Dell Command | Monitor バージョン 10.4

ユーザーズガイド

December 2020
Rev. A00

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その危険を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

目次

1

Dell Command | Monitor 10.4 の概要

Dell Command | Monitor ソフトウェア アプリケーションにより、IT 管理者は、導入された Dell クライアント システムに関するフリート インベントリーの管理、システム正常性の監視、BIOS 設定の変更、リモートからの情報収集を簡単に行うことができます。

アクティブなシステム正常性の監視機能は、すべてのネットワーク デバイスの総合的な管理機能の一部で、システムの総所有コストを削減に有効です。

Dell Command | Monitor は、Dell Enterprise クライアント システム、Dell IoT Gateway システム、Dell Embedded PC 向けに設計されています。

このドキュメントでは、Dell Command | Monitor とその機能の概要を説明します。サポート対象の Dell システムについては、**dell.com/dellclientcommandsuitemanuals** にあるリリース ノートを参照してください。

トピック：

本リリースの新機能：Dell Command | Monitor 10.4

次の新しい BIOS 属性のサポート：

- Thermal Management
- Microcode Update Support
- Disable Password Jumper
- Nvme Password Feature
- Allow Non-Admin PSID Revert
- Enable Hybrid Graphics
- PCIe Bifurcation
- HTTP(s) Boot Feature
- HTTP(s) Boot Mode
- Device Configuration Hotkey Access
- Power Button Override
- Disable USB4 PCIE Tunneling
- TME Enable
- Video/Power only on Type-C Ports
- Type-C Dock Override
- Safe Shutter

Dell Command | Monitor の概要

メモ: Dell Command | Monitor for Linux では、Simple Network Management Protocol（SNMP）はサポートされません。

Dell Command | Monitor では、管理プロトコルである Common Information Model（CIM）標準および Simple Network Management Protocol（SNMP）を使用してクライアント システムを管理します。システムの総所有コストが削減され、セキュリティが向上するとともに、ネットワーク デバイス内のすべてのデバイスを総合的に管理することができます。

CIM を使用することにより、Web Services for Management Standards（WSMAN）を介して Dell Command | Monitor にアクセスすることができます。

Dell Command | Monitor には、BIOS、CMOS、システム管理 BIOS（SMBIOS）、システム管理インターフェイス（SMI）、オペレーティング システム、アプリケーション プログラミング インターフェイス（API）などのさまざまなソースからクライアント システム情報を収集する、基礎となるドライバー セットが含まれています。Dell Command | Monitor for Windows は、ダイナミックリンク ライブラリー（DLL）とレジストリー設定からもクライアント システム情報を収集します。Dell Command | Monitor for Windows は、

CIM オブジェクト マネージャー (CIMOM) インターフェイス、Windows Management Instrumentation (WMI) スタック、または SNMP エージェントを経由してこうした情報を入手します。一方で Dell Command | Monitor for Linux は、Open Management Infrastructure (OMI) インターフェイスを介してこれらの情報を入手します。

Dell Command | Monitor では、IT 管理者が、資産情報の収集、BIOS 設定の変更、潜在的な障害条件に関する事前通知の受信、および潜在的なセキュリティ侵害に関するアラートの受信がリモートで行えるようになります。Windows を実行しているシステムでは、これらのアラートは、NT イベントログのイベント、WMI イベント、または SNMP トラップ v1 として利用できます。Linux を実行しているシステムでは、これらのアラートは、Syslog、OMI イベント、またはアプリケーション ログとして受信できます。

Dell Command | Monitor for Windows は、CIM 情報に直接アクセスすることによって、または Dell Command | Monitor 統合を実装している他のコンソール ベンダーを介して、Microsoft System Center Configuration Manager などのコンソールに統合できます。また、カスタム スクリプトを作成して、重要な関心領域にターゲットを絞ることもできます。サンプル スクリプトについては、Dell Knowledge Library の Dell Command | Monitor ページを参照してください。これらのスクリプトを使用して、インベントリ、BIOS 設定、およびシステム正常性を監視できます。

メモ: デフォルトインストールは SNMP サポートを有効化しません。Dell Command | Monitor for Windows の SNMP サポートを有効にする方法の詳細については、**dell.com/dellclientcommandsuitemanuals** にある『Dell Command | Monitor インストール ガイド』を参照してください。

メモ: デフォルトインストールは SNMP サポートを有効化しません。Dell Command | Monitor for Windows の SNMP サポートを有効にする方法の詳細については、『Dell Command | Monitor インストール ガイド』を参照してください。

2

Windows SMM Security Mitigations Table（WSMT）準拠

Windows（SMM）Security Mitigations Table には、Windows オペレーティングシステム用に作成された ACPI テーブルについての情報が記載されています。ACPI テーブルは、Windows 仮想化ベースセキュリティ（VBS）機能をサポートします。Dell Command | Monitor は WSMT に対応しています。WSMT 対応 BIOS 搭載の Dell クライアント システムでプラットフォーム機能を設定する場合に使用します。

WSMT 準拠により変更になった動作は、次のとおりです。

WMI/ACPI をサポートする互換性のあるバージョンの BIOS を搭載した Dell クライアント プラットフォームで、Dell Command | Monitor の機能を使用できます。

3

Dell Command | Monitor 10.4 の標準およびプロトコル

Dell Command | Monitor は、CIM 標準に基づいています。CIM 仕様は、管理プロトコルとの互換性を向上させるために、マッピング技法について詳しく定めています。

WMI、SNMP、WSMAN などの管理プロトコルは、リモート監視に使用されます。

メモ: Dell Command | Monitor for Windows は、シンプルネットワーク管理プロトコル（SNMP）を使用して、システムの一部の変数を記述します。

Desktop Management Task Force（DMTF）は、管理標準（CIM および ASF を含む）の開発、採用、統一、ならびにデスクトップ、エンタープライズ、インターネット諸環境に関するイニシアチブを先導周知する標準団体です。

4

Dell Command | Monitor 10.4 を使用したユース ケース シナリオ

本章では、Dell Command | Monitor のさまざまなユース ケース シナリオについて説明します。

Dell Command | Monitor を使用して次のことを行うことができます。

- 資産管理
- 設定管理
- 正常性監視
- プロファイル

トピック：

シナリオ 1：資産管理

多数の Dell システムを所有しているある企業が、業務および IT スタッフの変更により、正確なインベントリー情報を保存していませんでした。CIO (最高情報責任者) は、Windows の最新バージョンにアップグレードできるシステムを決定するための計画を要求しています。これには、導入されているシステムのアセスメントを実施して、このようなプロジェクトのサイズ、範囲、財務面への影響を判断する必要があります。情報の収集には、かなりの努力が伴います。各クライアント システムへの IT スタッフの導入には、労働時間とエンドユーザーによる中断のために、高いコストがかかります。

各 Dell システムに Dell Command | Monitor を使用すれば、IT マネージャーはリモートに情報を迅速に収集することができます。Microsoft System Center Configuration Manager (SCCM) などのツールを使用して、各クライアント システムをネットワーク経由で照会し、CPU のタイプと速度、メモリー サイズ、ハード ドライブ容量、BIOS バージョン、および現在のオペレーティング システムなどの情報を収集します。収集した情報を解析すれば、Windows の最新バージョンにアップグレードできるシステムを特定することができます。

