Dell OpenManage Essentials
バージョン 2.0.1 ユーザーズガイド

メモ、注意、警告

メモ: コンピュータ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。

2014 - 12

Rev. A00

目次

1

OpenManage Essentials について

OpenManage Essentials は、企業ネットワーク内で Dell システム、デバイスおよび、コンポーネントの全体を表示できるハードウェア管理アプリケーションです。Dell システムおよびその他デバイスのための、ウェブベースの 1 対多システム管理アプリケーションである OpenManage Essentials では、次が可能です。

- システムの検出およびインベントリ
- システムの正常性の監視
- システムアラートの表示および管理
- システムアップデートおよびリモートタスクの実行
- ハードウェアインベントリおよび準拠レポートの表示

本リリースの新機能

- 第 13 世代 Dell PowerEdge サーバーの追加モデルのサポート。
- 複数の計算ノードを含むデバイスの自動導入のサポート。

メモ: サポートされているデバイスモデルの完全なリストについては、**dell.com/openmanagemanuals** で『OpenManage Essentials バージョン 2.0.1 サポートマトリックス』を参照してください。

その他の情報

本ガイドの他に以下の文章が必要な場合があります：

文書	説明	可用性
Dell OpenManage Essentials サポートマトリクス	OpenManage Essentials がサポートするデバイスのリストです。	**dell.com/OpenManageManuals**
Dell OpenManage Essentials Readme	OpenManage Essentials の既知の問題とその回避策を提供します。	
Dell OpenManage Mobile ユーザーズガイド	OpenManage Mobile アプリケーションのインストールおよび使用に関する情報を提供します。	
Dell License Manager ユーザーズガイド	ライセンスの管理と License Manager のトラブルシューティングに関する情報を提供します。	

文書	説明	可用性
Dell Repository Manager ユーザーズガイド	システムアップデートを管理するための Repository Manager の使用方法に関する情報を提供します。	
Dell OpenManage Essentials REST API ガイド	Representational State Transfer（REST）API を使用した OpenManage Essentials の統合に関する情報および、一般的なタスクを実行するための REST API の使用例を説明しています。	**dell.com/OpenManageManuals** または **DellTechCenter.com/OME**
Dell SupportAssist ユーザーズガイド	SupportAssist のインストール、設定、使用およびトラブルシューティングに関する情報を提供します。	**dell.com/ServiceabilityTools**
トラブルシューティングツールのオンラインヘルプ	ツール、関連したプロトコル、デバイス、およびその他の使用方法に関する情報を提供します。	トラブルシューティングツールに統合されています。トラブルシューティングツールからオンラインヘルプを起動するには、? アイコンをクリックします。
Dell OpenManage Essentials MIB Import Utility オンラインヘルプ	ツール、MIB のインポートと削除、トラブルシューティングの手順、およびその他に関する情報を提供します。	MIB Import Utility に統合されています。MIB Import Utility からオンラインヘルプを起動するには、? アイコンをクリックします。

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。

2

OpenManage Essentials のインストール

関連リンク

OpenManage Essentials のダウンロード
インストールの前提条件と最小要件
OpenManage Essentials のインストール
IT Assistant から OpenManage Essentials への移行

インストールの前提条件と最小要件

サポートされているプラットフォーム、オペレーティングシステム、ブラウザのリストについては、**dell.com/OpenManageManuals** にある『*Dell OpenManage Essentials サポートマトリクス*』を参照してください。

OpenManage Essentials をインストールするには、ローカルシステムの管理者特権が必要です。また、使用しているシステムが「推奨される最小ハードウェア」と「最小要件」に示されている基準を満たしている必要があります。

関連リンク

OpenManage Essentials のインストール

最小推奨ハードウェア

最小推奨ハードウェア	大規模導入	大規模導入	中規模導入 [a]	小規模導入 [a]
デバイス数	最大 4,000 台	2000 以下	最高 500 台	100 以下
システムの種類	物理マシン / 仮想マシン	物理マシン / 仮想マシン	物理マシン / 仮想マシン	物理マシン / 仮想マシン
RAM	8 GB	8 GB	6 GB	4 GB
プロセッサ	合計 8 コア	合計 8 コア	合計 4 コア	合計 2 コア
データベース	SQL Standard	SQL Standard	SQL Express	SQL Express
データベースの場所	リモート **[b]**	リモート **[b]**	ローカル	ローカル
ハードディスクドライブ	20 GB	10 GB	6 GB	6 GB

[a] SQL Express を使用していない場合は、最大メモリをシステムメモリ全体よりも 2 GB 少ない値に制限して、SQL 解析とレポートサービスを無効にしてください。

[b] 8 台のコアプロセッサと 8 GB RAM をサポートするシステムにリモートデータベースをインストールしてください。

メモ: ドメインコントローラ上の OpenManage Essentials に推奨される最小ハードウェア要件は、8 GB RAM、8 コアプロセッサ、およびリモートデータベースです。

メモ: OpenManage Essentials と一緒に Dell SupportAssist がインストールされている場合は、上記の表に示されている最小要件の他に、2 GB の RAM と 2 つのコアが必要です。SQL Server Standard または Enterprise Editions を使用している場合は、最大 SQL Server メモリを SQL Server 内に設定し、システムメモリ全体を使用しないようにする必要があります。6 GB の RAM の場合は最大で 4 GB を使用することをお勧めします。

最小要件

項目	最小要件
オペレーティングシステム	• Microsoft Windows Server 2008 SP2（x64）Standard and Enterprise Edition • Windows Server 2008 R2 SP1 Standard および Enterprise Edition • Windows Server 2012 Standard および Datacenter Edition • Windows Server 2012 R2 Standard および Datacenter Edition **メモ:** OpenManage Essentials バージョン 2.0.1 は、x64 オペレーティングシステムのみでサポートされます。
ネットワーク	1 Gbps 以上
ウェブブラウザ	• Microsoft Internet Explorer 9、10、または 11 • Mozilla Firefox 22 または 23 • Google Chrome 30 または 31
データベース	Microsoft SQL Server 2008 以降 **メモ:** OpenManage Essentials インストールは、SQL Server の大文字と小文字を区別しないインスタンスのみでサポートされます。
ユーザーインタフェース	Microsoft Silverlight バージョン 5.1.30514
.NET	4.5
Microsoft Visual C++ 2012	Runtime 11.0

メモ: OpenManage Essentials バージョン 2.0.1 の最小要件に対する最新アップデートについては、**dell.com/OpenManageManuals** で『OpenManage Essentials バージョン 2.0.1 サポートマトリックス』を参照してください。

リレーショナルデータベース管理システムの利用規約

OpenManage Essentials のインストールに使用されるリレーショナルデータベース管理システム（RDBMS）は Microsoft SQL Server です。SQL Server には OpenManage Essentials データベースとは個別の構成設定があります。サーバーが保有するログイン（SQL または Windows）には、 OpenManage Essentials データベースへのアクセスがある場合とない場合があります。

OpenManage Essentials がインストールされると、HKLM および HKCU のための ZoneMaps へのレジストリエントリの追加によってインターネットセキュリティが変更されます。これにより、Internet Explorer が完全修飾ドメイン名をイントラネットサイトとして識別することを確実にします。

自己署名証明書が作成され、ルート認証局（CA）とマイ証明書にインストールされます。

証明書エラーを避けるため、リモートクライアントは CA およびルート証明書ストアの両方に OpenManage Essentials 証明書をインストールするか、ドメイン管理者によってクライアントシステムにカスタム証明書を発行する必要があります。

OpenManage Essentials の標準インストールの場合：

- サポートされるすべてのコンポーネントを持つ、ローカルインスタンスの SQL サーバーを使用してください。
- RDBMS は、SQL 認証と Windows 認証の両方をサポートするよう変更されます。
- SQL Server ログインユーザーは、OpenManage Essentials のサービス用に生成されます。このログインは、dbcreator 役割を持つ RDBMS SQL ログインとして追加され、ITAssist および OMEssentials データベースに対する db_owner 役割が与えられます。

メモ: 通常のインストールの自動生成された SQL Server ログインアカウントのパスワードは、アプリケーションによって制御され、システムごとに異なります。

セキュリティを最高レベルに保つために、SQL サーバーのカスタムインストール中に指定したドメインサービスアカウントを使用することが推奨されます。

実行時に、OpenManage Essentials ウェブサイトが無効な証明書または証明書バインディングがあるかどうかを判別し、自己署名証明書が再生成されます。

関連リンク

Microsoft SQL Server の最小ログインロール

Microsoft SQL Server の最小ログインロール

下記の表は、異なるインストールとアップグレード使用例に基づいた SQL サーバーの最小権限についての情報一覧です。

番号	使用例	SQL Server の最小ログインロール
1	OpenManage Essentials の初回インストールで、インストールプロセス中に **標準** オプションを選択した。	インストールしたインスタンスの sysadmin アクセス。
2	OpenManage Essentials の初回インストールで、インストールプロセス中に **カスタム** オプシ	OpenManage Essentials データベースの db_owner アクセス。

番号	使用例	SQL Server の最小ログインロール
	ョンを選択しており、空の OpenManage Essentials データベースが存在する（ローカルまたはリモート）。 **メモ: カスタム** インストールオプションを選択し、資格情報を入力しない場合、インストールは **標準** インストールとみなされ、sysadmin 権限が必要となります。	
3	OpenManage Essentials の初回インストールで、インストールプロセス中に **カスタム** オプションを選択しており、空の OpenManage Essentials データベースが存在しない。	サーバーの dbcreator アクセス。
4	OpenManage Essentials をバージョン 1.3 または 2.0 からバージョン 2.0.1 にアップグレードしており、OpenManage Essentials データベースが存在する（ローカルまたはリモート）。	OpenManage Essentials データベースの db_owner アクセス。

データベースのサイズと拡張性

次の表では、アラート、タスク、およびアラート処置に基づいた、4000 台のデバイスがある環境におけるデータベースサイズの変更について説明します。

イベント	データベースサイズ
初期データベースサイズ	60 MB
4000 台のデバイスの検出とインベントリ後	65 MB
2000 件のアラート生成後	73 MB
これらのアラートに対するタスク（状態ポーリング、OpenManage Server Administrator 導入タスク、リモートタスク、およびシステムアップデートタスク）の実行後	77 MB
すべてのアラートの削除後、およびすべてのアラート処置が設定された 20,000 件のアラートの送信後	127 MB
すべてのアラート処置が設定された 40,000 件のアラートの送信後	230 MB

毎日のメンテナンス中、OpenManage Essentials はデータベースを圧縮し、最適化します。OpenManage Essentials は管理下サーバーのためのアップデートもダウンロードします。これらのアップデートはデータベースではなく、OpenManage Essentials がインストールされているローカルファイルシステムに保存されます。

メモ: OpenManage Essentials は最大 17 万 5,000 件のタスク実行履歴詳細を問題なく維持することができます。タスク実行履歴詳細が 17 万 5,000 件を超える場合は、OpenManage Essentials の開始で問題が発生することがあります。不要になったタスク実行履歴詳細は、定期的に削除することをお勧めします。

メモ: 詳細については、**DellTechCenter.com/OME** でテクニカルホワイトペーパー『OpenManage Essentials Scalability and Performance』（OpenManage Essentials 拡張性とパフォーマンス）を参照してください。

OpenManage Essentials のダウンロード

OpenManage Essentials をダウンロードするには、**dell.com/support**、または **DellTechCenter.com/OME** の Dell TechCenter ウェブサイトにアクセスします。

OpenManage Essentials のインストール

OpenManage Essentials をインストールする前に、システム上のローカル管理者権限を持っていることを確認します。
OpenManage Essentials をインストールするには、次の手順を実行します。

1. OpenManage Essentials インストールパッケージを解凍します。
2. インストールパッケージを解凍したフォルダ内にある **Autorun.exe** ファイルをダブルクリックします。

   Dell OpenManage インストール 画面が表示されます。次のオプションの使用が可能です。

   - **Dell OpenManage Essentials** — このオプションを選択して、Dell OpenManage Essentials、Troubleshooting Tool、および Dell OpenManage Essentials MIB Import Utility をインストールします。
   - **Dell Repository Manager** — このオプションを選択して、Dell Repository Manager をインストールします。Repository Manager を使用することにより、Dell Update Packages、ソフトウェアユーティリティ（アップデートドライバ、ファームウェア、BIOS およびその他のアプリケーション）のカスタマイズされたバンドルおよびリポジトリを作成できます。
   - **Dell License Manager** -Dell license manager のインストールを選択します。Dell License Manager は、Dell Remote Access Controller(iDRAC) ライセンスと Dell Chassis Management Controller(CMC) ライセンスを統合する 1 対多のライセンス導入およびレポートツールです。
   - **Dell SupportAssist** — このオプションを選択して Dell SupportAssist をインストールします。SupportAssist は、対応している Dell サーバー、ストレージ、およびネットワークソリューションのためにプロアクティブなサポート機能を提供します。
   - **マニュアル** — クリックしてオンラインヘルプを表示します。
   - **Readme の表示** — クリックして Readme ファイルを表示します。最新の Readme を参照するには、**DellTechCenter.com/OME** にアクセスします。
3. **Dell OpenManage インストール** で、**Dell OpenManage Essentials** を選択し、**インストール** をクリックします。

   Dell OpenManage Essentials 必要条件 ウィンドウには、次の要件タイプが表示されます。

   - **重要** — このエラー状態は、機能のインストールを妨げます。
   - **警告** — この警告状態は、**標準** インストールは無効化されますが、インストール後半での機能の **アップグレード** は無効化されません。また、インストール後半では、機能の選択に **カスタム** インストールのセットアップタイプを使用します。
   - **情報** — この情報状態は、機能の **標準** 選択には影響しません。

   重大な依存関係を解決するためのオプションが 2 つあります。

   - **すべての重要な必要条件をインストール** をクリックして、他に操作を行うことなく、重要な必要条件すべてのインストールを即時に開始します。**すべての重要な必要条件をインストール** では、設定に応じて再起動が必要な場合があり、必要条件のインストールは再起動後自動的に再開されます。

- 各必要条件をひとつずつインストールするには、必要なソフトウェアに関連付けられているリンクをクリックします。

メモ: リモートデータベースの設定には、ローカルシステムへの SQL Express のインストールは必要はありません。リモート SQL Server での OpenManage Essentials データベースのセットアップを参照してください。リモートデータベースを設定しない場合は、警告必要条件リンクをクリックして SQL Express をインストールします。**すべての重要な必要条件のインストール** を選択しても、SQL Express はインストールされません。

メモ: SQL Server 2008、2008 R2、または 2012 Express Edition を使用した OpenManage Essentials のローカルデータベースへのインストールは、OpenManage Essentials 固有の SQLEXPRESSOME というインスタンスが利用可能な場合にのみサポートされます。

4. **Essentials をインストール** をクリックします。

メモ: OpenManage Essentials を初めてインストールする場合、ダイアログボックスが表示され、OpenManage Essentials をローカルデータベースとリモートデータベースのどちらにインストールするかを選択するよう求められます。OpenManage Essentials をローカルデータベースにインストールすることを選択した場合、SQL Server 2012 Express がシステムにインストールされます。OpenManage Essentials をリモートデータベースにインストールすることを選択した場合、カスタムセットアップのインストールの手順に従ってインストールされます。

5. OpenManage Essentials のインストールウィザードで、**次へ** をクリックします。
6. **ライセンス契約** ページで、ライセンス契約を読み、**ライセンス契約の条件に同意します** を選択して **次へ** をクリックします。
7. **セットアップの種類** で、**標準** インストールまたは **カスタム** インストールを選択します。
   - **標準** を選択した場合は、**次へ** をクリックします。**プログラムのインストールの準備完了** ページのインストール設定を確認し、**インストール** をクリックします。

     メモ: OpenManage Essentials サービス用に割り当てられているデフォルトのポートが、ブロックされているか他のアプリケーションで使用されている場合、ポートのブロックを解除するか、他のポートを指定できる **カスタム** インストールを選択するように促すメッセージが表示されます。

     メモ: 作成したすべてのタスクのパラメータは、暗号化されて保存されます。再インストール時に、前回の OpenManage Essentials のインストールから保持されたデータベースの使用を選択した場合、既存のタスクが正常に実行されません。この問題を解決するには、インストール後のタスクすべてを作成し直す必要があります。
   - **カスタム** を選択した場合は、**カスタムセットアップ** で、**次へ** をクリックし、カスタムセットアップインストールの手順に従ってください。
8. インストールが完了したら、**終了** をクリックします。

OpenManage Essentials が仮想マシン (VM) 上にインストールされている場合は、OpenManage Essentials VM の推奨設定は次の通りです。

- リソースの利用可能時間に基づいた CPU 使用率の向上
- **動的メモリ** を無効にする
- **メモリの重み** を高に増加させる

カスタムセットアップインストール

カスタムセットアップを使用して OpenManage Essentials をインストールするには、次の手順を実行します。

1. **カスタムセットアップ** で、**変更** をクリックしてインストールの場所を変更し、**次へ** をクリックします。
2. ポート番号のカスタム設定では、必要に応じて、**ネットワーク監視サービスポート番号**、**タスクマネージャサービスポート番号**、**パッケージサーバーポート**および **コンソール起動ポート** のデフォルト値を変更して、**次へ** をクリックします。
3. **データベースサーバー** で以下のいずれかを行って、**次へ** をクリックします。
   - ローカルデータベース — 管理システム上で複数の SQL Server バージョンが使用可能であり、OpenManage Essentials データベースをセットアップする SQL Server を選択する場合は、**データベースサーバー** リストから SQL Server 選択して、認証タイプを選択し、認証詳細を指定します。データベースサーバーを選択しないと、デフォルトで使用可能な SQL Server Standard、Enterprise、または Express の対応バージョンがインストール用に選択されます。詳細については、**delltechcenter.com/ome** で『Dell OpenManage Essentials のインストール』テクニカルホワイトペーパーを参照してください。
   - リモートデータベース — 必要条件を完了します。詳細に関しては、「リモート SQL Server での OpenManage Essentials データベースの設定」を参照してください。必要条件が完了したら、**参照** をクリックし、リモートシステムを選択してから、認証詳細を提供します。また、**データベースサーバー**内のリモートシステムの IP アドレスまたはホスト名、およびデータベースのインスタンス名を提供することによっても、リモートシステムに OpenManage Essentials データベースを設定できます。

   メモ: カスタムインストールオプションを選択し、資格情報を入力しない場合、インポートは標準インストールとみなされ、sysadmin 権限が必要となります。

   メモ: 選択されたデータベースサーバーで複数のデータベースインスタンスが実行されている場合は、必要なデータベースインスタンス名を指定して Essentials データベース用に設定できます。たとえば、(local) \MyInstance を使用すると、ローカルサーバー上の Essentials データベースと MyInstance という名前のデータベースインスタンスが設定されます。

   メモ: 作成したすべてのタスクのパラメータは、暗号化されて保存されます。再インストール時に、前回の OpenManage Essentials のインストールから保持されたデータベースの使用を選択した場合、既存のタスクが正常に実行されません。この問題を解決するには、インストール後のタスクすべてを作成し直す必要があります。
4. **プログラムインストールの準備完了** ページでインストール設定を確認して、**インストール** をクリックします。

ドメインコントローラへの OpenManage Essentials インストール時の注意事項

ドメインコントローラへの OpenManage Essentials インストール時には、次の事柄に注意してください。

- Microsoft SQL Server は手動でインストールする必要があります。
- SQL Server がローカルでインストールされている場合、SQL Server サービスがドメインユーザーアカウントを使用して実行されるように設定する必要があります。

  メモ: デフォルトの NETWORK SERVICE または LOCAL SYSTEM アカウントを使用している場合、SQL Server サービスは開始されません。

ドメインコントローラへの OpenManage Essentials のインストール後は、次の事柄に注意してください。

- デフォルトで、**ドメイン管理者** グループが **OmeAdministrators** および **OmePowerUsers** 役割のメンバーとして追加されています。
- Windows のローカルユーザーグループは OpenManage Essentials の役割には含まれていません。**OmeAdministrators**、**OmePowerUsers**、または **OmeUsers** 特権は、ユーザーまたはユーザーグループを OpenManage Essentials Windows グループに追加することによって、ユーザーとユーザーグループに付与することができます。**OmeSiteAdministrators** 特権は、**OmeAdministrators** による **デバイスグループ許可** ポータルを介した付与が可能です。

リモート SQL サーバーでの OpenManage Essentials データベースのセットアップ

リモートシステムに存在する SQL Server を使用するように OpenManage Essentials を設定することができます。リモートシステムで OpenManage Essentials データベースをセットアップする前に、次の必要条件をチェックしてください。

- OpenManage Essentials システムとリモートシステムの間のネットワーク通信が機能している。
- OpenManage Essentials システムとリモートシステム間で、特定のデータベースインスタンスの SQL 接続が機能している。接続は、**Microsoft SQL Server Express 2012 Management Studio** ツールを使用して確認できます。リモートデータベースサーバーで、TCP/IP プロトコルを有効にし、SQL 認証を使用している場合は、リモート SQL Server で混在モードを有効にします。

次の場合に、データベースの再ターゲット化ができます。

- SQL Server に対する SQL 資格情報が失敗する。
- SQL Server に対する Windows 資格情報が失敗する。
- ログイン資格情報が失効した。
- データベースが移動された。

Dell SupportAssist のインストール

Dell SupportAssist は、Dell のエンタープライズサーバー、ストレージ、およびネットワーキングの各ソリューションに対して既存の環境データを使用したプロアクティブなサポート機能を提供するために OpenManage Essentials と統合されます。SupportAssist はサポートされているデバイスから情報を収集し、問題発生時にはサポートケースを自動で作成します。これは、Dell が高度かつ個々に応じた効率的なサポート体験を提供するために役立ちます。

SupportAssist をインストールするには、次の手順を実行します。

メモ: 作業を開始する前に、次を確認してください。

- システムはインターネットに接続することができる。
- システムの管理者権限を持っている。
- ファイアウォールで **https://ftp.dell.com** にアクセスするためのポート 443 が開いている。

メモ: SupportAssist のインストールに失敗した場合、後ほどインストールを再試行することができます。インストールを再試行するには、**C:\Program Files\Dell\SysMgt\Essentials\SupportAssistSetup** にある **DellSupportAssistSetup.exe** ファイルを右クリックして、**管理者として実行** を選択します。

1. OpenManage Essentials インストールパッケージを解凍します。
2. インストールパッケージを解凍したフォルダで、 **Autorun.exe** ファイルをダブルクリックします。
   Dell OpenManage インストール ウィンドウが表示されます。
3. OpenManage Essentials バージョン 2.0 がシステムにインストールされていない場合は、**Dell OpenManage Essentials** が選択されていることを確認してください。

4. **Dell SupportAssist** を選択して、**インストール** をクリックします。

   Dell OpenManage Essentials と **Dell SupportAssist** を選択した場合は、OpenManage Essentials のインストールが完了してから SupportAssist がインストールされます。SupportAssist インストールのためのシステムの必要条件が検証されます。システムの必要条件が満たされていれば、**Dell SupportAssist インストーラへようこそ** ウィンドウが表示されます。
5. **次へ** をクリックします。

   ライセンス契約 ウィンドウが表示されます。
6. 通信要件の条項を読み、**同意します** をクリックします。

   メモ: SupportAssist のインストールでは、ユーザーが連絡先、および監視対象となるデバイスの管理者資格情報などの特定個人情報（PII）の保存をデルに許可する必要があります。SupportAssist のインストールは、 ユーザーが PII の保存をデルに許可しない限り、続行されません。
7. ソフトウェアライセンス契約を読み、**同意します** をクリックしてから **次へ** をクリックします。

   プロキシサーバ経由でシステムがインターネットに接続している場合は、**プロキシ設定** ウィンドウが表示されます。そうでない場合は、**SupportAssist のインストール** ウィンドウが一瞬表示され、その後 **インストールの完了** ウィンドウが表示されます。
8. **プロキシ設定** ウィンドウが表示されたら、次の情報を入力します。
   a. **サーバーアドレス** フィールドに、プロキシサーバーアドレスまたは名前を入力します。
   b. **ポート** フィールドに、プロキシのポート番号を入力します。

      メモ: プロキシサーバー資格情報が指定されないと、SupportAssist は匿名のユーザーとしてプロキシサーバーに接続します。
   c. プロキシサーバーが認証を必要とする場合、**プロキシには認証が必要** を選択して、以下の情報をそれぞれのフィールドに入力します。
      - **ユーザー名** – 1 つ、または複数の印刷可能な文字が含まれており、104 文字を越えないようにする必要があります。
      - **パスワード** – 1 つ、または複数の印刷可能な文字が含まれており、127 文字を越えないようにする必要があります。
      - **パスワードの確認** – パスワードをもう一度入力します。パスワードは、 **パスワード** フィールドで入力したものと一致している必要があります。
   d. **インストール** をクリックします。

      プロキシ設定が検証されます。検証に失敗した場合は、プロキシ設定を確認してから再試行する、またはネットワーク管理者にお問い合わせください。
   e. **検証に成功しました** ダイアログボックスで、**OK** をクリックします。

   SupportAssist のインストール ウィンドウが一瞬表示され、その後 **インストールの完了** ウィンドウが表示されます。
9. **終了** をクリックします。

SupportAssist を起動すると、 **SupportAssist のセットアップウィザード** が表示されます。 SupportAssist を使用する前に、**SupportAssist セットアップウィザード** のすべての手順を完了する必要があります。詳細については、**Dell.com/ServiceabilityTools** で『 *Dell SupportAssist ユーザーズガイド*』 を参照してください。

Repository Manager のインストール

Dell Repository Manager は、システムアップデートを簡単かつ効率的に管理するために役立つアプリケーションです。Repository Manager を使用して、OpenManage Essentials から取得した管理下システム設定に基づいたカスタムリポジトリを構築することができます。

Repository Manager をインストールするには、次の手順を実行します。

1. OpenManage Essentials 実行可能ファイルをダブルクリックします。
2. **Dell OpenManage インストール** で **Dell Repository Manager** を選択して、**インストール** をクリックします。
3. **Dell Repository Manager - InstallShield ウィザード** で、**次へ** をクリックします。
4. **ライセンス契約** で、**ライセンス契約の条件に同意します** を選択して **次へ** をクリックします。
5. **カスタマー情報** で以下を行って、**次へ** をクリックします。
   a. ユーザー名と組織情報を指定します。
   b. **このコンピュータを使用するユーザー（すべてのユーザー）** を選択してすべてのユーザーに対してこのコンピュータを利用可能にするか、**自分のみ（Windows ユーザー）** を選択してアクセス権を維持します。
6. **宛先フォルダ** で、デフォルトの場所を使用するか、**変更** をクリックして別の場所を指定して、**次へ** をクリックします。
7. **プログラムインストールの準備完了** で、**インストール** をクリックします。
8. インストールが完了したら、**終了** をクリックします。

Dell License Manager のインストール

Dell License Manager は、Integrated Dell Remote Access Controller（iDRAC）ライセンスおよび Dell Chassis Management Controller（CMC）ライセンスのための 1 対多のライセンス展開およびレポートツールです。

Dell License Manager をインストールするには、次の手順を実行します。

1. OpenManage Essentials 実行可能ファイルをダブルクリックします。
2. **Dell OpenManage インストール** で、**Dell License Manager** を選択します。
3. インストール用の言語を選んで、**OK** をクリックします。
4. **ようこそ** 画面で、**次へ** をクリックします。
5. **ライセンス契約** で、**ライセンス契約の条件に同意します** を選択して **次へ** をクリックします。
6. **セットアップタイプ** で、次のいずれかを選択します。
   - デフォルトのインストールパスを受け入れる場合は、**標準**インストールを選択し、**次へ** をクリックします。
   - 特定のプログラム機能を有効化する、およびインストールパスを変更するには、**カスタム**インストールを選択し、**次へ** をクリックします。**カスタムセットアップ** で必要な License Manager の機能を選択し、ディスク容量をチェックして、Dell License Manager をインストールするための新しい場所を割り当てます。
7. **インストールの準備完了** ウィンドウで、**インストール** をクリックします。
8. インストールが完了したら、**終了** をクリックします。

OpenManage Essentials のアンインストール

メモ: OpenManage Essentials をアンインストールする前に、**Dell OpenManage Essentials MIB Import Utility** と **Dell SupportAssist**（インストールされている場合）をアンインストールする必要があります。

OpenManage Essentials をアンインストールするには、次の手順を実行します。

1. **スタート → コントロールパネル → プログラムと機能**をクリックします。
2. **プログラムのアンインストールまたは変更** で **Dell OpenManage Essentials** を選択して、**アンインストール** をクリックします。

3. `Are you sure you want to uninstall OpenManage Essentials?` というメッセージで、**はい** をクリックします。
4. `Uninstalling OpenManage Essentials removes the OpenManage Essentials database. Do you want to retain the database?` というメッセージで、データベースを保持する場合は **はい** を、削除する場合は **いいえ** をクリックします。

OpenManage Essentials のアップグレード

OpenManage Essentials バージョン 1.3 および 2.0 を、バージョン 2.0.1 にアップグレードすることができます。
アップグレードする前に、ハードウェアドライブ上の最小使用可能空き容量が約 10 GB あることを確認してください。
アップグレードするには、次の手順を実行します。

1. OpenManage Essentials 実行可能ファイルをダブルクリックします。

   Dell OpenManage インストール 画面が表示されます。次のオプションの使用が可能です。

   - **Dell OpenManage Essentials** — このオプションを選択して、Dell OpenManage Essentials、Troubleshooting Tool、および Dell OpenManage Essentials MIB Import Utility をインストールします。
   - **Dell Repository Manager** — このオプションを選択して、Dell Repository Manager をインストールします。Repository Manager を使用することにより、Dell Update Packages、ソフトウェアユーティリティ（アップデートドライバ、ファームウェア、BIOS およびその他のアプリケーション）のカスタマイズされたバンドルおよびリポジトリを作成できます。
   - **Dell License Manager** — このオプションを選択して、Dell License Manager をインストールします。Dell License Manager は、Dell iDRAC 7 ライセンスを管理するための、一対多でのライセンス展開およびレポート実行ツールです。
   - **Dell SupportAssist** — このオプションを選択して Dell SupportAssist をインストールします。SupportAssist は、対応している Dell サーバー、ストレージ、およびネットワークソリューションのためにプロアクティブなサポート機能を提供します。

     メモ: SupportAssist がシステムにすでにインストールされている場合は、デフォルトで **Dell SupportAssist** オプションが選択され、グレーアウト表示されます。OpenManage Essentials のアップグレード後、SupportAssist もアップグレードされます。該当する場合は、SupportAssist のアップグレード中にプロキシ設定を提供する必要が生じる場合があります。詳細については、**dell.com/ServiceabilityTools** で『Dell SupportAssist ユーザーズガイド』を参照してください。
   - **マニュアル** — クリックしてオンラインヘルプを表示します。
   - **Readme の表示** — クリックして Readme ファイルを表示します。最新の Readme を参照するには、**dell.com/OpenManageManuals** にアクセスします。
2. **Dell OpenManage インストール** で、**Dell OpenManage Essentials** を選択し、**インストール** をクリックします。

   Dell OpenManage Essentials 必要条件 ウィンドウには、次の要件タイプが表示されます。

   - **重要** — このエラー状態は、機能のインストールを妨げます。
   - **警告** — この警告条件は **標準** インストールを無効化する場合がありますが、インストール後半での機能の **アップグレード** は無効化されません。
   - **情報** — この情報状態は、機能の **標準** インストールには影響しません。

メモ: OpenManage Essentials バージョン 1.1 が SQL Server 2008 Express edition を使用するローカルデータベース上のシステムにインストールされ、OpenManage Essentials 固有の名前が付いたインスタンス SQLEXPRESSOME が利用可能ではない場合、SQL Server の必須条件に 重大 アイコンが表示されます。インストールを続行するには、SQLEXPRESSOME インスタンスのある SQL Server Express 2012 SP1 をインストールする必要があります。SQL Server の旧バージョンのデータは自動的に移行されます。

3. **Essentials をインストール** をクリックします。
4. OpenManage Essentials のインストールウィザードで、**次へ** をクリックします。
5. **ライセンス契約** ページで、ライセンス契約を読み、**ライセンス契約の条件に同意します** を選択して **次へ** をクリックします。
6. 該当する場合、**パッケージサーバーポート** および **タスクマネージャーサービスポート** を入力します。パッケージサーバーポートまたはタスクマネージャーサービスポートのどちらかがアップグレード中にブロックされていた場合は、新しいポートを入力します。**次へ** をクリックします。

