




Dell Command | Monitor バージョン 9.2.1 ユーザースガイド



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、その問題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 はじめに.....	5
本リリースの新機能.....	5
Dell Command Monitor 概要.....	5
2 機能.....	7
CIM スキーマのサポート.....	7
BIOS 設定の構成および列挙.....	7
WMI/OMI セキュリティ.....	7
アラートレポート.....	8
リモートシャットダウン.....	8
システム情報へのアクセス.....	8
詳細な資産情報.....	8
リモートウェイクアップ設定.....	8
システム BIOS 設定のリモート変更.....	8
システムの正常性とステータス.....	8
Intel および LSI コントローラの RAID の監視とアラート発行.....	8
SNMP の監視とトラップ.....	9
3 標準およびプロトコル.....	10
4 ユーザーシナリオ.....	11
シナリオ 1：資産管理.....	11
SCCM 統合.....	11
シナリオ 2：設定管理.....	11
シナリオ 3：正常性監視.....	12
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.....	12
シナリオ 4：プロファイル.....	12
バッテリープロファイル.....	12
BIOS 管理プロファイル.....	13
起動制御.....	13
ベースデスクトップモバイル.....	13
ログレコード.....	13
物理的資産.....	14
システムメモリプロファイル.....	14
5 Dell Command Monitor の使用.....	15
ポーリング間隔の設定.....	15
RAID 状態の報告.....	15
Dell クライアントシステムの監視.....	15
Dell Command Monitor for Linux のアプリケーションログ.....	16
設定ファイル.....	16



アドバンスフォーマットドライブの検出.....	16
起動設定.....	16
DCIM_BootConfigSetting.....	17
DCIM_BootSourceSetting.....	17
DCIM_OrderedComponent.....	17
システム設定の変更.....	17
Windows を実行するシステムでの PowerShell コマンドを使用した BIOS 属性の設定.....	17
Linux を実行しているシステムでの BIOS 属性の設定.....	18
起動順序の変更.....	20
リモートから Windows システムのシャットダウンと再起動.....	21
Windows システムのシステム時刻値をリモートから取得する.....	21
6 Dell クライアントシステムのローカルでの管理.....	22
PowerShell を使用した Windows システムのローカルでの管理.....	22
OMICLI を使用した Linux システムのローカルでの管理.....	22
7 リモートから Dell クライアントシステムの管理.....	24
PowerShell を使用した Windows システムのリモートからの管理 (Windows システム経由)	24
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)	24
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)	25
8 よくあるお問い合わせ (FAQ)	26
DCIM_OrderedComponent.AssignedSequence プロパティを使って起動設定での起動順序 (シーケンス) を見つける方法を教えてください。.....	26
起動順序はどのように変更すればよいですか?.....	26
起動デバイスを無効にする方法を教えてください。.....	26
wbemtest を使用して名前空間に接続すると、ログイン失敗のメッセージが表示されます。解決方法を教えてください。.....	26
TechCenter スクリプトを問題なく実行させるにはどうすればよいですか?.....	26
BIOS の属性はどのように設定すればよいですか?.....	27
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?.....	27
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?.....	27
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?.....	27
SCCM OMCI_SMS_DEF.mof ファイルはどこにありますか?.....	27
9 トラブルシューティング.....	28
Windows Management Instrumentation にリモート接続できない.....	28
Windows を実行するシステムでのインストールの失敗.....	29
BIOS 設定の列挙値として 1 が表示される	29
libsmbios の依存関係が原因で hapi のインストールが失敗する.....	29
CIM のリソースを使用できない.....	29
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が実行できない.....	29
10 デルへのお問い合わせ.....	30
その他の必要マニュアル.....	30
Dell EMC サポートサイトからのドキュメントへのアクセス.....	30

はじめに

Dell Command | Monitor ソフトウェアアプリケーションは、情報へのアクセス、ステータスの監視、またはシステムのリモートシャットダウンといったシステム状態の変更を行うためにアプリケーションプログラムを使用して、リモート管理を可能にします。Dell Command | Monitor は、標準的なインタフェースを介して主要システムパラメータを使用するため、システム管理者は導入済み Dell システムのインベントリの管理、システム正常性の監視、および情報の収集を行うことができます。Dell Command | Monitor は、Dell 組み込み PC の他、Dell Enterprise クライアントシステム、Dell IoT Gateway システム向けに設計されています。サポートされる Dell システムについての詳細は、Dell.com/dellclientcommandsuitemanuals にあるリリースノートを参照してください。本書では Dell Command | Monitor とその各種機能の概要について説明しています。