WSMAN/WinRM コマンド ラインまたは任意の CIM クライアント コマンド ラインを使用して、資産のインベントリーを取得することもできます。

SCCM 統合

SCCM は、次の方法で Dell Command | Monitor for Windows に統合することができます。

- すべての Dell Command | Monitor のクラスが含まれる Dell Command | Monitor インストール パッケージ内の MOF ファイルを使用して、ConfigMgr にインポートする

  MOF ファイルは次の場所にあります：

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

- コレクションを使用して資産報告機能を拡張する

シナリオ 2：設定管理

ある企業が、クライアントプラットフォームを標準化し、各システムをそのライフサイクルを通じて管理することを計画しています。その一環として、ツール一式を購入し、PXE ブート環境を使用して、新しいクライアント オペレーティング システムの導入を自動化する予定です。

ここでの課題は、デスクトップに直接アクセスすることなく、各クライアント システムの BIOS パスワードを変更することです。各クライアント システムに Dell Command | Monitor をインストールすると、企業の IT 部門はリモートに起動順序を変更する複数のオプションを利用できます。OpenManage Essentials (OME) は、Dell Command | Monitor に統合可能な管理コンソールで、すべてのクライアント システム上の BIOS 設定をリモートに監視できます。また、スクリプト (CIM、WinRM/WSMAN/PowerShell/WMIC) を記述して、BIOS 設定を変更することもできます。スクリプトはネットワーク経由でリモート配信して、各クライアント システム上で実行できます。

Dell Command | Monitor の詳細については、**dell.com/dellclientcommandsuitemanuals** で『Dell Command | Monitor リファレンス ガイド』を参照してください。

Dell Command | Monitor の詳細については、『Dell Command | Monitor リファレンス ガイド』を参照してください。

設定の標準化により、企業規模の大小によらず、大幅にコストを削減できます。多くの組織が標準化されたクライアントシステムを導入していますが、コンピュータの寿命の全期間にわたってシステム設定を管理している組織はほとんどありません。Dell Command | Monitor を各クライアントシステムにインストールすることによって、IT 部門は未承認の周辺機器の使用を防止するためにレガシー ポートをロックダウンする、または非ピーク時間にシステムをスリープ状態から回復させるために Wake On LAN (WOL) を有効化してシステム管理タスクを実行することができます。

シナリオ 3：正常性監視

クライアント システムのハード ドライブ上の特定のファイルにアクセスしようとすると、読み取りエラー メッセージが発生します。システムを再起動すると、ファイルがアクセス可能であるように見えます。最初の問題が解決されているようなので、無視します。その間、Dell Command | Monitor は、予測される障害に対してハード ドライブのクエリーを実行して、管理コンソールに Self-Monitoring、Analysis and Reporting Technology (SMART) アラートを送信します。また、SMART エラーがローカル ユーザーに表示されます。アラートは、ハード ドライブ内で複数の読み取り/書き込みエラーが発生していることを示しました。企業の IT 部門は、重要なデータ ファイルを直ちにバックアップするよう推奨しました。サービス技術者が交換用ドライブと共に派遣されます。

ハード ドライブは故障する前に交換されるため、ユーザーのダウンタイムを防ぎ、ヘルプ デスクへの電話連絡や技術者がデスクトップの元に赴いて問題を診断する手間を省くことができます。

オペレーティングシステムの Event Viewer/Syslog/CIM インディケーションによるシステムアラートの監視

Dell Command | Monitor は、次の手順によるイベントの監視をサポートします。

- CIM クラス DCIM_LogEntry 経由のログの取得
- DCIM_AlertIndication クラス経由の CIM インディケーションの監視
- (Dell Command | Monitor for Windows のみ) Simple Network Management Protocol (SNMP) および Windows Event Viewer によるイベントの監視
- (Dell Command | Monitor for Linux のみ) Syslog によるイベントの監視

Dell Command | Monitor の詳細については、**dell.com/dellclientcommandsuitemanuals** で『Dell Command | Monitor リファレンス ガイド』を参照してください。

Dell Command | Monitor の詳細については、『Dell Command | Monitor リファレンス ガイド』を参照してください。

シナリオ 4：プロファイル

メモ: DMTF プロファイルは、Dell Command | Monitor for Windows でのみ実装されています。

IT 管理者は、マルチベンダーかつ分散型のエンタープライズ環境でクライアントシステムを管理する必要があります。また、多様なツールやアプリケーションに習熟し、さまざまなネットワークの複数のデスクトップおよびモバイルのクライアントシステムを管理するという課題に取り組む必要もあります。これらの要件のコストを削減し、提供される管理データを整理して表現するために、業界標準の Distributed Management Task Force (DMTF) プロファイルおよび Data Center Infrastructure Management (DCIM-OEM) プロファイルが Dell Command | Monitor に実装されています。本ガイドでは、それら DMTF プロファイルの一部が説明されています。

Dell Command | Monitor の詳細については、**dell.com/dellclientcommandsuitemanuals** にある『Dell Command | Monitor リファレンス ガイド』を参照してください。

Dell Command | Monitor の詳細については、『Client Command | Monitor リファレンス ガイド』を参照してください。

資産プロファイル

エンドポイント デバイスの保証ステータスを示します。

- **DCIM_AssetWarrantyInformation** クラスのインスタンスを列挙または取得することで、保証ステータスを特定します。
- **DCIM_AssetWarrantyInformation** クラスの **WarrantyStartDate** および **WarrantyEndDate** プロパティを使用して、保証ステータスを特定できるかどうかを確認します。

  メモ: DCIM_AssetWarrantyInformation を使用するには、インターネットに接続していることが前提条件となります。プロキシ サーバーの背後で Dell Command | Monitor を実行している場合は、プロキシ設定を正しく設定するようにしてください。

  詳細については、Dell サポート サイトを参照してください。

  1. Dell.com/support にアクセスします。
  2. ページの下部にある国/地域の選択ドロップダウン リストで、お住まいの国または地域を確認します。
  3. サポート カテゴリーの [保証および契約] を選択します。
- 保証機能と後続のリフレッシュ呼び出しを無効にします。
- オンデマンドで保証情報を取得します。

メモ: 保証情報は 15 日ごとに自動的に更新されます。最近の保証ステータスの場合、列挙される保証情報は Dell サポート サイトに表示される内容と異なる場合があります。

バッテリプロファイル

- **DCIM_Battery** クラスのインスタンスを列挙または取得することによって、バッテリの状態を特定します。
- 予測稼働時間を決定し、予測充電残量を確認します。
- **DCIM_Battery** クラスの Operational Status プロパティおよび HealthState プロパティを使用して、バッテリー正常性の情報を判別できるか確認します。
- **DCIM_Sensor.CurrentState** プロパティまたは **CIM_NumericSensor.CurrentState** プロパティを使用して、バッテリ正常性の追加情報を取得します。