   メモ: サポートされるポートとプロトコルの詳細に関しては、管理下ノードでサポートされるプロトコルとポートと管理ステーションでサポートされるプロトコルおよびポートを参照してください。

   `Please backup OMEssentials database before upgrading to the latest version of OpenManage Essentials` というメッセージが表示されます。
7. **OK** をクリックします。
8. **インストール** をクリックします。
9. インストールが完了したら、**終了** をクリックします。

アップグレードが完了したら、次の手順を実行する必要があります。

1. すべての既存の検出範囲について検出とインベントリを実行します。
2. **デバイスの検索** ポータルで、すべてのデバイス照会で期待通りの結果が得られたことを確認します。
3. **システムアップデート** ポータルで、既存カタログが最新のものでない場合は、必ず最新のカタログを取得します。

VMware ESXi 5 のセットアップと設定

メモ: VMware ESXi 5 をセットアップおよび設定する前に、ESXi 5 ビルド 474610 以上をお持ちであることを確認してください。必要なビルドがない場合は、**vmware.com** から最新のビルドをダウンロードしてください。

VMware ESXi 5 を設定するには、次の手順を実行します。

1. **dell.com/support** から ESXi 用の Dell OpenManage オフラインバンドルの最新バージョン（7.4）をダウンロードします。
2. SSH を有効にしている場合は、WinSCP または同様のアプリケーションを使用してファイルを ESXi 5 ホストの **/tmp** フォルダにコピーしてください。
3. Putty を使用し、`chmod u+x <Dell OpenManage version 7.4 offline bundle for ESXi file name>.zip` コマンドで ESXi 用 Dell OpenManage オフラインバンドルの許可を変更します。

   メモ: WinSCP を使用して許可を変更することもできます。
4. 以下を使用して次のコマンドを実行します：
   - Putty — `esxcli software vib install -d /tmp/<Dell OpenManage version 7.4 VIB for ESXi file name>.zip`

- VMware CLI — `esxcli -server <IP Address of ESXi 5 Host> software vib install -d /tmp/<Dell OpenManage version 7.4 VIB for ESXi file name>.zip`

メッセージ `VIBs Installed: Dell_bootbank_OpenManage_7.4-0000` が表示されます。

5. ホストシステムを再起動します。
6. 再起動した後、以下を使用して次のコマンドを実行し、OpenManage がインストールされているかどうかを確認します。
   - Putty — `esxcli software vib list`
   - VMware CLI — `esxcli -server <IP Address of ESXi 5 Host> software vib list`
7. ESXi 5 ホスト上でのハードウェアアラートのため、SNMP トラップを OpenManage Essentials に送信するように SNMP を設定します。SNMP は検出には使用されません。ESXi 5 ホストの検出とインベントリには WS-Man が必要です。VM 検出後に OpenManage Essentials デバイスツリーで VM を ESXi ホストとグループ化するには、SNMP が ESXi ホストと VM で有効化されている必要があります。
8. 検出範囲を作成して、WS-Man を設定します。

   ESXi 5 のセットアップと設定の詳細に関しては、**delltechcenter.com/ome** にあるホワイトペーパー『OME での使用のための ESXi 5 のセットアップと設定方法』を参照してください。

IT Assistant から OpenManage Essentials への移行

IT Assistant から OpenManage Essentials バージョン 2.0.1 への直接移行はサポートされていません。ただし、IT Assistant を OpenManage Essentials の以前のバージョンに移行した後で、OpenManage Essentials バージョン 2.0.1 にアップグレードすることは可能です。IT Assistant から OpenManage Essentials の以前のバージョンへの移行の詳細に関しては、**dell.com/OpenManageManuals** にある、該当する『Dell OpenManage Essentials ユーザーズガイド』を参照してください。

関連リンク

OpenManage Essentials のインストール

3

OpenManage Essentials はじめに

OpenManage Essentials の起動

OpenManage Essentials を起動するには、次のいずれかを実行します。

メモ: OpenManage Essentials を立ち上げる前に、お使いのブラウザで Javascript が有効になっていることを確認してください。

- 管理ステーションデスクトップで、**Essentials** アイコンをクリックします。
- 管理ステーションデスクトップで、**スタート → すべてのプログラム → Dell OpenManage アプリケーション → Essentials → Essentials** の順にクリックします。
- ローカルシステムまたはリモートシステムから、対応ブラウザを起動します。アドレスフィールドに、次のいずれかをタイプします。
  - **https://< 完全修飾ドメインネム（FQDN） >:**
  - **https://<IP アドレス、ホスト名、または完全修飾ドメインネーム（FQDN） >:<ポート番号>/web/default.aspx のいずれかを入力します。**
  - **https://<IP アドレス>:<ポート番号>**

メモ: FQDN は、有効な証明書を示すために必要です。IP アドレスまたはローカルホストが使用されている場合、証明書はエラーを示します。

リモートシステムのブラウザから OpenManage Essentials を起動するには、コンソール起動ポート番号（デフォルトのポート番号は 2607）が必要です。OpenManage Essentials のインストール中に **カスタムインストール** オプションを使用してポートを変更した場合は、先行の URL にある選択されたコンソール起動ポートを使用します。

最初のセットアップページが表示されます。

メモ: 異なるユーザーとしてサインイン オプションを使用すれば、別のユーザーとしていつでも OpenManage Essentials にログオンできます。詳細に関しては、「異なるユーザーとしてログオン」を参照してください。

関連リンク

OpenManage Essentials ホームポータルの使い方

OpenManage Essentials の設定

OpenManage Essentials に初めてログインする場合、**初回セットアップ** チュートリアルが表示されます。このチュートリアルは、OpenManage Essentials と通信するサーバーとデバイスの環境を設定する段階的な手順を提供します。この手順は次のとおりです。

- 各ターゲットサーバーでの SNMP プロトコルの設定。
- SNMP ツールのインストール（Windows Server 2012 以降）。
- 各ターゲットサーバーでの Dell OpenManage Server Administrator のインストール。

- 各ターゲットサーバーでのネットワーク検出の有効化（Windows Server 2008 ベースのサーバー）。
- ネットワークでのデバイスの検出。

初回セットアップ ウィザードを完了すると、**検出ウィザードの設定** ウィンドウが表示されます。詳しくは「検出ウィザードの設定」を参照してください。

コンソールに表示される日付や時刻は、ブラウザ設定で選択され、地域で使用されるフォーマットです。タイムゾーンが変更されたり、夏時間変更が発生すると、コンソールにおける時刻はそれに従ってアップデートされます。タイムゾーンまたは夏時間の変更はコンソールの時刻を変更しますが、データベースの時刻は変更しません。

関連リンク

OpenManage Essentials ホームポータルの使い方

検出ウィザードの設定

検出ウィザードの設定 ウィンドウを使用すると、デバイスの検出に使用するウィザードのタイプを設定できます。**検出ウィザードの設定** ウィンドウで表示されるオプションは、以下の表に記載されています。

オプション	説明
標準ウィザード（デフォルト）	これを選択すると、**デバイスの検出** ウィザードに、デバイス検出に用いるプロトコルの一覧が表示されます。
ガイド付きウィザード	選択した場合、**デバイスの検出** ウィザードに、デバイスタイプと、選択されたデバイスの検出と管理に必要なプロトコルの一覧が表示されます。必要なプロトコルの設定が完了すると、デフォルトでは、このウィザードは検出とインベントリの両方を実行します。 **メモ: ガイド付きウィザード**では、Dell EMC ストレージアレイの検出はサポートされていません。

ウィザードのタイプを選択して **完了** をクリックすると、設定が **プリファランス → 検出設定** に保存されます。

デフォルトでは、以下の時に **検出ウィザードの設定** ウィンドウが表示されます。

- OpenManage Essentials の初回起動時
- **検出とインベントリ** ポータルで、初めて **検出範囲の追加** をクリックした時。

デバイスの検出に使用するウィザードのタイプを後から設定したい場合には、**検出設定** ページで行うことができます。詳細については、「検出設定の指定」を参照してください。

検出設定の指定

検出の設定 ページで、デバイスの検出に使用するウィザードのタイプを設定できます。

検出設定を指定するには、次の手順を実行します。

1. **プリファランス → 検出設定** をクリックします。

検出設定 ページが表示されます。

2. 次のいずれか 1 つを選択します。
   - **標準ウィザード** — これを選択すると、**デバイス検出** ウィザードに、デバイス検出に用いるプロトコルの一覧が表示されます。
   - **ガイド付きウィザード** — 選択した場合、**デバイス検出** ウィザードに、デバイスタイプと、選択されたデバイスの検出と管理に必要なプロトコルの一覧が表示されます。必要なプロトコルの設定が完了すると、デフォルトでは、このウィザードは検出とインベントリの両方を実行します。

     メモ: ガイド付きウィザードでは、Dell EMC ストレージアレイの検出はサポートされていません。
3. **適用** をクリックします。

OpenManage Essentials ホームポータルの使い方

OpenManage Essentials のユーザーインタフェースには次のコンポーネントが含まれています。

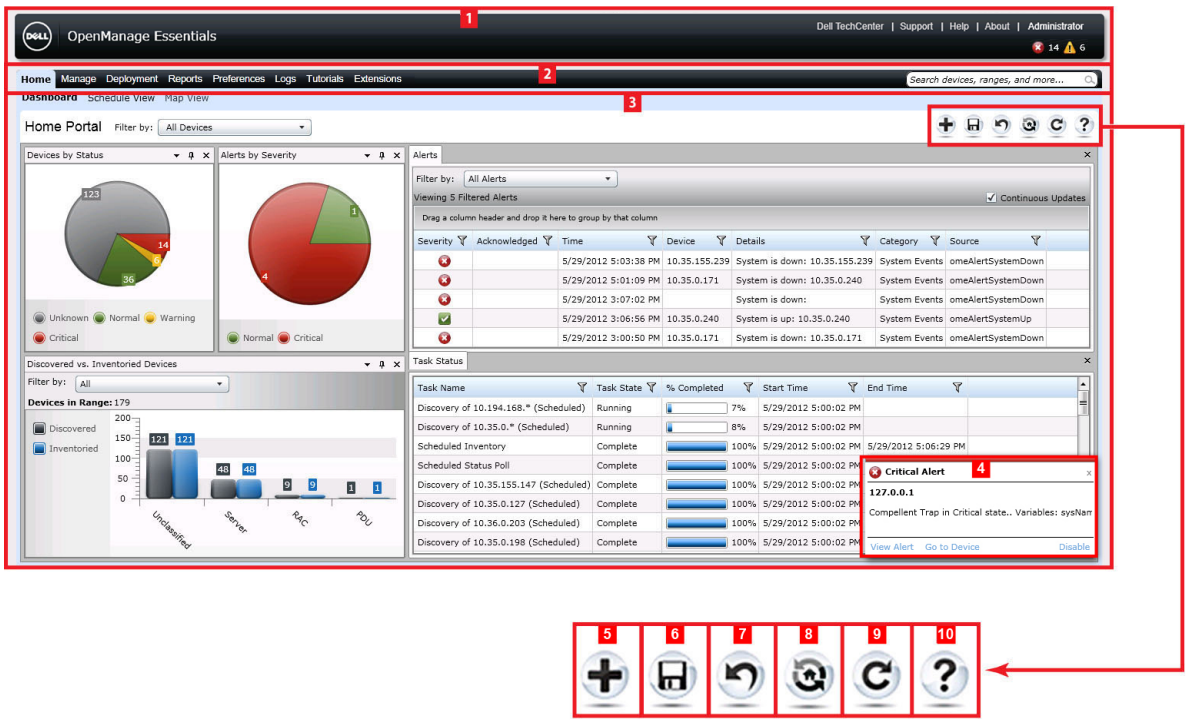


図 1. OpenManage Essentials ホームポータル

1. ヘッダバナー
2. メニューアイテムと検索バー
3. コンソールエリア
4. アラートポップアップ通知
5. ホームポータルにレポートを追加
6. 現在のホームポータルレイアウトを保存
7. 最後に保存されたホームポータルレイアウトをロード
8. デフォルトのホームポータルレイアウトをロード

9. ホームポータルページを更新
10. オンラインヘルプを起動

関連リンク

マップビュー（ホーム）ポータル
ダッシュボード
検索バー

OpenManage Essentials ヘッダバナー

バナーには以下のアイコンが表示される場合があります。

- 重要アイコン と警告アイコン とデバイス数。アイコンまたは数字をクリックして、いずれかの状態のデバイスを表示することができます。
- OpenManage Essentials サービス停止中アイコン（点滅する下向き矢印） 。アイコンをクリックして詳細を表示し、サービスを再起動することができます。
- アップデートの利用可能通知アイコン は、OpenManage Essentials の新バージョンが利用可能か否かを示します。アイコンをクリックしてウェブサイトを開き、OpenManage Essentials の新バージョンをダウンロードすることができます。
- 保証スコアボード通知アイコン は、保証が *x* 日以下のデバイスの数を含みます。アイコンまたは数字をクリックして **デバイス保証レポート** を表示し、保証期間が指定日数以下のデバイスの一覧を確認することができます。保証スコアボード通知アイコンは、**プリファランス → 保証通知設定** で **保証スコアボード通知の有効化** を選択している場合にのみ表示されます。

アイコンの他に、バナーにも以下へのリンクが含まれます。

- **Dell TechCenter** — クリックすると、デル製品に関する様々なテクノロジー、ベストプラクティス、ナレッジ共有、情報が表示されます。
- **サポート** — クリックすると、**dell.com/support** が開きます。
- **ヘルプ** — クリックすると、オンラインヘルプが開きます。
- **バージョン情報** — クリックすると、一般的な OpenManage Essentials 製品情報が表示されます。
- ***ユーザー名*** — 現在ログインしているユーザーのユーザー名が表示されます。マウスポインタをユーザー名の上に移動すると、以下のオプションが表示されます。
  - **ユーザー情報** — クリックして、現在のユーザーに関連付けられている OpenManage Essentials の役割を表示します。
  - **異なるユーザーとしてサインイン** — クリックして、OpenManage Essentials に異なるユーザーとしてログインします。

    メモ: 異なるユーザーとしてサインイン オプションは、Google Chrome ではサポートされていません。

メモ: バナーはすべてのページで利用可能です。

関連リンク

ユーザー情報の表示
異なるユーザーとしてログオン
アップデートの利用可能通知アイコンの使用
保証スコアボード通知アイコンの使用

ポータルのカスタマイズ

ポータルページのレイアウトを変更して、次を行うことができます。

- 使用可能なレポートを追加表示する。

  メモ: このオプションは、ホームポータルでのみ使用できます。
- グラフとレポートを非表示にする。
- ドラッグ＆ドロップで、グラフおよびレポートの配置を変更、またはサイズを変更する。

画面上のポップアップウィンドウが画面よりも大きく、スクロールが可能でない場合は、ブラウザのズーム値を 75% 以下に設定します。

利用できる様々なレポートから特定のレポートを選択し、それらをダッシュボードに表示するように設定することができます。これらのレポートをクリックして詳細を取得することも可能です。利用できるレポートのリストは、「ホームポータルレポート」を参照してください。

詳細については、それぞれを参照してください。

- ホームポータルには、「OpenManage Essentials ホームポータル リファレンス」。
- デバイスポータルには、「デバイス リファレンス」。
- 検出とインベントリポータルには、「検出とインベントリ リファレンス」。
- レポートポータルには、「レポート リファレンス」。

をクリックします。

利用可能な追加レポートとグラフの表示

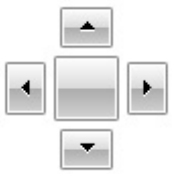
チャートにはドリルダウン機能があります。追加レポートとグラフを表示するには、

右上隅にあるアイコンをクリックします。以下の利用可能なレポートとグラフのリストが表示されます。

- **重大度ごとのアラート**
- **ステータスごとのデバイス**
- **検出済み対インベントリ済みデバイス**
- **アラート**
- **アセット取得情報**
- **アセットメンテナンス情報**
- **アセットサポート情報**
- **ESX 情報**
- **FRU 情報**
- **ハードドライブ情報**
- **HyperV 情報**
- **ライセンス情報**
- **メモリ情報**

- **モジュラーエンクロージャ情報**
- **NIC 情報**
- **PCI デバイス情報**
- **サーバーコンポーネントとバージョン**
- **サーバーの概要**
- **ストレージコントローラ情報**
- **タスク状態**

希望のレポートまたはグラフを選択した後、次のコントロールを使用して、このレポートまたはグラフを希望の場所にドッキングさせます。



詳細情報取得のためのチャートとレポートのドリルダウン

より詳しい情報を得るためにドリルダウンを行うには、次のいずれかを実行します。

- レポートチャートで、チャートをクリックします。
- レポート表で、ドラッグアンドドロップオプション、またはじょうごオプションを使用して必要なデータをフィルタし、表の行を右クリックして様々なタスクを実行します。

ホームポータルレイアウトの保存とロード

ポータルレイアウトを保存およびロードするには、

アイコンをクリックします。
ポータル上の現在のレイアウト設定および表示されているレポートは、すべてポータルページに保存されます。

以前のポータルのレイアウトをロードするには、

アイコンをクリックします。

ポータルデータのアップデート

ポータルページを手動で更新するには、

アイコンをクリックします。

ポータルのデフォルトレイアウトをロードするには、

アイコンをクリックします。

グラフおよびレポート（コンポーネント）の非表示

グラフおよびレポート（コンポーネント）を非表示にするには、

レポートまたはグラフ上のアイコンをクリックし、**非表示** オプションを選択してポータルページからコンポーネントを取り除くか、**自動非表示** オプションを選択してコンポーネントをサイドバーに移動させます。

ポータルページからコンポーネントを取り除くには、レポートまたはグラフの **X** アイコンをクリックします。

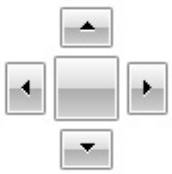
レポートをサイドバーに移動させるには、

アイコンをクリックします。

グラフおよびレポート（コンポーネント）の配置変更およびサイズ変更

ネットワークアダプタの追加プロパティを表示するには、 アイコンをクリックして、次のオプションから選択します。

- **フロート** — ポータルページ内でコンポーネントを自由に移動させます。
- **ドッキング可** — ポータルページでコンポーネントをドッキングします。コンポーネントがフロートの時、タイトルを右クリックしてコンポーネントをドッキングするか、タブ付きにします。
- **タブ付きドキュメント** — コンポーネントをポータルページ内のタブに移動します。



コントロールを選択して、フロート状態のコンポーネントをドッキングします。ペインを他のペイン内でドッキングするか、ペインをメインウィンドウの最上部、最下部、左端、または右端にドッキングして、タブ表示を作成できます。

ペインのサイズ変更が可能で、ドッキングを行うと選択したエリア全体にすべてのペインが収まります。

コンポーネントをサイドバーに移動させるには、

アイコンをクリックして、復元し、コンポーネントを選択して、

アイコンをクリックします。

レポートグリッドでフィルタを作成するには、

アイコンをクリックします。これはポータルページのレイアウトに固有なものではなく、これらの関連付けに関する設定は保存されません。

データのフィルタリング

行のヘッダーをレポート上にドラッグ&ドロップして、結果をフィルタできます。表示を必要に応じて変更する場合、1 つ、または複数の属性を選択できます。

たとえば、**状態ごとのデバイス** 円グラフで、**重要** などの状態をクリックします。**デバイス概要** ページで、**デバイスの種類** と **サービスタグ** をレポートの最上部にドラッグします。表示内容は、プリファランスに基づいて、ネスト情報に瞬時に変わります。この例では、この情報は、まず最初に **デバイスの種類** によってグループ化され、次に **サービスタグ** によってグループ化されています。デバイスの残りの情報を表示するには、フィルタリングされたこれらのグループをドリルダウンします。

詳細に関しては、「デバイスサマリの表示」を参照してください。

検索バー

検索バーは、ヘッダーバナーの下にあるダッシュボードの右上に表示されます。 検索バーは、ポップアップまたはウィザードが表示される場合を除き、すべてのポータルページからアクセス可能です。検索バーにテキストを入力するにつれ、一致するまたは類似のアイテムがドロップダウンリストに表示されます。

関連リンク

検索アイテム
検索ドロップダウンリスト
選択処置

検索アイテム

検索バーを使用すると以下の項目を検索することができます。

- デバイス
- デバイスグループ
- 検出範囲
- 検出範囲グループ
- 除外範囲
- ポータル
- ウィザード
- リモートタスク
- プリファランスおよび設定

範囲、タスク、デバイス、およびその他がコンソールで変更または作成されると、20 秒以内にそれらが検索可能アイテムに追加されます。

関連リンク

検索バー

検索ドロップダウンリスト

検索バーにテキストを入力していくと、検索バーにリストが表示されます。入力される文字を含むアイテムが検索ドロップダウンリストに投入されます。ドロップダウンリストに表示される各アイテムには、2 つのアイコンとアイテムの名前が含まれます。最初のアイコンはアイテムのカテゴリ（**デバイス**、**起動ウィザード**等）を示します。2 つ目のアイコンは、アイテムの状態（**正常**、**重要**、または**警告**等）を示します。2 つのアイコンのすぐ後に、アイテムの名前が表示されます。ドロップダウンリストのアイテムの上にマウスポインタを移動すると、ツールチップが表示されます。ツールチップに表示される情報は、アイテムによって替わります。例えば、マウスポインタをデバイスの上に移動すると、**名前**、**種類**、**正常性状態**、**電源状態**、**IP アドレス**、**サービスタグ**、および **MAC アドレス** が表示されます。ツールチップに表示されたアイテムを選択すると、デフォルトの処置が実行されます。

関連リンク

検索バー

選択処置

検索バーに表示されたアイテムを選択またはクリックすると、以下のデフォルト処置が行われます：

選択されたアイテム	処置
デバイス	デバイスの詳細を表示します。
デバイスグループ	デバイスグループの概要を表示します。
検出範囲	検出範囲を表示します。
検出範囲グループ	検出範囲グループの概要を表示します。
ポータル	適切なポータルに移動します。
ウィザード	適切なウィザードを起動します。
除外範囲	範囲の概要を表示します。
リモートタスク	タスクツリー内のタスクを選択します。

関連リンク

検索バー

マップビュー（ホーム）ポータル

メモ: マップビュー 機能は、ライセンスを持つ Dell PowerEdge VRTX デバイスを WS-Man プロトコルを使用して検出した場合にのみ利用可能です。ライセンスを持つ PowerEdge VRTX デバイスが SNMP プロトコルを使用して検出された場合、**マップビュー** 機能は利用できません。この場合、WS-Man プロトコルを使用して PowerEdge VRTX デバイスを再検出する必要があります。

マップビュー（ホーム）ポータルへは、**ホーム** ポータル 内の **マップビュー** リンクをクリックすることでアクセスできます。

メモ: デバイス ポータルからアクセスできるマップの別の実装（**マップビュー** タブ）にアクセスすることもできます。

マップビュー（ホーム）ポータルの機能は、次のとおりです。

- **マップビュー**（ホーム）ポータルは、デバイスツリーには統合されていません。
- マップ上部にある **次でフィルタ** ドロップダウンボックスを使用して、マップに表示するデバイスグループを選択することができます。
- **マップビュー**（ホーム）ポータル上のピン（デバイス）をクリックすると、そのデバイスの詳細を表示した **デバイス** ポータルが開きます。
- **マップビュー**（ホーム）ポータル上でのデバイスまたは設定に対する変更は、いずれも **デバイス** ポータルからアクセスできる **マップビュー** タブと同期化されます。
- **マップビュー**（ホーム）ポータルのズームレベルおよび可視領域は、**デバイス** ポータルからアクセスできる **マップビュー** タブとは同期化されません。

メモ: **マップビュー** で使用できる機能の詳細に関しては、「マップビューの使用」を参照してください。

関連リンク

OpenManage Essentials ホームポータルの使い方
マップビュー（ホーム）ポータルのインタフェース

ユーザー情報の表示

OpenManage Essentials 役割などの、現在のユーザーに関連するユーザー情報の表示は、次の手順で行います。

1. マウスポインタをヘッダバナーのユーザー名の上に移動します。
2. 表示されたメニューで、**ユーザー情報** をクリックします。
   ユーザー情報を表示した **<ユーザー名>のユーザー情報** ダイアログボックスが開きます。

関連リンク

OpenManage Essentials ヘッダバナー

異なるユーザーとしてログオン

メモ: Google Chrome および Mozilla Firefox ブラウザでは **異なるユーザーとしてサインイン** オプションは表示されません。Chrome または Firefox の使用時に異なるユーザーとしてログオンするには、ブラウザを閉じてから再度開き、プロンプトで新しいユーザーの資格情報を入力して **OK** をクリックします。

メモ: Internet Explorer で **異なるユーザーとしてサインイン** オプションを使用する場合、資格情報の入力を複数回求められる場合があります。

OpenManage Essentials に異なるユーザーとしてログオンするには、次を実行します。

1. マウスポインタをヘッダバナーのユーザー名の上に移動します。
2. 表示されたメニューで、**異なるユーザーとしてサインイン** をクリックします。
   Windows セキュリティ ダイアログボックスが表示され、ユーザー名とパスワードの入力を求められます。
3. **ユーザー名** および **パスワード** を入力して **OK** をクリックします。

関連リンク

OpenManage Essentials ホームポータルの使い方
OpenManage Essentials ヘッダバナー

アップデートの利用可能通知アイコンの使用

メモ: アップデートの利用可能通知アイコンは、ウェブブラウザの更新後にのみ OpenManage Essentials ヘッダーバナーに表示されます。

アップデートの利用可能通知アイコン  は OpenManage Essentials の新バージョンが利用可能になると OpenManage Essentials ヘッダーバナーに表示されます。マウスポインタをアイコンの上に移動すると、利用可能な新バージョンに関する情報を示すツールチップが表示されます。  アイコンをクリックして Dell TechCenter OpenManage Essentials ウェブページを開き、OpenManage Essentials の新バージョンをダウンロードします。

関連リンク

OpenManage Essentials ヘッダバナー

保証スコアボード通知アイコンの使用

保証スコアボード通知アイコン  は、**プリファランス → 保証通知設定** で設定した基準に基づいて OpenManage Essentials ヘッダーバナーに表示されます。保証スコアボード通知には、設定した基準を満たすデバイスの数も表示されます。  をクリックして **デバイス保証レポート** を表示します。このレポートには **保証スコアボード通知** 設定に基づいてデバイスの保証情報が表示されます。

関連リンク

OpenManage Essentials ヘッダバナー
保証スコアボード通知の設定
デバイス保証レポート

4

OpenManage Essentials ホームポータル - 参照

関連リンク

- OpenManage Essentials ヘッダバナー
- ダッシュボード
- スケジュールビュー
- 検索バー
- マップビュー（ホーム）ポータルのインタフェース

ダッシュボード

このダッシュボードページには、サーバー、ストレージ、スイッチなどを含む管理下デバイスのスナップショットが表示されます。**次でフィルタ：** ドロップダウンリストをクリックすることにより、デバイスに基づいてビューをフィルタできます。また、**次でフィルタ：** ドロップダウンリストから **新規グループの追加** をクリックすることにより、ダッシュボードからデバイスの新しいグループを追加することもできます。

関連リンク

- 検索バー
- 検出済み対インベントリ済みデバイス
- タスク状態
- ホームポータルレポート
- 状態ごとのデバイス
- 重大度ごとのアラート

ホームポータルレポート

ホームポータルダッシュボードページから、次のコンポーネントを監視できます。

- **重大度ごとのアラート**
- **ステータスごとのデバイス**
- **検出済み対インベントリ済みデバイス**
- **アラート**
- **アセット取得情報**
- **アセットメンテナンス情報**
- **アセットサポート情報**
- **ESX 情報**
- **FRU 情報**
- **ハードドライブ情報**
- **HyperV 情報**

- **ライセンス情報**
- **メモリ情報**
- **モジュラーエンクロージャ情報**
- **NIC 情報**
- **PCI デバイス情報**
- **サーバーコンポーネントとバージョン**
- **サーバーの概要**
- **ストレージコントローラ情報**
- **タスク状態**

状態ごとのデバイス

状態ごとのデバイス は、デバイスの状態に関する情報を円グラフ形式で提供します。円グラフのセグメントをクリックすると、デバイスの概要が表示されます。

フィールド	説明
不明	これらのデバイスの正常性状態は不明です。
正常	デバイスは期待どおりに動作中です。
警告	これらのデバイスは、正常ではない動作を示しており、詳細を調べる必要があります。
重要	これらのデバイスは、非常に重要な側面において不具合が発生したことを示唆する動作を示しています。

重大度ごとのアラート

重大度ごとのアラートは、デバイスのアラート情報を円グラフフォーマットで提供します。円グラフのセグメントをクリックすると、デバイスが表示されます。

フィールド	説明
不明	これらのデバイスの正常性状態は不明です。
正常	これらのデバイスからのアラートは、デバイスに期待される動作に従っています。
警告	これらのデバイスは、正常ではない動作を示しており、詳細を調べる必要があります。
重要	これらデバイスからのアラートは、非常に重要な側面において不具合が発生したことを意味しています。

検出済み対インベントリ済みデバイス

グラフは、検出またはインベントリされたデバイスおよび Dell サーバーの数を表示します。このレポートを使用して、分類されていない検出済みデバイスおよび Dell サーバーを確認できます。概要情報のフィルタオプションの詳細に関しては、「デバイス概要の表示」を参照してください。

グラフの一部分をクリックして、選択した領域の **デバイス概要** を表示します。デバイス概要内の行をダブルクリックし、詳細（そのデバイスのインベントリビュー）を表示します。または、右クリックしてインベントリビューの詳細を選択するか、右クリックしてそのデバイスに固有のアラートのためのアラートを選択します。

フィールド	説明
次でフィルタ	これを選択し、次のオプションを使用して検索結果をフィルタします。 • **すべて** • **範囲** — これを選択して、選択した範囲に基づいたフィルタを実行します。

関連リンク

検出とインベントリタスクの設定
設定済みの検出とインベントリ範囲の表示
範囲の除外
検出のスケジュール
インベントリのスケジュール
状態ポーリング頻度の設定
検出とインベントリポータル

タスク状態

グリッドは現在実行されているタスク、および以前実行されたタスクとそれらの状態のリストを提供します。このページの **タスク状態** グリッドは、検出、インベントリ、およびタスク状態だけを表示しますが、メインポータルはすべての種類のタスク状態を表示します。

関連リンク

検出とインベントリタスクの設定
設定済みの検出とインベントリ範囲の表示
範囲の除外
検出のスケジュール
インベントリのスケジュール
状態ポーリング頻度の設定
検出とインベントリポータル

スケジュールビュー

スケジュールビュー から、次の操作を実行できます。

- 予定のタスクと完了したタスクを表示する。

- タスクのタイプ（データベースメンテナンスタスク、サーバーの電源オプションなど）、アクティブなタスク、タスク実行履歴に基づきビューのフィルタを行う。

  メモ: 次によってフィルタ ドロップダウンリストに表示されるオプションは、作成されたタスクによって異なります。 例えば、**サーバーオプションタスク** が作成されていない場合、そのオプションは **次によってフィルタ** ドロップダウンリストには表示されません。
- 特定の日、週、または月のタスクを表示する。また、カレンダーアイコンをクリックすることにより特定の日のタスクを表示することもできる。
- カレンダーの時刻スロットにタスクをドラッグアンドドロップする。
- ズームスライダを変更してズーム値を設定する。

  メモ: ズームスライダは **月** ビューでは無効化されています。
- スケジュールを、**.ics** ファイルにエクスポートして、このファイルを Microsoft Outlook にインポートする。
- 設定アイコンをクリックすることにより、スケジュールビュー設定を変更する。  をクリックします。

詳細は、「スケジュールビュー設定」を参照してください。

関連リンク

スケジュールビュー設定

スケジュールビュー設定

フィールド	説明
向き	**スケジュールビュー** ページと、表示されたタスクの向きを変更することができます。**縦** 方向、または **横** 方向のいずれかを選択できます。 **メモ: 向き** 設定が変更されても、**月** ビューは影響を受けません。
スケジュールアイテムサイズ	表示するタスクのサイズを変更できます。
タスクの種類別色カテゴリ	このオプションを選択すると、色ごとにタスクが分類されます。
タスクの実行履歴の表示	このオプションを選択すると、完了したタスクが表示されます。
データベースメンテナンスの表示	このオプションを選択すると、データベースメンテナンスが発生する時刻を表示できます。

デバイス保証レポート

デバイス保証レポート を表示するには、OpenManage Essentials ヘッダーバナーで  アイコンをクリックします。**デバイス保証レポート** には以下のフィールドが表示されます。