 **メモ:** Dell Command | Monitor はこれまで Dell OpenManage Client Instrumentation (OMCI) と呼ばれていました。OMCI バージョン 8.2.1 以降、OMCI は Dell Command | Monitor にブランド変更されます。

本リリースの新機能

- 新しいプラットフォームのサポート：Dell Edge Gateway 3000 シリーズ
- 新しいオペレーティングシステムのサポート：Ubuntu Core 16
- 次の新しい BIOS 設定のサポート：
 - アナログデジタルインタフェースモードチャンネル 1
 - アナログデジタルインタフェースモードチャンネル 2
 - アナログデジタルインタフェースモードチャンネル 3
 - アナログデジタルインタフェースモードチャンネル 4
 - アナログデジタルインタフェースモードチャンネル 5
 - アナログデジタルインタフェースモードチャンネル 6
 - アナログデジタルインタフェースモードチャンネル 7
 - アナログデジタルインタフェースモードチャンネル 8
 - 自動ウェイク期間
 - BIOS ログのクリア
 - 電源ログのクリア
 - サーマルログのクリア
 - MEMS センサー
 - ZigBee

トークンの詳細については、[dell.com/dellclientcommandsuitemanuals](https://Dell.com/dellclientcommandsuitemanuals) にある『Dell Command | Monitor Reference Guide』(Dell Command | Monitor リファレンスガイド) を参照してください。

Dell Command | Monitor 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 は、管理プロトコルとして 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。これにより、クライアント、サーバ、ストレージ、ネットワーク、ソフトウェアデバイスを含むネットワーク内のすべてのデバイスの管理において、TCO の削減、セキュリティの強化を実現し、全体的なアプローチを提供します。



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

Dell Command | Monitor には、BIOS、CMOS、システム管理 BIOS (SMBIOS)、システム管理インタフェース (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フェース (API) などの異なるソースからクライアントシステム情報を収集する基礎的なドライバセットが含まれています。Dell Command | Monitor for Windows はまた、ダイナミックリンクライブラリ (DLL) およびレジストリ設定から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 (CIMOM) インタフェース、Windows Management Instrumentation (WMI) スタック、または SNMP エージェントを介してこれらの情報を取得します。一方、Dell Command | Monitor for Linux は、Open Management Infrastructure (OMI) インタフェースを介してこれらの情報を取得します。

IT 管理者は Dell Command | Monitor を使用することにより、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、シスログ、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 TechCenter 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 ために SNMP サポートを有効化する方法の詳細については、dell.com/dellclientcommandsuite/manuals で『*Dell Command | Monitor* インストールガイド』を参照してください。**

機能

Dell Command | Monitor の主な機能は次のとおりです。

- CIM スキーマのサポート
- BIOS 設定
- WMI/OMI セキュリティ
- イベント報告
- リモートシャットダウン
- CIM スキーマ経由のシステム情報へのアクセス (WSMAN プロトコル使用)
 - ✎ **メモ: Dell Command | Monitor for Windows を使用している場合、SNMP 経由でも情報にアクセスできます。**
- 詳細な設備資産情報の編集
- リモートウェイクアップの設定機能
- システム設定のリモート変更
- システム正常性の監視とステータスの報告
- Intel 内蔵コントローラおよび LSI 内蔵コントローラに対する RAID の監視とアラート発行
 - ✎ **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の Intel 内蔵コントローラはサポートされません。**
- SNMP 監視とトラップ (Dell Command | Monitor for Windows 経由のみ)

CIM スキーマのサポート

Dell Command | Monitor for Windows は CIM 2.17 スキーマに準拠し、次の 2 つの WMI プロバイダが含まれています。

- WMI インジケーションプロバイダまたはポーリングエージェント
- WMI インスタンスまたはメソッドプロバイダ

Dell Command | Monitor for Linux は CIM 2.32.0 スキーマに準拠し、次の 2 つの WMI プロバイダが含まれています。

- WMI インジケーションプロバイダまたはポーリングエージェント
- WMI インスタンスまたはメソッドプロバイダ

BIOS 設定の構成および列挙

Dell Command | Monitor には、システム BIOS を設定する機能が備わっています。

WMI/OMI セキュリティ

WMI には、CIM データとメソッドへのアクセスを許可する前に、ユーザー認証を行う機能があります。アクセス権限は、分散コンポーネントオブジェクトモデル (DCOM) セキュリティと CIMOM によって強制的に設定されます。完全なアクセス権限または制限付きアクセス権限が、名前空間ごとに、ユーザーに付与されます。クラスの実装やプロパティレベルでのセキュリティはありません。デフォルトでは、管理者グループのメンバーであるユーザーは、WMI へのローカルおよびリモートの完全なアクセス権限を持ちます。



