informationen ist ein umfangreiches Unterfangen. Die Bereitstellung von IT-Mitarbeitern für jedes Client-System ist teuer in Hinsicht auf die Arbeitsstunden und Unterbrechungen für die Endbenutzer.

Mithilfe von Command | Monitor auf den einzelnen Dell Systemen kann der IT-Manager die benötigten Informationen schnell per Remote-Zugriff sammeln. Mit Hilfsprogrammen, wie Microsoft System Center Configuration Manager (SCCM), fragt der IT-Manager jedes Client-System über das Netzwerk ab und trägt Informationen zusammen, 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 ein Skript oder eine beliebige Windows Management Instrumentation (WMI)-Befehlszeile ermitteln.

SCCM-Integration

Sie können SCCM wie folgt in Command | Monitor integrieren:

- Verwenden der MOF-Datei im Installationspaket von Command | Monitor mit sämtlichen Command | Monitor-Klassen und Importieren nach ConfigMgr

  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 beabsichtigt, die Client-Plattform zu standardisieren und jedes System über seinen Lebenszyklus zu verwalten. Als Teil dieses Unterfangens erwirbt das Unternehmen eine Suite von Hilfsprogrammen, mit der es die automatisierte Bereitstellung eines neuen Client-Betriebssystems unter Verwendung der Preboot Execution Environment (PXE) plant.

Die Schwierigkeit besteht im Ändern der Einstellung für die Startreihenfolge im BIOS der einzelnen Client-Computer, ohne manuell auf die einzelnen Desktop-Computer zugreifen zu müssen. Wenn Command | Monitor auf jedem Client-System installiert ist, hat die IT-Abteilung des Unternehmens mehrere Optionen, die Startreihenfolge per Remote-Zugriff zu ändern. OpenManage Essentials (OME) ist eine Verwaltungskonsole, mit der die BIOS-Einstellungen auf allen Enterprise-Client-Systemen remote überwacht werden können. Eine weitere Möglichkeit ist das Erstellen eines Skripts (VB/PowerShell/ WMIC), das die Einstellung der Startreihenfolge ändert. Das Skript kann remote über das Netzwerk bereitgestellt und auf jedem der Client-Systeme ausgeführt werden.

Weitere Informationen über Command | Monitor finden Sie im Referenzhandbuch *Dell Command | Monitor Reference Guide* unter **dell.com/clientsystemsmanagement**.

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

Szenario 3: Überwachung des Funktionszustands

Ein Benutzer erhält Lesefehlernachrichten, während er versucht, auf gewisse Dateien auf der Festplatte des Client-Systems zuzugreifen. Der Benutzer startet das System neu, und die Dateien scheinen nun zugreifbar zu sein. Der Benutzer schenkt dem anfänglichen Problem keine Beachtung, denn es scheint sich von selbst gelöst zu haben. Inzwischen fragt Command | Monitor die Festplatte mit dem Problem und dem vorhergesagten Ausfall ab und sendet eine SMART (Self-Monitoring, Analysis and Reporting Technology)-Warnung an die Verwaltungskonsole. Sie zeigt den SMART-Fehler auch für den lokalen Benutzer an. Die Warnung gibt an, dass mehrere Lese-/Schreibfehler auf der Festplatte aufgetreten sind. Die IT-Abteilung des Unternehmens empfiehlt, dass der Benutzer sofort ein Backup der kritischen Datendateien erstellt. Ein Techniker mit einem Ersatzlaufwerk wird 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.

Überwachen von Systemereignissen über Windows-Ereignisanzeige oder CIM-Indikation

Command | Monitor unterstützt die Überwachung von Ereignissen über folgende Verfahren:

- Ziehen des Protokolls durch WMI-Klasse **DCIM_LogEntry**.
- Überwachen der CIM-Indikation durch **DCIM_AlertIndication**-Klasse.

- Verwalten von Ereignissen durch einfaches Netzwerkverwaltungsprotokoll (SNMP, Simple Network Management Protocol).

Weitere Informationen über Command | Monitor finden Sie im Referenzhandbuch *Dell Command | Monitor Reference Guide* unter **dell.com/clientsystemsmanagement**.

Szenario 4: Profile

IT-Administratoren sind mit der Verwaltung von Client-Systemen in Umgebungen mit mehreren Anbietern und verteilten Unternehmen betraut. Die Herausforderung besteht darin, dass sie sich mit verschiedenen Hilfsprogrammen und Anwendungen auskennen müssen, um mehrere Desktop- und mobile Client-Systeme in verschiedenen Netzwerken zu verwalten. Um die Kosten für die Erfüllung dieser Anforderungen zu senken und die vorhandenen Verwaltungsdaten darzustellen, werden die DMTF- und DCIM-OEM-Profile des Branchenstandards in Command | Monitor implementiert. Einige der DMTF-Profile werden in diesem Handbuch erläutert.