BIOS 管理プロファイル

- **DCIM_BIOSElement** クラスのインスタンスを列挙して BIOS バージョンを判断します。
- BIOS 属性値を変更できるかどうかを確認します。**DCIM_BIOSEnumeration** クラスのインスタンスを取得します。**IsReadOnly** プロパティが FALSE に設定されている場合は、属性を変更できます。
- システム パスワード(SystemPwd)を設定します。**DCIM_BIOSService.SetBIOSAttributes()**メソッドを実行して、SystemPwd を AttributeName パラメーターに、パスワード値を AttributeValue パラメーターにそれぞれ設定します。
- BIOS または管理者パスワード (AdminPwd) を設定します。**DCIM_BIOSService.SetBIOSAttributes()**メソッドを実行して、AdminPwd を AttributeName パラメーターに、パスワード値を AttributeValue パラメーターにそれぞれ設定します。
- **DCIM_BIOSService.SetBIOSAttributes()** メソッドを実行し、AttributeName および AttributeValue パラメータを指定します。
- BIOS または Admin パスワードが設定されている時に BIOS Attribute を変更するには、**DCIM_BIOSService.SetBIOSAttributes()** メソッドを実行し、AttributeName、AttributeValue、および現在の BIOS パスワードを AuthorizationToken 入力パラメータとして指定します。

起動制御

- レガシーおよび UEFI ブート リストの起動項目の順序を変更します。
- レガシーおよび UEFI ブート リストの起動項目を有効または無効にします。
- **IsCurrent** プロパティが **1** に設定されている **DCIM_ElementSettingData** クラスのインスタンスを列挙することにより、現在の起動設定を見つけます。**DCIM_BootConfigSetting** は、現在の起動設定を表します。

ベースデスクトップモバイル

- クラス **DCIM_ComputerSystem** のインスタンスを列挙して、システムモデル、サービスタグ、およびシリアルナンバーを判定します。
- **DCIM_ComputerSystem.RequestStateChange()**メソッドを実行して RequestedState パラメーター値を **3** に設定します。システムの電源を切り落とす。

- システムを再起動します。**DCIM_ComputerSystem.RequestStateChange()**メソッドを実行して **RequestedState** パラメーター値を **11** に設定します。
- システムの電源状態を判定します。
- **DCIM_SystemDevice** アソシエーションによって Central Instance に関連付けられた **DCIM_Processor** のインスタンスをクエリして、システムのプロセッサ数を判定します。
- システム時刻を取得します。**DCIM_TimeService.ManageTime()**メソッドを実行して **GetRequest** パラメーターを **True** に設定します。
- 管理下要素の正常性ステータスをチェックします。

ログレコード

- **DCIM_RecordLog** インスタンス中の **ElementName** プロパティが目的の名前に該当する DCIM_RecordLog インスタンス を選択することにより、ログ名を特定します。
- 個々のログ エントリーを検索します。**DCIM_LogManagesRecord** の関連づけによって、**DCIM_RecordLog** の特定のインスタンスに関連づけられている **DCIM_LogEntry** のすべてのインスタンスを取得します。**RecordID** に基づいてインスタンスを並び替えます。
- プロパティ **Enabledstate** が **2**（有効を表す）に設定されており、**EnabledState** が **3**（無効を表す）に設定されているクラス **DCIM_RecordLog** のインスタンスを列挙して、レコードログが有効化されているかをチェックします。
- ログ エントリーのタイムスタンプに基づいて、ログ レコードを並び替えます。**DCIM_LogManagesRecord** の関連づけによって、**DCIM_RecordLog** の特定のインスタンスに関連づけられている **DCIM_LogEntry** のすべてのインスタンスを取得します。**CreationTimeStamp** プロパティ値に基づいて、**DCIM_LogEntry** のインスタンスを後入れ先出し（LIFO）順に並び替えます。
- **ClearLog()** メソッドを **DCIM_RecordLog** の所定のインスタンスに対して実行してログをクリアします。

物理的資産

- システム内の全デバイスの物理インベントリを取得します。
- システムシャーシの物理インベントリを取得します。
- 不具合のあるコンポーネントのパーツナンバーを判別します。
- スロットが空いているか否かを判定します。

システムメモリプロファイル

- システムのメモリ情報を取得します。
- システムの物理メモリの情報を取得します。
- システムのメモリサイズをチェックします。
- 利用できるシステムのメモリサイズをチェックします。
- 物理的なシステムのメモリサイズをチェックします。
- システムメモリの正常性状態をチェックします。

5

Dell Command | Monitor 10.4 の使用

以下にアクセスすると、Dell Command | Monitor からの情報を表示することができます。 `root\dcim\sysman (standard)`

Dell Command | Monitor は、これらの名前空間のクラスを経由して情報を提供します。

クラスの詳細については、**dell.com/dellclientcommandsuitemanuals** で『Dell Command | Monitor リファレンス ガイド』を参照してください。

トピック：

ポーリング間隔の設定

Dell Command | Monitor を使用して、ファン プローブ、温度プローブ、電圧プローブ、電流プローブ、ディスク容量の増減、メモリー サイズの増減、およびプロセッサー数の増減のポーリング間隔を変更することができます。

- Windows では、`dcsbdy32.ini` または `dcsbdy64.ini` ファイルが `<Dell Command | Monitor installed location>\omsa\ini` にあります。
- Linux では、`AlertPollingSettings.ini` ファイルが`/opt/dell/dcm/conf` にあります。

メモ: INI ファイル内の数値は **23** の倍数です。ディスク容量および Self-Monitoring、Analysis and Reporting Technology (SMART) アラートのデフォルトのポーリング間隔は **626** 秒 (実際の時間 = 626 X 23 秒 (約 3 時間)) です。

RAID ステータス報告

Dell Command | Monitor RAID 設定情報が有効になり、クライアント システムの RAID 機能を監視して、ハードウェアとドライバーをサポートします。RAID クラスを使用して、RAID レベル、ドライバー情報、コントローラー設定、コントローラー ステータスに関する詳細を取得することができます。RAID 設定が有効になると、ドライブとコントローラーの劣化や故障に関するアラートを受信することができます。

メモ: RAID ステータス報告は、Common Storage Management Interface (CSMI) バージョン 0.81 準拠のドライバーで動作する RAID コントローラーに対してのみサポートされています。OMCI 8.1 以降のバージョンでは、インテル オンチップ RAID コントローラー上の監視のみがサポートされています。OMCI 8.2 以降のバージョンでは、インテル オンチップ RAID コントローラーでアラートがサポートされています。

Dell クライアントシステムの監視

- Dell Command | Monitor for Windows は、Simple Network Management Protocol (SNMP) に対応して、ノートパソコン、デスクトップ、ワークステーションなどのクライアント システムを監視および管理します。管理情報ベース (MIB) ファイルは、Dell Command | Monitor と Server Administrator との間で共有されます。Dell Command | Monitorfor Windows は、バージョン 9.0 から、コンソールによるクライアント システムの識別のためにクライアント OID (10909) に固有の OID を使用するように変更されました。

SNMP の詳細については、**dell.com/dellclientcommandsuitemanuals** で『Dell Command | Monitor SNMP リファレンス ガイド』を参照してください。