Dell Command | Monitor for Windows では、サービスとアプリケーションセクションにあるコンピュータ管理コンソールで WMI コントロールを使用して、WMI セキュリティを設定できます。**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。名前空間固有のセキュリティを、**セキュリティ** タブで設定できます。また、**スタート** メニューまたは **CLI** から `wiimgmt.msc` を実行して、**WMI コントロール** を実行することもできます。

アラートレポート

Dell Command | Monitor は Dell システムでイベントを検出し、潜在的な故障、設定変更、コンポーネントのインベントリ、Intel および LSI の内蔵 RAID コントローラ、プローブおよびシャーシインテリジェクションについて、ローカルユーザーおよびネットワーク管理者にアラートを発行します。これらのイベントは、OpenManage Essentials (OME) などのシステム管理アプリケーションで表示されます。

リモートシャットダウン

Dell Command | Monitor for Windows は、リモートシステムのシャットダウンと再起動をサポートします。

システム情報へのアクセス

Dell Command | Monitor では、WMI/OMI 経由で CIM を使用して、BIOS リビジョン、BIOS の製造元/ベンダー、サービスタグ、システムモデル、最初に電源オンした日付、システムモデルなどのシステム情報にアクセスできます。これらの情報には、WSMAN プロトコルで WMI/OMI 経由してアクセスすることもできます。

詳細な資産情報

Dell Command | Monitor では、プロセッサ、メモリ、PCI デバイス、バッテリーなどの詳細なインベントリ情報へもアクセスできます。

リモートウェイクアップ設定

Dell Command | Monitor では、リモートウェイクアップ設定を構成する機能がサポートされています。リモートウェイクアップは、クライアントシステムとネットワークインタフェースカード (NIC) の機能です。

システム BIOS 設定のリモート変更

Dell Command | Monitor を使用することにより、管理者は、USB ポートの設定および NIC の設定などのビジネスクライアント BIOS の設定を取得し、設定できます。

システムの正常性とステータス


Dell Command | Monitor は、ファンのステータス、メモリ、温度、プローブ、バッテリー、RAID コントローラ、ドッキングステーションなどのシステム正常性を監視し、ステータスを報告します。

Intel および LSI コントローラの RAID の監視とアラート発行

Dell Command | Monitor for Windows では、Intel および LSI の RAID コントローラの物理ドライブおよび論理ドライブの監視とアラート発行がサポートされています。Dell Command | Monitor for Linux では、LSI コントローラに対してのみ監視とアラート発行がサポートされています。

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 (CSMI v0.81 以降に準拠)

 **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の Intel 内蔵コントローラはサポートされません。

- LSI 内蔵 RAID コントローラ、および 9217、9271、9341、9361 と、それらに関連付けられたドライバ（物理および論理）

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。

SNMP の監視とトラップ

Dell Command | Monitor for Windows は SNMP v1 に準拠し、システム属性とトラップの監視をサポートします。



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。

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

 **メモ: Dell Command | Monitor for Windows は、Simple Network Management Protocol (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の標準団体です。

ユーザーシナリオ

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

Dell Command | Monitor は次の目的で使用することができます。

- [資産管理](#)
- [設定管理](#)
- [正常性監視](#)
- [プロフィール](#)

シナリオ 1：資産管理

Dell システムを多数利用しているある企業。これまでは、事業の変化や IT 担当者の変更などが原因で、正確なインベントリ情報を維持管理できていませんでした。最高情報責任者（CIO）は Microsoft 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ための計画を要求しています。このためには、展開済みのシステムを評価して、そのようなプロジェクトの規模、適用範囲、および財務的な影響を判断する必要があります。情報収集には多大な労力が必要です。IT 担当者を各クライアントシステムの対応に充てるのは、工数およびエンドユーザーの作業中断の観点でコストがかかりすぎます。

各 Dell システムで Dell Command | Monitor を使用すると、IT マネージャはリモートから情報を迅速に収集できます。IT マネージャは Microsoft System Center Configuration Manager（SCCM）などのツールを使用して、ネットワーク経由で各クライアントシステムをクエリし、CPU のタイプと速度、メモリサイズ、ハードドライブ容量、BIOS のバージョン、現在のオペレーティングシステムのバージョンなどの情報を収集します。その後、収集した情報を分析して、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します。