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

Batterieprofil

- Bestimmen Sie den Status der Batterie, indem Sie die Instanz der Klasse **DCIM_Batterie** aufzählen/ ermitteln.
- Bestimmen Sie die geschätzte Laufzeit und sehen Sie die geschätzte verbleibende Ladung.
- Überprüfen Sie, ob die Funktionszustandsdaten der Batterie unter Verwendung der Eigenschaften *Betriebsstatus* und *Funktionszustand* der Klasse **DCIM_Batterie** bestimmt werden können.
- Ermitteln Sie zusätzliche Informationen über den Funktionszustand der Batterie, indem Sie die Eigenschaft **DCIM_Sensor.CurrentState** oder die Eigenschaft **CIM_NumericSensor.CurrentState** verwenden.

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, falls 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

Hier können Sie die Informationen anzeigen, die Command | Monitor bereitstellt:

- root\dcim\sysman (Standard)

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

Weitere Informationen über die Klassen finden Sie im Referenzhandbuch *Dell Command | Monitor Reference Guide* unter **dell.com/clientsystemsmanagement**.

Abfrageintervalleinstellungen

Sie können das Abfrageintervall für die Lüftersonde, Temperatursonde, Spannungssonde, Stromsonde, Festplattenkapazitätserhöhung/-verringerung, Speichergrößenerhöhung/-verringerung und Prozessoranzahlerhöhung/-verringerung mithilfe der Dateien **dcsbdy32.ini** oder **dcsbdy64.ini** ändern. Die Datei **dcsbdy32/64.ini** befindet sich an folgendem Speicherort:

<Command | Monitor installed location>\omsa\ini

ANMERKUNG: Die Zahlen in der .ini-Datei sind Mehrfache von **23**. Das Standard-Abfrageintervall für die Festplattenkapazität und 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

Command | Monitor aktiviert die RAID-Konfigurationsinformationen und überwacht die RAID-Funktionalität für Client-Systeme mit Hardware- und Treibersupport. Sie können RAID-Klassen verwenden, um die Details über RAID-Stufen, Treiberinformationen, die Controller-Konfiguration und den Controller-Status zu erhalten. Wenn die RAID-Konfiguration aktiviert ist, können Sie Warnungen über Leistungsherabsetzungen oder Laufwerks- und Controllerausfälle erhalten.

ANMERKUNG: Der RAID-Status-Report wird nur für RAID-Controller, die auf Treibern, die mit Common Storage Management Interface (CSMI) Version 0.81 kompatibel sind, unterstützt. Ab OMCI 8.1 wird nur die Überwachung auf dem Intel On-Chip-RAID-Controller unterstützt. Ab OMCI 8.2 werden Warnmeldungen für Intel On-Chip-RAID-Controller unterstützt. Ab Command | Monitor 9.0 wird außerdem die Überwachungs- und Warnfunktion für den LSI-Controller unterstützt.

Überwachen der Client-Systeme

Command | Monitor unterstützt das Simple Network Management Protocol (SNMP)) zur Überwachung und Verwaltung von Client-Systemen wie Notebooks, Desktops und Workstations. Die MIB-Datei

(Management Information Base) wird von Command | Monitor und Server Administrator gemeinsam verwendet.

Command | Monitor verwendet ab Version 9.0 eine spezifische Client-OID (10909), mit der Konsolen Client-Systeme identifizieren können.

Weitere Informationen über SNMP finden Sie im Referenzhandbuch *Dell Command | Monitor SNMP Reference Guide* unter **dell.com/clientsystemsmanagement**.

Erkennen von Advanced Format-Laufwerken

Client-Systeme 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 Client-Systemen, was dazu führt, dass sektorbasierte Verschlüsselungssoftwarepakete, die 512e-Festplatten handhaben, ausfallen. Command | Monitor ermöglicht Ihnen, festzustellen, ob die Festplatte auf einem System eine 4KB-AF-Festplatte ist, was es wiederum ermöglicht, diese Probleme zu verhindern.