フィールド	説明
保証残存期間が x 日またはそれ以下のすべてのデバイス	**デバイス保証レポート** に含むデバイスを決定します。保証残存期間が指定した日数以下のデバイスが保証レポートに含まれます。
保証期限が切れたデバイスを含める	保証が切れた（0 日）または保証情報のないデバイスを保証通知電子メールに含めるかどうかを指定します。
プレビュー	**保証残存期間が x 日またはそれ以下のすべてのデバイス** で設定した基準に基づく保証レポートを表示します。
OK	**デバイスの保証レポート** で行った変更を保存してレポートを閉じます。
保証事項の表示と更新	デルのウェブサイトを開く際にクリックするリンクを表示します。このサイトでは、デバイスの保証を表示または更新できます。
システム名	ネットワーク上のシステムを識別する一意のシステム名を表示します。
デバイスモデルの種類	システムのモデル情報を表示します。
デバイスタイプ	デバイスの種類を表示します。例えば、サーバーまたは Remote Access Controller です。
残りの日数	デバイスの保証を使用可能な日数を表示します。
出荷日	デバイスが工場から発送された日付を表示します。
サービスタグ	デルが使用するシステムに固有のバーコードラベル識別子を表示します。
サービスレベルコード	特定のシステムに対するパーツのみの保証（POW）、翌営業日オンサイト（NBD）、その他のサービスレベルコードを表示します。
サービスプロバイダ	デバイスへの保証サービスサポートを提供する組織の名前を表示します。
開始日	保証が開始される日付を表示します。
終了日	保証が失効する日付を表示します。
保証の説明	デバイスに適用される保証の詳細を表示します。

関連リンク

保証スコアボード通知アイコンの使用
保証スコアボード通知の設定

マップビュー（ホーム）ポータルのインタフェース

ホーム ポータルからアクセス可能な **マップビュー**（ホーム）ポータルには、**次でフィルタ** ドロップダウンリストがあり、これを使用してマップ上に表示されたデバイスグループをフィルタすることができます。**マップビュー**（ホーム）ポータルで使用可能なメニューとオプションは、**デバイス** ポータルにある **マップビュー** タブ内のものと同じです。**マップビュー** 内のメニューとオプションの詳細に関しては、「マップビュー（デバイス）タブインタフェース」を参照してください。

関連リンク

マップビュー（ホーム）ポータル

5

デバイスの検出とインベントリ

ネットワークデバイスを管理するには、検出とインベントリを実行します。

関連リンク

検出とインベントリタスクの設定
設定済みの検出とインベントリ範囲の表示
検出のスケジュール
インベントリのスケジュール
範囲の除外
対応デバイス、プロトコル、および機能マトリックス

対応デバイス、プロトコル、および機能マトリックス

メモ: 次の表にリストされている機能の説明については、凡例と定義を参照してください。

プロトコル / メカニズム		簡易ネットワーク管理プロトコル (SNMP)	Windows Management Instrumentation (WMI)	Web Services-Management (WS-Man)
OpenManage Server Administrator をインストールした Dell サーバー	Windows / Hyper-V	検出 相関 分類 ハードウェアインベントリ ソフトウェアインベントリ監視 トラップ / アラート アプリケーションの起動 • OpenManage Server Administrator コンソール • リモートデスクトップ	検出 相関 分類 ハードウェアインベントリ ソフトウェアインベントリ監視 アプリケーションの起動 • OpenManage Server Administrator コンソール • リモートデスクトップ	非対応
	Linux/VMware ESX	検出 相関	非対応	非対応

プロトコル / メカニズム		簡易ネットワーク管理プロトコル(SNMP)	Windows Management Instrumentation (WMI)	Web Services-Management（WS-Man)
		分類 ハードウェアインベントリ ソフトウェアインベントリ 監視 トラップ / アラート		
	VMware ESXi	トラップ / アラート	非対応	検出 相関 分類 ハードウェアインベントリ ソフトウェアインベントリ 仮想マシン情報 仮想ホストの製品情報 監視（OpenManage Server Administrator の正常性のみ） アプリケーションの起動
OpenManage Server Administrator をインストールしていない Dell サーバー	Windows / Hyper-V	非対応	検出 相関 分類 ハードウェアインベントリ アプリケーションの起動 • リモートデスクトップ	非対応
	Linux/VMware ESX	非対応	非対応	非対応

プロトコル / メカニズム		簡易ネットワーク管理プロトコル(SNMP)	Windows Management Instrumentation（WMI）	Web Services-Management（WS-Man）
	VMware ESXi	非対応	非対応	検出 相関 分類 ハードウェアインベントリ（ストレージインベントリなし）
iDRAC/DRAC/BMC		検出 相関 分類 トラップ / プラットフォームイベントトラップ（PET）の監視 アプリケーションの起動 • RAC • コンソール	非対応	検出 ハードウェアインベントリ システムアップデート **メモ:** iDRAC 6 バージョン 1.3 以降にのみ適用されます。iDRAC 6 バージョン 1.25 以前では、検出およびハードウェアインベントリはサポートされません。
モジュールエンクロージャ（PowerEdge M1000e）		検出 相関 分類 エンクロージャ正常性 トラップ アプリケーションの起動 • CMC • コンソール	非対応	検出 相関 分類 エンクロージャ正常性 トラップ アプリケーションの起動 • CMC • コンソール

プロトコル / メカニズム	簡易ネットワーク管理プロトコル(SNMP)	Windows Management Instrumentation (WMI)	Web Services-Management (WS-Man)
			メモ: CMC ファームウェアバージョン 5.0 の PowerEdge M1000e のみに該当します。
Dell PowerEdge VRTX	検出 相関 分類 エンクロージャ正常性 トラップ アプリケーションの起動 • CMC • コンソール	非対応	検出 相関 分類 ハードウェアインベントリ システムアップデート エンクロージャ正常性 トラップ アプリケーションの起動 • CMC • コンソール マップビュー (PowerEdge VRTX のみ)
Dell Networking W シリーズのモビリティコントローラとアクセスポイント	検出 インベントリ 分類 アプリケーションの起動 トラップ / アラート 正常性 - アクティブおよび非アクティブ 役割の切り替え	非対応	非対応
Dell SonicWALL ファイアウォールアプライアンス	検出	非対応	非対応

プロトコル / メカニズム	簡易ネットワーク管理プロトコル(SNMP)	Windows Management Instrumentation（WMI）	Web Services-Management（WS-Man）
	分類 アプリケーションの起動 トラップ / アラート		
Dell Networking イーサネットスイッチ	検出 相関 分類 アプリケーションの起動 トラップ / アラート 正常性 役割の切り替え	非対応	非対応
Brocade ファイバチャネルスイッチ	検出 分類 アプリケーションの起動 トラップ / アラート 正常性 役割の切り替え	非対応	非対応

メモ: OpenManage Essentials でシャーシの全機能をサポートするには、適切なプロトコルを使用して、シャーシおよび関連デバイスを検出する必要があります。

対応オペレーティングシステム（サーバー）、プロトコル、および機能マトリックス

メモ: 次の表にリストされている機能の説明については、凡例と定義を参照してください。

プロトコル / メカニズム		Intelligent Platform Management Interface（IPMI）	コマンドラインインタフェース（CLI）	セキュアシェル（SSH）
OpenManage Server Administrator を	Windows/Hyper-V	非対応	OpenManage Server Administrator CLI	非対応

プロトコル / メカニズム		Intelligent Platform Management Interface（IPMI）	コマンドラインインタフェース（CLI）	セキュアシェル（SSH）
インストールした Dell サーバー			OpenManage Server Administrator の導入 サーバーアップデート • BIOS • ファームウェア • ドライバ	
	Linux/VMware ESX	非対応	OpenManage Server Administrator CLI OpenManage Server Administrator の導入 サーバーアップデート • BIOS • ファームウェア • ドライバ	検出 相関 分類 ハードウェアおよびソフトウェアインベントリ（最小限）
	VMware ESXi	非対応	非対応	検出 相関 分類 ハードウェアおよびソフトウェアインベントリ（最小限）
	XenServer	非対応	RACADM CLI IPMI CLI OpenManage Server Administrator CLI 電源タスク	非対応
OpenManage Server Administrator をインストールし	Windows/Hyper-V	非対応	OpenManage Server Administrator の導入	非対応

プロトコル / メカニズム		Intelligent Platform Management Interface（IPMI）	コマンドラインインタフェース（CLI）	セキュアシェル（SSH）
ていない Dell サーバー	Linux/VMware ESX	非対応	OpenManage Server Administrator の導入	検出 相関 分類 ハードウェアおよびソフトウェアインベントリ（最小限）
	VMware ESXi	非対応	非対応	検出 相関 分類 ハードウェアおよびソフトウェアインベントリ（最小限）
	PowerEdge C	検出 分類 アプリケーションの起動	RACADM CLI IPMI CLI	非対応
iDRAC/DRAC/BMC		検出 分類 相関 iDRAC の正常性 アプリケーションの起動 RAC コンソール	RACADM CLI IPMI CLI	非対応
モジュラーエンクロージャ（M1000e）/ PowerEdge VRTX/PowerEdge FX		非対応	RACADM CLI IPMI CLI	非対応
Dell Networking W シリーズのモビリティコントローラとアクセスポイント		非対応	非対応	非対応
Dell SonicWALL ファイアウォールアプライアンス		非対応	非対応	非対応
Dell Networking イーサネットスイッチ		非対応	非対応	非対応

プロトコル / メカニズム	Intelligent Platform Management Interface（IPMI）	コマンドラインインタフェース（CLI）	セキュアシェル（SSH）
Brocade ファイバチャネルスイッチ	非対応	非対応	非対応

a) デバイスが検出されていない、インベントリされていない、またはその両方の場合、このタスクを実行することはできません。

対応ストレージデバイス、プロトコル、および機能マトリックス

メモ: 次の表にリストされている機能の説明については、「凡例と定義」を参照してください。

プロトコル / メカニズム		簡易ネットワーク管理プロトコル（SNMP）	シンボル	EMC Navisphere CLI
ストレージデバイス	Dell EqualLogic	検出 相関 分類 ハードウェアインベントリ 監視 トラップ / アラート アプリケーションの起動 — EqualLogic コンソール **メモ:** グループ管理 IP またはストレージグループ管理 IP のみを使用して EqualLogic ストレージアレイを検出し、検出範囲の設定にあるいずれのメンバー IP も含まないことをお勧めします。	非対応	非対応
	Dell|EMC	検出 相関 分類	非対応	ハードウェアインベントリ 監視

プロトコル / メカニズム		簡易ネットワーク管理プロトコル（SNMP）	シンボル	EMC Navisphere CLI
	メモ: Dell| EMC デバイスを完全に管理するには、SNMP と Navisphere の両方が必要です。	トラップ / アラート		アプリケーションの起動 — EMC Navisphere Manager
	PowerVault	トラップ / アラート	検出 相関 分類 ハードウェアインベントリ 監視 アプリケーションの起動 — Modular Disk Storage Manager（a）	非対応
	Compellent	検出 分類 ハードウェアインベントリ 監視 トラップ / アラート アプリケーションの起動 — Compellent コンソール	非対応	非対応
	テープ	検出 相関 分類 ハードウェアインベントリ 監視 トラップ / アラート	非対応	非対応

プロトコル / メカニズム		簡易ネットワーク管理プロトコル（SNMP）	シンボル	EMC Navisphere CLI
		アプリケーションの起動 テープコンソール		

a）OpenManage Essentials システムに モジュラディスクストレージマネージャコントローラソフトウェアがインストールされている必要があります。

凡例と定義

- **検出：**ネットワーク上のデバイスを検出する機能。
- **相関：**次の装置を相関させる機能。
  - 検出済みサーバー、および DRAC、iDRAC、または BMC デバイス。
  - 検出済みモジュラシステムまたはスイッチ。
  - ESX、ESXi、または Hyper-V ホストとゲスト仮想マシン。
- **分類**：タイプごとにデバイスを分類する機能。例えば、サーバー、ネットワークスイッチ、ストレージなどです。
- **ハードウェアインベントリ：**デバイスの詳細なハードウェアインベントリを取得する機能。
- **監視または正常性：**デバイスの正常性状態および接続状態を取得する機能。
- **トラップ、アラート、または PET：**デバイスから SNMP トラップを受け取る機能。
- **アプリケーションの起動：**1x1 コンソールまたはアプリケーションを起動するため、検出済みデバイスで右クリック処置のメニューアイテムを提供。
- **OpenManage Server Administrator CLI：**リモート（検出済み）サーバーで OpenManage Server Administrator 対応コマンドを実行する機能。
- **OpenManage Server Administrator の導入：**OpenManage Server Administrator をリモート（検出済み）サーバーに導入する機能。
- **サーバーアップデート：**リモート（検出済み）サーバーに、BIOS、ファームウェア、ドライバアップデートを導入する機能。
- **RACADM CLI：**リモート（検出済み）サーバーで、RACADM ツール対応コマンドを実行する機能。
- **IPMI CLI：**リモート（検出済み）サーバーで、IPMI ツール対応コマンドを実行する機能。
- **スイッチ役割：**管理またはスタックといったユニットのタイプを示します。

検出とインベントリのポータルの使い方

検出とインベントリポータルにアクセスするには、**管理 → 検出とインベントリ** の順にクリックします。

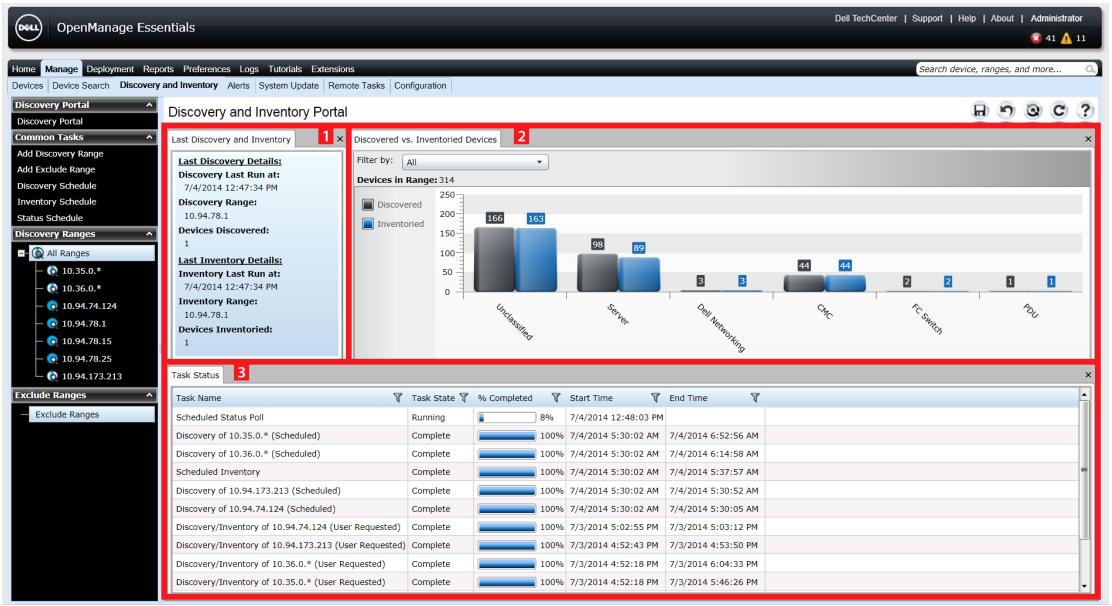


図 2. 検出とインベントリポータル

1. 最後に実行された検出とインベントリタスクの詳細。
2. 以前に検出およびインベントリされたデバイスの詳細。
3. タスクとその状態の詳細。

検出用のプロトコルサポートマトリックス

次の表は、デバイス検出での対応プロトコルに関する情報を示しています。推奨プロトコルは ***斜体*** で表記されます。

デバイス / オペレーティングシステム	プロトコル				
	簡易ネットワーク管理プロトコル（SNMP）	**Web Services-Management（WS-Man）**	**Windows Management Instrumentation（WMI）**	**Intelligent Platform Management Interface（IPMI）**	**セキュアシェル（SSH）**
iDRAC 6、iDRAC 7、または iDRAC 8	対応	***対応***	該当なし	対応	非対応
Linux	***OpenManage Server Administrator（OMSA）インストール済みの場合に対応***	該当なし	該当なし	該当なし	対応
Windows	***OMSA インストール済みの場合に対応***	該当なし	OMSA インストール済みの場合に対応、OMSA 未インストール	該当なし	該当なし

デバイス / オペレーティングシステム	プロトコル				
	簡易ネットワーク管理プロトコル（SNMP）	**Web Services-Management（WS-Man）**	**Windows Management Instrumentation（WMI）**	**Intelligent Platform Management Interface（IPMI）**	**セキュアシェル（SSH）**
			済みの場合は正常性情報なし		
ESXi	OMSA インストール済みの場合に対応	***OMSA インストールに関わらず対応***	該当なし	該当なし	非対応
Citrix XenServer	***OMSA インストール済みの場合に対応***	該当なし	該当なし	該当なし	OMSA インストール済みの場合に対応、OMSA 未インストール済みの場合は正常性情報なし
PowerEdge M1000e（CMC）	***対応***	CMC ファームウェアバージョン 5.0 以降がインストール済みの場合に対応	該当なし	該当なし	非対応
PowerEdge VRTX（CMC）	対応	***対応***	該当なし	該当なし	非対応
PowerEdge-C	該当なし	該当なし	該当なし	***対応***	非対応
クライアント	インストールされた Dell コマンド | 監視によってサポート；Dell コマンド | 監視がない場合は正常性情報なし	該当なし	***インストールされた Dell コマンド| 監視によってサポート；Dell コマンド| 監視がない場合は正常性情報なし***	該当なし	該当なし
ストレージデバイス	対応	該当なし	該当なし	該当なし	該当なし
イーサネットスイッチ	対応	該当なし	該当なし	該当なし	該当なし

システムアップデート用のプロトコルサポートマトリックス

次の表は、システムアップデートタスクでの対応プロトコルに関する情報を示しています。推奨プロトコルは ***斜体*** で表記されます。

デバイス / オペレーティングシステム	プロトコル				
	簡易ネットワーク管理プロトコル（SNMP）	Web Services-Management（WS-Man）	Windows Management Instrumentation（WMI）	Intelligent Platform Management Interface（IPMI）	セキュアシェル（SSH）
iDRAC 6、iDRAC 7、または iDRAC 8	非対応	*対応*	該当なし	該当なし	該当なし
Linux	*OpenManage Server Administrator（OMSA）インストール済みの場合に対応*	該当なし	該当なし	該当なし	非対応
Windows	*OMSA インストール済みの場合に対応*	該当なし	OMSA インストール済みの場合に対応	該当なし	該当なし
ESXi	非対応	*iDRAC 6、iDRAC 7、または iDRAC 8 に対応*	該当なし	該当なし	該当なし
Citrix XenServer	非対応	該当なし	該当なし	該当なし	該当なし
PowerEdge M1000e（CMC）	*対応、RACADM ツールが必要*	CMC ファームウェアバージョン 5.0 以降がインストール済みの場合に対応	該当なし	該当なし	該当なし
PowerEdge VRTX（CMC）	非対応	*対応、RACADM ツールが必要*	該当なし	該当なし	該当なし

サービスタグをレポートしないデバイス

以下のデバイスでは、OpenManage Essentials コンソールにサービスタグが表示されません。

- KVM
- Dell PowerVault 132T
- PowerVault 136T
- PowerVault ML6000
- Dell Networking W シリーズモビリティコントローラ
- Dell SonicWALL ファイアウォールアプライアンス（グローバル正常性状態も使用不可です）
- プリンタ
- PDU
- UPS

メモ: サービスタグ情報がないため、これらのデバイスの保証情報は使用できません。

検出とインベントリタスクの設定

1. OpenManage Essentials から、**管理 → 検出とインベントリ → 一般タスク → 検出範囲の追加** をクリックします。

   デバイスの検出 ウィザードが表示されます。表示されるウィザードの種類は、**プリファランス → 検出設定** の設定によって異なります。「検出の設定の指定」を参照してください。
2. **検出範囲の設定** で、次の手順を行います。
   a. 範囲のグループを作成する場合は、**グループとして保存** を選択し、**グループ名** を入力します。
   b. IP アドレス / 範囲またはホスト名およびサブネットマスクを指定します。**追加** をクリックします。

      メモ: 複数の IP アドレス、範囲、またはホスト名を追加できます。複数のホスト名をコンマ区切り記号で区切って（例えば、ホスト名 1, ホスト名 2, ホスト名 3）追加することもできます。
   c. ホスト名および IP アドレスをインポートするには、**インポート** をクリックします。.CSV ファイルに行項目として含まれたホスト名および IP アドレスを使用してインポートすることもできます。Microsoft Excel を使用して、ホスト名または IP アドレスを含む .CSV ファイルを作成できます。
   d. **次へ** をクリックします。
3. 検出設定 で **標準ウィザード** を選択した場合 – 少なくとも 1 つの IP アドレス、IP 範囲、ホスト名、またはこれらの組み合わせの指定後、検出とインベントリオプションのカスタマイズを続行するか、デフォルトのオプションを使用して設定を完了します。これ以上の設定を行わずに **終了** をクリックすると、デフォルトの SNMP および ICMP プロトコルを使用して検出とインベントリがただちに実行されます。**終了** をクリックする前に、プロトコル設定を確認し、修正することをお勧めします。

   リストの各プロトコルについての情報は、ヘルプアイコンをクリックしてください。  適切なプロトコル設定画面です。

   メモ: ESXi ベースのサーバーを検出する場合、ホストと共にグループ化されたゲスト仮想マシンを表示するには、WS-Man プロトコルを有効にして設定します。

   メモ: デフォルトでは、SNMP が有効になっており、値は割り当てられた ICMP パラメータです。

   メモ: 次のいずれかの手順を完了したら、**次へ** をクリックして続行するか、**終了** をクリックして **検出範囲の設定** を完了します。

   - ネットワーク上のデバイスを検出するために、**ICMP 設定** で ICMP パラメータを編集します。
   - サーバーを検出するために、**SNMP の設定** で SNMP パラメータを指定します。**コミュニティの取得** で指定した SNMP コミュニティ文字列が、デバイスまたは検出しようとしているデバイスの SNMP コミュニティ文字列と一致していることを確認してください。

     メモ: iDRAC はデフォルトの SNMP ポート 161 のみをサポートします。デフォルトの SNMP ポートが変更されている場合、iDRAC は検出されない可能性があります。
   - 認証してリモートデバイスに接続するためには、**WMI 設定** で WMI パラメータを指定します。WMI の資格情報を入力するためのフォーマットは、ドメインベースのネットワークでは *ドメイン\ユーザー名*、非ドメインベースのネットワークでは *ローカルホスト\ユーザー名* です。
   - PowerVault モジュラディスクアレイまたは EMC デバイスを検出するには、**ストレージ設定** でパラメータを編集します。
   - **WS-Man 設定** で、WS-Man パラメータを入力して Dell PowerEdge VRTX、iDRAC 6、iDRAC 7、および ESXi がインストールされたサーバーの検出を有効化します。
   - **SSH 設定** で、SSH パラメータを入力して Linux ベースのサーバーの検出を有効化します。

- サーバーの検出を有効にするには、**IPMI 設定** で IPMI パラメータを指定します。IPMI は、通常、Dell サーバーでの BMC または iDRAC の検出に使用されます。RAC デバイスを検出する場合、オプションの KG キーを含めることができます。
- **検出範囲処置** で、検出またはインベントリを選択するか、両方のタスクを実行します。デフォルトのオプションでは、検出とインベントリの両方を実行します。
- **検出のみを実行** または **検出とインベントリの両方を実行** を選択して、タスクをただちに実行します。
- 後でタスクを実行するようスケジュールするには、**検出またはインベントリを実行しない** を選択して、検出のスケジュール および インベントリのスケジュール の手順に従います。

4. 検出設定 で **ガイド付きウィザード** を選択している場合 – 少なくとも 1 つの IP アドレス、IP 範囲、ホスト名、またはこれらの組み合わせを指定して、**次へ** をクリックします。すると、**デバイスタイプのフィルタリング** ウィンドウが表示されます。「デバイスタイプのフィルタリング」を参照してください。
   a. 検出および管理したいデバイスタイプを選択します。
      選択されたデバイスの検出に必要なプロトコルが、**デバイスの検出** ウィザードに追加されます。
   b. ウィザードに、表示されたすべてのプロトコルの設定詳細を入力して **次へ**をクリックします。
5. サマリ画面で選択内容を確認し、**終了** をクリックします。前の設定画面のパラメータを変更するには、**戻る** をクリックします。完了したら、**終了** をクリックします。

関連リンク

検出とインベントリポータル
最後の検出とインベントリ
検出済み対インベントリ済みデバイス
タスク状態

デフォルト SNMP ポートの変更

SNMP は、一般の SNMP メッセージには、デフォルトの UDP ポート 161 を、SNMP トラップメッセージには、UDP ポート 162 を使用します。これらのポートが他のプロトコルまたはサービスによって使用されている場合は、システムのローカルサービスファイルで設定を変更できます。

管理下ノードを設定し、OpenManage Essentials がデフォルトではない SNMP ポートを使用するようにするには、次の手順を実行します。

1. 管理ステーションと管理下ノードの両方で、C:\Windows\System32\drivers\etc に移動します。
2. メモ帳で Windows SNMP **サービス** ファイルを開いて以下を編集します。
   - 受信 SNMP トラップポート（OpenManage Essentials でアラートを受信）– 「`snmptrap 162/udp snmp-trap #SNMP trap`」の行のポート番号を変更します。変更後、SNMP トラップサービスと SNMP サービスを再起動します。管理ステーションでは、DSM Essentials ネットワークモニターサービスを再起動します。
   - 送信 SNMP リクエスト（OpenManage Essentials での検出 / インベントリ）– 「`snmp 161/udp #SNMP`」の行のポート番号を変更します。変更後、SNMP サービスを再起動します。管理ステーションでは、DSM Essentials ネットワークモニターサービスを再起動します。
3. 送信トラップポート – OpenManage Essentials トラップ転送アラートアクションで、**宛先** フィールドに *<<トラップ宛先アドレス：ポート番号>>* を指定します。

メモ: デフォルトポートで IP セキュリティが SNMP メッセージを暗号化するように設定していた場合は、IP セキュリティポリシーを新しいポートの設定でアップデートしてください。

ルート証明書付き WS-Man プロトコルを使用した Dell デバイスの検出とインベントリ

始める前に、ルート CA サーバー、OpenManage Essentials 管理サーバー、WS-Man ターゲットがホスト名で互いに ping できることを確認してください。

ルート証明書付き WS-Man プロトコルを使用して Dell デバイスの検出とインベントリを行うには、以下の手順を実行します。

1. ターゲットデバイス（iDRAC または CMC）のウェブコンソールを開きます。
2. 新規証明書署名要求ファイルの生成：
   a. **ネットワーク** をクリックしてから **SSL** をクリックします。
      SSL メインメニュー ページが表示されます。
   b. **新規証明書署名要求（CSR）の生成** を選択して **次へ** をクリックします。
      証明書署名要求（CSR）の生成 ページが表示されます。
   c. 該当する場合は、必須フィールドに適切な情報を入力します。**コモンネーム** がデバイスのウェブコンソールへのアクセスに使用するホスト名と同じであることを確認し、**生成** をクリックします。
   d. プロンプトが表示されたら、**request.csr** ファイルを保存します。
3. **Microsoft Active Directory 証明書サービス – root CA** ウェブサーバー：**http://signingserver/certsrv** を開きます。
4. **タスクの選択** で **証明書の要求** をクリックします。
   証明書の要求 ページが表示されます。
5. **証明書の要求の詳細設定** をクリックします。
   証明書の要求の詳細設定 ページが表示されます。
6. **Base 64 エンコーディングされた CMC または PKCS #10 ファイルを使用して証明書要求を送信、または Base 64 エンコーディングされた PKCS #7 ファイルを使用して更新要求を送信** をクリックします。
7. テキストエディタを使用して、手順 2 d で保存した証明書署名要求（.csr または .txt）ファイルを開きます。
8. 証明書署名要求ファイルの内容をコピーして **保存済み要求** フィールドに貼り付けます。
9. **証明書テンプレート** リストで **ウェブサーバー** を選択し、**送信 >** をクリックします。
   発行済み証明書 ページが表示されます。
10. **Base 64 エンコーディング済み** をクリックし、次に **証明書のダウンロード** をクリックします。
11. プロンプトが表示されたら、**certnew.cer** ファイルを保存します。
12. ターゲットデバイス（iDRAC または CMC）のウェブコンソールを開きます。
13. **ネットワーク** をクリックしてから **SSL** をクリックします。
    SSL メインメニュー ページが表示されます。
14. **生成された CSR に基づいたサーバー証明書のアップロード** を選択して **次へ** をクリックします。
    証明書アップロード ページが表示されます。
15. **参照** をクリックし、手順 11 で保存した **certnew.cer** ファイルを選択して **適用** をクリックします。
16. RootCA 署名済み証明書（**newcert.cer**）を **信頼できる root 証明機関** として OpenManage Essentials 管理サーバーにインストールします。

    メモ: インストールする証明書ファイルが、root CA が発行した Base64 エンコーディング済み証明書ファイルであることを確認します。

    a. **certnew.cer** ファイルを右クリックし、**証明書のインストール** をクリックします。
       証明書のインポートウィザード が表示されます。
    b. **次へ** をクリックします。
    c. **すべての証明書を以下のストアに置く** を選択して **参照** をクリックします。
       証明書ストアの選択 ダイアログボックスが表示されます。
    d. **信頼できるルート証明機関** を選択して **OK** をクリックします。
    e. **次へ** をクリックします。
    f. **終了** をクリックします。

セキュリティ警告 ダイアログボックスが表示されます。

g. **はい** をクリックします。

17. ウェブブラウザを閉じ、ターゲットデバイス（iDRAC または CMC）のウェブコンソールを新しいブラウザウィンドウで開きます。
18. **newcert.cer** RootCA 署名証明書ファイルを使用して WS-Man ターゲットを OpenManage Essentials で検出してインベントリします。

範囲の除外

除外範囲を設定して、サーバーが検出されるまたは 再検出されることを防止するか、デバイスツリーに表示されるデバイス数を制限します。

検出タスクから範囲を除外するには、次の手順を行います。

1. OpenManage Essentials から、**管理 → 検出とインベントリ → 一般タスク → 除外範囲の追加** を選択します。
2. **除外範囲の設定** で、IP アドレス / 範囲またはホスト名を指定し、**追加** をクリックします。
3. **終了** をクリックします。

関連リンク

検出とインベントリポータル
最後の検出とインベントリ
検出済み対インベントリ済みデバイス
タスク状態

設定済みの検出とインベントリ範囲の表示

OpenManage Essentials で、**管理 → 検出とインベントリ → 検出範囲 → すべての範囲** をクリックします。

関連リンク

検出とインベントリポータル
最後の検出とインベントリ
検出済み対インベントリ済みデバイス
タスク状態

検出のスケジュール

メモ: 検出タスクは **データベースメンテナンスの実行スケジュール** と同時にスケジュールしないことをお勧めします。データベースメンテナンス中はコンソールの反応が遅くなるためです。

検出をスケジュールするには、次の手順を実行します。

1. **管理 → 検出とインベントリ → 共通タスク → 検出のスケジュール** をクリックします。
2. **検出スケジュールの設定** で、次を実行します。
   - 希望のスケジュールパラメータを選択します。
   - （オプション）より高速なタスク実行のためにタスク速度のスライダを調整することができますが、速度を上昇させると、より多くのシステムリソースが消費されます。
   - 計装デバイスをすべて検出します。

関連リンク

検出とインベントリポータル

最後の検出とインベントリ
検出済み対インベントリ済みデバイス
タスク状態

検出速度スライダ

これは検出スロットルとも呼ばれ、検出の速度、および検出によって消費されるネットワークとシステムのリソースを制御します。これは次を制御することによって行われます。

- ある時点で実行することが可能な検出スレッド数
- ネットワークの ping スイープ中における通信デバイス間でのミリ秒単位の遅延

メモ: スロットル制御の各目盛りは 10 % であり、範囲は 10～100 % になっています。OpenManage Essentials では、検出スロットルはデフォルトで 60 % に設定されています。IT Assistant からのアップグレード後も、スロットル制御は以前設定した値が維持されます。

マルチスレッディング

Dell OpenManage Essentials は、IT Assistant で導入されたネットワーク監視サービスにおける最適化されたパラレルスレッディングの実装を改善します。