また、CIM クライアントコマンドラインで WSMAN/WinRM コマンドラインなどを使用して、資産インベントリを取得することもできます。

SCCM 統合

SCCM は、次の手順で Dell Command | Monitor for Windows に統合できます。

- すべての Dell Command | Monitor クラスを含む 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、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。この取り組みの一環として、この企業は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、各クライアントコンピュータの BIOS で 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 部門はリモートから起動順序を変更するための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 Enterprise クライアント



システム上の BIOS 設定をリモートから監視できます。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/dellclientcommandssuitemanuals で『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。IT 部門は 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、周辺機器の未承認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ことができます。また、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もできます。

シナリオ 3 : 正常性監視

クライアントシステムハードディスクドライブ上の特定のファイルへのアクセス試行中に、ユーザーが読み取りエラーメッセージを受け取ります。ユーザーがシステムを再起動すると、ファイルがアクセス可能になったようであったことから、ユーザーは問題が解決したと見なして当初の問題を無視します。一方、Dell Command | Monitor は、予測障害の問題についてハードドライブをクエリし、Self-Monitoring, Analysis and Reporting Technology (SMART) アラートを管理コンソールに渡します。さらに、ローカルユーザーに SMART エラーを表示します。アラートには、ハードドライブに複数の読み取り / 書き込みエラーが発生していることが示されていたため、社内の IT 部門は、ユーザーがただちに重要なデータファイルのバックアップを作成することを推奨しました。交換用ドライブを携えたサービス技術者が派遣されます。

ハードディスク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、ヘルプデスクへの電話連絡、技術者がデスクトップに赴いて問題を診断する手間を防ぎます。

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ています。

- 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/dellclientcommandssuitemanuals で『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/dellclientcommandssuitemanuals で『Dell Command | Monitor リファレンスガイド』を参照してください。

バッテリープロファイル

- **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、バッテリー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** クラスのプロパティ *Operational Status* および *HealthState* 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、バッテリー正常性の追加情報を取得します。

BIOS 管理プロファイル

- クラス **DCIM_BIOSElement** 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 属性値が変更可能であるかどうかをチェックします。クラスのインスタンスである **DCIM_BIOSEnumeration** 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、その属性を変更することができます。
- システムパスワード (*SystemPwd*) を設定します。**DCIM_BIOSService.SetBIOSAttribute()** メソッドを実行して、*SystemPwd* を *AttributeName* に、パスワード値を *AttributeValue* パラメータ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* に、パスワード値を *AttributeValue* パラメータ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 起動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 起動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めます。**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、*RequestedState* パラメータ値を **3** に設定してから、システムの電源を切ります。
- 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を検索します。**DCIM_LogManagesRecord** アソシエーションによって関連付けられている **DCIM_RecordLog** の所定のインスタンスと関連付けられた **DCIM_LogEntry** インスタンスをすべて取得します。インスタンスは *RecordID* に基づいて並べ替えます。
- 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。
- ログエントリのタイムスタンプに基づいてログレコードを並べ替えます。**DCIM_LogManagesRecord** アソシエーションによって **DCIM_RecordLog** の所定のインスタンスと関連付けられている **DCIM_LogEntry** のインスタンスをすべて取得します。**DCIM_LogEntry** のインスタンスを *CreationTimeStamp* プロパティ値に基づいて後入れ先出し (LIFO) 順に並べ替えます。
- **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。

Dell Command | Monitor の使用

次の場所にアクセスすることにより、Dell Command | Monitor から提供された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/dellclientcommandssuitemanuals で『Dell Command | Monitor Reference Guide』(Dell Command | Monitor リファレンスガイド) を参照してください。

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、メモリサイズの増減、およびプロセッサ数の増減のポーリング間隔を変更できます。

- Windows の場合、dcsbdy32.ini ファイルまたは dcsbdy64.ini ファイルは、<Dell Command | Monitor がインストールされている場所> \omsa\ini にあります。
- Linux の場合、AlertPollingSettings.ini ファイルは /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 SMART (Self-Monitoring, Analysis and Reporting Technology) 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 × 23 秒 (約 3 時間)) です。

RAID 状態の報告

Dell Command | Monitor は、RAID 設定情報を有効にし、クライアントシステムの RAID 機能を監視します (クライアントのハードウェアとドライバでサポートされている場合)。RAID クラスを使用して、RAID レベル、ドライバ情報、コントローラ設定、およびコントローラの状態の詳細を取得できます。RAID 設定を有効にすると、ドライブおよびコントローラの劣化や故障に関するアラートを受信できます。