Startkonfigurationen

Ein Client-System kann zwei Startkonfigurationen haben:

- Legacy (BIOS)
- UEFI

In Dell Command | Monitor wird die Startkonfiguration (Legacy oder UEFI) mithilfe der 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 Startsequenz mithilfe der ChangeBootOrder-Methode

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`
   - PowerShell-Befehl: `gwmi –namespace root\dcim\sysman -class 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`
   - PowerShell-Befehl: `gwmi –namespace root\dcim\sysman -class 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`
   - PowerShell-Befehl: `(gwmi –namespace root\dcim\sysman -class dcim_bootconfigsetting).getmethodparameters("ChangeBootOrder")`

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

Einstellen der BIOS-Attribute

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

- **SetBIOSAttributes** – Zum Ändern der BIOS-Einstellung
- **ChangeBootOrder** – Zum Ändern der Startkonfiguration
- **RequestStateChange** – Zum Herunterfahren und Neustarten des Systems
- **ManageTime** – Gibt die Systemzeit wieder

Sie können diese Methoden unter Verwendung von winrm, dem VB-Skript, Powershell-Befehlen, wmic, wbemtest.exe und WMI CIM Studio ausführen.

Sie können BIOS-Attribute unter Verwendung der SetBIOSAttributes-Methode einstellen. 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 aktivieren Sie das TPM:

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

   ```
   (gwmi -Class DCIM_BIOSService -Namespace root\dcim
   \sysman).SetBIOSAttributes($null,$null,"AdminPwd","enter a new password")
   ```

2. Aktivieren Sie die TPM-Sicherheit mit dem folgenden Befehl, und starten Sie das System anschließend neu:

   ```
   (gwmi -Class DCIM_BIOSService -Namespace root\dcim
   \sysman).SetBIOSAttributes($null,$null,"Trusted Platform
   Module","1","provide the password")
   ```

3. Aktivieren Sie das TPM mit dem folgenden Befehl, und führen Sie einen weiteren Neustart des Systems durch:

   ```
   (gwmi -Class DCIM_BIOSService -Namespace root\dcim
   \sysman).SetBIOSAttributes($null,$null,"Trusted Platform Module
   Activation","2","provide the password")
   ```

4. Starten Sie das System neu.

   ANMERKUNG: Verwenden Sie PowerShell mit Administratorrechten.

6

Häufig gestellte Fragen

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

Wenn einer **DCIM_BootConfigSetting**-Instanz (Legacy oder UEFI) mehrere **DCIM_BootSourceSetting**-Instanzen (Startgeräte) durch Instanzen der **DCIM_OrderedComponent**-Zuordnung zugeordnet sind, wird der Wert der Eigenschaft **DCIM_OrderedComponent.AssignedSequence** dazu verwendet, die Reihenfolge festzulegen, in der die zugeordneten **DCIM_BootSourceSetting**-Instanzen (Startgeräte) im Startvorgang verwendet werden. Ein **DCIM_BootSourceSetting**, deren zugeordnete **CIM_OrderedComponent.AssignedSequence**-Eigenschaft gleich **0** ist, wird ignoriert und nicht als Teil der Startreihenfolge betrachtet.

Wie ändere ich die Startreihenfolge?

Die Startreihenfolge kann mithilfe der Methode **DCIM_BootConfigSetting.ChangeBootOrder()** geändert werden. Die Methode **ChangeBootOrder()** stellt die Reihenfolge ein, in der die Instanzen von **DCIM_BootSourceSetting** einer **DCIM_BootConfigSetting**-Instanz zugeordnet 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_BootSourceSetting**-Instanzen (Startgeräten) und einer **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. Wie kann ich dies vermeiden?

Starten Sie **wbemtest** mit Administratorrechten, um Anmeldungsmeldungen zu umgehen. Machen Sie Internet Explorer in der Liste **Alle Programme** ausfinding, und 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?

Nachfolgend sind die Voraussetzungen aufgeführt, die zur Ausführung von VBS-Skripts im Command | Monitor-Techcenterlink erfüllt sein müssen:

1. Konfigurieren Sie **winrm** unter Verwendung des Befehls `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.

Wie stelle ich die BIOS-Attribute ein?

BIOS-Attribute können unter Verwendung der Methode **DCIM_BootService.SetBIOSAttributes()** geändert werden. Die Methode **SetBIOSAttributes()** stellt den Wert der Instanz ein, die in der Klasse **DCIM_BIOSEnumeration** definiert wird. Diese Methode hat sieben Eingabeparameter. Die ersten zwei Parameter können leer oder null sein. Der dritte Parameter **AttributeName** muss die Eingabezuweisung auf den Wert der AttributeName-Instanz der Klasse **DCIM_BIOSEnumeration** setzen. Der vierte Parameter **AttributeValue** kann ein beliebiger Wert von Attribute-Name sein, der in der Klasse **DCIM_BIOSEnumeration** definiert ist. Wenn das BIOS-Kennwort auf dem System eingestellt ist, dann müssen Sie es im fünften Argument eingeben. Das sechste und siebte Argument kann wieder leer oder null sein.