SNMP の詳細については、『Dell Command | Monitor SNMP リファレンス ガイド』を参照してください。

- Dell Command | Monitor for Linux は、WinRM コマンドおよび WSMan コマンドを使用して監視に対応します。

Dell Command | Monitor for Linux のアプリケーション ログ

Dell Command | Monitor for Linux は、レポート作成やデバッグのためにアプリケーションのログとアラートを分類します。Dell Command | Monitor に対して生成されたアラートとログの履歴は、`/opt/dell/dcm/var/log` の **dcm_application.log** ファイルで確認できます。

設定ファイル

`/opt/dell/dcm/conf` の **log.property** 設定ファイルを更新して、次のように必要な設定と DEBUG を適用できます。

メモ: 設定ファイルに変更を加えた後で OMI サーバーを再起動して、変更を適用します。

- Log_Level - システム メッセージを分離するには、ERROR、INFO、DEBUG の 3 つのログ レベルがあります。

  設定ファイルからログ レベルを変更できます。ログ レベルを DEBUG に設定した場合、Dell Command | Monitor アプリケーション ログのすべての情報が指定したログファイルに送信されます。

  メモ: デフォルトのログ レベルは INFO に設定されています。
- File_Size - **dcm_application.log** ファイルの最大サイズを指定できます。デフォルトのファイル サイズは 500 MB です。

  メモ: File_Size 値はバイト単位で表される必要があります。
- BackupIndex - **dcm_application.log** ファイルのロールオーバー数を指定できます。デフォルトのロールオーバー数が 2 の場合、3 番目のバックアップ ファイルは最も古いファイルを上書きします。

アドバンスフォーマットドライブの検出

クライアント システムは、ストレージ容量がより大きく、512 バイト セクター ハード ドライブ (HDD) の制限に対応している、Advanced Format (AF) ドライブに移行しています。4KB セクターに移行しているハード ドライブは、後方互換性を維持します。また、512e ハード ドライブと呼ばれる現在の AF ハード ドライブは、512 バイト SATA に対応し、4KB で動作します。移行中に、クライアント システムでドライブ パーティションの不整列などのパフォーマンスの問題が発生し、512e ドライブを処理するセクターベースの暗号化ソフトウェア パッケージに障害が生じる可能性があります。Dell Command | Monitor では、システムのハード ドライブが 4KB AF ドライブかどうかを識別することが可能になり、これらの問題の回避に役立ちます。

起動設定

メモ: Dell Command | Monitor for Linux には、起動設定機能はありません。したがって、このセクションは、Dell Command | Monitor for Linux には適用されません。

クライアントシステムの起動設定のタイプは、次の 2 つのいずれかになります。

- レガシー (BIOS)
- UEFI

Dell Command | Monitor では、次のクラスを使用して起動設定 (レガシーまたは UEFI) がモデル化されています。

- DCIM_ElementSettingData
- DCIM_BootConfigSetting
- DCIM_OrderedComponent
- DCIM_BootSourceSetting
- DCIM_SmartAttributeInfo

メモ: 起動設定とブート リスト タイプという用語は同じ意味で使用され、レガシーまたは UEFI を示します。

DCIM_AssetWarrantyInformation

- エンドポイント デバイスの保証ステータスを照会するには、次のコマンドを実行します。

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

- WarrantyEndDate の古いものから保証資格を一覧表示するには、次のコマンドを実行します。

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

- 保証機能と後続のリフレッシュ呼び出しを無効にするには、次のコマンドを実行します。

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

- オンデマンドで保証情報を取得するには、次のコマンドを実行します。

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

メモ: プロキシ設定のセットアップ オプション：

- デフォルト プロキシ - Dell Command | Monitor はデフォルトのシステム プロキシを選択します (IE で設定)
- カスタム プロキシ

  Dell Command | Monitor のプロキシ設定を変更するには、プロキシ環境ごとに、**DCIM_ApplicationProxySetting** クラスを使用します。

DCIM_BootConfigSetting

DCIM_BootConfigSetting インスタンスは、起動プロセス中に使用される起動設定を表します。たとえば、クライアント システムでは、レガシーと UEFI の 2 つのタイプの起動構成があります。したがって、**DCIM_BootConfigSetting** が表すインスタンスは最大で 2 つあり、それぞれレガシーと UEFI になります。

DCIM_BootConfigSetting がレガシーを表しているかどうかは、次のプロパティを使って判別できます。

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

DCIM_BootConfigSetting が UEFI を表しているかどうかは、次のプロパティを使って判別できます。

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

DCIM_BootSourceSetting

このクラスは、起動デバイスまたはソースを表します。**ElementName**、**BIOSBootString**、**StructuredBootString** の各プロパティには、起動デバイスを識別する文字列が含まれています。例は、フロッピー、ハード ディスク、CD/DVD、ネットワーク、パーソナル コンピューター メモリー カード国際協会 (PCMCIA)、バッテリー電動車 (BEV)、USB です。デバイスのブート リスト タイプに基づいて、**DCIM_BootSourceSetting** のインスタンスは **DCIM_BootConfigSetting** のインスタンスの 1 つに関連づけられています。

DCIM_OrderedComponent

DCIM_OrderedComponent 関連付けクラスは、**DCIM_BootConfigSetting** インスタンスに **DCIM_BootSourceSetting** のインスタンスを関連づけて、起動デバイスが属するブート リスト タイプ (レガシーまたは UEFI) のいずれかを表すために使用されます。**DCIM_OrderedComponent** の **GroupComponent** プロパティは、**DCIM_BootConfigSetting** インスタンスを参照し、**PartComponent** プロパティは **DCIM_BootSourceSetting** インスタンスを参照します。

DCIM_Smart 属性

Smart 属性値を読み取るには、次のコマンドを実行します。

例:

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

カスタム閾値を設定するには、次のコマンドを実行します。

例:

- Get-CimInstance -Namespace root\dcim\sysman DCIM_SmartAttributeInfo -Filter "AttributeID like '<Attribute ID Value>'" | Invoke-CimMethod -MethodName "SetCustomThreshold" -Arguments @{CustomThresholdValue="<custom threshold value to be set>"}

DCIM_ThermalInformation

DCIM_ThermalInformation は、サーマル モード、AAC モード、ファン障害モードなどの温度設定を管理します。

- デバイスの温度情報を照会するには、次のコマンドを実行します。

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

- サーマル モードの値を設定するには、次のコマンドを実行します。

```
Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ThermalInformation |Where-
Object {$_.AttributeName -eq "Thermal Mode"} | Invoke-CimMethod -MethodName
ChangeThermalMode -Arguments @{AttributeName=@("Thermal Mode");AttributeValue=@("2")}
```

システム設定の変更

Dell Command | Monitor では、次のメソッドを使用してローカルまたはリモート システムのシステム設定と状況を変更します。

- SetBIOSAttributes - BIOS 設定を変更する

  メモ: Dell Command | Monitor for Linux では、SetBIOSAttributes メソッドのみがサポートされています。
- ChangeBootOrder - 起動設定を変更する
- RequestStateChange - システムをシャットダウンおよび再起動する
- ManageTime - システム時刻を表示する

Dell Command | Monitor for Windows では、winrm、VB スクリプト、PowerShell コマンド、wmic、WMI wbemtest を使用してこれらのメソッドを実行できます。