検出処理では I/O インテンシブであるため、検出処理をパラレル操作にすることによって検出処理を最適化することができます。この操作では、パラレルに実行されるスレッド（マルチスレッドとして知られています）が、複数のデバイスに対するリクエスト送信と応答処理を一度に実行します。

パラレスで動作するスレッド（それぞれ異なるデバイスとの通信）の数が多くなるほど検出速度が早くなり、ネットワーク全体の輻そうや遅延が回避されます。検出処理では、デフォルトで一度に最大 32 のスレッドをパラレル（同時）に実行することが可能です。

パラレルスレッドの実行数を制御するには、検出スロットルコントロールを左右いずれかに動かします。最大に設定すると、32 のパラレルスレッドの実行が可能になります。スロットルが 50% の時、一度に実行可能なスレッド数は 16 のみです。

検出サービスはパラレルスレッディング動作に最適化されているため、システムは、同じスロットル設定であっても、より多くのシステムリソースを活用できます。検出速度と OpenManage Essentials で使用可能なシステムリソースの間で、納得のいくバランスを取るために、システムリソースを監視することが推奨されます。スロットルの増減は、実行されているシステムと、利用できるリソースに左右されます。検出サービスが新しいスロットル設定に適応するには、数分かかる場合があることに留意してください。

メモ: 中～大規模（数百～数千デバイス）ネットワーク上での検出時間を最短にするためには、マルチプロセッサシステムに、OpenManage Essentials サービスをインストールすることを推奨します。

インベントリのスケジュール

メモ: インベントリタスクは **データベースメンテナンスの実行スケジュール** と同時にスケジュールしないことをお勧めします。データベースメンテナンス中はコンソールの反応が遅くなるためです。

インベントリをスケジュールするには、次の手順を実行します。

1. **管理** → **検出とインベントリ** → **共通タスク** → **インベントリのスケジュール** をクリックします。
2. **インベントリポーリング設定** で、次の手順を実行します。
   - **インベントリの有効化** を選択します。

- 希望のスケジュールパラメータを選択します。
- （オプション） より高速なタスク実行のために **インベントリポーリング速度** スライダを調整することができますが、より多くのシステムリソースが消費されます。

関連リンク

検出とインベントリポータル
最後の検出とインベントリ
検出済み対インベントリ済みデバイス
タスク状態

状態ポーリング頻度の設定

メモ: 状態ポーリングは **データベースメンテナンスの実行スケジュール** と同時にスケジュールしないことをお勧めします。データベースメンテナンス中はコンソールの反応が遅くなるためです。

OpenManage Server Administrator など正常性計装手段を備えた、すべての検出されたデバイスの正常性状態をチェックするように OpenManage Essentials を設定できます。ステータスは、正常性状態が常に最新のものであるように、状態ポーリングを使用して所定の間隔でスケジュールできます。

状態ポーリングを設定するには、次の手順を行います。

1. **管理 → 検出とインベントリ → 共通タスク → 状態スケジュール** をクリックします
2. **状態ポーリングスケジュールの設定** で **状態ポーリングを有効にする** を選択し、時間およびパフォーマンスなどのポーリングパラメータを入力します。
3. **OK** をクリックします。

関連リンク

検出とインベントリポータル
最後の検出とインベントリ
検出済み対インベントリ済みデバイス
タスク状態

6

検出とインベントリ - 参照

検出とインベントリ ポータルページでは、次のことができます。

- 検出およびインベントリが行われたデバイスおよび Dell サーバーのグラフィックレポートを表示。
- デバイスおよび Dell サーバーの検出範囲を管理。
- デバイスおよび Dell サーバーの検出、インベントリ、および状態ポーリングを設定。

検出とインベントリポータルページのオプション

- 検出ポータル
- 一般タスク
  - 検出範囲の追加
  - 除外範囲の追加
  - 検出のスケジュール
  - インベントリスケジュール
  - 状態スケジュール
- 検出範囲
- 除外範囲

検出とインベントリポータル

検出とインベントリポータルページでは、次の情報が提供されます。

- 最後の検出とインベントリの詳細
- 検出済み対インベントリ済みデバイス
- タスク状態

関連リンク

検出とインベントリタスクの設定
設定済みの検出とインベントリ範囲の表示
範囲の除外
検出のスケジュール
インベントリのスケジュール
状態ポーリング頻度の設定
最後の検出とインベントリ
検出済み対インベントリ済みデバイス
タスク状態

最後の検出とインベントリ

フィールド	説明
最後の検出の詳細	
最後に検出が実行された時間	最後に実行された検出の時間および日付情報を表示します。
検出範囲	IP アドレス範囲またはホスト名を表示します。
検出されたデバイス	検出されたデバイスの数に関する情報を表示します。
最後のインベントリの詳細	
最後にインベントリが実行された時間	最後に実行されたインベントリの時間および日付情報を表示します。
インベントリ範囲	IP アドレス範囲またはホスト名を表示します。
インベントリされたデバイス	インベントリされたデバイスの数に関する情報を表示します。

関連リンク

検出とインベントリタスクの設定
設定済みの検出とインベントリ範囲の表示
範囲の除外
検出のスケジュール
インベントリのスケジュール
状態ポーリング頻度の設定
検出とインベントリポータル

検出済み対インベントリ済みデバイス

グラフは、検出またはインベントリされたデバイスおよび Dell サーバーの数を表示します。このレポートを使用して、分類されていない検出済みデバイスおよび Dell サーバーを確認できます。概要情報のフィルタオプションの詳細に関しては、「デバイス概要の表示」を参照してください。

グラフの一部分をクリックして、選択した領域の **デバイス概要** を表示します。デバイス概要内の行をダブルクリックし、詳細（そのデバイスのインベントリビュー）を表示します。または、右クリックしてインベントリビューの詳細を選択するか、右クリックしてそのデバイスに固有のアラートのためのアラートを選択します。

フィールド	説明
次でフィルタ	これを選択し、次のオプションを使用して検索結果をフィルタします。 • **すべて**

フィールド	説明
	• **範囲** — これを選択して、選択した範囲に基づいたフィルタを実行します。

関連リンク

検出とインベントリタスクの設定
設定済みの検出とインベントリ範囲の表示
範囲の除外
検出のスケジュール
インベントリのスケジュール
状態ポーリング頻度の設定
検出とインベントリポータル

タスク状態

グリッドは現在実行されているタスク、および以前実行されたタスクとそれらの状態のリストを提供します。このページの **タスク状態** グリッドは、検出、インベントリ、およびタスク状態だけを表示しますが、メインポータルはすべての種類のタスク状態を表示します。

関連リンク

検出とインベントリタスクの設定
設定済みの検出とインベントリ範囲の表示
範囲の除外
検出のスケジュール
インベントリのスケジュール
状態ポーリング頻度の設定
検出とインベントリポータル

デバイスサマリの表示

1. **OpenManage Essentials** で、**管理** → **検出とインベントリ** → **検出ポータル** → **検出ポータル** の順にクリックします。
2. **検出済み対インベントリ済みデバイス** グラフィックレポートで、検出またはインベントリされたデバイスを示すバーをクリックして、選択したグラフの詳細を表示する **デバイス概要** ページを開きます。
3. （オプション）サマリ情報をフィルタするには、じょうごアイコンをクリックします。
   フィルタオプションが表示されます。「デバイスサマリフィルタオプションの表示」を参照してください。
4. （オプション）**フィルタ** をクリックして、フィルタされたサマリ情報を表示します。
5. （オプション）**フィルタのクリア** をクリックして、フィルタされたサマリ情報を削除します。
6. デバイス概要を右クリックして、使用可能なオプションから選択します。「デバイス状態」を参照してください。

デバイス概要フィルタオプションの表示

フィールド	説明
すべて選択	これを選択して、行項目ごとにフィルタします。
オプション、デバイス、または Dell サーバーを選択します。	これを選択して、オプション、デバイス、または Dell サーバーに基づいてフィルタします。
フィルタオプション	これらのオプションを伴うフィルタを作成します。 • **同じ** — これを選択して、「*と同じ*」ロジックを作成します。 • **異なる** — これを選択して、「*と異なる*」ロジックを作成します。 • **未満** — これを選択して、指定する値未満の値を検索します。 • **以下** — これを選択して、指定する値以下の値を検索します。 • **以上** — これを選択して、指定する値以上の値を検索します。 • **超過** — これを選択して、指定する値を超える値を検索します。 **正常性状態** オプション： • **不明** • **正常** • **警告** • **重要** **接続状態** オプション： • **オン** • **オフ**

検出範囲の追加

1. **管理** → **検出とインベントリ** → **一般タスク**をクリックします。
2. **検出範囲の追加** をクリックします。詳細については、「検出とインベントリタスクの設定 を参照してください。
3. 検出、インベントリ、またはその両方に、適切なプロトコルの情報を指定します。
   - 検出設定
   - ICMP 設定
   - SNMP 設定
   - WMI 設定
   - ストレージ設定
   - WS-Man 設定
   - SSH 設定
   - IPMI 設定

- 検出範囲処置
- 概要

検出設定

検出範囲は、デバイスの検出のために OpenManage Essentials に登録されたネットワークセグメントです。OpenManage Essentials は、有効化されているすべての登録済み検出範囲にあるデバイスの検出を試みます。検出範囲には、サブネット、サブネット上の IP アドレスの範囲、個々の IP アドレス、または個々のホスト名が含まれます。検出プロセスには IP アドレス、IP アドレス範囲、またはホスト名を指定してください。詳細は、「検出設定オプション」を参照してください。

検出設定オプション

フィールド	説明
グループとして保存	検出範囲をグループとして保存する場合は、このオプションを選択します。
グループ名	検出範囲のグループ名を指定します。
IP アドレス / 範囲	IP アドレスまたは IP アドレスの範囲を指定します。 次は、有効な検出範囲の種類のアドレス指定の例です（* はワイルドカード文字で、指定範囲内で可能なすべてのアドレスです）。 • 193.109.112.* • 193.104.20-40.* • 192.168.*.* • 192.168.2-51.3-91 • 193.109.112.45-99 • システム IP アドレス — 193.109.112.99 **メモ:** IP アドレスの複数の範囲を追加するには、追加をクリックします。IPV6 アドレスはサポートされていません。
検出範囲名	IP アドレス / 範囲の検出範囲名を指定します。
ホスト名	ホスト名を指定します（例：**mynode.mycompany.com**）。 複数のホスト名を追加するには、追加 をクリックします。 **メモ:** コンマを使用して、複数のホスト名を追加できます。 **メモ:** ホスト名にある無効文字はチェックされません。指定したホスト名に無効な文字が含まれていても、その名前は受け入れられますが、検出サイクル中にデバイスは検出されません。

フィールド	説明
サブネットマスク	IP アドレス範囲のサブネットマスクを指定します。サブネットマスクは、範囲のサブネットの部分のブロードキャストアドレスを特定するために使用されます。OpenManage Essentials ネットワーク監視サービスでは、IP アドレス範囲でデバイスを検出するときに、ブロードキャストアドレスは使用されません。次は有効なサブネットマスクの仕様例です。 • 255.255.255.0（クラス C ネットワーク用のデフォルトのサブネットマスク） • 255.255.0.0（クラス B のネットワークのデフォルトのサブネットマスク） • 255.255.242.0（カスタムサブネットマスクの仕様） デフォルトではサブネットマスクは 255.255.255.0 に設定されています。
インポート	このオプションを選択して、CSV フォーマットのファイルからホスト名および IP アドレスをインポートします。ただし、インポートできるのはタスクごとに 500 行項目のみです。異なるサブネットマスクで異なる検出範囲をインポートすることができます。例：192.168.10.10、255.255.255.128、10.10.1.1、255.255.0.0、および 172.16.21.1、255.255.128.0 です。 .CSV フォーマットの Active Directory エクスポートファイルをインプットとして使用できます。また、*名前*ヘッダを使用し、ヘッダの下の行に（セルごとに 1 つの）システム IP アドレスまたはホスト名を入力して、スプレッドシートエディタで .CSV ファイルを作成できます。.CSV フォーマットでファイルを保存し、今後、インポート機能でインプットとして使用します。ファイル内に無効なエントリが含まれている場合、OpenManage Essentials によるデータのインポート時にメッセージが表示されます。CSV ファイルの例は、「IP、範囲、またはホスト名の指定」を参照してください。

デバイスタイプのフィルタリング

検出設定 で **ガイド付きウィザード** が選択されている場合、**デバイスの検出** ウィザードに **デバイスタイプのフィルタリング** オプションが表示されます。このウィンドウでは、検出するデバイスタイプを選択できます。デバイスタイプを選択すると、選択されたデバイスタイプの検出と管理に必要なプロトコルが、**デバイスの検出** ウィザードに追加されます。例えば、**ESXi ホスト** を選択した場合、**SNMP 設定** 、および **WS-Man 設定** オプションがウィザードに追加されます。以下の表は、**デバイスタイプのフィルタリング** ウィンドウに表示されるフィールドを説明するものです。

フィールド	説明
デバイスタイプ	検出および管理の対象となる、選択可能なデバイスタイプが表示されます。
必要なプロトコル	選択されたデバイスタイプの検出と管理に必要なプロトコルが表示されます。

ICMP 設定

ICMP は、指定された IP アドレスを持つデバイスがあるかどうかを判断するために、検出エンジンによって使用されます。検出エンジンは要求を送信し、「タイムアウト」時間まで応答の受信を待ちます。デバイスが他の動作を行っていてビジー状態である場合、デバイスは、ICMP 要求に対して低負荷状態時ほど素早く応答しない場合があります。検出エンジンによってテストされている IP アドレスが割り当てられたデバイスがない場合、応答は全くありません。タイムアウト時間内に応答が受信されない場合、検出エンジンは「再試行」回数だけ要求を繰り返します（要求するたびに「タイムアウト」時間終了まで待機）。ICMP パラメータを設定するには、ICMP 設定オプションを参照してください。

詳細については、ヘルプアイコン をクリックします。

ICMP 設定オプション

フィールド	説明
タイムアウト（ミリ秒）	ICMP 要求の発行後、検出エンジンが応答を待つ最大ミリ秒数を指定します。デフォルトのタイムアウト期間は 1000 ミリ秒です。この値が大きいほど、ビジーデバイスから応答を受け取るための時間が長くなりますが、指定された IP アドレスを持つデバイスがない場合の待機時間も長くなることになります。
再試行（試み）	最初の ICMP 要求がタイムアウトした場合に、検出エンジンが要求を送信する追加回数の最大数を指定します。デバイスが過重なビジー状態で以前の ICMP 要求に応答できなかった場合でも、その後の要求には応答できることがあります。その IP アドレスを持つデバイスが使用されていない場合は、再試行もタイムアウトするので、再試行回数を少なくする必要があります。デフォルト値は 1 です。

SNMP 設定

SNMP は、サーバー、ストレージ、スイッチなどネットワーク上のデバイスを管理するためのインタフェースを提供します。デバイス上の SNMP エージェントを使用すると、OpenManage Essentials でデバイスの正常性およびインベントリデータをクエリできます。サーバー、ストレージデバイス、および他のネットワークデバイスの検出およびインベントリを実行するには、「SNMP 設定オプション」を参照してください。

詳細については、ヘルプアイコン をクリックします。

SNMP 設定オプション

フィールド	説明
SNMP 検出の有効化	検出範囲（サブネット）用の SNMP プロトコルを有効または無効にします。
Get コミュニティ	OpenManage Essentials ユーザーインタフェースから、SNMP **get** 呼び出し用のコミュニティ名を指定します。**Get コミュニティ** は、管理下デバイスにインストールされている SNMP エージェントが認証のために使用する読み取り専用パスワードです。**Get コミュニティ** は、OpenManage Essentials による SNMP データの参照と取得を可能にします。このフィールドは大文字と小文字を区別します。OpenManage Essentials は最初に成功したコミュニティ名を使用してデバイスと通信します。複数の SNMP コミュニティ文字列はコンマで区切って入力してください。
Set コミュニティ	OpenManage Essentials UI から、SNMP **set** 呼び出しのためのコミュニティ名を指定します。**Set コミュニティ** は、管理下デバイスにインストールされた SNMP エージェントが認証用に使用する読み取り / 書き込みパスワードです。**Set コミュニティ** は、OpenManage Essentials による SNMP プロトコルを必要とするタスク（システムのシャットダウンなど）の実行を可能にします。 このフィールドは大文字と小文字を区別し、カンマで区切られた複数の SNMP コミュニティ文字列を入力することができます。OpenManage Essentials は、最初に成功したコミュニティ名を使用してデバイスと通信します。 **メモ:** デバイス上で SNMP タスクを実行するには、**Set コミュニティ** 名のほかに計装パスワードも必要です。
タイムアウト（秒）	検出エンジンが **get** または **set** 呼び出しを発行した後、呼び出しに失敗したと見なすまで待機する最大秒数を指定します。有効範囲は 1〜15 秒で、デフォルト値は 4 秒です。
再試行（試み）	最初の **get** または **set** 呼び出しがタイムアウトした後、検出エンジンがそれらの呼び出しを再発行する追加回数の最大数を指定します。検出エンジンは、呼び出しが成功するまで、またはすべての再試行の試みがタイムアウトするまで、呼び出しを再発行します。有効範囲は 1〜10 回で、デフォルトは 2 回です。

WMI 設定

Window を実行しているサーバーに関する検出情報、インベントリ情報、および正常性情報の収集には WMI プロトコルを使用します。このプロトコルは、デバイスについて提供する情報が SNMP よりも少なくなりますが、ネットワークで SNMP が無効になっている場合に便利です。Windows サーバー専用の WMI パラメータを設定するには、「WMI 設定オプション」を参照してください。

WMI 設定オプション

フィールド	説明
WMI 検出を有効化	これを選択して、WMI 検出を有効化します。
ドメイン\ユーザー名	ドメインおよびユーザー名を提供します。
パスワード	パスワードを入力します。

ストレージ設定

Dell PowerVault MD または Dell|EMC アレイの検出を有効にすると、OpenManage Essentials でこれらのアレイに関するインベントリ情報および正常性情報を収集することができます。PowerVault MD アレイまたは Dell|EMC デバイスを検出するには、「ストレージ設定オプション」を参照してください。

ストーレジ設定オプション

フィールド	説明
PowerVault MD アレイの検出を有効にする	これを選択して、PowerVault MD アレイを検出します。この検出設定には資格情報は必要ありません。
Dell/EMC アレイの検出を有効にする	これを選択して、Dell/EMC アレイを検出します。
Dell/EMC ユーザー名	ユーザー名を入力します。
Dell/EMC パスワード	パスワードを入力します。
Dell/EMC ポート	ポート番号を増分または減分します。1〜65535 範囲の TCP/IP ポート番号を入力します。デフォルト値は 443 です。

WS-Man 設定

WS-Man プロトコルを使用して、iDRAC、ESXi ベースのサーバー、Dell PowerEdge VRTX、および Dell PowerEdge FX デバイスのインベントリと正常性ステータスを検出および収集します。詳細に関しては、「WS-Man 設定オプション」を参照してください。

メモ: 検出およびインベントリの実行は、iDRAC6 バージョン 1.3 以降がインストールされたサーバーに対してのみ可能です。バージョンが 1.25 より古い iDRAC6 ではサーバーの検出およびインベントリはサポートされていません。

WS-Man 設定オプション

フィールド	説明
WS-Man 検出を有効にする	これを選択して、Dell PowerEdge FX、Dell PowerEdge VRTX、iDRAC6、iDRAC7、iDRAC8、および ESXi がインストールされたデバイスを検出します。
ユーザー ID	認証済みユーザー ID を入力します。
パスワード	パスワードを提供します。
タイムアウト（秒）	WS-Man 接続要求の発行後、検出エンジンが待機する最大秒数を指定します。有効範囲は 1〜360 秒で、デフォルトは 15 秒です。
再試行（試み）	最初の WS-Man 接続要求がタイムアウトした場合に、検出エンジンがデバイスに接続要求を送信する追加回数の最大数を指定します。検出エンジンは、要求が成功するまで、またはすべての再試行の試みがタイムアウトするまで、要求を再発行します。有効範囲は 1〜10 回で、デフォルトは 4 回です。
ポート	ポート情報を入力します。デフォルトポート番号は 623 です。
セキュアモード	これを選択して、デバイスおよびコンポーネントをセキュアに検出します。
コモンネームチェックの省略	これを選択して、コモンネームチェックを省略します。
信頼済みサイト	検出中のデバイスが信用済みデバイスである場合に選択します。
証明書ファイル	**参照** をクリックしてファイルの場所に移動します。

SSH 設定

Linux を実行しているサーバーの検出およびインベントリを行うには、SSH プロトコルを使用します。SSH 設定パラメータを設定するには、「SSH 設定オプション」を参照してください。

SSH 設定オプション

フィールド	説明
SSH 検出の有効化	検出範囲ごとに SSH プロトコルを有効または無効にします。
ユーザー名	ユーザー名を入力します。
パスワード	パスワードを入力します。
ポート	ポート情報を指定します。デフォルトポート番号は 22 です。
再試行（試み）	最初の SSH 接続要求がタイムアウトした場合に、検出エンジンがデバイスに接続要求を送信する追加回数の最大数を指定します。検出エンジンは、要求が成功するまで、またはすべての再試行の試みがタイムアウトするまで、要求を再発行します。有効範囲は 1～10 回の再試行で、デフォルト値は 3 です。
タイムアウト（秒）	デバイスに SSH 接続要求を送信した後、検出エンジンが待機する最大秒数を指定します。有効範囲は 1～360 秒で、デフォルト値は 3 秒です。

IPMI 設定

RAC、DRAC および iDRAC の帯域外検出には、IPMI プロトコルを使用します。このオプションは、Lifecycle Controller が有効化された検出およびインベントリ用です。DRAC および iDRAC の IP アドレスが選択されていることを確認してください。IPMI バージョン 2.0 パラメータを設定するには、「IPMI 設定オプション」を参照してください。この設定は検出に必要です。

IPMI 設定オプション

フィールド	説明
IPMI 検出を有効にする	検出範囲ごとに IPMI プロトコルを有効または無効にします。
ユーザー名	Baseboard Management Controller（BMC）または DRAC ユーザー名 を入力します。 **メモ:** デフォルトのユーザー名は **root** です。このユーザー名は、安全のため変更することが推奨されます。
パスワード	BMC または DRAC パスワードを入力します。 **メモ:** デフォルトのパスワードは **calvin** です。このパスワードは、安全のため変更することが推奨されます。

フィールド	説明
KG キー	KG キー値を入力します。DRAC は IPMI KG キーもサポートしています。個々の BMC または DRAC は、ユーザーの資格情報のほかにアクセスキーも要求するように設定されています。 **メモ:** KG キーは、ファームウェアとアプリケーション間で使用される暗号化キーを生成するために使用する公開キーです。KG キーの値は、16 進数文字の偶数です。
タイムアウト（秒）	IPMI 要求の発行後、検出エンジンが待機する最大時間を指定します。有効範囲は 1～60 秒で、デフォルトは 5 秒です。
再試行（試み）	最初の呼び出しがタイムアウトした後、検出エンジンが IPMI 要求を再発行する最大回数を指定します。検出エンジンは、要求が成功するまで、またはすべての再試行の試みがタイムアウトするまで、要求を再発行します。有効範囲は 0～10 回で、デフォルトは 1 回です。

メモ: 再試行とタイムアウトのパラメータは、リモート管理制御プロトコル（RMCP）の ping と IPMI 接続の両方で使用されます。

検出範囲処置

これらのオプションを選択して、デバイス、コンポーネント、およびサーバーの検出とインベントリを行います。

フィールド	説明
検出またはインベントリは実行しない	このオプションを選択し、検出およびインベントリを（後で）実行するスケジュールを設定します。
検出のみを実行する	このオプションを選択して、検出を実行します。
検出とインベントリの両方を実行する	このオプションを選択して、検出とインベントリを両方実行します。

概要

選択した設定を表示します。設定を変更するには、**戻る** をクリックします。

除外範囲の追加

OpenManage Essentials から、**管理 → 検出とインベントリ → 一般タスク → 除外範囲の追加** を選択します。検出から除外する新しい範囲を登録、または以前に設定された除外範囲を削除します。

また、**除外範囲** を右クリックして **除外範囲の追加** を選択することもできます。

除外範囲の追加オプション

フィールド	説明
IP アドレス / 範囲	デバイスの IP アドレスまたは IP アドレス範囲を指定して、新しいデバイスを検出処理から除外するように登録します。 次は、有効な検出範囲の種類のアドレス指定の例です (* はワイルドカード文字で、指定範囲内で可能なすべてのアドレスを含みます)。 • 除外範囲 — 193.109.112.* • 193.104.20-40.* • 192.168.*.* • 192.168.2-51.3-91 • 除外範囲 — 193.109.112.45-99 • システム IP アドレス — 193.109.112.99
名前	IP アドレス / 範囲のための除外範囲名を追加します。
ホスト名	デバイスのホスト名（例：**mynode.mycompany.com**）を指定して、検出処理から除外するように登録します。 **メモ:** OpenManage Essentials はホスト名の無効な文字をチェックしません。指定したホスト名に無効な文字が含まれていても、その名前は受け入れられますが、その名前のデバイスは検出サイクル中に検索されません。

検出のスケジュール

OpenManage Essentials を設定してデバイスを検出し、**デバイス** ツリーにそれらを表示することができます。

- デバイス検出を有効にします。
- デバイス検出を開始します。
- 検出速度を設定します。
- デバイスの検出方法を指定します。
- 検出試行の失敗には、トラブルシューティングツールを使用してください。

関連リンク

検出スケジュール設定

検出設定の表示

検出設定を表示するには、**管理 → 検出とインベントリ → 検出のスケジュール** の順にクリックします。

検出スケジュール設定

OpenManage Essentials を設定してネットワーク上の新規デバイスを検出します。この設定はすべての検出範囲に適用されます。OpenManage Essentials は、すべてのエージェント、IP アドレス、およびデバイスの正常性を記録します。

フィールド	説明
検出の有効化	これを選択してデバイスの検出をスケジュールします。
グローバルデバイス検出間隔の設定	検出頻度を毎週または毎日に設定します。 • **毎週**— 検出をスケジュールする曜日（1 日または複数日）、および検出を開始する時間を指定します。 • **<n> 日 <n> 時間ごと** — 検出サイクル間の間隔を指定します。最大検出間隔は 365 日 / 23 時間です。
検出速度	検出速度を速めるために使用できるリソース（システムとネットワーク）量を指定します。速度を速くするほど、検出の実行に必要なリソース量は増えますが、時間は短縮されます。
検出	デバイスの検出方法を指定します。 • **すべてのデバイス** — インターネットコントロールメッセージプロトコル（ICMP）の ping に応答するすべてのデバイスを検出するには、このオプションを選択します。 • **計装化されたデバイス** — シンプルネットワーク管理プロトコル（SNMP）、Windows Management Instrumentation（WMI）、Intelligent Platform Management Interface（IPMI）管理または WS-Management（WS-Man）用の計装を備えたデバイス（Dell OpenManage Server Administrator、Dell OpenManage Array Manager、Dell Networking イーサネットスイッチ など）のみを検出するにはこのオプションを選択します。システム管理計装エージェントの詳細については、サポートされるエージェントを参照してください。
名前解決	デバイス名の解決方法を指定します。クラスタを管理している場合は、NetBIOS 名前解決を使用してそれぞれ独立したシステムを識別します。クラスタを管理していない場合は、DNS 名前解決が推奨されます。 • **DNS** — このオプションを選択し、ドメイン命名サービスを使用して名前を解決します。 • **NetBIOS** — このオプションを選択し、システム名を使用して名前を解決します。

関連リンク

検出のスケジュール

インベントリスケジュール

インベントリポーリング を使用して、OpenManage Essentials のデフォルトイベントリ設定を指定します。OpenManageEssentials は、ソフトウェアとファームウェアのバージョンや、デバイスのメモリ、プロセッサ、電源、周辺機器連相互接続（PCI）カード、組み込みデバイス、ストレージなどに関するインベントリ情報を収集します。

関連リンク

インベントリスケジュール設定

インベントリスケジュール設定

フィールド	説明
インベントリを有効にする	これを選択して、インベントリをスケジュールします。
グローバルインベントリポーリング間隔の設定	インベントリの頻度を毎週または毎日に設定します。 **メモ:** OpenManage Essentials は、すでに検出済みのデバイスに対してはインベントリのみを実行します。 • **毎週の曜日** — インベントリ をスケジュールする曜日（1 日または複数日）と、 インベントリ を開始する時刻を設定します。 • **<n> 日 <n> 時間ごと** — 検出サイクル間の間隔を指定します。最大検出間隔は 365 日 / 23 時間です。
インベントリポーリングの速度	インベントリポーリングの速度を速めるために使用できるリソース量を指定します。インベントリポーリングの速度を早くするほど、必要なリソース量が増えますが、インベントリの実行時間は短縮されます。 速度の変更後、OpenManage Essentials が新しい速度に適応するまで数分かかる場合があります。

関連リンク

インベントリスケジュール

状態スケジュール

このウィンドウを使用して、OpenManage Essentials 用の状態ポーリングのデフォルト設定を指定します。状態ポーリングは、すべての検出したデバイスに対して正常性および電源チェックを実行します。たとえば、このポーリングによって、検出したデバイスが正常であるか電源が切れているかを判断します。

関連リンク

ステータスポーリングスケジュールの設定

ステータスポーリングスケジュールの設定

フィールド	説明
OnDemand ポーリングの有効化	デバイスからアラートを受信した時、デバイスのグローバル状態をクエリするために選択します。 **メモ:** 多数のアラートを受信した場合は、複数のオンデマンドポーリングがキューされるので、システムパフォーマンスに影響する可能性があります。このシナリオでは、オンデマンドポーリングをオフにし、通常の状態ポーリング間隔を有効にして、管理下デバイスの正常性状態を取得することが推奨されます。 オンデマンドポーリングが無効にされている場合、デバイス状態は、通常の状態ポーリングでのみアップデートされます。
状態ポーリングを有効にする	これを選択して、デバイス状態ポーリングをスケジュールします。
デバイス状態ポーリング間隔	デバイス状態ポーリングの頻度を、日、時間、分の間隔で設定します。状態ポーリングは前のポーリングが完了するまで開始されません。 **日** – デバイス状態ボーリングサイクル間の日数を指定します。 **時間** –デバイス状態ポーリングサイクル間の時間数を指定します。 **分** – デバイス状態ボーリングサイクル間の分数を指定します。 最大検出間隔は 365 日/23 時間/59 分です。
状態ポーリングの速度	デバイス状態ポーリング速度を早くするために使用できるリソース量を指定します。状態ポーリングの速度を速くするほど必要なリソース量は増えますが、状態ポーリングの実行時間は短くなります。

関連リンク

状態スケジュール

検出範囲

検出範囲 の項には、検出に設定した IP アドレスまたは IP アドレスの範囲がすべて表示されます。検出範囲の横に表示されるアイコンは、検出に使用したウィザードの種類によって異なります。**標準ウィザード** を使用して検出範囲を設定する場合は、 アイコンが表示されます。検出範囲を **ガイド付きウィザード** で設定する場合は、 アイコンが表示されます。また、検出範囲を右クリックして、検出範囲で使用可能なオプションを表示することができます。右クリックでのオプションについての詳細は、「包括範囲の管理」を参照してください。

除外範囲

除外範囲 の項には、検出処理から除外するように設定した IP アドレスまたは IP アドレスの範囲が表示されます。

7

デバイスの管理

OpenManage Essentials では、種類別にデバイスがリストされます。例えば、Dell PowerEdge サーバーは、**サーバー** というデバイスの種類にリストされています。OpenManage Essentials にはデバイスの種類の定義済みリストが含まれています。検出およびインベントリを行うデバイスは、これらのデバイスの種類に分類されます。未分類のデバイスは、**不明** というデバイスの種類にリストされます。定義されたデバイスの種類を組み合わせることによってデバイスグループを作成することはできますが、デバイスの種類を新しく作成することはできません。

デバイス ページでは、次が可能です。

- ネットワーク上で検出されたデバイスの種類の表示。
- デバイスに関するインベントリ情報の表示。
- デバイスのために生成された全アラートの表示。
- デバイスのハードウェアログの表示。
- グループ分けのプリファレンスに基づいたデバイスグループの作成とそのグループへのデバイスの包含。例えば、グループを作成して、このグループにひとつの地理的場所に存在するすべてのデバイスを含めることができます。
- **マップビュー** を使用して、Dell PowerEdge VRTX デバイスを表示して管理します。