 **メモ:** RAID 状態の報告機能は、Common Storage Management Interface (CSMI) バージョン 0.81 互換のドライバで動作する RAID コントローラでのみサポートされています。監視機能は、OMCI 8.1 以降のバージョンで、Intel RAID オンチップコントローラに対してのみサポートされています。アラート機能は、OMCI 8.2 以降のバージョンで、Intel RAID オンチップコントローラに対して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) を使用して、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。MIB ファイルは、Dell Command | Monitor と Server Administrator との間で共有されます。Dell Command | Monitor for 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/dellclientcommandssuitemanuals で *Dell Command | Monitor SNMP Reference Guide* (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、レポートとデバッグでの使用を想定した、アプリケーションログおよびアラートの分類を行います。Dell Command | Monitor アプリケーション用に生成されたアラートおよびログの履歴は、`/opt/dell/dcm/var/log` にある `dcm_application.log` ファイルで確認できます。

設定ファイル

`/opt/dell/dcm/conf` にある設定ファイル `log.property` を更新して、希望する設定と DEBUG を適用できます。

 **メモ:** 設定ファイルの変更後、変更を適用するには OMI サーバを再起動します。

- **Log_Level** — システムメッセージは、ERROR、INFO、DEBUG の 3 つのログレベルに分類されます。
ユーザーは、設定ファイルでログレベルを変更できます。ログレベルを DEBUG に設定すると、Dell Command | Monitor アプリケーションログによってすべての情報が指定したログファイルに書き込まれます。
 **メモ:** デフォルトのログレベルは INFO に設定されます。
- **File_Size** — ユーザーは `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` 値はバイト単位で指定する必要があります。
- **BackupIndex** — ユーザーは、`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、より大きなストレージ容量と、512 バイトセクタハードドライブ (HDD) の制限に対処するため、アドバンスフォーマット (AF) ドライブに移行しています。4KB セクタ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が、512e ハードドライブとして知られる現在の AF ハードドライブは 512 バイト SATA に一致し、4KB で動作します。移行中は、512e ドライブを処理するセクタベースの暗号化ソフトウェアパッケージの不具合を生じるパーションの開始位置がずれたドライブなどのパフォーマンス問題がクライアントシステムで発生す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。このため、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`

 **メモ:** 「起動設定」と「起動リストタイプ」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_BootConfigSetting

DCIM_BootConfigSetting のインスタンスは、起動プロセス中に使用される起動設定を表します。例えば、クライアントシステムでは、起動設定にレガシーと UEFI の 2 タイプがあるため、**DCIM_BootConfigSetting** には表現するインスタンスが最大 2 つ (レガシーと UEFI それぞれに一個ずつ) あります。

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** および **StructuredBootString** プロパティには、起動デバイスを特定する文字列 (例えば、floppy、hard disk、network、Personal Computer Memory Card International Association (PCMCIA)、Battery Electric Vehicle (BEV)、USB など) が含まれます。そのデバイスの起動リストタイプに基づいて、1 つの **DCIM_BootSourceSetting** のインスタンスが **DCIM_BootConfigSetting** のインスタンスのいずれかひとつに関連付けられます。


DCIM_OrderedComponent

DCIM_OrderedComponent アソシエーションクラスは、**DCIM_BootConfigSetting** のインスタンスを、起動デバイスが属する起動リストタイプ (レガシーまたは UEFI) のいずれかを表す **DCIM_BootSourceSetting** のインスタンスに関連付けるために使用されます。

DCIM_OrderedComponent の **GroupComponent** プロパティは **DCIM_BootConfigSetting** のインスタンスを参照し、**PartComponent** プロパティは **DCIM_BootSourceSetting** のインスタンスを参照します。

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、システム設定の変更とローカルシステムまたはリモートシステムの状態の変更を行います。

- **SetBIOSAttributes** — BIOS 設定を変更します。
 **メモ:** Dell Command | Monitor for Linux では、現在、**SetBIOSAttributes** メソッドのみがサポートされています。
- **ChangeBootOrder** — 起動設定を変更します。
- **RequestStateChange** - システムをシャットダウンし再起動します。
- **ManageTime** - システム時刻を表示します。

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

Windows を実行するシステムでの PowerShell コマンドを使用した BIOS 属性の設定

BIOS 属性は、SetBIOSAttributes メソッドを使用して設定できます。次に、トラステッドプラットフォームモジュール (TPM) を有効にするタスクを例に挙げて、設定を行う手順を説明します。