PowerShell コマンドを使用して Windows を実行しているシステムでの BIOS 属性の設定

BIOS 属性は、SetBIOSAttributes メソッドで設定することができます。以下の例では、Trusted Platform Module (TPM) を有効にするタスクの手順を説明します。

メモ: 次の手順を実行して TPM を有効にする前に、BIOS で TPM オプションがクリアされていることを確認してください。

メモ: システム管理者権限で PowerShell を使用します。

TPM を有効にするには、次の手順を実行します。

1. システムの BIOS パスワードがまだ設定されていない場合は、次の PowerShell コマンドを使用して設定します。

   ```
   Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSService | Invoke-CimMethod -
   MethodName SetBIOSAttributes -Arguments
   @{AttributeName=@("AdminPwd");AttributeValue=@("<Admin password>")}
   ```
2. 次のコマンドを使用して TPM セキュリティを有効にします。

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

3. システムを再起動します。
4. 次のコマンドを使用して TPM をアクティブ化します。

```
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. システムを再起動します。

Linux を実行しているシステムでの BIOS 属性の設定

BIOS 属性は、以下のいずれかの方法で設定できます。

- OMICLI の使用
- WinRM の使用
- WSMan の使用

メモ: OMI サーバーが起動されて実行されていることを確認してください。

OMICLI を使用した BIOS 属性の設定

BIOS 属性は、SetBIOSAttributes メソッドで設定することができます。以下の例では、Trusted Platform Module (TPM) を有効にするタスクの手順を説明します。

メモ: 次の手順を実行して TPM を有効にする前に、BIOS で TPM オプションがクリアされていることを確認してください。

OMICLI コマンドを使用して BIOS 属性を設定するには、次の手順を実行してください。

1. システムの BIOS パスワードが設定されていない場合に設定するには、以下を実行します。

```
./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. TPM セキュリティを有効にするには、以下のコマンドを実行します。

```
./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. システムを再起動します。
4. TPM をアクティブにするには、以下を実行します。

```
./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. システムを再起動します。
6. BIOS パスワードをリセットするには、以下を実行します。

```
./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>”  }
```

WinRM を使用した BIOS 属性の設定

BIOS 属性は、SetBIOSAttributes メソッドで設定することができます。以下の例では、Trusted Platform Module (TPM) を有効にするタスクの手順を説明します。

メモ: 次の手順を実行して TPM を有効にする前に、BIOS の TPM オプションをクリアするようにしてください。

WinRM コマンドを使用して BIOS 属性を設定するには、次の手順を実行してください。

1. DCIM_BIOSService クラスを列挙して、selector セットを取得します。次のコマンドを実行します。

```
winrm e wsman/DCIM_BIOSService?__cimnamespace=root/dcim/sysman -auth:basic -r:https://
<system IP or system name>:<Port Number (5985/5986)> -username:<user name> -
password:<password> -skipCAcheck -skipCNcheck -encoding:utf-8 -returnType:epr
```

メモ: この例では、selector セット値 (SystemName=<DCIM_BIOSService クラスのシステム名>winrm i SetBIOSAttributes wsman/DCIM_BIOSService?SystemName=dt: +SystemCreationClassName=DCIM_ComputerSystem+Name=DCIM:BiosService +CreationClassName=DCIM_BIOSService+) はセット操作に使用します。

2. システムの BIOS パスワードが未設定の場合は、次のコマンドを使用して設定してください。

```
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. 次のコマンドを実行して TPM セキュリティを有効にします。

```
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. システムを再起動します。
5. 次のコマンドを使用して TPM をアクティブ化します。

```
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>"}
```

WSMan を使用した BIOS 属性の設定

WSMan を使用して、Linux を実行しているシステムで BIOS 属性を設定することができます。以下の例では、Trusted Platform Module (TPM) を有効にするタスクの手順を説明します。

メモ: 次の手順を実行して TPM を有効にする前に、BIOS の TPM オプションをクリアするようにしてください。

1. DCIM_BIOSService クラスを列挙して、selector セットを取得します。次のコマンドを実行します。

```
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. システムの BIOS パスワードが未設定の場合は、次のコマンドを使用して設定してください。

```
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. 次のコマンドを使用して TPM セキュリティを有効にします。

```
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. システムを再起動します。
5. 次のコマンドを使用して TPM をアクティブ化します。

```
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>"
```

ブート シーケンスの変更

ブート シーケンスを変更するには、次の手順に従います。

1. 次のコマンドを使用して、起動順序タイプ (レガシーまたは UEFI) をチェックします。
   - WMIC コマンド：`wmic /namespace:\\root\dcim\sysman path dcim_BootConfigSetting get ElementName/format:list`.
   - PowerShell コマンド：`gwmi -namespace root\dcim\sysman -class dcim_BootConfigSetting -Property ElementName`.
2. 次のコマンドを使用して、現在の起動順序タイプ (レガシーまたは UEFI) をチェックします。
   - WMIC コマンド：`wmic /namespace:\\root\dcim\sysman path dcim_ElementSettingData.IsCurrent=1 get SettingData /format:list .`
   - PowerShell コマンド：`gwmi -namespace root\dcim\sysman -class dcim_elementSettingData -Filter "IsCurrent=1" -Property SettingData`.
3. 起動順序を変更するには、次のコマンドを使用します。
   - WMIC コマンド：`wmic /namespace:\\root\dcim\sysman path dcim_bootconfigsetting call ChangeBootOrder /?:full .`
   - PowerShell コマンド：`(gwmi -namespace root\dcim\sysman -class dcim_bootconfigsetting).getmethodparameters("ChangeBootOrder") .`

     メモ: `dcim_BootConfigSetting` インスタンスは、変更する起動設定 (タイプ 1(レガシー) またはタイプ 2 (UEFI) のいずれか) を表しています。
   - 引数は次のとおりです。
     - `Authorization Token` - 管理者または起動パスワードです。
     - `Source` - `dcim_OrderedComponent.PartComponent` プロパティから取得した起動順序のリストです。新しい起動順序は、ソースアレイの起動デバイスの順序によって決まります。
4. タイプ 1 ブート リストの起動順序の PowerShell を使用した変更：
   a. タイプ 1 ブート リストの現在の起動順序を取得するには、`$boLegacy = gwmi -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-1'} | select -expand partcomponent.` コマンドを実行します。
   b. PowerShell 変数を定義して、`$newboLegacy.` を設定する起動順序を指定します。新しい起動順序をこれに割り当てます。たとえば、次のように指定すると、現在の起動順序タイプが保持されます。

c. $newboLegacy = $boLegacy
d. タイプ 1 ブート リストに対応する dcim_bootconfigsetting インスタンスを取得するには、$bcsLegacy = Gwmi -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 1'}. コマンドを実行します。
e. $ bcsLegacy.changebootorder($newboLegacy, $AuthorizationToken) コマンドを実行して、メソッドを起動します。BIOS パスワードを渡すには $AuthorizationToken 変数を使用します。

5. タイプ 2 ブート リストの起動順序の PowerShell を使用した変更：
a. タイプ 2 ブート リストの現在の起動順序を取得するには、$boUefi = gwmi -namespace root\dcim\sysman -class dcim_orderedcomponent | where {$_.partcomponent -match 'BootListType-2'} | select -expand partcomponent.コマンドを実行します。
b. PowerShell 変数を定義して、$newboUefi を設定する起動順序を指定します。新しい起動順序をこれに割り当てます。たとえば、次のように指定すると、現在の起動順序タイプが保持されます。
c. タイプ 2 ブート リストに対応する dcim_bootconfigsetting インスタンスを取得するには、$bcsUefi = Gwmi -Namespace root\dcim\sysman -ClassName dcim_bootconfigsetting | where {$_.ElementName -eq 'Next Boot Configuration Setting : Boot List Type 2'}コマンドを実行します。
d. $ bcsUefi.changebootorder($newboUefi, $AuthorizationToken) コマンドを実行して、メソッドを起動します。BIOS パスワードを渡すには $AuthorizationToken 変数を使用します。

Windows システムのリモートでのシャットダウンと再起動

RequestStateChange メソッドを使用して、Windows システムをリモートでシャットダウンまたは再起動することができます。

1. Windows システムをリモートでシャットダウンするには、次のコマンドを使用します。

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

2. Windows システムをリモートで再起動するには、次のコマンドを使用します。

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

Windows システムのシステム時刻値のリモートでの取得

Windows システムのシステム時刻値は、ManageTime メソッドを使用してリモートで取得することができます。例:

コマンド ライン インターフェイスで、次のコマンドを実行します。

a. $cred = Get-Credential
b. $session = New-CimSession -ComputerName "Server01" -Credential $cred
c. Get-CimInstance -CimSession $session -Namespace root\dcim\sysman -ClassName DCIM_TimeService | Invoke-CimMethod -MethodName ManageTime -Arguments @{GetRequest="TRUE"}

6

Dell Command | Monitor 10.4 をローカルで使用した Dell クライアント システムの管理

Dell クライアントシステムは、次の方法でローカルに管理します。

- Windows を実行しているシステムの場合、PowerShell を使用します
- Linux を実行しているシステムの場合、OMICLI を使用します

トピック：

- PowerShell を使用した Windows システムのローカルでの管理
- OMICLI を使用した Linux システムのローカルでの管理

PowerShell を使用した Windows システムのローカルでの管理

PowerShell コマンドを使用して、Windows を実行している Dell クライアント システムをローカルから管理することができます。

- DCIM クラスのインスタンスの列挙
  - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSEnumeration`
  - `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BIOSPassword`
- BIOS 設定のプロパティの取得

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

- BIOS 設定の変更

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

- 重要ではない値の変更

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

- アラートのサブスクライブ