関連リンク

デバイスの表示
デバイスインベントリの表示
アラート概要の表示
システムイベントログの表示
デバイスの検索
新規グループの作成
新しいグループへのデバイスの追加
既存グループにデバイスを追加する
グループの非表示
グループの削除
カスタム URL の作成
マップビューの使用

デバイスの表示

検出されたデバイスを表示することができます。デバイスの検出およびインベントリの詳細については、「デバイスの検出とインベントリ」を参照してください。
デバイスを表示するには、**管理 → デバイス** の順にクリックします。

関連リンク

デバイスの管理

デバイスサマリページ

デバイス概要ページで、デバイスの種類を展開してデバイスを表示します。次のデバイスの種類が表示されます。

- **Citrix XenServers**
- **クライアント**
- **高可用性（HA）クラスタ**
- **KVM**
- **Microsoft 仮想化サーバー**
  - **仮想マシン**
- **モジュラシステム**
  - **PowerEdge シャーシ**
  - **PowerEdge FX2**
  - **PowerEdge M1000e**
  - **PowerEdge VRTX**
- **ネットワークデバイス**
  - **Dell Networking スイッチ**
  - **ファイバチャネルスイッチ**
  - **ネットワークアプライアンス**
- **OEM デバイス**
- **OOB 分類されていないデバイス**
  - **IPMI 分類されていないデバイス**
- **電源デバイス**
  - **PDU**
  - **UPS**
- **PowerEdge C サーバー**
- **プリンタ**
- **RAC**

  メモ: DRAC または iDRAC が検出されると、**サーバー** グループではなく、**RAC** グループの下に表示されます。DRAC/iDRAC の両方と対応するサーバーが検出されると、1 つのデバイスに関連付けられます。デバイスは **RAC** および **サーバー** グループに表示されます。

  メモ: IPMI を使用して、Dell PowerEdge C サーバー上で RAC が検出されると、**OOB 分類されていないデバイス** に表示されます。
- **再利用およびベアメタル**

  メモ: 再利用およびベアメタルデバイス グループのデバイスが、デバイス構成導入のターゲットとして表示されます。デバイス構成の導入に対して、このグループにデバイスを明示的に追加し、導入完了後はグループからデバイスを削除する必要があります。 詳細については、デバイス設定導入の管理を参照してください。
- **サーバー**
- **ストレージデバイス**
  - **Dell Compellent アレイ**

  - **Dell EqualLogic グループ**
  - **Dell NAS アプライアンス**
  - **Dell|EMC アレイ**
  - **PowerVault MD アレイ**
  - **テープデバイス**
- **不明**
- **VMware ESX サーバー**
  - **仮想マシン**

現在のデータでデバイスツリーをアップデートするには、更新ボタンを使用します。デバイスツリーをアップデートするには、**すべてのデバイス** を右クリックし、**更新** を選択します。

メモ: デバイスツリーは、変更が行われると自動的にアップデートされます。情報は SQL データベースからユーザーインタフェースに伝達されるため、一部の変更は、管理下サーバーのパフォーマンスに応じてわずかに遅れて表示される場合があります。

ノードおよび記号の説明

表 1. ノードおよび記号の説明

ノード記号	説明
	デバイスが重要状態であり、注意が必要なことを示します。この情報は親デバイスの種類にロールアップされています。例えば、サーバーが重要状況にあり注意が必要な場合、同じ記号が親デバイスの種類に割り当てられます。サーバー状態の中では重要な状況が最優先されます。つまり、1 つのグループ内で異なるデバイスが異なる状態にある場合、1 つのデバイスが重要な状況であれば、親デバイスの種類の状況は重要に設定されます。
	この種類のデバイスがネットワーク上で検出されていない、またはデバイスツリー内で分類されていないことを示します。
	デバイスに期待される動作からの逸脱があるが、引き続き管理可能であることを示します。
	デバイスが期待どおりに動作していることを示します。
	デバイスの種類が不明であり、不明デバイスとして分類されているか、正常性状態を判断できないかを示します。これは、デバイスに適切な計装がないか、デバイスの検出に適切なプロトコルが使用されなかったためです。

デバイス詳細

デバイス詳細には、デバイスに応じて次の情報が含まれています。

- デバイス概要
- OS 情報
- データソース
- NIC 情報
- 仮想マシンのホスト製品情報
- RAC デバイス情報
- プロセッサ情報
- メモリデバイス情報
- ファームウェア情報
- 電源装置情報
- 組み込みデバイス情報
- デバイスカード情報
- コントローラ情報
- コントローラバッテリ情報
- エンクロージャ情報
- 物理ディスク情報
- 仮想ディスク情報
- 連絡先情報
- アプライアンスノード情報
- スイッチデバイス情報
- EqualLogic ボリューム情報
- デバイスプロパティ
- ストレージグループ情報
- iDRAC 情報
- テープドライブ情報とテープライブラリ情報
- 物理バッテリ情報
- Fluid Cache 情報
- Fluid Cache プール情報
- Fluid Cache ディスク
- ソフトウェアインベントリ情報
- 信頼できるプラットフォームモジュール情報
- スロット情報
- 仮想フラッシュ情報
- FRU 情報
- プリンタカバー表
- プリンタマーカー供給情報
- プリンタの給紙トレイ情報
- プリンタの排紙トレイ情報
- 取得情報
- 減価償却情報
- リース情報
- メンテナンス情報
- サービス契約情報
- 延長保証情報
- 所有者情報
- アウトソース情報
- マスター情報

メモ: 特定のサービスタグに対して OpenManage Essentials に表示された保証情報（失効および更新情報を含む）が、**support.jp.dell.com** に表示される保証記録と一致しない場合があります。**support.jp.dell.com** に表示された保証記録のサービスレベルコードとモデル名は、OpenManage Essentials の保証レポートと完全に一致しないことがあります。

メモ: デバイスインベントリの **データソース** の表には、Dell Command | Monitor （以前は OMCI）エージェント名が **システム管理者** として表示されます。

メモ: ハードウェアインベントリは、OpenManage Server Administrator VIB がインストールされていれば、WS-Man プロトコルを使用して iDRAC6/7 および ESXi から取得できます。

メモ: デバイスインベントリの **データソース** 表には、次の場合に限り、iDRAC Service Module についての情報が表示されます。

- iDRAC が検出された。
- iDRAC が検出され、サーバーが WMI または SSH プロトコルを使用して検出された。

デバイスインベントリの表示

インベントリを表示するには、**管理 → デバイス** の順にクリックし、デバイスの種類を展開して、デバイスをクリックします。

関連リンク

デバイスの管理

アラート概要の表示

デバイスに対して生成されたすべてのアラートを表示できます。アラート概要を表示するには、次の手順を行います。

1. **管理** → **デバイス** をクリックします。
2. デバイスの種類を展開して、デバイスをクリックします。
3. 詳細ページで、**アラート** をクリックします。

関連リンク

デバイスの管理

システムイベントログの表示

1. **管理** → **デバイス** をクリックします。
2. デバイスの種類を展開して、**ハードウェアログ** を選択します。

関連リンク

デバイスの管理

デバイスの検索

デバイスツリーの最上部にある **すべてのデバイス** を右クリックし、**デバイスの検索** をクリックします。論理引数を使用してデバイスを検索し、将来のためにクエリを保存することもできます。

例えば、重要状態で、10.35 という値が IP アドレスに含まれており、電源状態が電源投入になっているサーバーを検索するためのクエリを作成するには次の操作を行います。

1. **管理** → **デバイスの検索** の順にクリックしてから、**新しいクエリの作成** を選択し、隣にあるテキストフィールドにクエリ名を入力します。
2. **場所** から始まる最初の行で **デバイスの種類**、**である**、**サーバー** の順に選択します。
3. 次の行でチェックボックスを選択して、**および**、**デバイスの正常性**、**である** と選択して、**重要** を選択します。
4. 次の行でチェックボックスを選択して、**および**、**IP アドレス**、**を含む** を選択して、隣のフィールドに **10.35** を入力します。
5. 次の行でチェックボックスを選択して、**および**、**電源状態**、**である** を選択し、**電源投入** を選択します。
6. **クエリの保存** をクリックします。

   メモ: クエリの実行 をクリックすると、ただちにクエリを実行できます。

既存のクエリを実行するには、ドロップダウンリストからクエリを選択し、**クエリの実行** をクリックします。結果をフィルタし、HTML ファイル、TXT ファイル、または CSV ファイルにエクスポートできます。

関連リンク

デバイスの管理

新規グループの作成

1. **管理** → **デバイス** をクリックします。
2. **すべてのデバイス**を右クリックして**新しいグループ**を選択します。
3. グループの名前と説明を入力してから**次へ**をクリックします。
4. **デバイスの選択** で、次のいずれかを選択します。
   - **クエリを選択して**動的グループを作成します。**新規**をクリックして新しいクエリを作成するか、またはドロップダウンリストから既存クエリを選択します。
   - **下のツリーからデバイス / グループを選択して**、静的グループを作成します。
5. **次へ** をクリックします。
6. 概要を確認して、**終了**をクリックします。

詳細 タブのデバイスを右クリックして、新しいグループまたは既存グループに追加します。ホームまたはレポートポータルから新しいグループを作成することもできます。**フィルタ基準** をクリックし、**新規グループの追加** をクリックして、**新規グループ** ウィザードを起動します。グループが静的か動的かを知るには、カーソルをグループの上に置きます。例えば、カーソルを **サーバー** の上に置くと、グループタイプが、**サーバー（ダイナミック | システム）**として表示されます。

関連リンク

デバイスの管理

新しいグループへのデバイスの追加

1. **管理** → **デバイス** をクリックします。
2. デバイスを右クリックして、**新規グループに追加** を選択します。
3. **グループ設定** で、名前と説明を入力します。**次へ** をクリックします。
4. デバイス選択に、選択したデバイスが表示されます。必要に応じて、さらにデバイスを追加または削除します。**次へ** をクリックします。
5. 概要を確認して、**終了** をクリックします。

関連リンク

デバイスの管理

既存グループにデバイスを追加する

1. **管理** → **デバイス** をクリックします。
2. デバイスを右クリックして、**既存グループへ追加**を選択します。

   メモ: デバイスを手動で動的グループに追加している場合、メッセージが画面に表示されます。動的グループへのデバイスの手動追加は、グループを動的から静的に変更することから、オリジナルのダイナミッククエリが削除されます。グループを動的のままにしたい場合は、グループを定義するクエリを変更します。**Ok** をクリックして続行するか、**キャンセル** をクリックして手順を中止します。
3. **OK** をクリックします。

関連リンク

デバイスの管理

グループの非表示

グループを非表示にするには、グループを右クリックしてから **非表示** を選択します。
グループを非表示にすると、コンソールのデバイスグループコントロールには表示されなくなります。非表示グループのデバイスはホームおよびレポートポータルのレポートおよびチャートに表示されません。非表示グループのデバイスに対するアラートはアラートポータルに表示されません。

親グループ（子グループを包含）が非表示の場合、子グループもデバイスツリーで非表示になります。ただし、子グループは、データベースに引き続き存在しており、コンソールのその他のインスタンスでは表示されます。

関連リンク

デバイスの管理

グループの削除

1. グループを右クリックして **削除** を選択します。
2. **削除** 画面で、**はい** をクリックします。

   メモ: 親グループを削除すると、そのグループはデバイスツリーから削除されます。親グループ下にリストされていた子グループとデバイスもデバイスツリーから削除されます。ただし、子グループとデバイスはデータベースに残り、コンソールの他のインスタンスに表示されます。

関連リンク

デバイスの管理

シングルサインオン

iDRAC または CMC デバイスにシングルサインオンが設定され、OpenManage Essentials にドメインユーザーとしてログオンしている場合、**アプリケーションの起動** オプションまたはエージェントリンクによって iDRAC または CMC コンソールを開くことができます。iDRAC または CMC でのシングルサインオン設定の詳細については、以下を参照してください。

- **dell.com/support/manuals** にある『Dell Chassis Management Controller ユーザーズガイド』の「CMC のシングルサインオンまたはスマートカードログイン設定」の項
- **dell.com/support/manuals** にある『Integrated Dell Remote Access Controller 7 ユーザーズガイド』の「iDRAC7 のシングルサインオンまたはスマートカードログイン設定」の項
- **DellTechCenter.com** にある『iDRAC7 と Microsoft Active Directory の統合』ホワイトペーパー
- **DellTechCenter.com** にある『IDRAC6 Integrated Dell Remote Access Controller 6 のセキュリティ』ホワイトペーパー

カスタム URL の作成

メモ: 検出時に、デバイスツリーに子サブグループを作成する親デバイスグループに、カスタム URL を割り当てることはできません。親デバイスグループの例には、**HA クラスタ**、**Microsoft 仮想化サーバー**、**PowerEdge M1000e**、**PowerEdge VRTX**、**VMware ESX サーバー** があります。これらの親デバイスグループのデバイスにカスタム URL を割り当てるには、デバイスをカスタムデバイスグループに追加し、カスタム URL を割り当てます。

1. **プリファランス → カスタム URL 設定** をクリックします。
2.  アイコンをクリックします。
   カスタム URL の起動 画面が表示されます。
3. 名前、URL、説明を入力して、ドロップダウンリストからデバイスグループを選択します。

   メモ: URL のテスト をクリックして、指定した URL がアクティブであることを確認します。
4. **OK** をクリックします。
   カスタム URL が作成されます。

関連リンク

デバイスの管理
カスタム URL 設定

カスタム URL の起動

1. **管理 → デバイス** の順にクリックして、ツリーからデバイスを選択します。
2. デバイスを右クリックして、**アプリケーションの起動** を選択します。
3. URL 名をクリックして、サイトにアクセスします。

関連リンク

カスタム URL 設定

保証電子メール通知の設定

お使いのデバイスの保証情報を定期的な間隔で電子メールで送信されるように OpenManage Essentials を設定することができます。設定可能なオプションの情報は、「保証通知設定」を参照してください。

保証電子メール通知 を設定するには、次の手順を実行します。

1. **プリファランス → 保証通知設定** とクリックします。
   保証通知設定 ページが表示されます。
2. **保証電子メール通知** で **保証電子メール通知の有効化** を選択します。
3. **宛先** フィールドに、受信者の電子メールアドレスを入力します。

   メモ: 電子メールアドレスを複数入力する場合には、アドレス間をセミコロンで区切ります。
4. **差出人** フィールドに、保証通知電子メールの送信者の電子メールアドレスを入力します。

   メモ: 差出人 フィールドには、電子メールアドレスを 1 つだけ入力する必要があります。
5. 保証通知電子メールに含めるデバイスの基準を設定するには、**保証が x 日以下のすべてのデバイス** フィールドで、日数を選択します。

6. 保証通知電子メールを受け取る頻度を設定するには、**x 日ごとに電子メールを送信** フィールドで、日数を選択します。
7. 保証通知電子メールに保証期限切れまたは保証情報のないデバイスを含めるには、**保証期限切れのデバイスを含む** を選択します。
8. **次回の電子メール送信日** フィールドで、次回の保証通知電子メールを受信する日時を選択します。
9. 電子メール の SMTP サーバーを設定する場合は、**電子メール設定** をクリックします。

   電子メール設定 ページが表示されます。**電子メール設定** の詳細は、「電子メール設定」を参照してください。
10. **適用** をクリックします。

OpenManage Essentials はお使いの設定に応じて保証通知電子メールを送信します。保証通知電子メールは、デバイスのリストと、クリックしてデバイスの保証を更新することができる適切なリンクを提供します。

関連リンク

保証通知の設定

保証スコアボード通知の設定

OpenManage Essentials を設定して ヘッダーバナーに保証スコアボード通知アイコンを表示することができます。設定可能なオプションの詳細については、「保証通知設定」を参照してください。

保証スコアボード通知 を設定するには、次の手順を実行します。

1. **プリファランス → 保証通知設定** とクリックします。

   保証通知設定 ページが表示されます。
2. **保証スコアボード通知** で **保証スコアボード通知の有効化** を選択します。
3. 保証スコアボード通知に含むデバイスの基準を設定するには、**保証残存期間が x 日またはそれ以下のすべてのデバイス** フィールドで、日数を選択します。
4. 保証スコアボード通知に保証期限切れまたは保証情報のないデバイスを含めるには、**保証期限が切れたデバイスを含む** を選択します。
5. **適用** をクリックします。

デバイスが設定された条件を満たすと、OpenManage Essentials のヘッダバナーに、デバイスの数などを含む保証スコアボード通知アイコンが表示されます。

関連リンク

保証スコアボード通知アイコンの使用
デバイス保証レポート
保証通知の設定

保証ポップアップ通知の設定

デバイスの保証状況に応じて保証ポップアップ通知を表示するよう OpenManage Essentials を設定することができます。設定可能なオプションについての詳細は、「保証通知設定」を参照してください。

保証ポップアップ通知を設定するには、次の手順を実行します。

1. **プリファランス → 保証通知設定** とクリックします。

   保証通知設定 ページが表示されます。
2. **保証ポップアップ通知設定** で次を行います。
   - 保証ポップアップ通知を有効にするには、**保証ポップアップ通知の有効化** を選択します。

- 保証ポップアップ通知を無効にするには、**保証ポップアップ通知の有効化** をクリアします。

3. **適用** をクリックします。

マップビューの使用

メモ: マップビュー 機能は、ライセンスを持つ Dell PowerEdge VRTX デバイスを WS-Man プロトコルを使用して検出した場合にのみ利用可能です。ライセンスを持つ PowerEdge VRTX デバイスが SNMP プロトコルを使用して検出された場合、**マップビュー** 機能は利用できません。この場合、WS-Man プロトコルを使用して PowerEdge VRTX デバイスを再検出する必要があります。

メモ: マップビュー に表示されるマップは、マップのサービスプロバイダから *現状のまま* 提供されたと見なす必要があります。OpenManage Essentials は、マップまたは住所の情報の正確さを制御することができません。

メモ: ズーム、住所検索、およびその他のマップ機能を実行するには、インターネットの接続が必要なものがあります。インターネットに接続されていない場合、マップに次のメッセージが表示されます : `Warning — Unable to connect to the Internet!` (警告 — インターネットに接続できません!)。

マップビュー 機能は、インタラクティブな地図上での Enterprise ライセンスを持つ PowerEdge VRTX デバイスの表示および管理を可能にします。Enterprise ライセンスを持つ PowerEdge VRTX デバイスは、地図上のピンとして表示されます。Enterprise ライセンスを持つすべての PowerEdge VRTX デバイスの正常性と接続状態を、一目で確認することができます。

マップビュー へは **ホームポータル** または **管理 → デバイス** ポータルページからアクセスできます。

マップの右上にある **オーバーレイ** メニューは、デバイスの正常性および接続性の状態をピンに重ねることを可能にします。 マップの右上にある**処置** メニューは、様々な機能をマップで実行することを可能にします。以下は、実行可能な処置のリストです :

処置	説明
すべてのマップの位置の表示	すべてのマップの位置を表示する
ホームビューに移動	事前に保存されている場合は、ホームビューを表示します。
現在のビューをホームビューとして保存	現在のビューをホームビューとして保存します。
ライセンス済みデバイスの追加	Enterprise ライセンスを持つ PowerEdge VRTX デバイスを追加することができます。
ライセンス済みデバイスのインポート	Enterprise ライセンスを持つ PowerEdge VRTX デバイスをインポートすることができます。
すべてのマップの位置の削除	すべてのマップの位置を削除できます。
エクスポート	すべてのマップの位置を **.csv** ファイルにエクスポートできます。
設定	**マップ設定** ダイアログボックスが開きます。
位置詳細の編集	デバイス名、アドレス、連絡先情報が表示された **位置詳細の編集** ダイアログボックスが開きます。

処置	説明
位置の削除	選択したデバイスをマップから削除できます。
ストリートレベルに拡大 **メモ:** このオプションはデバイスがマップ上で選択されている場合にのみ表示されます。	現在選択しているデバイス位置をストリートレベルまで拡大できます。

メモ: **アクション** メニューの **位置詳細の編集**、**位置の削除**、および **ストリートレベルに拡大** オプションはデバイス固有のオプションです。これらのオプションはマップ上でデバイスを選択してから使用する必要があります。

マップ左上の **アドレスの検索** ボックスではアドレスを検索できます。

マップ下部に表示されるナビゲーションツールバーでは以下を実行できます。

- マップのズームインとズームアウト
- マップの上下左右への移動
- マップのプロバイダタイプの選択

図 3. ナビゲーションツールバー

マップのズームレベルは、マップの右下に表示される縮尺で識別できます。

関連リンク

デバイス - 参照
マップビュー（ホーム）ポータル
マップビュー（ホーム）ポータルのインタフェース
一般的なナビゲーションとズーミング
ホームビュー
ツールチップ
検索ピン
マップのプロバイダ
マップビュー（デバイス）タブインタフェース
マップの設定
マップビューでのデバイスの選択
正常性および接続性のステータス
同位置にある複数のデバイス
ホームビューの設定
すべてのマップの位置の表示
マップへのデバイスの追加
位置詳細の編集オプションを使用したデバイス位置の移動
ライセンス済みデバイスのインポート
マップビュー検索バーの使用
検索ピンを使用したデバイスの追加
検索ピンを使用したデバイス位置の移動

[すべてのマップの位置の削除]
[マップの位置の編集]
[マップの位置の削除]
[すべてのデバイスの位置のエクスポート]
[デバイスの管理]

マップのプロバイダ

マップのプロバイダとして MapQuest と Bing のいずれかを選択するには、ナビゲーションツールバーの  アイコンを使用します。デフォルトでは、マップは MapQuest プロバイダを使用して表示されます。下表に、サポートされるマップのプロバイダの情報を示します。

MapQuest	Bing
無料	有効な Bing マップキーの購入が必要です。有効な Bing マップキーを入手するには、**microsoft.com/maps/** に移動してください。 **メモ:** Bing マップキーの入手方法については、**microsoft.com** から「Bing マップキーの入手」を参照してください。 有効な Bing マップキーを入手した後は、そのキーを**マップ設定**ダイアログボックスに入力する必要があります。
マップ上の最初のいくつかのズームレベルへのアクセスにはインターネット接続は不要です。追加のズームレベルや検索機能ではインターネット接続が必要です。	すべてのズームレベルへのアクセスおよび検索機能の使用にはインターネット接続が必須です。
システムがプロキシサーバー経由でインターネットに接続している場合は、OpenManage Essentials で設定した **プリファランス → コンソール設定** ページで設定した **プロキシ設定** が使用されます。	システムがプロキシサーバー経由でインターネットに接続している場合は、ウェブサーバーで設定したプロキシ設定が使用されます。
	マップには、次の 2 つのタイプがあります。 • ロードマップ — 最小限の詳細のシンプルな高速ロードマップです。 • 衛星マップ — 世界の詳細な衛星画像を提供します。

メモ: Bing マップのプロバイダは、マップを表示するためインターネットへの常時接続を必要とします。プロキシサーバーを経由してインターネットに接続している場合、ウェブブラウザで設定したプロキシ設定が Bing プロバイダによって使用されます。

関連リンク

[マップビューの使用]

マップの設定

メモ: OpenManage Essentials 管理者およびパワーユーザーのみに、**マップの設定**が許可されています。

マップの設定 ダイアログボックスでは、インターネット接続状態通知の有効化 / 無効化と、Bing マップのプロバイダが要求する有効な Bing キーを提供することができます。

マップの設定を行うには、次の手順を実行します。

1. 次のいずれかの手順を実行してください。
   - **ホーム → マップビュー** の順にクリックします
   - **管理 → デバイス → マップビュー** の順にクリックします。
2. **マップビュー** 上で：
   - マップ上で右クリックし、**設定** をクリックします。
   - マウスポイントを **処置** メニューの上に移動し、**設定** をクリックします。

   マップの設定 ダイアログボックスが表示されます。
3. デバイスツリーで選択したデバイスまたはデバイスグループに対応するピンのみをマップに表示する場合は、**デバイスまたはデバイスグループの選択でマップビューをアップデート** を選択します。
4. インターネット接続が利用できない場合にマップ上に警告を表示するには、**インターネットに接続できない時はインターネット接続警告を表示する** を選択します。
5. **Bing キー** フィールドに有効な Bing キーを入力します。
6. **適用** をクリックします。

関連リンク

マップビューの使用

一般的なナビゲーションとズーミング

マップを移動するには、マップをクリックして希望の方向にドラッグするか、ナビゲーションツールバーのナビゲーション矢印を使用します。

マップのズームインまたはズームアウトには、次のいずれかを使用できます：

- ピンをダブルクリックして、ピン周辺の地上レベルまでズームインします。また、次の方法で地上レベルまでズームインすることもできます：
  - ピンを右クリックし、**地上レベルまでズーム** をクリック
  - マウスポインタを **処置** メニューの上に移動し、**地上レベルまでズーム** をクリック
- ピンが地上レベルで表示されている場合、ピンをダブルクリックすると世界レベルのビューにズームアウトします。
- マップの位置をダブルクリックすると、その位置で 1 段階ズームインされます
- マウスのホイールを上下に動かすと、マップ上をすばやくズームアウトまたはズームインできます
- ナビゲーションツールバーにある虫眼鏡アイコン  をクリックすると表示されるスライドを使用して、マップのズームインまたはズームアウトができます。

メモ: マップビュー（ホーム）ポータルのズームレベルおよび可視領域は、**デバイス** ポータルからアクセスできる **マップビュー** タブとは同期化されません。

関連リンク

マップビューの使用

ホームビュー

マップの特定の地域をホームビューとして保存した場合、マップは **マップビュー** が開いたときにデフォルトでそのホームビューを表示します。マップ上の地域をホームビューとして設定する手順は、「ホームビューの設定」を参照してください。

関連リンク

マップビューの使用

ツールチップ

マウスポインタをピンの上に移動すると、以下の情報を含むツールチップが表示されます：

- デバイス名
- 説明
- Address（住所）
- Contact（連絡先）
- モデル
- サービスタグ
- アセットタグ
- グローバルステータス
- 接続ステータス

関連リンク

マップビューの使用

マップビューでのデバイスの選択

マップ上でデバイスを選択するには、該当するピンをクリックします。デバイスツリーで対応するデバイスが強調表示され、その他すべてのピンは非表示となります。デバイスツリーでデバイスが選択されると、マップにもそれが反映されます。**モジュラーシステム** または **PowerEdge VRTX** グループがデバイスツリーで選択されていると、これらのグループに対して置かれているピンはすべてマップに表示されます。

メモ: デバイスツリーでデバイスグループを非表示にしても、マップ上の対応するピンは非表示になりません。例えば、デバイスツリーで **モジュラーシステム** グループを非表示にしても、**モジュラーシステム** グループのデバイスを表すマップ上のピンは非表示になりません。

メモ: マップビュー（ホーム）ポータル上でピンをクリックすると、そのデバイスの詳細を表示した **デバイス** ポータルが表示されます。

関連リンク

マップビューの使用

正常性および接続性のステータス

デバイスの正常性および接続性のステータスもまた、マップに表示されます。デバイスの正常性および接続性のステータスをピンに重ねて表示するには、マップ右上の **オーバーレイ** メニューにマウスのポインタを移動し、**正常性** または **接続性** をクリックします。 正常性および接続性のステータスは、表示されるピンの色とアイコンで示されます。次の表は、正常性のステータスとピンのオーバーレイに関する情報を表しています。

ピンの色	アイコン	正常性状態
赤色		重要
黄色		警告
緑色		正常
灰色		不明

次の表は、接続性のステータスとピンのオーバーレイに関する情報を表しています。

ピンの色	アイコン	接続状態
青色		オン
灰色		オフ

関連リンク

マップビューの使用

同位置にある複数のデバイス

ライセンスされたデバイスが 2 台以上同じ場所に位置する場合があります。これらのデバイスは、マップ上でマルチピングループとして表示されます。デバイスがマップ上で非常に近接しており、マップがズームアウトされている場合、それらのピンはまとめてマルチピングループとして表示されます。マルチピングループ内のデバイスの数と名前を表示するには、マウスポインタをマルチピングループの上に移動させます。マルチピングループをダブルクリックまたは右クリックし、**詳細** を選択してその場所にあるデバイスをリストする **この場所のデバイス** ウィンドウを開きます。**この場所のデバイス** ウィンドウでは、次の操作が可能です。

- デバイスをダブルクリックして、マップにそのデバイスのみを表示します。
- デバイスを右クリックして、**インベントリの更新**、**アプリケーションの起動** 等の標準的なオプションおよび、**場所の詳細を編集** 等の、その他のマップ特有のオプション を表示します。

メモ: ライセンス済みデバイスのみマップ上に配置することができます。デバイスグループはマップ上に配置できません。

関連リンク

マップビューの使用

ホームビューの設定

概してデバイスを特定の地理的地域で管理する場合、その地域をホームビューとして設定することができます。各 OpenManage Essentials ユーザーが、マップの別々のビューをそれぞれのホームビューとして保存できます。デフォルトで、**マップビュー** を開いたときまたは **ホームビューに移動** オプションを選択すると、ホームビューが表示されます。

1. 次のいずれかの手順を実行してください。
   - **ホーム → マップビュー** の順にクリックします

- **管理** → **デバイス** → **マップビュー** の順にクリックします。

2. **マップビュー** で、希望のビューになるまで移動してズームします。
3. 次のいずれかの手順を実行してください。
   - マップを右クリックし、**現在のビューをホームビューとして保存する** をクリックします。
   - マウスポインタを **処置** メニューの上に移動し、**現在のビューをホームビューとして保存する** をクリックします。

関連リンク

マップビューの使用

すべてのマップの位置の表示

単一のデバイスが選択されている場合、マップにはそのデバイスのみが表示されます。マップに置かれたすべての **マップビュー** の位置を表示するには：

- マップを右クリックして、**すべてのマップの位置を表示する** をクリックします。
- マウスポインタを **処置** メニューの上に移動し、**すべてのマップの位置を表示する** をクリックします。

関連リンク

マップビューの使用

マップへのデバイスの追加

メモ: マップに追加できるのは、マップにまだ置かれていない Enterprise ライセンスを持つ Dell PowerEdge VRTX デバイスのみです。

メモ: OpenManage Essentials 管理者およびパワーユーザーのみに、マップにデバイスを追加する権利が与えられています。

マップにデバイスを追加するには：

1. 次のいずれかの手順を実行してください。
   - **ホーム** → **マップビュー** の順にクリックします
   - **管理** → **デバイス** → **マップビュー** の順にクリックします。
2. **マップビュー** 上で：
   - マップを右クリックし、**ライセンス済みデバイスの追加** をクリックします。
   - マウスポインタを **処置** メニューの上に移動し、**ライセンス済みデバイスを追加する** をクリックします。

   デバイスの位置の詳細 ダイアログボックスが表示されます。
3. **デバイス** リストから、追加するデバイスを選択します。
4. 必要であれば、**説明** フィールドにそのデバイスの適切な説明を入力します。
5. マップ上で右クリックした位置とは異なる位置にデバイスを追加するには、**住所** フィールドに位置のアドレス（例：シカゴ）を入力します。

   メモ: 住所 フィールドを使用してマップにデバイスを追加するには、マップのプロバイダ経由でインターネットを検索して、入力したアドレスを解決する必要があります。デバイスはインターネット検索で検出された最適な位置に追加されます。マップのプロバイダがアドレスを解決できない場合は、メッセージが表示されます。
6. 必要であれば、**連絡先** フィールドに連絡先情報を入力します。
7. **保存** をクリックします。

関連リンク

マップビューの使用
検索ピンを使用したデバイスの追加

位置詳細の編集オプションを使用したデバイス位置の移動

メモ: マップの位置を編集できるのは、OpenManage Essentials 管理者とパワーユーザーのみです。

1. 次のいずれかの手順を実行してください。
   - **ホーム → マップビュー** の順にクリックします
   - **管理 → デバイス → マップビュー** の順にクリックします。
2. マップ上のピンを右クリックし、**位置詳細の編集** を選択します。
   デバイスの位置の詳細 ダイアログボックスが表示されます。
3. **アドレス** フィールドに、位置名または空港コードを入力します。例：ニューヨーク。

   メモ: アドレス フィールドを使用してデバイスの位置を移動するには、マップのプロバイダ経由でインターネットを検索して、入力したアドレスを解決する必要があります。デバイスはインターネット検索で検出された最適な位置に移動されます。マップのプロバイダが住所を解決できない場合は、メッセージが表示され、デバイスは現在の位置のままになります。
4. **保存** をクリックします。
   マップのプロバイダが住所または空港コードを解決できた場合は、ピンがマップ上の指定された位置に移動します。