 **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 をアクティブにします。

```
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

次のどの方法を使用しても BIOS 属性を設定できます。

- [OMICLI の使用](#)
- [WinRM の使用](#)
- [WSMan の使用](#)

 **メモ:** OMI サーバが起動し実行されていることを確認します。

OMICLI を使用した BIOS 属性の設定

BIOS 属性は、SetBIOSAttributes メソッドを使用して設定できます。次に、トラステッドプラットフォームモジュール (TPM) を有効にするタスクを例に挙げて、設定を行う手順を説明します。

 **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、次のコマンドを実行して設定します。

```
./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、次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、次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 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、次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 "AdminPwd" AttributeValue "" AuthorizationToken "<password>" }
```

WinRM を使用した BIOS 属性の設定


BIOS 属性は、SetBIOSAttributes メソッドを使用して設定できます。次に、トラステッドプラットフォームモジュール (TPM) を有効にするタスクを例に挙げて、設定を行う手順を説明します。詳細については、[リモートから Dell クライアントシステムの管理](#) を参照してください。

 **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。

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

1. DCIM_BIOSService クラスを列挙して、セレクトASET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:** セレクトASET値 (SystemName=<system name from DCIM_BIOSService class>winrm i SetBIOSAttributes wsman/DCIM_BIOSService?SystemName=dt: +SystemCreationClassName=DCIM_ComputerSystem +Name=DCIM:BiosService+CreationClassName=DCIM_BIOSService+) が、この例のセット操作に使用されます。

2. 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、次のコマンドを使用して設定します。

```
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="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
Activation");AttributeValue=("2");AuthorizationToken="<Admin password>"}
```

WSMan を使用した BIOS 属性の設定

Linux を実行しているシステムで、WSMan を使用して BIOS 属性を設定できます。次に、トラステッドプラットフォームモジュール (TPM) を有効にするタスクを例に挙げて、設定を行う手順を説明します。詳細については、[リモートから Dell クライアントシステムの管理](#) を参照してください。

 **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。

1. DCIM_BIOSService クラスを列挙して、セレクトア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 パスワードがまだ設定されていない場合は、次のコマンドを使用して設定します。

```
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" -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/name> -P 5985 -u <user name> -p <password> -y basic -v -V -k "AttributeName=AdminPwd" -k "AttributeValue=" -k "AuthorizationToken=<password>"
```

起動順序の変更

起動順序を変更するには、次の手順に従います。

1. 次のコマンドを使用して、起動リストタイプをチェックします。

- **WMIC コマンド:** `wmic /namespace:\\root\dcim\sysman path dcim_BootConfigSetting get ElementName/format:list`
- **PowerShell コマンド:** `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_BootConfigSetting -Property ElementName`

2. 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_ElementSettingData.IsCurrent=1 get SettingData /format:list`
- **PowerShell コマンド:** `Get-CimInstance -Namespace root\dcim\sysman -ClassName DCIM_ElementSettingData -Filter "IsCurrent=1" -Property SettingData`

3. 次のコマンドを使用して、起動順序を変更します。

- **WMIC コマンド:** `wmic /namespace:\\root\dcim\sysman path dcim_bootconfigsetting call ChangeBootOrder /?:full`
- **PowerShell コマンド:** `(Get-CimClass -namespace root\dcim\sysman -ClassName DCIM_Bootconfigsetting).CimClassMethods["ChangeBootOrder"].Parameters`

ChangeBootOrder メソッドには次の引数が必要です。

- 認証トークン - 管理者または起動パスワードです。
- ソース - DCIM_OrderedComponent.PartComponent プロパティから取得された起動順序リストです。新しい起動順序は、**source** 配列での起動デバイスの順序によって決定されます。

リモートから Windows システムのシャットダウンと再起動

RequestStateChange メソッドを使用することで、Windows システムのリモートからのシャットダウンと再起動が行えます。

1. Windows システムをリモートから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から再起動するには、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をリモートから取得する

ManageTime メソッドを使用して、Windows システムのシステム時刻値をリモートから取得できます。たとえば、次のとおりです。

コマンドラインインタフェースで、次のように実行します。

- 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"}`



Dell クライアントシステムのローカルでの管理

次の方法を使用して、Dell クライアントシステムをローカルで管理できます

- Windows を実行しているシステムの場合は、「[PowerShell を使用した Windows システムのローカルでの管理](#)」を参照してください。
- Linux を実行しているシステムの場合は、「[OMICLI を使用した Linux システムのローカルでの管理](#)」を参照してください。

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で管理できます。

- **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"}
```