```
$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)
```

- WMI でユーザーの同意を得るコマンド：

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

- WMI でユーザーの同意を設定するコマンド：

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

メモ: 向上プログラムに参加するオプションは、DCM 10.4 x64 ビット バージョンでのみ利用できます。

- WMI でプロキシを取得するコマンド：

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

- WMI でプロキシを設定するコマンド：

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

OMICLI を使用した Linux システムのローカルでの管理

OMICLI コマンドを使用して、Linux システムをローカルで管理できます。Linux を実行しているシステムでは、/opt/omi/bin に OMICLI がインストールされています。

- DCIM クラスのインスタンスの列挙
  - ./omicli ei root/dcim/sysman DCIM_BIOSEnumeration
  - ./omicli ei root/dcim/sysman DCIM_BIOSPassword
- BIOS 設定のプロパティの取得

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

- 管理者パスワードの設定

```
./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 }
```

- BIOS 設定の変更
  - ./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> }
```

- アラートのサブスクライブ

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

7

リモートから Dell Command | Monitor 10.4 を使用した Dell クライアント システムの管理

Dell クライアントシステムは、次の方法でリモートに管理します。

- Windows を実行しているシステムの場合、リモートからの PowerShell を使用した Windows システムの管理(Windows システム経由) 、p. 23
- Linux を実行しているシステムの場合、リモートから WinRM を使用した Linux システムの管理 (Windows システム経由) 、p. 23

トピック：

リモートからの PowerShell を使用した Windows システムの管理 (Windows システム経由)

PowerShell を使用して Windows システムを介して、リモートで Windows システムにアクセスし、監視することができます。

Windows システム管理の前提条件：

- Windows PowerShell 3.0
- リモート スクリプトを実行するために設定された PowerShell

管理対象 Windows システムの前提条件：

- Dell Command | Monitor
- Windows PowerShell 3.0
- リモート スクリプトを実行するために設定された PowerShell
- PowerShell リモート処理機能の有効化

> **メモ:**
>
> Windows PowerShell をリモートで使用するには、リモート PC をリモート管理のために設定する必要があります。手順などの詳細については、`- Get-Help` about_remote_requirements PowerShell コマンドを実行してください。

リモートから WinRM を使用した Linux システムの管理 (Windows システム経由)

WinRM コマンドを使用して、Windows を実行しているシステムを介して Linux を実行しているシステムにアクセスし、監視することができます。

Windows システムの前提条件

- サポートされている Windows オペレーティング システム
- リモート管理向けに設定され実行されている WinRM サービス

Linux システムの前提条件

- Root 権限
- Dell Command | Monitor
- サポートされている Linux オペレーティング システム
- WMI サーバーで 5985 および 5986 ポートを有効にする
- お使いの環境用に構成されたシステム

コマンド ライン インターフェイスで、以下を実行する

```
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
```

リモートから WSMan を使用した Linux システムの管理 (Linux システム経由)