関連リンク

マップビューの使用
検索ピンを使用したデバイス位置の移動

ライセンス済みデバイスのインポート

メモ: マップにインポートできるのは、マップにまだ置かれていない Enterprise ライセンスを持つ Dell PowerEdge VRTX デバイスのみです。

メモ: OpenManage Essentials 管理者およびパワーユーザーのみに、ライセンス済みデバイスのインポートが許可されています。

メモ: 一度にインポートできるのは、最高 500 台までのデバイスです。

.csv ファイルによって、マップにライセンス済みデバイスを大量にインポートできます。現在検出されている、ライセンス済み PowerEdge VRTX デバイスの名前がすでに入力された **.csv** ファイルを作成する、**テンプレートのエクスポート** 機能が使用可能です。
ライセンス済みデバイスをインポートするには：

1. 次のいずれかの手順を実行してください。
   - **ホーム → マップビュー** の順にクリックします
   - **管理 → デバイス → マップビュー** の順にクリックします。
2. **マップビュー** で、次のいずれかを行います。
   - マップを右クリックし、**ライセンス済みデバイスをインポートする** をクリックします。
   - マウスポイントを **処置** メニューの上に移動し、**ライセンス済みデバイスをインポートする** をクリックします。

   ライセンス済みデバイスをインポートする ダイアログボックスが表示されます。
3. **テンプレートのエクスポート** をクリックして、ライセンス済み PowerEdge VRTX デバイスのインポートに使用できる **.csv** テンプレートをダウンロードします。

メモ: テンプレートの詳細は、「デバイスのインポート用テンプレート」を参照してください。

名前を指定して保存 ダイアログボックスが表示されます。

4. **.csv** ファイルを保存する場所を参照して、**保存** をクリックします。
5. .csv ファイルを開き、次のいずれかを実行します：
   - **緯度** および **経度** の列に、各デバイスの緯度と経度を入力します。
   - **住所** の列に、各デバイスの住所を入力します。例えば、1 dell way, round rock, TX となります。

     メモ: 住所を使用してデバイスをインポートする前に、システムがインターネットに接続されていることを確認します。システムがプロキシサーバーを介してインターネットに接続されている場合、プロキシ設定が **プリファランス → コンソール設定** ページで設定されていることを確認します。また、1 度にインポートするデバイスが多すぎると、インターネット検索プロバイダが住所検索の要求を拒否する場合があります。その場合、少し待ってから再度インポートします。
6. **インポート** をクリックします。

   開く ダイアログボックスが表示されます。
7. アップデートされた **.csv** ファイルのある場所を選択して、**開く** をクリックします。

   インポート概要 ダイアログボックスが表示されます。
8. **OK** をクリックします。

メモ: インポート処理の間に発生するすべてのエラーは、**ログ → UI ログ** に表示されます。

関連リンク

マップビューの使用
デバイスのインポート用テンプレート

デバイスのインポート用テンプレート

Enterprise ライセンスを持つ PowerEdge VRTX デバイスのインポート用テンプレートは、マップにインポートするデバイスについての詳細を提供するために使用できる **.csv** ファイルです。テンプレート内で使用できるフィールドは次のとおりです。

フィールド	説明
名前	Enterprise ライセンスを持つ PowerEdge VRTX デバイスの名前です。このフィールドには、まだマップ上に置かれていない、現在検出済みの Enterprise ライセンスを持つ PowerEdge VRTX デバイスがすでに入力されています。
緯度	デバイスの位置を示す緯度の座標です。
経度	デバイスの位置を示す経度の座標です。
住所	デバイスがある場所の住所です。緯度と経度の両方が指定された場合は、住所を指定する必要はありません。
説明（オプション）	デバイスに関する情報を入れます。
連絡先（オプション）	デバイスに追加する連絡先情報を入れます。

Enterprise ライセンスを持つ PowerEdge VRTX デバイスをインポートするには、**.csv** ファイルを次のいずれかでアップデートする必要があります。

- 緯度および経度
- 住所

関連リンク

ライセンス済みデバイスのインポート

マップビュー検索バーの使用

メモ: マップのプロバイダがアドレスまたは空港コードを正しく解決できない場合もあります。

マップビュー の検索バーを使用すると、アドレスや空港コードを使用してマップ上の位置を検索することができます。位置を検索するには、位置の名前または空港コード（例えば、ニューヨークまたは JFK）を検索バーに入力し、エンター・キーを押すか、矢印アイコンをクリックします。マップのプロバイダが住所または空港コードを解決できる場合、検索ピンがマップ上の該当する位置に表示されます。

関連リンク

マップビューの使用

検索ピン

検索ピンはマップ上に検索結果を示す大きいピンです。検索ピンには以下の特徴があります。

- いかなる場合にも、マップ上には検索ピンが 1 つだけ表示されます。地図上に表示された検索ピンは、削除するか新しい検索を実行するまでその位置のままです。検索ピンを削除するには、検索ピンを右クリックして **削除** をクリックします。
- デバイスピンと異なり、検索ピンは状態の上に重ねて表示されません。
- 検索ピンをダブルクリックすると、位置のズームインとズームアウトができます。
- マウスポインタを検索ピンの上に移動すると、位置のアドレスを含むツールチップが表示されます。
- ライセンス済み PowerEdge VRTX デバイスを検索ピン位置で追加または移動できます。

関連リンク

マップビューの使用

検索ピンを使用したデバイスの追加

メモ: マップに追加できるのは、マップにまだ置かれていない Enterprise ライセンスを持つ Dell PowerEdge VRTX デバイスのみです。

メモ: OpenManage Essentials 管理者およびパワーユーザーのみに、マップにデバイスを追加する権利が与えられています。

1. 次のいずれかの手順を実行してください。
   - **ホーム → マップビュー** の順にクリックします
   - **管理 → デバイス → マップビュー** の順にクリックします。
2. 検索バーに住所または空港コード（例：ニューヨークまたは JFK）を入力し、エンター・キーを押すか矢印アイコンをクリックします。

   マップのプロバイダが住所または空港コードを解決できた場合は、検索ピンがマップ上の位置に表示されます。
3. 検索ピンを右クリックして **ライセンス済みデバイスをここに追加** をクリックします。

   デバイスの位置の詳細 ダイアログボックスが表示されます。
4. **デバイス** リストから、追加するデバイスを選択します。
5. **保存** をクリックします。

関連リンク

マップビューの使用
マップへのデバイスの追加

検索ピンを使用したデバイス位置の移動

メモ: OpenManage Essentials 管理者およびパワーユーザーのみに、マップにデバイスを追加する権利が与えられています。

デバイス位置を移動するには、以下の手順を実行します。

1. 次のいずれかの手順を実行してください。
   - **ホーム → マップビュー** の順にクリックします
   - **管理 → デバイス → マップビュー** の順にクリックします。
2. マップ上で、ライセンス済み PowerEdge VRTX デバイスのピンを選択します。
3. 検索バーに住所または空港コード（例：ニューヨークまたは JFK）を入力し、エンター・キーを押すか矢印アイコンをクリックします。

   マップのプロバイダが住所または空港コードを解決できた場合は、検索ピンがマップ上の位置に表示されます。
4. 検索ピンを右クリックして **選択したデバイスをここに移動** をクリックします。
5. **デバイスの移動** 確認ダイアログボックスで、**はい** をクリックします。

   選択したデバイスが検索ピンの位置に移動します。

関連リンク

マップビューの使用
位置詳細の編集オプションを使用したデバイス位置の移動

すべてのマップの位置の削除

メモ: すべてのマップの位置を削除できるのは、OpenManage Essentials 管理者とパワーユーザーのみです。

すべてのマップの位置を削除するには：

1. 次のいずれかの手順を実行してください。
   - **ホーム → マップビュー** の順にクリックします
   - **管理 → デバイス → マップビュー** の順にクリックします。
2. **マップビュー** 上で、次を行います。
   - マップを右クリックし、**すべてのマップの位置の削除** をクリックします。
   - マウスポインタを **処置** メニューの上に移動し、**すべてのマップの位置の削除** をクリックします。

   すべてのマップアイテムの削除 ダイアログボックスが表示されて確認が求められます。
3. **はい** をクリックします。

関連リンク

マップビューの使用

マップの位置の編集

メモ: マップの位置を編集できるのは、OpenManage Essentials 管理者とパワーユーザーのみです。

マップの位置を編集するには：

1. マップ上のピンを右クリックし、**位置詳細の編集** を選択します。
   デバイスの位置の詳細 ダイアログボックスが表示されます。
2. **説明** フィールドで、必要な編集を行います。
3. デバイスを新しい位置に移動するには、**住所** フィールドに位置名を入力します。
4. **連絡先** フィールドで、連絡先情報を必要に応じて編集します。
5. **保存** をクリックします。

関連リンク

マップビューの使用

マップの位置の削除

メモ: マップの位置を削除できるのは、OpenManage Essentials 管理者とパワーユーザーのみです。

マップ上の位置を削除するには：

1. 次のいずれかの手順を実行してください。
   - **ホーム → マップビュー** の順にクリックします
   - **管理 → デバイス → マップビュー** の順にクリックします。
2. **マップビュー** 上で、削除する位置を右クリックし **位置を削除する** を選択します。
   位置の削除 ダイアログボックスが表示されて確認が求められます。
3. **Yes**（はい）をクリックします。

関連リンク

マップビューの使用

すべてのデバイスの位置のエクスポート

すべてのデバイスの位置をエクスポートすると、デバイスに関する情報とそれらの緯度と経度の座標を **.csv** ファイルにして保存することができます。ピンの住所がわかっている場合、.csv ファイルの **説明** フィールドに含まれます。このファイルを使用して、いつでもデバイスの位置をインポートできます。

メモ: デフォルトで、以前は緯度と経度の座標が提供されなかった場合でも、各デバイスの緯度と経度の座標が .csv ファイルに保存されます。

マップに現在置かれているすべてのデバイスの位置をエクスポートするには：

1. **マップビュー** 上で、マウスポインタを **処置** メニューの上に移動し、**エクスポート** をクリックします。
   名前を指定して保存 ダイアログボックスが表示されます。
2. **.csv** ファイルを保存する場所を参照して、適切なファイル名を入力し、**保存** をクリックします。

関連リンク

マップビューの使用

Dell PowerEdge FX シャーシビュー

PowerEdge FX2 および FX2s デバイスは、デバイスツリー内にある **すべてのデバイス → モジュラーシステム → PowerEdge FX** 下にデフォルトで分類されます。PowerEdge FX シャーシに取り付けられている計算スレッドは、検出されるとデバイスツリー内の適切な PowerEdge FX デバイスグループ下に表示されます。

デバイスツリーで PowerEdge FX シャーシを選択すると、シャーシ前面の図解（**シャーシビュー**）がデバイスの詳細ページに表示されます。シャーシのインベントリ情報は、**シャーシビュー** 下に表示されます。

メモ: シャーシビュー は、PowerEdge FX シャーシが WS-Man プロトコルを使用して検出され、かつ、少なくとも 1 つのスロットにスレッドが取り付けられている場合にのみ表示されます。

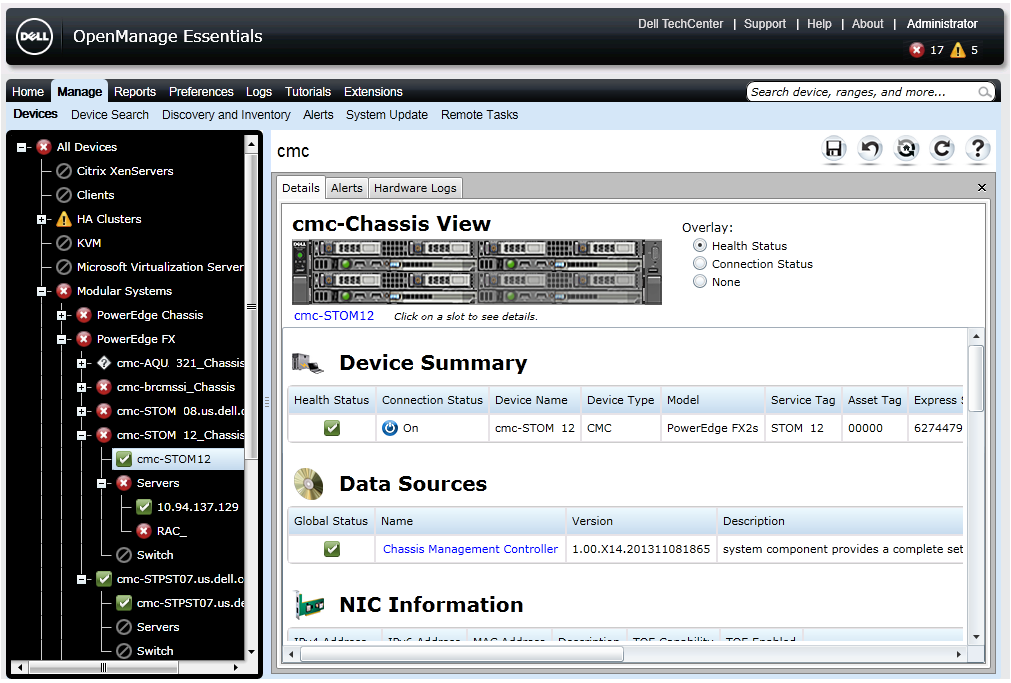


図 4. シャーシビュー

ツールチップとデバイスの選択

シャーシ内のスレッド上にマウスポインタを動かすと、スレッドを囲む黄色の長方形ボックスとツールチップが表示されます。

メモ: ツールチップは、スロットにスレッドが取り付けられている場合に限り表示されます。

ツールチップに表示される情報は、スレッドの検出およびインベントリステータスによって異なります。複数の計算ノードを含むスレッド（たとえば、PowerEdge FM120x4）が検出されてインベントリされると、ツールチップに次が表示されます。

- スロット名
- 正常性状態
- 接続状態

他の計算スレッドが検出およびインベントリされると、ストレージスレッドにはツールチップに次の内容が表示されます。

- スロット名
- スレッドモデル
- サービスタグ
- 資産タグ

- 正常性状態
- 接続状態

スロットを選択するには、**シャーシビュー** にあるスレッドの図解をクリックします。スレッドが選択されると、スレッドを囲む黄色の長方形ボックスが表示されます。

- 計算スレッドがあるスロットが選択されているときは、スレッドインベントリ（利用可能な場合）が **シャーシビュー** 下に表示されます。
- 複数の計算ノードが含まれたスレッドがあるスロットが選択されている場合、検出されたデバイス（ノード）の概要が **シャーシビュー** の下に表示されます。ノードのインベントリ情報を表示するには、概要内のノードをダブルクリックします。
- ストレージスレッドのあるスロットが選択されている場合、シャーシインベントリ情報は **シャーシビュー** 下に表示されます。ストレージスレッドのインベントリ情報は、シャーシ内に表示されます。

メモ: スレッドの完全なインベントリ情報が表示されるのは、シャーシとスレッドが適切なプロトコルを使用して検出された場合のみです。

メモ: デバイスツリー内でスレッドを選択した場合、**シャーシビュー** は表示されません。**シャーシビュー** を表示するには、デバイスツリーで PowerEdge FX シャーシをクリックします。

オーバーレイ

スロットが使用されており、かつ計算スレッドが検出された場合、計算スレッドの正常性状態が **シャーシビュー** 内にデフォルトでオーバーレイ表示されます。以下は使用可能なオーバーレイオプションとそれらの説明です。

オーバーレイオプション	オーバーレイ色	デバイス状態
正常性状態	赤色	警告
	黄色	重要
	灰色	不明
接続状態	濃い灰色	オフ（切断）
	オーバーレイなし	オン（接続）
なし	オーバーレイなし	適用なし

メモ: 計算スレッドの正常性および接続状態を表示させるには、スレッドが検出されている必要があります。スレッドが検出されなかった、またはスレッドの状態が不明の場合、正常性および接続状態は正常として表示されます。

複数の計算ノードを含むスレッドの正常性状態は、最も重大度の高い計算ノードの正常性状態を反映します。たとえば、1 つのノードが **警告** 状態で、残りの計算ノードが **重要** 状態の場合、スレッドには **重要** 状態が表示されます。

メモ: PowerEdge FX シャーシの **サーバーモードでのシャーシ管理** オプションは、ラックスタイル管理の設定に使用することができます。PowerEdge FX シャーシでラックスタイル管理が無効化されている場合、シャーシの正常性状態ロールアップは、OpenManage Essentials でアップデートされません。また、PSU およびファンから生成されたアラートは、OpenManage Essentials で受信されません。

右クリックアクション

検出され、デバイスツリーで使用可能になっている任意の計算スレッドでの右クリック処置は、デバイスツリーでそのスレッドを右クリックする場合と同じです。

メモ: 複数の計算ノードを含むスレッドとストレージスレッドには、右クリック処置は使用できません。

ナビゲーショントレイル

ナビゲーショントレイルは **シャーシビュー** の下にリンクとして表示され、現在選択されているデバイスを示します。ナビゲーショントレイル内のデバイス名をクリックして、シャーシインベントリに戻ることができます。

PowerEdge FX シャーシスレッドのサポート

PowerEdge FX2 と PowerEdge FX2s に取り付け可能なスレッドは異なる場合があります。スレッドタイプと、それらの OpenManage Essentials でのサポートは次のとおりです。

- 計算スレッド - インベントリ情報およびその他機能を取得するためには検出とインベントリが必要です。これらのスレッドの検出および分類は、OMSA（帯域内）または iDRAC（帯域外）を使用して実行できます。
- ストレージスレッド - これらのスレッドは検出不能で、デバイスツリー、デバイス概要、またはデバイスの標準的な場所には表示されません。ストレージスレッドは **シャーシビュー** に表示され、ストレージスレッドインベントリはシャーシインベントリページに表示されます。
- 複数の計算ノードのあるスレッド - このタイプのスレッドの例には、計算ノードを 4 台装備した PowerEdge FM120x4 スレッドがあります。スレッドの計算ノードが検出されると、これらは **すべてのデバイス → モジュラーシステム → PowerEdge FX → シャーシグループ → スレッドグループ → サーバーノード** 下にあるデバイスツリーに表示されます。各計算ノードは、対応するスレッドの下に表示されます。デバイスツリー内の **スレッドグループ** 名は、必要に応じて編集することができます。

  メモ: PowerEdge FM120x4 スレッドの帯域内（OMSA なし）検出および監視では、WMI または SSH プロトコルのどちらかが有効になっておりセットアップされていることを確認します。

メモ: PowerEdge FX シャーシに取り付けられているスレッドは、デバイスツリー内で、スロット番号ではなくデバイス名に基づいて分類されます。

Dell NAS アプライアンスサポート

次の表では、対応 Dell NAS アプライアンス向けの検出と分類、アプライアンスノード情報の可用性、およびアラート相関についての情報が提供されています。

	FluidFS バージョン 1 搭載の Dell EqualLogic FS7500	**FluidFS バージョン 3 搭載の Dell EqualLogic FS7500**	**FuildFS バージョン 1 搭載の Dell PowerVault MD NX3500**
検出と分類	EqualLogic Group Manager IP および管理 IP の両方を使用した検出のサポート。 コントローラ IP を使用して検出された場合は、複数のエントリが検出されます。	コントローラ / ノード IP を使用した検出のサポート。 EqualLogic Group Manager IP を使用して検出された場合、デバイスは Dell EqualLogic グループ下に分類されます。	両方のコントローラ IP を使用した検出のサポートです。 PowerVault MD Series アレイ IP を使用して検出された場合は、デバイスが PowerVault MD アレイデバイスとして分類されます。
アプライアンスノード情報	デバイスインベントリに表示されます。	デバイスインベントリに表示されます。	デバイスインベントリに表示されます。

	FluidFS バージョン 1 搭載の Dell EqualLogic FS7500	FluidFS バージョン 3 搭載の Dell EqualLogic FS7500	FuildFS バージョン 1 搭載の Dell PowerVault MD NX3500
アラート	コントローラから受信されたアラートは、デバイスに相関されません。	コントローラ / ノードから受信されたアラートは、デバイスに相関されます。 **メモ:** FluidFS バージョン 3.0 を使用して NAS クラスタを検出しているときは、検出範囲内設定に、すべてのコントローラ / ノード IP アドレスを含めることを強くお勧めします。これにより、OpenManage Essentials があらゆる参加コントローラ / ノードから受信した SNMP アラートと検出されたクラスタを適切に相関させることが可能になります。	デバイスから受信されたアラートの一部は、不明として表示される場合があります。

OEM デバイスサポート

Dell OEM デバイス（リブランディングされた、またはブランド排除された Dell サーバーおよび Compellent S8000 iDRAC）は、検出されると、デバイスツリー内の **OEM デバイス** 下に分類されます。タスク、レポート、およびフィルタなどの Dell サーバーで利用できる機能のほとんどが Dell OEM サーバーにも適用されます。ただし、OEM デバイスモジュールによってサポートされていない場合は、システムアップデートができない場合があります。対応プロトコルおよび機能についての詳細は、対応デバイスプロトコルおよび機能マトリックスで Dell サーバー / デバイスについての情報を参照してください。

OEM サーバーは、常にデバイスツリー内の **OEM デバイス** グループ下に分類されます。これらは、**サーバー** または **RAC** グループ下には表示されません。OEM デバイスのサーバーおよび RAC の両方が検出された場合、これらは相関され、**OEM デバイス** グループ下にひとつのデバイスとして表示されます。サーバーおよび RAC 以外のその他 OEM デバイスは、それらが満たす分類条件に基づいて、Microsoft Virtualization Server、VMware ESX サーバーなどの異なるサーバーグループに分類されます。

8

デバイス - 参照

このページは次の情報を提供します。

- デバイスの種類、例えば HA クラスタやサーバーなどに基づいたデバイスのリスト。
- デバイスおよびアラートの概要。
- 特定のデバイスに対して生成されたアラート。
- 正常、重要、不明、警告タイプに基づいたデバイスの正常性。

  メモ: WMI および SNMP プロトコルを使用して検出された、Dell の第 12 世代 PowerEdge サーバー [*yx2x* と記述され、*y* は例えば、M（モジュラ）、R（ラック）、または T（タワー）というようにアルファベットを示し、*x* は数字を表します] では、サーバーに OpenManage Server Administrator がインストールされていなくても、DRAC の正常性ステータスが（サーバーの下に）表示されます。

  メモ: 検出されたデバイスのエージェントの重大度に基づいて、全体的な正常性は重大度の最も重大なものになります。例えば、**警告** と **重要** という 2 種類のステータスの 2 台のサーバーがサーバータイプのデバイスツリーに存在する場合、親サーバーのステータスは **重要** に設定されます。
- デバイスの接続状態 — サーバー（帯域内）および DRAC / iDRAC（帯域外）の両方が検出されて相互に関連付けられると、**デバイス概要** の下の **接続状態** にサーバーの接続状態が表示されます。**RAC デバイス情報** の下の **RAC 接続状態** には、DRAC / iDRAC の接続状態が表示されます。DRAC / iDRAC（帯域外）のみが検出されると（サーバーは検出されない）、**接続状態** および **RAC 接続状態** には同じ情報が表示されます。サーバーのみ（帯域内）が検出されると（DRAC / iDRAC は検出されない）、**接続状態** にはサーバーの接続状態が表示されます。**RAC 接続状態** は **オフ** に設定されます。
- デバイスに関するインベントリ情報。
- サーバーに関するハードウェアログの表示。
- グリッドのフィルタ機能：
  - グループ化バー
  - フィルタアイコンオプション
  - 列をクリックすることによる並べ替え
  - 列の順序変え

  メモ: コンソールが閉じられ、再起動された場合、これらのいずれも保存されません。

関連リンク

デバイスの表示
デバイスインベントリの表示
新規グループの作成
既存グループにデバイスを追加する
グループの非表示
マップビューの使用

インベントリの表示

インベントリを表示するには、**すべてのデバイス** から該当するデバイスに移動して、そのデバイスをクリックします。

デバイスの詳細と、アラートのリンクが表示されます。

アラートの表示

アラートを表示するには、インベントリの詳細ページから、**アラート** をクリックします。

アラート詳細

フィールド	説明
重大度	正常、重要、警告、不明に基づいたアラートの重大度です。
確認済み	アラートのためにフラグされた状態です。
時間	日時フォーマットでのアラート生成時刻です。
デバイス	デバイスの IP アドレスです。
詳細	アラート情報をリストします。例えば、システムがダウンしています：<デバイスの IP アドレス> などがあります。
カテゴリ	アラートカテゴリの種類、例えばシステムイベントをリストします。
ソース	アラートソース名をリストします。

ハードウェアログの表示

サーバーに関するハードウェアログを表示することができます。ハードウェアログを表示するには、インベントリの詳細ページから、**ハードウェアログ** をクリックします。

ハードウェアログの詳細

フィールド	説明
重要度	正常、重要、警告、不明に基づいたアラートの重大度です。
時間	管理下ノードで日時フォーマットでのアラートが生成されたシステム時間です。
詳細	ハードウェアログの詳細をリストします。

フィールド	説明
	例えば、電源の冗長性喪失などです。

アラートフィルタ

アラートにこれらのフィルタを適用できます。**連続的アップデート** を選択して、新たなアラートが受信されるたびにユーザーインタフェースが自動的に更新されるようにします。

フィールド	説明
重大度	**すべて、正常、重要、警告、**および**不明** といったアラートから選択します。
確認済み	アラートのためにフラグされた状態です。
時間	日時フォーマットでのアラート生成時刻です。
デバイス	このデバイスの IP アドレスまたはホスト名です。
詳細	アラート情報です。例えば、システムがダウンしています：<デバイスの IP アドレス> などがあります。
カテゴリ	アラートカテゴリの種類、例えばシステムイベントです。
ソース	アラートソースです。

非対応システムの表示

非対応システムを表示するには、**非対応システム** タブをクリックします。

メモ: 非対応システムは、サーバー、RAC、およびカスタムグループなどのデバイスグループでのみ使用可能です。個々のデバイスでは使用できません。

非準拠システム

非準拠システムタブでは、次の情報が提供されます。

フィールド	説明
システム名	システムのドメイン名です。
モデルタイプ	システムのモデル名です。例えば、Dell PowerEdge があります。
オペレーティングシステム	システムにインストールされているオペレーティングシステムです。

フィールド	説明
サービスタグ	サービスライフサイクル情報を提供する固有の識別子です。
アップデート方法	OpenManage Server Administrator および iDRAC などのアップデート方法を表示します。
検出された時間	検出された日付と時間です。
インベントリ日時	インベントリされた日付と時間です。

非準拠システムを選択して適用するアップデートを選択し、**選択したアップデートを適用** をクリックします。

フィールド	説明
システム名	システムのドメイン名です。
重要	システム用のソフトウェアアップデートの要件です。
アップデート方法	OpenManage Server Administrator および iDRAC などのアップデート方法を表示します。
コンポーネント	ソフトウェア情報です。
種類	ソフトウェアアップデートの種類です。
インストールされたバージョン	インストールされたバージョン番号です。
アップグレード / ダウングレード	緑の矢印は、およびアップグレードを示します。
使用可能なバージョン	使用可能なバージョン番号です。
パッケージ名	ソフトウェアアップデートの名前です。

関連リンク

システムアップデート

デバイスの検索

次の検索オプションがあります。

- 既存クエリの実行
- 新規クエリの作成
- クエリの削除

フィールド	説明
既存のクエリを実行する	このオプションを選択してからドロップダウンリストでクエリを選択します。
クエリの削除	これを選択して、次の処置を完了した後でクエリを削除します。 **既存のクエリを実行する** オプションを選択し、削除したいクエリをドロップダウンリストから選択します。
新しいクエリの作成	このオプションを選択してクエリを作成し、隣のフィールドにクエリの名前を入力します。
クエリロジック	クエリロジックオプションから選択して、複数のクエリオプションを作成します。チェックボックスを選択して有効にし、引数を含めます。
クエリの実行	選択したクエリを実行します。
クエリの保存	選択したクエリを保存します。

関連リンク

クエリ結果

クエリ結果

デバイス検索にはこれらのオプションがリストされます。

フィールド	説明
正常性状態	デバイスの正常性状態を表示します。状態オプションは、**正常**、**警告**、**重要**、および **不明** です。
接続状態	デバイスの接続状態を表示します。接続状態は **オン** または **オフ** です。
名前	デバイスの名前を表示します。
OS 名	デバイスにインストールされているオペレーティングシステムを表示します。
OS リビジョン	デバイスにインストールされているオペレーティングシステムのバージョンを表示します。
サービスタグ	サービスライフサイクル情報を提供する固有の識別子を表示します。
アセットタグ	デバイスに定義されているアセットタグを表示します。

フィールド	説明
デバイスモデル	システムのモデル名が表示されます。例えば、PowerEdge R710 があります。
デバイスタイプ	デバイスの種類を表示します。例えば、デバイスモデル PowerEdge R710 では、デバイスの種類の値がサーバーになります。
システムリビジョン番号	デバイスのリビジョン履歴を表示します。

デバイスグループの作成

デバイスグループ設定

フィールド	説明
名前	新規グループの名前を提供します。
親	このグループは、このデバイスから作成されます。
説明	デバイスグループを説明します。

デバイスの選択

事前に定義したグループ（デバイスの種類）、カスタムグループ、特定のグループ、またはデバイスクエリを選択できます。
デバイスクエリを使用するには、リストからクエリを選択します。

新規 をクリックして、デバイスを検索し、アラート処置に割り当てるための新規デバイスクエリを作成します。

クエリロジックを変更するには、**編集** をクリックします。

ツリーからグループまたはデバイスを選択すると、クエリオプションを使用して、選択内容に対する特有の基準を作成できます。

デバイス選択オプション

フィールド	説明
すべてのデバイス	これを選択して、OpenManage Essentials で管理されているデバイスすべてを含めます。
Citrix XenServers	これを選択して、Citrix XenServer を含めます。
クライアント	これを選択して、デスクトップ、ポータブル、ワークステーションなどのクライアントデバイスを含めます。

フィールド	説明
HA クラスタ	これを選択して、高可用性サーバークラスタを含めます。
KVM	これを選択して、KVM（キーボード、ビデオ、マウス）デバイスを含めます。
Microsoft 仮想化サーバー	このオプションを選択して、Microsoft 仮想化サーバーを含めます。
モジュラーシステム	これを選択して、モジュラーシステムを含めます。
ネットワークデバイス	これを選択して、ネットワークデバイスを含めます。
OOB 分類されていないデバイス	これを選択して、Lifecycle コントローラ対応デバイスなど、帯域外の分類されていないデバイスを含めます。
電源デバイス	これを選択して、PDU および UPS サーバーを含めます。
PowerEdge C サーバー	これを選択して、PowerEdge C サーバーを含めます。
プリンタ	これを選択して、プリンタを含めます。
RAC	これを選択して、Remote Access controller を備えたデバイスを含めます。
サーバー	これを選択して、Dell サーバーを含めます。
ストレージデバイス	これを選択して、ストレージデバイスを含めます。
不明	これを選択して、不明デバイスを含めます。
VMware ESX サーバー	これを選択して、VMware ESX サーバーを含めます。

サマリ — グループ設定

選択内容を表示して、編集します。

マップビュー（デバイス）タブインタフェース

以下は、**マップビュー** に表示されるアイテムとそれらの説明を示します。

項目	説明
検索バー	マップ上の位置を検索できます。
インターネット接続警告	システムがインターネットに接続されていないことを示します。

項目	説明
メモ: インターネット接続警告は、**マップ設定** で **インターネットに接続できない場合にインターネット接続警告を表示** オプションが選択されている場合にのみ、表示されます	
オーバーレイ メニュー	ピンに、デバイスに関する正常性および接続性の状態を重ねることができます。使用可能なオプションには以下があります： • **正常性** • **接続性** 選択されているオプションの横にチェックマークがつきます。
処置 メニュー	実行できる処置のリストを選択できます。使用可能な処置には以下があります： • **すべてのマップの位置の表示** • **ホームビューに移動** • **現在のビューをホームビューとして保存** • **ライセンス済みデバイスの追加** • **ライセンス済みデバイスのインポート** • **すべてのマップの位置の削除** • **エクスポート** • **設定** • **位置詳細の編集** • **位置の削除** • **ストリートレベルに拡大** **メモ: ストリートレベルに拡大** オプションはデバイスがマップ上で選択されている場合にのみ表示されます。 **メモ: アクション** メニューの **位置詳細の編集**、**位置の削除**、および **ストリートレベルに拡大** オプションはデバイス固有のオプションです。これらのオプションはマップ上でデバイスを選択してから使用する必要があります。
ナビゲーションツールバー	マップの移動、ズームインまたはズームアウト、マップサービスプロバイダの選択が可能です。利用可能なマッププロバイダのオプションは以下のとおりです。 • **MapQuest プロバイダ（無料）** • **Bing ロードプロバイダ（ライセンス）** • **Bing 衛星プロバイダ（ライセンス）**
縮尺	マップの現在のズームレベルを、メートルまたはキロメートルで表示します。