- **アラートの受信**

```
$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)
```

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、OMICLI は /opt/omi/bin にインストールされます。

- **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> }
```

- **アラートの受信**

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

リモートから Dell クライアントシステムの管理

次のいずれかの方法で、リモートから Dell クライアントシステムを管理できます

- Windows を実行しているシステムの場合、[PowerShell を使用した Windows システムのリモートからの管理 \(Windows システム経由\)](#)
- 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 \(Windows システム経由\)](#)

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

PowerShell を使用することによって、Windows システム経由でリモートから別の Windows システムにアクセスして監視できます。

管理側 Windows システムの前提条件

- 対応 Windows オペレーティングシステムパッケージがインストール済み
- お使いの環境用に設定されたシステム

管理対象 Windows システムの前提条件

- システム管理者権限
- Dell Command | Monitor
- 対応 Windows オペレーティングシステムパッケージがインストール済み
- PowerShell のリモート処理機能が有効化済み
- お使いの環境用に設定されたシステム

1. コマンドラインインタフェースを開いてセッションを作成し、次のコマンドを実行します。

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

2. パスワードを入力します。

3. 次のコマンドを実行し、Windows システムにアクセスして監視します。

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

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 コマンドを使用することによって、Microsoft Windows を実行しているシステム経由でリモートから Linux を実行しているシステムにアクセスし監視できます。

Windows システムのための前提条件

- 対応 Windows オペレーティングシステム
- WinRM サービスが実行中
- お使いの環境用に設定されたシステム

Linux システムのための前提条件

- root 権限
- Dell Command | Monitor

- 対応 Linux オペレーティングシステム
- WMI サーバ上のポート 5985 / 5986 が有効
- お使いの環境用に設定されたシステム

コマンドラインインタフェースで、次のコマンドを実行します。

```
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 コマンドを使用することによって、Linux を実行しているシステム経由でリモートから Linux を実行しているシステムにアクセスし監視できます。

管理側 Linux システムの前提条件

- 対応 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済み
- wsmancli パッケージがインストール済み

管理対象 Linux システムの前提条件

- root アクセス権限
- 対応 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て次のコマンドを実行します。

```
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
```

よくあるお問い合わせ（FAQ）

DCIM_OrderedComponent.AssignedSequence プロパティを使って起動設定での起動順序（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（起動リストタイプ - 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 インスタンスをソースパラメータの入力配列に存在しない DCIM_BootSourceSetting インスタンスに関連づける 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 を使用して名前空間に接続すると、ログイン失敗のメッセージが表示されます。解決方法を教えてください。

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、それを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、名前空間関連のエラーを回避できます。

TechCenter スクリプトを問題なく実行させるにはどうすればよいですか？

次の前提条件は、Dell Command | Monitor TechCenter リンクで提供された 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、システムの winrm を設定します。
2. 次を参照して、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、システムに存在することになるスクリプトで定義されるキーの値をチェックします。

 **メモ:** デルでは、dell.com/support にある最新の BIOS のご使用をお勧めします。詳細については、dell.com/dellclientcommandssuitemanuals で『Dell Command | Monitor』を参照してください。

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 **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。BIOS パスワードがシステムで設定されている場合は、5 番目の引数に同じパスワード値を指定する必要があります。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 (CSMI v0.81 以降に準拠)
 - **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の Intel 内蔵コントローラはサポートされません。**
- LSI 内蔵 RAID コントローラ、および 9217、9271、9341、9361 と、それらに関連付けられたドライバ (物理および論理)

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/dellclientcommandssuitemanuals で『Dell Command | Monitor 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。



トラブルシューティング

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。サーバのコマンドプロンプトで、
ping <Host Name or IP Address> と入力し、<Enter> キーを押します。
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。

- サーバーが最新の Windows Server で実行されていることを確認してください。

 **メモ:** レジストリを変更する前に、システムデータファイルをバックアップします。レジストリを誤って編集すると、オペレーティングシステムが使用不能になることがあります。

3. クライアントシステムでレジストリを変更します。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。**レジストリエディタ** ウィンドウで、My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa を参照します。
4. **forcequest** 値を **0** に設定します (デフォルトは **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資格情報を入力した場合でもゲスト権限しか持ちません。
 - 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 (configservices.exe) を実行します。このユーティリティは、IT Assistant インストールディレクトリの下での /bin にあります。ローカル管理者アカウントとして IT Assistant を実行できるように構成します。これにより、リモートクライアント上でも管理者になります。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。ユーザー名には、<クライアントマシン名>\<アカウント名> を入力します。システムが既に検出されている場合、検出済みシステム一覧から削除し、サブネット検出を設定して、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/dellclientcommandsuite/manuals を参照してください。