WSMan コマンドを使用して、Linux を実行しているシステムを介して Linux を実行しているシステムにアクセスし、監視することができます。

Linux システム管理の前提条件：

- サポートされている Linux オペレーティング システム パッケージがインストールされている
- wsmancli パッケージがインストールされている

管理対象 Linux システムの前提条件：

- root ログイン権限
- サポートされている Linux オペレーティング システム
- Dell Command | Monitor

ターミナルを起動し、以下を実行します。

```
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

Dell Command | Monitor 10.4 に関するよくある質問

DCIM_OrderedComponent.AssignedSequence プロパティを使って起動設定の起動順序（シーケンス）を見つける方法を教えてください。

DCIM_BootConfigSetting インスタンス（レガシーまたは UEFI）が、**DCIM_OrderedComponent** アソシエーションによってそれに関連付けられた複数の **DCIM_BootSourceSetting** インスタンス（起動デバイス）を持つとき、起動プロセス中に関連付けられた **DCIM_BootSourceSetting** インスタンス（起動デバイス）が使用されるシーケンスを決定するために **DCIM_OrderedComponent.AssignedSequence** プロパティの値が使用されます。関連付けられた **CIM_OrderedComponent.AssignedSequence** プロパティが **0** である **DCIM_BootSourceSetting** は無視され、起動順序の一部としては見なされません。

起動順序はどのように変更すればよいですか？

起動順序を変更するには、**DCIM_BootConfigSetting.ChangeBootOrder()** メソッドを使用します。**ChangeBootOrder()** メソッドは、**DCIM_BootSourceSetting** インスタンスが **DCIM_BootConfigSetting** インスタンスに関連付けられるように順序を設定します。このメソッドの入力パラメータは **Source** だけです。**Source** パラメーターは、**DCIM_OrderedComponent** クラスの **PartComponent** プロパティの順序付き配列で、**DCIM_BootSourceSetting** インスタンス（起動デバイス）と **DCIM_BootConfigSetting** インスタンス（ブート リスト タイプ - レガシーまたは UEFI）との間の関連付けを表します。

起動デバイスを無効にする方法を教えてください。

起動順序の変更時、ターゲット **DCIM_BootConfigSetting** インスタンスを **Source** パラメーターの入力配列に存在しない **DCIM_BootSourceSetting** インスタンスに関連付ける、**DCIM_OrderedComponent** の各インスタンスにある **AssignedSequence** の値を、デバイスが無効化されていることを示す **0** に設定します。

wbemtest を使用して<接続しようとしているデバイス>がネームスペースに接続しようとすると、ログイン失敗メッセージが表示されます。

ログインメッセージの問題を解決するには、**wbemtest** を管理者権限レベルで起動します。**すべてのプログラム**リストから Internet Explorer に移動し、右クリックしてから**管理者として実行**をクリックして **wbemtest** を起動すると、ネームスペースのエラーを回避できます。

Knowledge Library スクリプトを問題なく実行するにはどうすればよいですか？

次の手順は、Dell Command | Monitor Knowledge Library リンクで提供されている VBS スクリプトを実行する際のものです。

1. `winrm quickconfig` コマンドを使用して、システムで **winrm** を設定してください。
2. 次の手順に従って、システムでトークンがサポートされるかどうかをチェックしてください。
   - BIOS セットアップの **F2 画面**。
   - wbemtest のようなツールを使用して、スクリプトで定義されるキーの値がシステムに存在するか確認します。

   メモ: **dell.com/support** にある最新の BIOS の使用をお勧めします。詳細については、**dell.com/dellclientcommandsuitemanuals** にある『Dell Command | Monitor リファレンス ガイド』を参照してください。

   メモ: 最新の BIOS を使用してください。

BIOS の属性はどのように設定すればよいですか?

BIOS の属性は、**DCIM_BIOSService.SetBIOSAttributes()** メソッドを使用して変更できます。**SetBIOSAttributes()**メソッドは、**DCIM_BIOSEnumeration** クラスで定義されているインスタンスの値を設定します。このメソッドには 7 つの入力パラメータがあります。最初の 2 つのパラメータは空白または NULL にすることができます。3 番目のパラメーター **AttributeName** には、**DCIM_BIOSEnumeration** クラスの属性名インスタンスに対応付けられる値を指定する必要があります。4 番目のパラメータまたは **AttributeValue** には、**DCIM_BIOSEnumeration** クラスで定義されている Attribute Name の任意の許容される値を指定できます。5 番目のパラメーター AuthorizationToken はオプションです。5 番目のパラメーターの入力は BIOS パスワードです。5 番目のパラメーターは、BIOS パスワードがシステムに設定されている場合にのみ使用します。設定されていない場合は空白にします。6 番目と 7 番目の引数も、空白または NULL にできます。

Dell Command | Monitor は、Windows オペレーティング システムおよび Linux オペレーティング システムのストレージとセンサーを監視できますか。

はい。Dell Command | Monitor は、サポートされる Windows オペレーティング システムおよび Linux オペレーティング システムのストレージとセンサーの両方を監視できます。

ストレージ監視に関しては、Dell Command | Monitor は、次の機器の監視とアラート発行をサポートします。

- Intel 内蔵コントローラー (CSMI v0.81 以降に準拠)
- LSI 内蔵 RAID コントローラー、および 9217、9271、9341、9361 と、それらに関連付けられたドライバー (物理および論理)

メモ: Linux オペレーティング システムを実行しているシステムでは、Intel 内蔵コントローラーの監視はサポートされません。

センサー監視に関しては、Dell Command | Monitor は、電圧、温度、アンペア数、冷却デバイス (ファン)、およびシャーシ センサーの監視とアラート発行をサポートします。

クラスとアラート発行の詳細については、**dell.com/dellclientcommandsuitemanuals** にある『Dell Command | Monitor リファレンス ガイド』を参照してください。

Dell Command | Monitor は他のアプリケーション / コンソールと統合できますか。

はい。Dell Command | Monitor は、業界標準をサポートする主要なエンタープライズ管理コンソールと連携できます。次に、統合可能な既存のエンタープライズ管理ツールを示します。

- Dell Client Integration Suite for System Center 2012
- Dell OpenManage Essentials
- Dell Client Management Pack for System Center Operation Manager

インベントリのために SCCM にクラスをインポートすることはできますか?

はい、個々の MOF または OMCI_SMS_DEF.mof ファイルをインベントリ用に SCCM コンソールにインポートできます。

SCCM OMCI_SMS_DEF.mof ファイルはどこにありますか?

OMCI_SMS_DEF.mof ファイルは、C:\Program Files\Dell\Command_Monitor\ssa\omacim\OMCI_SMS_DEF.mof にあります。

DCM 10.2.1 のプロキシを設定するにはどうすればよいですか ?

DCM 10.2.1 は保証情報を読み込めません。

DCIM_ApplicationProxySetting クラスで、アプリケーション プロキシ設定が正しく設定されていることを確認してください。

Dell Command | Monitor のプロキシ認証情報を設定するにはどうすればよいですか ?

Dell Command | Monitor にログイン済みであれば、プロキシ認証にも同じ認証情報を使うことができます。

9

Dell Command | Monitor 10.4 を使用したトラブルシューティング手順

トピック：

Windows Management Instrumentation にリモート接続できない

管理アプリケーションでリモートクライアントコンピュータシステムの共通情報モデル (CIM) 情報を使用できない場合、または分散型コンポーネントオブジェクトモデル (DCOM) を使用するリモート BIOS アップデートが失敗した場合、次のエラーメッセージが表示されます。

- **アクセスが拒否されました**
- **Win32:RPC サーバーが使用できません**

1. クライアントシステムがネットワークに接続されていることを確認します。サーバーのコマンドプロンプトで、「`ping <Host Name or IP Address>`」と入力し、`<Enter>`を押します。