この位置のデバイス

マルチピングループをダブルクリックまたは右クリックして **詳細** を選択すると、**この位置のデバイス** ウィンドウが表示されます。以下は、**この位置のデバイス** ウィンドウに表示されるフィールドです。

フィールド	説明
正常性状態	デバイスの正常性状態を表示します。状態オプションは、**正常**、**警告**、**重要**、および **不明** です。
接続状態	デバイスの接続状態を表示します。接続状態は **オン** または **オフ** です。
デバイス名	デバイスの名前を表示します。
サービスタグ	サービスライフサイクル情報を提供する固有の識別子を表示します。
アセットタグ	デバイスに定義されているアセットタグを表示します。
モデル	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
説明	デバイスの説明を表示します。
Address（住所）	デバイスの位置情報を表示します。
Contact（連絡先）	デバイスの連絡先情報を表示します。

マップ設定

下表に **マップ設定** ダイアログボックスに表示されるフィールドの情報を示します。

フィールド	説明
任意のデバイスまたはデバイスグループ選択でのマップビューのアップデート	選択すると、デバイスツリーで選択したデバイスまたはデバイスグループに対応するピンのみを表示するように、マップを設定できます。
インターネットに接続できない場合にインターネット接続警告を表示	選択すると、インターネット接続が利用できない場合にマップ上にメッセージが表示されます。
Bing キー	Bing マップのプロバイダによって要求される有効な Bing キーを入力することができます。
キャンセル	クリックすると **マップ設定** ダイアログボックスが閉じます。
適用	クリックするとアップデートが **マップ設定** ダイアログボックスに保存されます。

関連リンク

マップビューの使用

9

サーバーの導入と再プロビジョニング

サーバーとシャーシにはそれぞれ、デバイスの設定と機能を記述する属性値の大きなリストがあります。これらの設定は、サーバーを機能させるため、オペレーティングシステムの導入前に適切に設定する必要があります。**導入ポータル** では、サーバーまたはシャーシの初期設定、およびオペレーティングシステム導入を実行することができます。このポータルにより、Lifecycle Controller、システム、iDRAC、BIOS、RAID、サーバー用 NIC、およびシャーシ用 CMC の設定が含まれるサーバーまたはシャーシの設定テンプレートの作成が可能になります。これらの設定テンプレートは、オペレーティングシステムの導入プロセスが事前定義済みの起動可能 ISO イメージからキックオフされる前に、初期設定用に複数のサーバーまたはシャーシに導入できます。

導入ポータル を使用することにより、次の操作が可能になります。

- サーバーまたはシャーシ設定ファイルからの設定テンプレートの作成
- サーバーまたはシャーシからの設定テンプレートの作成
- 設定テンプレートの編集
- **再利用およびベアメタルデバイス** グループへのデバイスの追加
- **再利用およびベアメタルデバイス** グループのデバイスの変更または削除
- 別のサーバーまたはシャーシでの設定テンプレートの導入
- 作成済みのタスクとその状態の表示
- **再利用およびベアメタルデバイス** グループからのデバイスの削除
- ファイル共有導入の設定

メモ: 再利用およびベアメタルデバイス グループのデバイスが、デバイス設定導入のターゲットとして表示されます。デバイス設定の導入に対して、**再利用およびベアメタルデバイス** グループにデバイスを明示的に追加し、導入完了後はグループからデバイスを削除する必要があります。

メモ: *デバイス設定導入*および*設定コンプライアンス*機能は、対応サーバー（iDRAC 装備の PowerEdge 12G 以上）に対してライセンス付与（有料）されています。ただし、対応 Dell シャーシ上でのこれらの機能の使用は無料で、ライセンスは必要ありません。サーバーまたはシャーシからのデバイス設定テンプレートの作成にもライセンスは不要です。詳細については、OpenManage Essentials — サーバー設定管理ライセンスを参照してください。

関連リンク

導入ファイル共有の設定
デバイス設定テンプレートの作成
再利用およびベアメタルデバイスグループへのデバイスの追加
デバイス設定テンプレートの管理
デバイス設定テンプレートの導入
ネットワーク ISO イメージの展開
デバイスの自動導入設定
導入タスクの表示

追加情報

OpenManage Essentials — サーバー設定管理ライセンス

メモ: *OpenManage Essentials — サーバー設定管理*ライセンスは OpenManage Essentials のインストールと使用には必要ありません。*OpenManage Essentials — サーバー設定管理*ライセンスがターゲットサーバーにインストールされていることを必須とするのは、サーバー設定管理機能のみです。

*OpenManage Essentials — サーバー設定管理*ライセンスにより、ライセンス付与されたサーバーでのデバイス設定の導入、およびデバイス設定コンプライアンスの検証が可能になります。ライセンスは、サーバーの寿命到達まで有効な永久ライセンスで、一度に 1 台のサーバーのサービスタグにのみバインドすることができます。

メモ: OpenManage Essentials のサーバー設定管理機能の有効化に個別のコードは必要ありません。*OpenManage Essentials — サーバー設定管理*ライセンスがターゲットサーバーにインストールされていれば、そのサーバーでサーバー設定管理機能を使用することができます。

メモ: *OpenManage Essentials — サーバー設定管理*ライセンスは、サーバー上でのデバイス設定導入、および設定コンプライアンスの検証にのみ必要です。次の操作にライセンスは必要ありません。

- サーバーまたはシャーシからデバイス設定テンプレートを作成する
- シャーシ上でデバイス設定を導入、または設定コンプライアンスを検証する

ライセンス可能サーバー

*OpenManage Essentials — サーバー設定管理*ライセンスは以下のサーバーに適用できます。

- ファームウェアバージョン 1.57.57 以降を持つ iDRAC 7 装備の Dell PowerEdge 第 12 世代サーバー
- ファームウェアバージョン 2.00.00.00 以降を持つ iDRAC 8 装備の Dell PowerEdge 第 13 世代（13G）サーバー

ライセンスの購入

*OpenManage Essentials — サーバー設定管理*ライセンスは、**dell.com/support/retail/lkm** の Dell ソフトウェアライセンス管理ポータルから購入およびダウンロードすることができます。また、サーバー購入時にライセンスを購入することもできます。

ライセンスの導入

サーバー購入後にライセンスを購入する場合は、Dell License Manager を使用してライセンスをサーバー上に導入することができます。License Manager は、OpenManage Essentials インストールパッケージを使用してインストールすることが可能です。ライセンスの導入についての情報は、**dell.com/OpenManageManuals** で『Dell License Manager ユーザーズガイド』を参照してください。

ライセンス情報の確認

*OpenManage Essentials — サーバー設定管理*ライセンスがサーバーにインストールされているかどうかは、以下のいずれかの方法で確認できます。

- **レポート** ポータルで、**ライセンス情報** をクリックします。ライセンス対象デバイスにインストールされているライセンスが **ライセンス説明** 列に示されます。

- デバイスツリーでデバイスを選択します。デバイスインベントリ内の **ライセンス情報** 表に、デバイスにインストールされているライセンスが示されます。

ライセンスのないサーバーターゲットの表示

*OpenManage Essentials — サーバー設定管理*ライセンスがインストールされていない設定管理対象サーバーターゲットを表示するには、次の手順を実行します。

1. **デバイスコンプライアンスポータル** に移動します。
2. **デバイスコンプライアンス** 円グラフで、**ライセンスなし** セグメントをクリックします。**ライセンスのないすべてのデバイス** ウィンドウに、ライセンスのないサーバー設定管理対象見込みターゲットが表示されます。

関連リンク

デバイス設定テンプレートの導入
デバイス設定自動導入のセットアップ
資格情報およびデバイス設定インベントリスケジュールの設定

導入およびコンプライアンスタスクのデバイス要件

デバイス設定導入および設定コンプライアンスタスクに対するデバイス要件は次のとおりです。

- サーバーの場合：
  - ファームウェアバージョン 1.57.57 以降を持つ iDRAC 7 装備の Dell PowerEdge 12G サーバー
  - ファームウェアバージョン 2.00.00.00 以降を持つ iDRAC 8 装備の Dell PowerEdge 13G サーバー
  - サーバーでは、Dell Lifecycle Controller 2 バージョン 1.4.*x* 以降を実行する必要があります。
  - iDRAC にインストールされている *OpenManage Essentials - サーバー設定管理*ライセンス。これは、iDRAC ライセンスとは別のライセンスです。
  - iDRAC Express または iDRAC Enterprise ライセンス。これは、*OpenManage Essentials - サーバー設定管理ライセンス*とは別のライセンスです。
- シャーシの場合：
  - ファームウェアのバージョンが 4.6 以降の PowerEdge M1000e
  - ファームウェアのバージョンが 1.3 以降の PowerEdge VRTX

関連リンク

デバイス設定ファイルからのデバイス設定テンプレートの作成
リファレンスデバイスからのデバイス設定テンプレートの作成
デバイス設定テンプレートの導入
ネットワーク ISO イメージの展開
デバイス設定自動導入のセットアップ
資格情報およびデバイス設定インベントリスケジュールの設定
インベントリ構成詳細の表示

デバイス設定導入を開始する前に

ターゲットデバイスへデバイス設定を導入する前に、次の手順を行う必要があります。

1. OpenManage Essentials を実行しているサーバー上で導入ファイル共有を設定します。
2. **再利用およびベアメタルデバイス** グループにターゲットデバイスを追加します。

関連リンク

デバイス設定導入の概要
導入ファイル共有の設定
再利用およびベアメタルデバイスグループへのデバイスの追加

デバイス設定導入の概要

ターゲットデバイスにデバイス設定テンプレートを導入する際の手順は次の通りです。

1. **デバイス設定テンプレートの作成** — **共通タスク** ペインの **テンプレートの作成** タスクを使用してデバイス設定テンプレートを作成します。設定ファイルまたはリファレンスデバイスから選んでテンプレートを作成することができます。
2. **デバイス設定テンプレートの編集** — **テンプレート** ペインからテンプレートを選択し、右ペインに表示されている設定属性を必要に応じて編集します。
3. **ターゲットデバイスでのデバイス設定テンプレートの導入** — **共通タスク** ペインの **テンプレートの導入** タスクを使用して、テンプレート、ターゲットデバイスを選択し、デバイス固有の属性を編集してから、設定の属性を導入します。また、**自動導入のセットアップ** タスクを使用して、後に検出するデバイスにデバイス設定テンプレートを導入することもできます。

メモ: デバイス構成テンプレートが作成された元のデバイスのハードウェアと、導入ターゲットのハードウェアが同一である場合、属性がうまく導入される可能性が向上します。ハードウェアが完全に一致しない場合、導入タスクが正常に完了しない場合があります。ただし、一致するコンポーネントの属性はうまく導入されます。

関連リンク

デバイス設定導入を開始する前に

導入ポータルの表示

導入ポータル を表示するには、**導入** → **導入ポータル** の順にクリックします。

導入ファイル共有の設定

デバイスからの設定テンプレートを作成また導入する前に、OpenManage Essentials を実行しているサーバーで導入ファイル共有を設定する必要があります。導入ファイル共有は、ターゲットサーバーまたはシャーシでの設定内容の取得および適用に使用される設定ファイルを一時的に保管します。

導入ファイル共有を設定するには、次の手順を実行します。

1. 次のいずれかの手順を実行してください。

   - **プリファレンス** → **導入設定** の順にクリックします。

- **導入** をクリックします。**共通タスク** ペインで、**ファイル共有設定** をクリックします。
- **導入** → **導入を開始する前に** → **導入ファイル共有の設定** の順にクリックします。
- **管理** → **設定** とクリックします。**共通タスク** ペインで、**ファイル共有設定** をクリックします。

ファイル共有設定 ウィンドウが表示されます。

2. 適切なフィールドに、OpenManage Essentials を実行しているサーバーのドメイン \ ユーザー名とパスワードを入力します。
3. **適用** をクリックします。
   ファイル共有が正しく設定されると、**ファイル共有状態** に **OK** が表示されます。

関連リンク

デバイス設定導入を開始する前に

デバイス設定テンプレートの作成

テンプレートの作成 タスクでは、サーバーまたはシャーシの属性を含むデバイス設定テンプレートを作成します。デバイス設定テンプレートを使用して、次の操作ができます。

- 別のサーバーまたはシャーシでの設定の導入。
- サーバーまたはシャーシの設定テンプレートへのコンプライアンスを確認。

以下からデバイス設定テンプレートを作成することができます。

- デバイス設定ファイル。
- 検出済みのサーバーまたはシャーシ。

関連リンク

デバイス設定ファイルからのデバイス設定テンプレートの作成
リファレンスデバイスからのデバイス設定テンプレートの作成

デバイス設定ファイルからのデバイス設定テンプレートの作成

デバイス設定ファイルを既存のサーバー設定ファイル（.xml）またはシャーシ設定ファイル（.ini）から作成することができます。
デバイス設定ファイルから設定テンプレートを作成する前に、次の項目を確認してください。

- 導入ファイル共有が設定されている。詳細については、「導入ファイル共有の設定」を参照してください。
- 設定ファイルは、導入およびコンプライアンスタスクのデバイス要件で指定した要件を満たすデバイスからのものです。

デバイス設定ファイルからデバイス設定テンプレートを作成するには、次の手順を実行します。

1. 次のいずれかの手順を実行してください。
   - **導入** → **導入ポータル** の順にクリックします。
   - **管理** → **設定** をクリックします。
2. 次のいずれかの手順を実行してください。
   - **共通タスク** ペインで、 **テンプレートの作成** をクリックします。
   - **テンプレート** ペインで、**サーバーテンプレート** または **シャーシテンプレート** を右クリックして、**テンプレートの作成** をクリックします。

- **共通タスク** ペインで、**導入を開始する前に** または **コンプライアンスを開始する前に** → **テンプレートの作成** をクリックします。

テンプレートの作成 ウィザードが表示されます。

メモ: 導入ファイル共有設定が設定されていない場合は、`One or more settings require configuring for this action` というメッセージが表示されます。**OK** をクリックすると **ファイル共有設定** ウィンドウが表示されます。ファイル共有の設定を行った後、**テンプレートの作成ウィザード** が表示されます。

3. **名前**フィールドに、テンプレートの名前を入力します。
4. **ファイルから作成** をクリックします。
5. **参照** をクリックします。
6. 設定ファイルを選択し、**開く** をクリックします。
7. **終了** をクリックします。

作成された設定テンプレートが **テンプレート** ペインに表示されます。

関連リンク

テンプレートの作成ウィザード
導入およびコンプライアンスタスクのデバイス要件

リファレンスデバイスからのデバイス設定テンプレートの作成

検出済みのサーバーまたはシャーシからデバイス設定テンプレートを作成することができます。
リファレンスデバイスから設定テンプレートを作成する前に、次の項目を確認してください。

- 導入ファイル共有が設定されている。詳細については、「導入ファイル共有の設定」を参照してください。
- デバイス要件導入とコンプライアンスタスクのデバイス要件で指定した要件を満たすデバイスからデバイス構成テンプレートを作成します。

リファレンスデバイスから、デバイス設定テンプレートを作成するには、次の手順を実行します。

1. 次のいずれかの手順を実行してください。
   - **導入** → **導入ポータル** の順にクリックします。
   - **管理** → **設定** をクリックします。
2. 次のいずれかの手順を実行してください。
   - **共通タスク** ペインで、**テンプレートの作成** をクリックします。
   - **テンプレート** ペインで、**サーバーテンプレート** または **シャーシテンプレート** を右クリックして、**テンプレートの作成** をクリックします。
   - **共通タスク** ペインで、**導入「はじめに」** または **コンプライアンス「はじめに」** → **テンプレートの作成** をクリックします。

   テンプレートの作成 ウィンドウが表示されます。

   メモ: 導入ファイルの共有設定ファイルが構成されていない場合は、`One or more settings require configuring for this action` (このアクションには 1 つ以上の設定が必要です) というメッセージが表示されます。**OK** をクリックすると、 **ファイル共有の設定** ウィンドウが表示されます。ファイル共有設定を行った後、**テンプレートの作成ウィザード** が表示されます。
3. テンプレートの **名前** を入力します。
4. デバイスを検索するか、または **デバイスの種類** を選択して、**該当するすべてのデバイス** ツリーからデバイスを選択します。

5. **実行の資格情報** で、システム管理者またはオペレーター権限のある iDRAC 資格情報を入力し、**終了** をクリックします。
6. タスク送信のメッセージで、 **OK** をクリックします。

テンプレートの作成 タスクが、右ペインの **タスク** タブに作成されます。右ペインの **タスク実行履歴** で設定テンプレート状態を表示できます。タスク実行の詳細を表示するには、**タスク実行履歴** 内のタスクをダブルクリックします。作成された設定テンプレートが **テンプレート** ペインに表示されます。

関連リンク

テンプレートの作成ウィザード
導入およびコンプライアンスタスクのデバイス要件

再利用およびベアメタルデバイスグループへのデバイスの追加

再利用およびベアメタル グループへのデバイスの追加は、それらのデバイス上での構成テンプレートまたはネットワーク ISO イメージのいずれを導入する場合も前提条件となります。

注意: 正しいデバイスのみが再利用およびベアメタルデバイスグループに追加されていることを確認してください。再利用およびベアメタルデバイスへの設定テンプレートが導入された後は、デバイスを元の設定に戻すことができないことがあります。

メモ: 再利用およびベアメタルデバイスグループ に追加するサーバーには、*OpenManage Essentials — サーバー設定管理ライセンス*がインストールされている必要があります。詳細に関しては、OpenManage Essentials — サーバー設定管理ライセンスを参照してください。

再利用およびベアメタルデバイスグループ にデバイスを追加するには、次の手順を実行します。

1. **導入** → **導入ポータル** の順にクリックします。
2. **再利用およびベアメタルデバイス** タブで、**デバイスの修正** をクリックします。
   再利用およびベアメタルデバイスグループのデバイスの変更 ウィンドウが表示されます。
3. **該当するすべてのデバイス** ツリーから、**再利用およびベアメタルデバイス** グループへ追加したいデバイスを選択します。
4. **終了** をクリックします。
   追加したデバイスが右ペインの **再利用およびベアメタルデバイス** タブとデバイスツリーの **再利用およびベアメタルデバイス** グループにリスト表示されます。

関連リンク

デバイス設定テンプレートの導入
デバイス設定導入を開始する前に
再利用およびベアメタルデバイス

デバイス設定テンプレートの管理

デバイス設定テンプレートには、サーバーまたはシャーシの様々な属性が含まれています。コンプライアンス状態の導入または確認にデバイス設定テンプレートを使用する前に、次の操作をすることができます。

- デバイス設定テンプレートの属性の表示
- デバイス設定テンプレートのクローン化
- デバイス設定テンプレートの編集

- デバイス設定テンプレートのエクスポート
- デバイス設定テンプレートのプロパティの表示

関連リンク

デバイス設定テンプレート属性の表示
デバイス設定テンプレートのクローン化
デバイス設定テンプレートの編集
デバイス設定テンプレートのエクスポート

デバイス設定テンプレート属性の表示

デバイス設定テンプレート属性を表示するには、次の手順を実行します。

1. 次のいずれかの手順を実行してください。
   - **導入 → 導入ポータル** の順にクリックします。
   - **管理 → 設定 → デバイスコンプライアンスポータル** の順にクリックします。
2. **テンプレート** ペインで、サンプルテンプレートまたは作成済みのテンプレートのいずれかをクリックします。
   テンプレートの属性が右ペインの **属性** タブに表示されます。テンプレートの属性合計数は、**属性** タブの右上に表示されます。

関連リンク

デバイス設定テンプレートの管理
デバイス設定テンプレートの詳細

デバイス設定テンプレートのクローン化

デバイス設定テンプレートをクローン化して、編集または導入が可能なテンプレートを作成することができます。
デバイス設定テンプレートをクローン化するには、次の手順を実行します。

1. 次のいずれかの手順を実行してください。
   - **導入 → 導入ポータル** の順にクリックします。
   - **管理 → 設定 → デバイスコンプライアンスポータル** の順にクリックします。
2. **テンプレート** ペインでテンプレートを右クリックし、**クローン化** をクリックします。
   クローン化設定テンプレート ウィンドウが表示されます。
3. テンプレートの名前を入力して、**OK** をクリックします。

クローンされたテンプレートは、サンプルテンプレートの下にある **テンプレート** ペインに表示されます。

関連リンク

デバイス設定テンプレートの管理

デバイス設定テンプレートの編集

コンプライアンスの確認にテンプレートを導入または使用する前に、デバイス設定テンプレートを編集して、テンプレートの内容を変更することができます。
デバイス設定テンプレートを編集するには、次の手順を実行します。

1. 次のいずれかの手順を実行してください。
   - **導入 → 導入ポータル** の順にクリックします。

- **管理** → **設定** → **デバイスコンプライアンスポータル** の順にクリックします。

2. **テンプレート** ペインでテンプレートを右クリックし、**編集** をクリックします。
   テンプレートの属性が、右ペインの **属性** タブに表示されます。
3. 特定の属性をテンプレートに導入せず、ターゲットデバイスで現在の属性値を維持したい場合は、**導入** コラムのその属性のチェックボックスからチェックを外します。
4. テンプレート内のすべての属性の選択をオンまたはオフにするには、**導入**カラムタイトルの横に表示されたチェックボックスを選択または選択解除します。

   メモ: 属性の値が別の属性に依存している場合、依存関係が設定テンプレートの **依存関係** 列に示されます。依存属性を導入するには、まず主要属性を編集してから、依存属性を編集する必要があります。
5. 複数の属性行を選択するには、最初の属性の行を選択し、<Shift> キーを押しながら、最後の属性の行をクリックします。選択した行の属性の選択をチェックまたはチェック解除するには、**チェック**または**チェック解除**を右クリックして選択します。
6. お好みに合わせて **値** のコラム内の値を選択するか、編集します。
   テンプレート内の属性の合計数と編集可能な属性の数が **属性** タブの右上に表示されます。
7. **保存** をクリックします。

関連リンク

デバイス設定テンプレートの管理

デバイス設定テンプレートのエクスポート

デバイス設定テンプレートは **.xml**（サーバー設定テンプレート）または **.ini**（シャーシ設定テンプレート）ファイルにエクスポートできます。属性をエクスポートすることにより、代替方法を使用して属性を編集することが可能になります。テンプレートを編集したら、そのテンプレートをインポートして、導入またはコンプライアンスの検証用に使用することができます。

デバイス設定テンプレートをエクスポートするには、次の手順を実行します。

メモ: デバイス設定テンプレートをエクスポートすると、選択されていない属性を含む設定テンプレートの全属性がエクスポートされます。

1. 次のいずれかの手順を実行してください。
   - **導入** → **導入ポータル** の順にクリックします。
   - **管理** → **設定** → **デバイスコンプライアンスポータル** の順にクリックします。
2. **テンプレート** ペインで、サンプルテンプレートまたは作成済みのテンプレートのいずれかを右クリックして **テンプレートのエクスポート** をクリックします。
3. テンプレートをエクスポートする場所に移動し、ファイル名を入力して **保存** をクリックします。

関連リンク

デバイス設定テンプレートの管理

デバイス設定テンプレートの導入

設定の導入 タスクでは、一連の設定属性を含む設定テンプレートを特定のデバイスに導入することができます。デバイス設定テンプレートをデバイスに導入することにより、複数のデバイスの設定を統一することができます。

デバイス設定テンプレートを導入する前に、次の項目を確認してください。

- 導入ファイル共有が設定されている。詳細については、導入ファイル共有の設定を参照してください。

- ターゲットデバイスが **再利用デバイスとベアメタルデバイス** に追加されている。詳細については、再利用およびベアメタルデバイスグループへのデバイスの追加を参照してください。
- デバイス設定テンプレートの作成またはサンプルテンプレートのクローニングが完了している。
- ターゲットデバイスが 導入およびコンプライアンスタスクのデバイス要件を満たしている。
- *OpenManage Essentials — サーバー設定管理*ライセンスがすべてのターゲットサーバーにインストールされている。詳細に関しては、OpenManage Essentials — サーバー設定管理ライセンスを参照してください。

注意: 設定テンプレートをデバイスに導入することにより、パフォーマンス、接続性、デバイスの起動能力を含むデバイス設定に対して破壊的な変化をもたらす可能性があります。

設定テンプレートをデバイスに導入するには、次の手順を実行します。

1. **導入** をクリックします。
   導入ポータル が表示されます。
2. **共通タスク** ペインで、 **テンプレートの導入** をクリックします。
   自動導入のセットアップ ウィザードが表示されます。
3. **名前および導入オプション** ページで次の手順を実行します。
   a. タスクに適切な名前を入力します。

      メモ: オペレーティングシステムおよび設定テンプレートを導入する場合は、**テンプレートの導入** および **ネットワーク ISO から起動** オプションの両方を選択できます。各操作に対して別々のタスクが作成されます。
   b. 導入の完了後、設定テンプレートを使用してデバイスのコンプライアンス状態を確認したい場合は、**導入後にこのテンプレートを使用してコンプライアンスを確認する** を選択します。
   c. **次へ** をクリックします。
4. **テンプレートの選択** ページで次の手順を実行します。
   a. ターゲットデバイスタイプに基づいて、**サーバーテンプレート** または **シャーシテンプレート** のいずれかをクリックしてテンプレートを選択してください。
   b. 導入したい設定テンプレートを選択します。

      メモ: 作成済みまたはクローン化が完了している設定テンプレートのみを選択することができます。
   c. **次へ** をクリックします。
5. **デバイスの選択** ページで、**再利用デバイスおよびベアメタルデバイス** ツリーからターゲットデバイスを選択し、**次へ** をクリックします。

   メモ: 導入用に選択できるのは、**再利用およびベアメタルデバイス** グループに追加されたデバイスのみです。
6. **属性の編集** ページで次の手順を実行します。

   メモ: OpenManage Essentials は、設定テンプレートの作成時にソースからのパスワードを含めません。ターゲットデバイス用にパスワードを設定する場合は、導入前に設定テンプレート内ですべてのパスワード属性を編集する必要があります。

   a. **テンプレート属性** タブをクリックします。
   b. 属性のグループ名をクリックして、グループ内の属性のリストを表示します。
   c. 特定の属性をテンプレートに導入せず、ターゲットデバイスで現在の属性値を維持したい場合は、**導入** コラムのチェックボックスからチェックを外します。
   d. お好みに合わせて **値** のコラム内の値を選択するか、編集します。

テンプレート内の属性の合計数と編集可能な属性の数が **以下によってグループ化** のバーに表示されます。

e. **属性固有の属性** タブをクリックし、ターゲットデバイスに固有の属性を属編集します。

メモ: デバイス固有属性 タブには、導入用に選択されたテンプレートに基づいた属性が表示される場合とされない場合があります。

f. 属性のグループ名をクリックして、グループ内の属性のリストを表示します。

g. 特定の属性をテンプレートに導入せず、ターゲットデバイスで現在の属性値を維持したい場合は、**導入** コラムのチェックボックスからチェックを外します。

h. お好みに合わせて **値** のコラム内の値を選択するか、編集します。

i. **保存** をクリックします。

j. **次へ** をクリックします。

7. **スケジュールの設定** ページで次の手順を実行します。

a. **今すぐ実行** を選択するか、カレンダーアイコンをクリックしてタスクを実行する日時を選択します。

b. **実行資格情報** で次の操作を行います。

- サーバー設定導入 — iDRAC 管理者資格情報を入力します。
- シャーシ設定導入 — CMC 管理者資格情報を入力します。

c. **次へ** をクリックします。

8. サマリページで、入力した情報を確認してから **終了する** をクリックします。

テンプレートの導入 の警告が表示されます。

9. 導入を続行するには、**はい** をクリックします。

テンプレートの導入 タスクが作成され、選択したスケジュールに基づいてタスクが実行されます。**タスク実行履歴** をダブルクリックして、タスク実行の詳細を表示することができます。

関連リンク

テンプレートの導入ウィザード
デバイス設定セットアップウィザード
OpenManage Essentials — サーバー設定管理ライセンス
導入およびコンプライアンスタスクのデバイス要件

ネットワーク ISO イメージの展開

構成の導入 タスクを行うと、ネットワーク ISO イメージで起動してから、サポートされているサーバーで ISO イメージを導入できます。

ネットワーク ISO イメージの導入を開始する前に、次の項目を確認してください。

- 導入ファイル共有が設定されている。詳細については、導入ファイル共有の設定を参照してください。
- ターゲットデバイスが **再利用デバイスとベアメタルデバイス** に追加されている。詳細については、再利用およびベアメタルデバイスグループへのデバイスの追加を参照してください。
- ISO イメージがあるネットワーク共有上で、**フルコントロール** のアクセス許可を有している。
- ターゲットデバイスが 導入およびコンプライアンスタスクのデバイス要件を満たしている。
- *OpenManage Essentials — サーバー設定管理*がすべてのターゲットサーバーにインストールされている。詳細に関しては、OpenManage Essentials — サーバー設定管理ライセンスを参照してください。

ネットワーク ISO イメージを導入するには、次の手順を実行します。

1. **導入** をクリックします。
2. **共通タスク** ペインで、**テンプレートの導入** をクリックします。
   テンプレートの導入ウィザード が表示されます。
3. **名前および導入オプション** ページで次の手順を実行します。
   a. タスクに適切な名前を入力します。

      メモ: オペレーティングシステムおよび設定テンプレートを導入したい場合は、**テンプレートの導入** および **ネットワーク ISO から起動** オプションの両方を選択できます。各操作に対して別々のタスクが作成されます。
   b. **テンプレートの導入** をクリアして、**ネットワーク ISO から起動** を選択します。
   c. **次へ** をクリックします。
4. **ISO の場所の選択** ページで次の手順を実行します。
   a. **ISO ファイル名** で、ISO イメージファイルの名前を入力します。
   b. **共有場所** で、ネットワーク共有の名前と IP アドレスを入力します。
   c. **共有資格情報** で、ユーザー名とパスワードを入力します。
   d. **次へ** をクリックします。
5. **デバイスの選択** ページで、**再利用デバイスおよびベアメタルデバイス** ツリーからターゲットデバイスを選択し、**次へ** をクリックします。
6. **スケジュールの設定** ページで次の手順を実行します。
   a. **今すぐ実行** を選択するか、カレンダーアイコンをクリックしてタスクを実行する日時を選択します。
   b. **実行資格情報** に iDRAC 管理者資格情報を入力します。
   c. **次へ** をクリックします。
7. サマリページで、入力した情報を確認してから **終了する** をクリックします。
8. 導入を続行するには、**はい** をクリックします。

ネットワーク ISO から起動タスク が作成され、選択したスケジュールに基づいて実行されます。 **タスクの実行履歴** でタスクをダブルクリックすると、タスク実行の詳細を表示できます。ネットワーク ISO イメージにターゲットサーバーが起動後、iDRAC 仮想コンソールを起動して、ISO イメージ展開のオプションを選択する必要があります。

関連リンク

テンプレートの導入ウィザード
デバイス設定セットアップウィザード
導入およびコンプライアンスタスクのデバイス要件

再利用およびベアメタルデバイスグループからのデバイスの削除

デバイス構成導入、ネットワーク ISO イメージ導入、自動導入タスクが完了した後、**再利用およびベアメタルデバイス** グループからデバイスを削除できます。

再利用およびベアメタルデバイスグループ からデバイスを削除するには、次の手順を実行します。

1. **導入** → **導入ポータル** の順にクリックします。
2. **再利用およびベアメタルデバイス** タブで、削除するデバイスを選択します。
3. 次のいずれかの手順を実行してください。
   - **選択したデバイスの削除**をクリックします。

- 右クリックして **削除** を選択します。

4. 確認ダイアログボックスで、**はい** をクリックします。
   デバイスが、右ペインの **再利用およびベアメタルデバイス** タブおよびデバイスツリーの **再利用およびベアメタルデバイス** グループから削除されます。

関連リンク

再利用およびベアメタルデバイス

デバイスの自動導入設定

自動導入のセットアップ タスクでは、後に検出するターゲットデバイスにデバイス設定またはネットワークの ISO イメージを導入することができます。例えば、お客様の会社で 500 台のシステムを発注し、今後 2 週間で配送される際に、デバイスが検出されると定期的に実行され設定を導入する **自動導入のセットアップ** タスクを作成することが可能です。