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 Firewall で TCP ポートの 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. リモートシステムから WMI wbemtest を使用してローカルシステム上の WMI (root\DCIM\SYSMAN) に接続します。例えば、\\[リモートターゲットシステムの IP アドレス]\root\DCIM\SYSMAN に接続します。
 - 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 の詳細に関しては、msdn.microsoft.com で該当する Microsoft 文書を参照してください。

Windows を実行するシステムでのインストールの失敗

Dell Command | Monitor for Windows のインストールを完了できない場合、次の点を確認します。

- 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 コンソールは開いていない。

 **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 と移動して、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、サポートされている 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 設定の列挙値として 1 が表示される

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-<version number>-<buid number>.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、ドライバモジュールがロードされていることを確認します。
 - a. コマンド `lsmod | grep dcdbas` を実行して、ドライバモジュールがロードされていることを確認します。
 - b. ドライバモジュールが使用できない場合は、コマンド `modinfo dcdbus` を実行してドライバの詳細を取得します。
 - c. コマンド `insmod <filename>` を実行して、ドライバモジュールをロードします。

libsmbios の依存関係が原因で hapi のインストールが失敗する

依存関係の問題が原因でインストールが失敗する場合、

`apt-get -f install` を実行して、依存関係にあるすべてのパッケージを強制的にインストールします。

CIM のリソースを使用できない

列挙中に、「CIM resource not available (CIM リソースを使用できません)」のエラーが表示された場合、


root 権限でコマンドを実行し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が実行できない

システム上の snap のバージョンが 2.23 以降であるようにします。



デルへのお問い合わせ

 **メモ:** お使いのコンピュータがインターネットに接続されていない場合は、購入時の納品書、出荷伝票、請求書、またはデルの製品カタログで連絡先をご確認ください。

デルでは、オンラインまたは電話によるサポートとサービスのオプションを複数提供しています。サポートやサービスの提供状況は国や製品ごとに異なり、国 / 地域によってはご利用いただけないサービスもございます。デルのセールス、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** にアクセスします。
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. 必要なサービスまたはサポートのリンクを選択します。

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/dellclientcommandssuitemanuals** 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。

- 『Dell Command | Monitor Reference Guide』(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 Installation Guide』(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 Reference Guide』(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。

Dell EMC サポートサイトからのドキュメントへのアクセス

次のリンクを使用して、必要なドキュメントにアクセスします。

- Dell EMC Enterprise システム管理マニュアル — [Dell.com/SoftwareSecurityManuals](https://dell.com/softwaresecuritymanuals)
- Dell EMC OpenManage マニュアル — [Dell.com/OpenManageManuals](https://dell.com/openmanagemanuals)
- Dell EMC リモートエンタープライズシステム管理マニュアル — [Dell.com/esrmanuals](https://dell.com/esrmanuals)
- iDRAC および Dell EMC Lifecycle Controller マニュアル — [Dell.com/idracmanuals](https://dell.com/idracmanuals)
- Dell EMC OpenManage Connections エンタープライズシステム管理マニュアル — [Dell.com/OMConnectionsEnterpriseSystemsManagement](https://dell.com/OMConnectionsEnterpriseSystemsManagement)
- Dell EMC 保守ツールマニュアル — [Dell.com/ServiceabilityTools](https://dell.com/serviceabilitytools)
- Client Command Suite システム管理マニュアル — [Dell.com/DellClientCommandSuiteManuals](https://dell.com/dellclientcommandssuitemanuals)
- a. [Dell.com/Support/Home](https://dell.com/support/home) に移動します。
- b. **すべての製品から選択** をクリックします。
- c. **すべての製品** セクションで **ソフトウェアおよびセキュリティ** をクリックして、次の中から必要なリンクをクリックします。

- エンタープライズシステム管理
 - リモートエンタープライズシステム管理
 - 保守ツール
 - Dell Client Command Suite
 - 接続クライアントシステム管理
- d. ドキュメントを表示するには、必要な製品バージョンをクリックします。
- 検索エンジンを使用します。
 - 検索 ボックスに名前および文書のバージョンを入力します。