7

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 Client-System an das Netzwerk angeschlossen ist. Geben Sie an der Befehlsaufforderung des Servers Folgendes ein:

   `ping <Host Name or IP Address>`, und drücken Sie auf `<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 in der Registrierung Änderungen vornehmen. Eine unsachgemäße Bearbeitung der Registrierung kann dazu führen, dass das Betriebssystem nicht mehr ausgeführt werden kann.
3. Um eine Änderung der Registrierung auf dem Client-System vorzunehmen, klicken Sie auf **Start** → **Ausführen**, geben Sie anschließend **regedit** ein, und klicken Sie auf **OK**. Navigieren Sie im Fenster **Registrierungs-Editor** zu Arbeitsplatz\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 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 (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 werden kann, 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, benutzen Sie das Administratorkonto, um die Subnetzermittlung für das Client-System zu konfigurieren. Geben Sie den Benutzernamen im Format <*Name Client-Rechner*>\<*Kontoname*> ein. Wenn das System bereits ermittelt wurde, entfernen Sie es aus der Liste ermittelter 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 OpenManage Essentials finden Sie unter **dell.com/clientsystemsmanagement**.

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 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-Hilfsprogramme** zusammen mit **wbemtest** auf dem lokalen System und installieren Sie dann Dell Command | Monitor auf dem Remote-System.
   b. Konfigurieren Sie die Firewall für die WMI-Remote-Konnektivität. Öffnen Sie zum Beispiel die TCP-Schnittstellen 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 eine Verbindung zur WMI (**root\DCIM/SYSMAN**) auf dem lokalen System von einem Remote-System mithilfe von WMI wbemtest her. 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**.

Fehlschlagen der Installation

If you are unable to complete Dell Command | Monitor installation, ensure that:

- You have Administrator privilages on the target system.
- The target system is a Dell manufactured system with SMBIOS version 2.3 or later.

ANMERKUNG: To check the SMBIOS version on the system, go to **Start** → **Run** and run the **msinfo32.exe** file and check for the SMBIOS version in System Summary page.

ANMERKUNG: The system must be running supported Microsoft Windows operating system.

ANMERKUNG: The sytsem has to be upgraded to .NET 4.0 or later versions.

8

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/clientsystemsmanagement** zugreifen. Klicken Sie auf Command Monitor (ehemals OpenManage Client Instrumentation), und klicken Sie dann im Bereich **Allgemeiner Support** auf den Link der jeweiligen Produktversion.

- Das Referenzhandbuch *Dell Command | Monitor Reference Guide* enthält detaillierte Informationen zu allen Client Instrumentationsklassen, -eigenschaften und deren Beschreibungen.
- Im Installationshandbuch *Dell Command | Monitor Installation Guide* finden Sie Informationen zum Installieren von Client Instrumentation.
- 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 Enerprise Systems Management-Dokumente – **dell.com/softwaresecuritymanuals**
  - Für Enterprise Systems Management-Dokumente – **dell.com/openmanagemanuals**
  - Für Remote Enterprise Systems Management-Dokumente – **dell.com/esmmanuals**
  - Für OpenManage Connections Enterprise Systems Management-Dokumente – **dell.com/OMConnectionsEnterpriseSystemsManagement**
  - Für Tools für die Betriebsfähigkeitsdokumente – **dell.com/serviceabilitytools**

- Für Client Systems Management-Dokumente – **dell.com/clientsystemsmanagement**
- Für OpenManage Connections Client Systems Management-Dokumente – **dell.com/connectionsclientsystemsmanagement**

- Gehen Sie auf der Dell Support-Website folgendermaßen vor:

  a. Rufen Sie die Website **dell.com/support/home** auf.

  b. Klicken Sie unter **Allgemeiner Support** auf **Software & Sicherheit**.

  c. Klicken Sie im Gruppenfeld **Software & Sicherheit** auf einen der folgenden Links:
     - **Enterprise Systems Management**
     - **Remote Enterprise Systems Management**
     - **Tools für die Betriebsfähigkeit**
     - **Client Systems Management**
     - **Connections Client Systems Management**

  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.