2. サーバーとクライアントシステムの両方が同じドメインに属している場合は、次の手順を実行します。
   - ドメイン管理者アカウントに両システムに対する管理者権限があることを確認します。

   サーバーとクライアントシステムの両方がワークグループ (同じドメインではない) に属している場合は、次の手順を実行します。
   - サーバーは、最新の Windows Server で実行するようにしてください。

   メモ: レジストリーを変更する前に、システム データ ファイルをバックアップしてください。レジストリーを誤って編集すると、オペレーティング システムが使用できなくなる場合があります。
3. クライアントシステムでレジストリーの変更を編集します。**スタート** > **ファイル名を指定して実行**をクリックしてから、「**regedit**」と入力し、**OK** をクリックします。**レジストリー エディター** ウィンドウで、`My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa` を参照します。
4. **forceguest** 値を 0 に設定します (デフォルト値は 1)。この値を変更しなければ、システムにリモートで接続しているユーザーは、システム管理者権限の認証情報を入力した場合でもゲスト権限しか持てません。
   a. WMI 管理アプリケーションを実行しているシステムの管理者アカウントと同じユーザー名とパスワードのアカウントをクライアント システムで作成します。
   b. IT Assistant を使用している場合は、IT Assistant ConfigServices ユーティリティー (IT Assistant のインストール ディレクトリー下の `/bin` ディレクトリーにある `configservices.exe`)を実行します。リモート クライアントの管理者でもあるローカル管理者アカウントで実行されるように IT Assistant を設定します。また、DCOM と CIM が有効になっていることを確認します。
   c. IT Assistant を使用している場合は、管理者アカウントを使用して、クライアント システムのサブネット検出を設定します。<クライアント マシン名>\<アカウント名>としてユーザー名を入力します。システムがすでに検出されている場合は、検出されたシステムのリストからシステムを削除し、サブネット検出を設定してから再検出します。

   メモ: IT Assistant の代替として、Dell OpenManage Essentials を使用することをお勧めします。Dell OpenManage Essentials の詳細については、**dell.com/dellclientcommandsuitemanuals** を参照してください。

   メモ: IT Assistant の代替には Dell OpenManage Essentials を使用してください。

5. システムの WMI にリモート接続するためにユーザーの特権レベルを変更するには、次の手順に従ってください。
   a. **スタート** > **ファイル名を指定して実行**をクリックしてから、「compmgmt.msc」と入力し、**OK** をクリックします。
   b. **サービスとアプリケーション** 下の **WMI コントロール** を参照します。
   c. **WMI コントロール** を右クリックし、**プロパティ** をクリックします。
   d. **セキュリティ** タブをクリックし、**Root** ツリーで **DCIM/SYSMAN** を選択します。
   e. **セキュリティ** をクリックします。
   f. アクセス制御の対象となるグループまたはユーザーを選択し、**許可** または **拒否** チェックボックスで権限を設定します。
6. WMI CIM Studio を使用してリモート システムからシステム上の WMI (root\DCIM\SYSMAN) に接続するには、次の手順を実行します。
   a. ローカル システム上に wbemtest と WMI ツールをインストールしてから、リモート システムに Dell Command | Monitor をインストールします。
   b. WMI リモート接続のためにシステムのファイアウォールを設定します。例えば、Windows ファイアウォールで TCP ポート 135 と 445 を開きます。
   c. **ローカル セキュリティ ポリシー**で、ローカル セキュリティ設定を**クラシック - ネットワークアクセスでローカルユーザーが自分自身を認証する：ローカルアカウントの共有とセキュリティモデル**に設定します。
   d. WMI wbemtest を使用して、リモート システムからローカル システムの WMI (root\DCIM\SYSMAN) に接続します。例えば、\\ [ターゲット リモート システムの IP アドレス] \root\DCIM\SYSMAN
   e. リモートターゲットシステムのシステム管理者の資格情報を求められた場合は、それを入力します。

   WMI の詳細については、msdn.microsoft.com で該当する Microsoft 文書を参照してください。

Windows を実行しているシステムでのインストール失敗

Dell Command | Monitor for Windows のインストールを完了できない場合は、次の事柄を確認してください。

- ターゲットシステムの管理者権限を持っている。
- ターゲット システムが、SMBIOS バージョン 2.3 以降がインストールされている Dell 製システムである。
- PowerShell コンソールが閉じている必要があります。

メモ: システムの SMBIOS バージョンをチェックするには、**スタート** > **ファイル名を指定して実行**の順に移動して、msinfo32.exe ファイルを実行します。システム概要ページで SMBIOS バージョンをチェックしてください。

メモ: システムは、サポート対象の Microsoft Windows オペレーティング システムを実行している必要があります。

メモ: システムは、.NET 4.0 またはそれ以降のバージョンにアップグレードする必要があります。

BIOS 設定の列挙値が 1 として表示される

1. 次のパッケージが root ユーザー権限でインストールされていることを確認します。
   - omi-1.0.8.ssl_100.x64.rpm
   - srvadmin-hapi-8.3.0-1908.9058.el7.x86_64
   - command_monitor-linux-<バージョン番号>-<ビルド番号>.x86_64.rpm
2. 上記のパッケージがインストールされている場合は、ドライバー モジュールが読み込まれていることを確認します。
   a. lsmod | grep dcdbas コマンドを実行して、ドライバー モジュールが読み込まれていることを確認します。
   b. ドライバー モジュールを使用できない場合は、modinfo dcdbus コマンドを実行してドライバーの詳細を取得します。
   c. insmod <filename>コマンドを実行して、ドライバー モジュールを読み込みます。

libsmbios の依存関係により、Hapi のインストールが失敗する

依存関係の問題によりインストールに失敗する場合があります。

この場合、apt-get -f install を実行して、すべての依存パッケージを強制的にインストールします。

CIM リソースを使用できない

列挙中に、CIM リソースを使用できないというエラーが表示されることがあります。

この場合、コマンドが root 権限で実行されていることを確認します。

Ubuntu Core 16 を実行しているシステムで DCM を使用するコマンドを実行できない

システムの snap バージョンが 2.23 以降であることを確認します。

10

その他の必要マニュアル

本ユーザーズガイドに加えて、**dell.com/dellclientcommandsuitemanuals** で次のマニュアルにアクセスすることができます。Dell Command | Monitor（以前の OpenManage Client Instrumentation）をクリックして、**一般的なサポート**セクションにある適切な製品バージョンのリンクをクリックします。

このユーザーズガイドに加えて、次のガイドにアクセスすることができます。

- 『Dell Command | Monitor リファレンス ガイド』には、すべてのクラス、プロパティ、および説明の詳細情報が記載されています。
- 『Dell Command | Monitor インストール ガイド』には、インストールについての情報が記載されています。
- 『Dell Command | Monitor SNMP リファレンス ガイド』には、Dell Command | Monitor に適用される簡易ネットワーク管理プロトコル（SNMP）管理情報ベース（MIB）が記載されています。

トピック：

- Dell EMC サポートサイトからの文書へのアクセス

Dell EMC サポートサイトからの文書へのアクセス

製品を選択して、必要な文書にアクセスできます。

1. www.dell.com/manuals にアクセスします。
2. [**すべての製品を参照**] をクリックし、[**ソフトウェア**] をクリックして、[**クライアント システム管理**] をクリックします。
3. 必要な文書を表示するには、必要な製品名とバージョン番号をクリックします。

11

Dell へのお問い合わせ

メモ: インターネットにアクセスできない場合には、注文書、配送伝票、請求書、または Dell 製品カタログにある、お問い合わせ情報をご利用ください。

Dell では、オンラインおよび電話によるサポートとサービスオプションをいくつかご用意しています。これらのサービスは国および製品によって異なり、お住まいの地域では一部のサービスがご利用いただけない場合があります。Dell のセールス、テクニカル サポート、またはカスタマー サービスへは、次の手順でお問い合わせいただけます。

1. **Dell.com/support** にアクセスしてください。
2. サポートカテゴリを選択します。
3. ページの下部にある **国 / 地域の選択** ドロップダウンリストで、お住まいの国または地域を確認します。
4. 目的のサービスまたはサポートを選択します。