タスクを作成するときは、設定の導入先となるターゲットデバイスのサービスタグまたはノード ID が含まれた .csv ファイルをインポートする必要があります。**自動導入のセットアップ** タスクはデフォルトで 60 分おきに実行され、ターゲットデバイスが検出されたかどうかを確認するようになっています。ターゲットデバイスが検出されると、そのターゲットデバイスにデバイス設定が自動的に導入されます。希望に応じて **自動導入のセットアップ** タスクの反復頻度を変更することもできます。

関連リンク

自動導入の設定
デバイス設定自動導入のセットアップ
自動導入資格情報の管理
自動導入検出範囲の追加

自動導入の設定

自動導入の設定 により、以下が可能になります。

- デバイス設定の自動導入を有効化または無効化する。
- デバイス設定自動導入タスクの反復頻度を設定する。

自動導入を設定するには、次の手順を実行します。

1. **プリファレンス → 導入設定** をクリックします。
   導入設定 ページが表示されます。
2. **最近検出されたデバイスへの自動導入を有効にする** を選択して（または選択解除して）、デバイス設定の自動導入を有効（または無効）にします。
3. 好みに合わせて **自動導入を xx 分ごとに実行する** を編集します。
4. **適用** をクリックします。

関連リンク

デバイスの自動導入設定

デバイス設定自動導入のセットアップ

自動導入のセットアップ タスクでは、一連の設定の属性が含まれる設定テンプレートを後に検出するデバイスに導入することができます。デバイスにデバイス設定テンプレートを導入することにより、複数のデバイスの設定を統一することができます。

デバイス設定自動導入タスクを作成する前に、次の項目を確認してください。

- 導入ファイル共有が設定されている。詳細については、導入ファイル共有の設定を参照してください。
- 自動導入が有効になっており、設定が完了していること。詳細については、自動導入の設定を参照してください。
- 各ターゲットデバイスのサービスタグまたはノード ID は .csv ファイルにあります。サービスタグまたはノード ID は、.csv ファイル内のタイトル、「サービスタグ」「サービスタグ」、「ノード ID」下に表示されています。

  メモ: ノード ID は、複数の計算ノードで構成されているデバイスの識別子です。例えば、PowerEdge FM120x4 スレッドには、4 台の計算ノードがあります。.csv ファイルでは、自動展開したい特定の計算ノードのノード ID を含める必要があります。
- デバイス設定テンプレートの作成またはサンプルテンプレートのクローニングが完了している。
- ターゲットデバイスが 導入およびコンプライアンスタスクのデバイス要件を満たしている。
- *OpenManage Essentials — サーバー設定管理*ライセンスがすべてのターゲットサーバーにインストールされている。詳細に関しては、OpenManage Essentials — サーバー設定管理ライセンスを参照してください。

注意: 設定テンプレートをデバイスに導入することにより、パフォーマンス、接続性、デバイスの起動能力を含むデバイス設定に対して破壊的な変化をもたらす可能性があります。

後に検出されるデバイスに設定テンプレートを自動導入するには、次の手順を実行します。

1. **導入** をクリックします。
   導入ポータル が表示されます。
2. 次のいずれかの手順を実行してください。
   - **共通タスク** ペインで、 **自動導入のセットアップ** をクリックします。
   - **自動導入** をクリックし、 **デバイスの追加** をクリックします。

   自動導入のセットアップ ウィザードが表示されます。
3. **導入オプション** のページで次の手順を実行します。
   a. オペレーティングシステムおよび設定テンプレートを自動導入したい場合は、**テンプレートの導入** および **ネットワーク ISO から起動** オプションの両方を選択できます。各操作に対して別々のタスクが作成されます。
   b. 導入の完了後、設定テンプレートを使用してデバイスのコンプライアンス状態を確認したい場合は、**導入後にこのテンプレートを使用してコンプライアンスを確認する** を選択します。
   c. **次へ** をクリックします。
4. **テンプレートの選択** ページで次の手順を実行します。
   a. ターゲットデバイスタイプに基づいて、**サーバーテンプレート** または **シャーシテンプレート** のいずれかをクリックしてテンプレートを選択してください。
   b. 導入したい設定テンプレートを選択します。

      メモ: 作成済みまたはクローン化が完了している設定テンプレートのみを選択することができます。

c. **次へ** をクリックします。

5. **サービスタグ / ノード ID のインポート** ページで、次の手順を実行します。
   a. **インポート** をクリックします。
   b. サービスタグまたはノード ID が含まれた .csv ファイルを参照して選択します。

      メモ: インポートできるのは、まだ検出されていない有効なサービスタグまたはノード ID のみです。

   c. **開く** をクリックします。

      インポート概要 が表示されます。
   d. **OK** をクリックします。
   e. **次へ** をクリックします。
6. **属性の編集** ページで次の手順を実行します。

   メモ: OpenManage Essentials は、設定テンプレートの作成時にソースからのパスワードを含めません。ターゲットデバイス用にパスワードを設定する場合は、導入前に設定テンプレート内ですべてのパスワード属性を編集する必要があります。

   a. **テンプレート属性** タブをクリックします。
   b. 属性のグループ名をクリックして、グループ内の属性のリストを表示します。
   c. 特定の属性をテンプレートに導入せず、ターゲットデバイスで現在の属性値を維持したい場合は、**導入** 列のチェックボックスからチェックを外します。
   d. お好みに合わせて **値** の列内の値を選択するか、編集します。

      テンプレート内の属性の合計数と編集可能な属性の数が **以下によってグループ化** のバーに表示されます。
   e. **デバイス固有属性** タブをクリックし、ターゲットデバイスに固有の属性を属編集します。

      メモ: デバイス固有属性 タブには、導入用に選択されたテンプレートに基づいた属性が表示される場合とされない場合があります。

   f. 属性のグループ名をクリックして、グループ内の属性のリストを表示します。
   g. 特定の属性をテンプレートに導入せず、ターゲットデバイスで現在の属性値を維持する場合は、**導入** 列のチェックボックスからチェックを外します。
   h. 希望に応じて **値** の列内の値を選択または編集します。

      メモ: デバイス固有属性 は、特定のデバイス、または全てのデバイス用に .csv ファイルとしてエクスポートし、属性を編集して、それらの属性をインポートすることもできます。**デバイス固有属性** をエクスポートまたはインポートするには、**インポート / エクスポート** をクリックします。

   i. **保存** をクリックします。
   j. **次へ** をクリックします。
7. **実行の資格情報** ページで次の手順を実行します。
   a. **資格情報** の項で、**新しい資格情報の追加** をクリックします。

      メモ: サーバー設定導入には iDRAC 管理者資格情報を入力し、シャーシ設定導入には CMC 管理者資格情報を入力します。

      資格情報の追加 ウィンドウが表示されます。
   b. ターゲットデバイスでタスクを実行するために必要な説明、管理者ユーザー名、およびパスワードを入力します。
   c. 資格情報をすべてのターゲットデバイス用のデフォルト資格情報として設定したい場合は、**デフォルト** を選択して **終了** をクリックします。
   d. すべてのターゲットデバイスでタスクを実行するために必要な資格情報が設定されるまで、手順 a～c を繰り返します。

e. **デバイス** の項で、各ターゲットデバイス用の **実行の資格情報** を設定します。
f. **次へ** をクリックします。

8. サマリページで、入力した情報を確認してから **終了する** をクリックします。
   テンプレートの導入 の警告が表示されます。
9. **自動導入の設定** タスク作成を続行する場合は、**はい** をクリックします。

自動導入の設定 タスクが作成され、**プリファレンス → 自動導入の設定** で設定されたスケジュールに基づいて実行されます。**タスクの実行履歴** でタスクをダブルクリックして、タスクの実行詳細を表示することができます。

デバイスが検出され、自動導入タスクが完了すると、デバイスが **再利用およびベアメタルデバイス** グループに移動されます。デバイス上で他のデバイス設定を導入しない場合は、**再利用およびベアメタルデバイス** グループからデバイスを削除できます。

メモ: 自動導入 タブ内のデバイスは、自動導入タスクが失敗した場合でも **再利用およびベアメタルデバイス** グループに移動されます。これらのデバイスに設定テンプレートを導入するには、新しい導入タスクを作成する必要があります。

関連リンク

デバイスの自動導入設定
自動導入のセットアップウィザード
デバイス固有属性のインポート
デバイス固有属性のエクスポート
OpenManage Essentials — サーバー設定管理ライセンス
導入およびコンプライアンスタスクのデバイス要件
自動導入

自動導入資格情報の管理

自動導入資格情報の管理 タブでは、自動導入用にセットアップされたターゲットデバイスへ資格情報の割り当ておよび設定ができます。
自動導入資格情報を管理するには、次の手順を実行します。

1. **導入** をクリックします。
   導入ポータル が表示されます。
2. **共通タスク** ペインで、 **自動導入資格情報の管理** をクリックします。
   自動導入資格情報の管理 ウィンドウが表示されます。
3. ターゲットデバイスに割り当てる新しい資格情報を追加する場合には、**新しい資格情報の追加** をクリックします。

   メモ: サーバー設定導入には iDRAC 管理者資格情報を入力し、シャーシ設定導入には CMC 管理者資格情報を入力します。

   a. **資格情報の追加** ウィンドウで、内容、ユーザー名、およびパスワードを入力します。
   b. 資格情報をすべてのターゲットデバイス用のデフォルト資格情報として設定したい場合は、**デフォルト** を選択して **終了** をクリックします。
      追加した資格情報が **資格情報** の項に表示されます。
4. 既存の資格情報を更新する場合は、更新アイコンをクリックします。
   a. **資格情報の追加** ウィンドウで、必要に応じて、内容、ユーザー名、およびパスワードを編集します。
   b. 資格情報を新しいターゲットデバイスすべてのデフォルト資格情報として設定したい場合は、**デフォルト** を選択して **終了** をクリックします。

5. 既存の資格情報を削除する場合は、削除アイコンをクリックし、**確認必須** ダイアログボックスで **OK** をクリックします。
   削除した資格情報は **資格情報** の項に表示されなくなります。
6. ターゲットデバイスに資格情報を割り当てる場合は、**デバイス** の項で、**実行の資格情報** から該当する資格情報を選択します。
7. **終了** をクリックします。

関連リンク

デバイスの自動導入設定
自動導入資格情報の管理

自動導入検出範囲の追加

自動導入 タブまたは **検出とインベントリ** ポータルで自動導入の検出範囲を作成できます。
自動導入 タブで検出範囲を追加する前に、自動導入タスクをセットアップする必要があります。
自動導入 タブを使用して検出範囲を追加するには、次の手順を実行します。

1. **導入** → **導入ポータル** の順にクリックします。
   再利用ベアメタルデバイス タブが右のペインに表示されます。
2. 右側のペインで、 **自動導入** タブをクリックし **、検出範囲の追加**をクリックします。
   デバイスの検出 ウィザードが表示されます。
3. 検出とインベントリタスクの設定 の手順 2~5 の手順に従って、検出範囲を検出します。
   検出範囲は **検出とインベントリ** ポータルで作成されます。

関連リンク

デバイスの自動導入設定
自動導入

自動導入タスクからのデバイスの削除

特定のデバイスで自動導入を実行しない場合は、それらのデバイスを自動導入タスクから取り外すことができます。
自動導入タスクからデバイスを削除するには、次の手順を実行します。

1. **導入** → **導入ポータル** の順にクリックします。
   再利用ベアメタルデバイス タブが右のペインに表示されます。
2. 右側のペインで、 **自動導入** タブをクリックし、削除するデバイスを選択します。
3. 次のいずれかの手順を実行してください。
   - **選択したデバイスの削除**をクリックします。
   - 右クリックして **削除** を選択します。
4. 確認ダイアログボックスで、**はい** をクリックします。
   これらのデバイスが **自動導入** タブから削除されます。

関連リンク

自動導入

デバイス固有属性のインポート

デバイス固有属性を含む .csv ファイルが既にある場合は、それらの属性も導入用にインポートすることができます。
開始する前に、インポートする .csv ファイルがファイルのインポート要件で指定されている要件を満たしていることを確認してください。
属性をインポートするには、次の手順を実行します。

1. **テンプレートの導入ウィザード** または **自動導入のセットアップ** ウィザードの **属性の編集** ページで、**インポート / エクスポート** をクリックします。
   デバイス固有属性のインポート / エクスポート ウィンドウが表示されます。
2. **インポート** をクリックします。
   インポートの確認ダイアログボックスが表示されます。
3. **はい** をクリックします。
4. .csv ファイルに移動して選択し、**開く** をクリックします。
   インポート概要 ダイアログボックスに、インポートされた属性の数が表示されます。
5. **OK** をクリックします。
6. **デバイス固有属性のインポート / エクスポート** ウィンドウで、**閉じる** をクリックします。

関連リンク

ファイルのインポート要件

ファイルのインポート要件

次の表は、デバイス固有属性のインポートのために使用される .csv ファイルに含まれる列のタイトルとデータを説明しています。

フィールド	説明
デバイス名	デバイスの名前。デバイス名は、インポート中、導入用に選択されたデバイスの名前と一致させるために使用されます。
サービスタグ	デバイスのサービスタグ。自動導入タスク用にはサービスタグを指定する必要があります。導入タスクでは、デバイス名が指定されていればサービスタグはオプションになります。
親	属性の直接親の完全修飾記述子（FQDD）。親の値はインポート中の一致のために使用されます。
属性	設定属性の未処理名。名前はインポート中の一致のために使用されます。
値	属性の値。 **メモ:** 空の値も有効で、インポートされます。セキュアな値はマスクされた形式でエクスポートされます。インポートされたすべての値が導入対象として選択されます。

フィールド	説明
可能な値	許容値のリスト。 **メモ:** 許可されていない値、またはリストにない値を含めても値はインポートされません。

デバイス固有属性のエクスポート

デバイス固有属性は、.csv ファイルにエクスポートして属性を編集してから、それらの属性をインポートすることもできます。属性のエクスポートにより、代替方法を使用して属性を編集することができます。
属性をエクスポートするには、次の手順を実行します。

メモ: 特定のデバイスのみためにデバイス固有属性をエクスポートする場合は、**属性の編集** ページでデバイスを選択します。

1. **テンプレートの導入ウィザード** または **自動導入のセットアップ** ウィザードの **属性の編集** ページで、**インポート / エクスポート** をクリックします。
   デバイス固有属性のインポート / エクスポート ウィンドウが表示されます。
2. プリファランスに応じて **選択したデバイスのエクスポート** または **すべてのデバイスのエクスポート** をクリックします。
   すべてのデバイスのエクスポート を選択した場合は、確認ダイアログボックスが表示されます。
3. **はい** をクリックします。
4. .csv ファイルを保存する場所に移動して、**保存** をクリックします。

導入タスクの表示

作成済みの導入タスクを表示するには、次の手順を実行します。

1. **導入 → 導入ポータル** の順にクリックします。
2. 左側の **タスク** ペインでタスクの種類を選択します。
   右ペインの **タスク** タブに作成済みのタスクが表示されます。

関連リンク

タスク

追加情報

delltechcenter.com で取得できる次の Dell テクニカルホワイトペーパーおよびファイルは、デバイス設定テンプレート、属性、およびワークフローについての追加情報を提供します。

- *サーバー設定プロファイルでのサーバークローン*
- *サーバー設定 XML ファイル*
- *設定 XML ワークフロー*
- *設定 XML ワークフロースクリプト*
- *XML 設定ファイル例*

10

導入 - リファレンス

次の項目に **導入 → 導入ポータル** ページからアクセスできます。

- デバイス設定の導入ポータル
  - 導入を開始する前に — デバイス設定導入機能のセットアップ、使用、および開始に必要な情報を表示します。
  - 導入ポータル — **導入ポータル** のデフォルトビューを表示します。
- 一般タスク — 導入セットアップタスク、および作成可能なタスクを表示します。
  - テンプレートの作成
  - テンプレートの導入
  - 自動導入のセットアップ
  - 自動導入資格情報の管理
  - ファイル共有の設定
- テンプレート - サンプルのデバイス設定テンプレート、および作成またはクローンしたテンプレートを表示します。
  - サーバーテンプレート
    * 例 - iDRAC SNMP 管理設定
    * 例 - iDRAC 自動アップデート設定
    * 例 - Broadcom パーティションの有効化
    * 例 - BIOS セットアップシステムパスワード
    * 例 - iDRAC 静的 IP アドレス
    * 例 - iDRAC システムの場所
    * 例 - iDRAC 熱アラート監視
    * 例 - iDRAC タイムゾーン NTP
    * 例 - iDRAC ユーザーの設定
    * 例 - iDRAC 初期化済み仮想ディスク
    * 例 - 仮想ディスクの起動ディスクとしての設定
    * 例 - BIOS システムセットアップパスワードの削除
    * 例 - PXE 起動の有効化
    * 例 - ワンタイム BIOS 起動デバイス
    * 例 - ワンタイム HD 起動デバイス
    * 例 - ワンタイム UEFI 起動デバイス

    * 例 - BIOS 起動順序の設定
    * 例 - HD 起動順序の設定
    * 例 - iDRAC 電力上限の設定
    * 例 - UEFI 起動順序の設定
    * 例 - SNMP E-メールアラートの設定
  – シャーシテンプレート
    * 例 - VRTX シャーシ
    * 例 - M1000e シャーシ
- タスク — 右側のペインの **タスク** タブに、選択したカテゴリのタスクを表示します。
  – 設定タスク
    * 未検出デバイスの導入 — 作成した **自動導入タスク** を表示します。
    * デバイス設定イメージ導入 — 作成した **ネットワーク ISO からの起動** タスクを表示します。
    * シャーシ設定導入 — シャーシ用に作成したデバイス設定導入タスクを表示します。
    * シャーシ設定インポート — シャーシ用に作成した **テンプレートの作成** タスクを表示します。
    * デバイス設定導入 — サーバー用に作成したデバイス設定導入タスクを表示します。
    * デバイス設定インポート — サーバー用に作成した **テンプレートの作成** タスクを表示します。

メモ: サンプルのデバイス設定テンプレートについての情報は、**dell.com/support/manuals** で iDRAC マニュアルを参照してください。

関連リンク

再利用およびベアメタルデバイス
自動導入
タスク
タスクの実行履歴
デバイス設定テンプレートの詳細
デバイス設定セットアップウィザード
テンプレートの作成ウィザード
テンプレートの導入ウィザード
自動導入のセットアップウィザード
自動導入資格情報の管理

再利用およびベアメタルデバイス

再利用およびベアメタルデバイス タブには、**再利用およびベアメタルデバイス** グループに追加したデバイスが表示されます。このタブには、最後の導入結果とデバイスに導入された最後のテンプレートも表示されます。

再利用およびベアメタルデバイス タブに表示されるフィールドは、次の表に記載されています。

フィールド	説明
前回の導入結果	前回行った導入タスクの結果を表示します。
デバイス名	デバイス名を表示します。
サービスタグ	システムに割り当てられた固有の識別子を表示します。
モデル	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
前回導入されたテンプレート	前回導入されたテンプレートを表示します。
終了時刻	前回のテンプレートが導入された日付および時刻を表示します。
デバイスの変更	**すべての該当デバイス** ツリービューを表示します。**再利用およびベアメタルデバイス** グループに対して追加または削除を行うデバイスを選択またはクリアします。
選択したデバイスの削除	**再利用およびベアメタルデバイス** グループから選択したデバイスを削除します。

関連リンク

再利用およびベアメタルデバイスグループからのデバイスの削除
再利用およびベアメタルデバイスグループへのデバイスの追加

自動導入

自動導入 タブには、自動導入タスク用に選択したターゲットデバイスが表示されます。

自動導入 タブに表示されるフィールドを、以下の表で説明します。

フィールド	説明
サービスタグまたはノード ID	システムに割り当てられた固有の識別子を表示します。
テンプレートの導入	デバイスで導入用に選択したテンプレートを表示します。
ネットワーク ISO からの起動	ネットワーク ISO イメージに対してサーバーを起動することを選択したかどうかを表示します。
作成日	自動導入タスクが作成された日付と時刻が表示されます。
作成者	タスクを作成したユーザーの名前を表示します。

フィールド	説明
検出範囲の追加	**検出範囲の構成** ウィザードが表示され、検出範囲を追加できます。
デバイスの追加	**自動導入のセットアップ** ウィザードを表示します。
選択したデバイスの削除	関連付けられた **自動導入のセットアップ** タスクから選択したデバイスを削除します。

関連リンク

自動導入検出範囲の追加
自動導入タスクからのデバイスの削除
デバイス設定自動導入のセットアップ

タスク

導入 ポータルの **タスク** タブに表示されるフィールドを次の表で説明します。

フィールド	説明
スケジュール	タスクのスケジュールが有効または無効かを表示します。
タスク名	タスクの名前を表示します。
種類	タスクの種類を表示します。
説明	タスクに関する簡単な説明が表示されます。
アップデート日	タスクがアップデートされた日付と時刻が表示されます。
アップデート者	タスクをアップデートしたユーザーの名前を表示します。
作成日	タスクが作成された日付と時刻が表示されます。
作成者	タスクを作成したユーザーの名前を表示します。

関連リンク

導入タスクの表示

タスクの実行履歴

タスクの実行履歴 タブにはタスクのステータスが表示されます。

タスク実行履歴 タブに表示されるフィールドは、次の表に記載されています。

フィールド	説明
状態	タスクの状態を示すアイコンを表示します。  – 実行中または保留中

フィールド	説明
	 - 完了  – 停止  – 失敗  – 警告
タスク名	タスクの名前を表示します。
開始時刻	タスクの開始時間を表示します。
% 完了	タスクの進捗状況の情報を表示します。
タスク状況	タスクの状態を表示します。 • 実行中 • 完了 • 停止 • 失敗 • 警告
終了時刻	タスクの終了時間を表示します。
ユーザーにより実行済み	タスクを実行したユーザーの名前を表示します。

デバイス設定テンプレートの詳細

導入 ポータルの **属性** ペインに表示されるフィールドは、次の表に記載されています。

フィールド	説明
元に戻す	設定テンプレートに加えられた変更を元に戻す場合はクリックします。
保存	設定テンプレートに加えられた変更を保存する場合はクリックします。
グループ化基準	グループとしての属性表示を選択した場合に表示されます。
合計	テンプレートの属性の合計数を表示します。
変更済み	変更した属性の数を表示します。
導入	これを選択して属性を導入します。属性を選択しない場合、属性値はターゲットデバイスに導入されず、ターゲットデバイスでは現在の値が維持されます。**導入** 列見出しのチェックボックスを選択することにより、テンプレートの全属性を選択できます。

フィールド	説明
変更済み	属性の値が変更されているかどうかが表示されます。
セクション	属性が属するコンポーネントが表示されます。たとえば、iDRAC、BIOS、NIC などです。
インスタンス	属性が属するコンポーネントのインスタンスが表示されます。
属性名	属性の名前を表示します。
値	属性の値を表示します。
依存関係	属性が他の属性に依存しているかどうかが表示されます。依存関係がある属性を編集するには、まず主要属性を設定する必要があります。
破壊的	属性の導入が、パフォーマンス、接続性、デバイス起動可能性などのデバイス設定に破壊的な変更をもたらす可能性があるかどうかを表示します。
グループ	属性が属するグループが表示されます。

関連リンク

デバイス設定テンプレート属性の表示

デバイス設定セットアップウィザード

デバイス設定セットアップウィザード は、設定導入およびコンプライアンスタスクを開始する手順をガイドします。

メモ: デバイス設定セットアップウィザード は、必要な情報が不足しているタスクを実行しようとする場合にのみ表示されます。

ファイル共有の設定

次の表に **ファイル共有の設定** ページの各フィールドが記載されています。

フィールド	説明
ドメイン\ユーザー名	OpenManage Essentials を実行しているサーバー上のファイル共有にアクセスするためのユーザー名。
パスワード	OpenManage Essentials を実行しているサーバー上のファイル共有にアクセスするためのパスワード。
ファイル共有の状態	導入ファイル共有設定の状態を示します。

再利用およびベアメタルデバイス グループへのデバイスの追加

メモ: 再利用およびベアメタルデバイスグループ へのデバイスの追加は、デバイス設定導入タスクのみに該当します。

メモ: 再利用およびベアメタルデバイスグループ に追加するサーバーには、*OpenManage Essentials — サーバー設定管理*ライセンスがインストールされている必要があります。

再利用およびベアメタルデバイス グループへのデバイスの追加ページには、**再利用およびベアメタルデバイスグループ** に追加できるサーバーおよびシャーシが表示されます。

テンプレートの作成ウィザード

下表に **テンプレートの作成ウィザード** に表示されるフィールドの情報を示します。

フィールド	説明
名前	設定テンプレートの名前を入力します。
ファイルから作成	既存ファイルから設定テンプレートを作成する場合に選択します。
デバイスから作成	参照サーバーまたはシャーシから設定テンプレートを作成する場合に選択します。
デバイスタイプ	設定テンプレートの作成元となるデバイスに基づいて、**シャーシ** または **サーバー** のいずれかを選択します。
すべての該当デバイス	設定テンプレートの作成元にすることができるデバイスが表示されます。
実行の資格情報	
ユーザー名	デバイスでタスクを実行するために必要なユーザー名を入力します。
パスワード	デバイスでタスクを実行するために必要なパスワードを入力します。

関連リンク

デバイス設定ファイルからのデバイス設定テンプレートの作成
リファレンスデバイスからのデバイス設定テンプレートの作成

テンプレートの導入ウィザード

テンプレートの導入ウィザード の指示に従うと、構成テンプレートおよび/またはネットワーク ISO イメージを導入する手順を実行できます。ウィザードに表示される手順は、選択した導入オプションによって異なる場合があります。ウィザードの各ページに表示されるフィールドは、次の項で説明されています。

関連リンク

名前および導入オプション
テンプレートの選択
デバイスの選択
ISO の場所の選択
属性の編集
スケジュールの設定

概要

名前および導入オプション

名前および導入オプション ページでは、タスクの名前を入力して、導入オプションを選択できます。

テンプレートの導入ウィザード の **名前および導入オプション** ページに表示されるフィールドを次の表で説明します。

フィールド	説明
名前	タスクの名前を入力します。
導入オプションの選択	
テンプレートの導入	選択して、デバイス設定テンプレートを導入します。
ネットワーク ISO からの起動	選択して、ネットワーク ISO イメージから起動します。

関連リンク

テンプレートの導入ウィザード

テンプレートの選択

テンプレートの選択 ページでは、ターゲットデバイスで導入するテンプレートを選択できます。

メモ: テンプレートの選択 ページは、**名前および導入オプション** または **導入オプション** ページで **テンプレートの導入** オプションを選択する場合にのみ表示されます。

次の表に **テンプレートの選択** ページの各フィールドが記載されています。

フィールド	説明
サーバーテンプレート	作成またはクローンしたサーバー設定テンプレートを表示します。
シャーシテンプレート **メモ: 名前および導入オプション** または **導入オプション** ページで **テンプレートの導入** と **ネットワーク ISO からの起動** の両方を選択すると、**シャーシテンプレート** オプションが無効になります。	作成またはクローンしたシャーシ設定テンプレートを表示します。

関連リンク

テンプレートの導入ウィザード

デバイスの選択

デバイスの選択 ページでは、導入するターゲットデバイスを選択できます。

デバイスの選択 ページには、ターゲットデバイスを含む **再利用およびベアメタルデバイス** ツリービューが表示されます。1 つ以上のターゲットデバイスを導入に選択できます。

関連リンク

テンプレートの導入ウィザード

ISO の場所の選択

ISO の場所の選択 ページで、ISO ファイルの詳細を指定できます。

メモ: ISO の場所の選択 ページは、**名前および導入オプション** または **導入オプション** ページで **ネットワーク ISO からの起動** オプションを選択する場合にのみ表示されます。

ISO の場所の選択 ページに表示されるフィールドを、以下の表で説明します。

フィールド	説明
ISO ファイル名	
ISO ファイル名	ISO ファイルの名前を指定します。
共有の場所	
共有 IP	ISO ファイルを使用できるネットワーク共有の IP アドレスを入力します。
共有名	ISO ファイルを使用できるネットワーク共有の名前を入力します。
共有の資格情報	
共有のユーザー名	ネットワーク共有にアクセスするために必要なユーザー名を入力します。
共有のパスワード	ネットワーク共有にアクセスするために必要なパスワードを指定します。

関連リンク

テンプレートの導入ウィザード

属性の編集

属性の編集 ページでは、選択した設定テンプレートの属性、およびデバイス固有の属性を編集することができます。

メモ: 属性の編集 ページは、**名前および導入オプション** または **導入オプション** ページで **テンプレートの導入** オプションを選択する場合にのみ表示されます。

テンプレート属性

属性の編集 ページの **テンプレート属性** タブに表示されるフィールドは、次の表に記載されています。

フィールド	説明
グループ化基準	グループとしての属性表示を選択した場合に表示されます。
合計	属性の合計数を表示します。
変更済み	変更した属性の数を表示します。
属性	選択したデバイス設定テンプレートの名前を表示します。

フィールド	説明
デバイス固有属性対象	次が表示されます： • 導入タスクの場合 — デバイス名、サービスタグ、およびデバイスモデル。 • 自動導入タスクの場合 — 後ほど検出されるデバイスのサービスタグ。
導入	これを選択して属性を導入します。属性を選択しない場合、属性値はターゲットデバイスに導入されず、ターゲットデバイスでは現在の値が維持されます。**導入** 列見出しのチェックボックスを選択することにより、テンプレートの全属性を選択できます。
変更済み	属性の値が変更されているかどうかが表示されます。
セクション	属性が属するコンポーネントが表示されます。たとえば、iDRAC、BIOS、NIC などです。
インスタンス	属性が属するコンポーネントのインスタンスが表示されます。
属性名	属性の名前を表示します。
値	属性の値を表示します。
依存関係	属性が他の属性に依存しているかどうかが表示されます。依存関係がある属性を編集するには、まず主要属性を設定する必要があります。
破壊的	属性の導入が、パフォーマンス、接続性、およびデバイスを起動させる能力を含む、デバイス設定に対する破壊的な変更を生じるす可能性があるかどうかを示します。
元に戻す	クリックして、設定テンプレートに加えられた変更を元に戻します。
保存	クリックして、設定テンプレートに加えられた変更を保存します。

デバイス固有属性

属性の編集 ページの **デバイス固有属性** タブに表示されるフィールドは、次の表に記載されています。

フィールド	説明
デバイスの選択	導入することを選択したデバイスが表示されます。デバイスを選択すると、そのデバイスに固有の属性が表示されます。
デバイス固有属性対象	選択したデバイスのモデル番号およびサービスタグを表示します。

フィールド	説明
グループ化基準	グループとしての属性表示を選択した場合に表示されます。
合計	属性の合計数を表示します。
変更済み	変更した属性の数を表示します。
導入	選択すると属性が導入されます。属性が選択されていない場合、ターゲットデバイスに属性が導入されず、ターゲットデバイスで現行値が維持されます。**導入** 列見出しのチェックボックスを選択することにより、テンプレートの全属性を選択できます。
変更済み	属性の値が変更されているかどうかが表示されます。
セクション	属性が属するコンポーネントが表示されます。たとえば、iDRAC、BIOS、NIC などです。
インスタンス	属性が属するコンポーネントのインスタンスが表示されます。
属性名	属性の名前を表示します。
値	属性の値を表示します。
依存関係	属性が他の属性に依存しているかどうかが表示されます。依存関係がある属性を編集するには、まず主要属性を設定する必要があります。
破壊的	属性の導入が、パフォーマンス、接続性、およびデバイスを起動させる能力を含む、デバイス設定に対する破壊的な変更を生じるす可能性があるかどうかを示します。
元に戻す	クリックして、設定テンプレートに加えられた変更を元に戻します。
保存	クリックして、設定テンプレートに加えられた変更を保存します。
インポート / エクスポート	**デバイス固有属性のインポート / エクスポート** ウィンドウが表示されます。

次の表に **デバイス固有属性のインポート / エクスポート** ページの各フィールドが記載されています。

フィールド	説明
選択したデバイスのエクスポート	クリックすると、選択したデバイスのデバイス固有の属性が **.csv** ファイルにエクスポートされます。
すべてのデバイスのエクスポート	クリックすると、すべてのデバイスのデバイス固有の属性が **.csv** ファイルにエクスポートされます。

フィールド	説明
インポート	クリックすると、デバイス固有の属性がインポートされます。
ファイル要件および情報	デバイス固有の属性をインポートするために必要な **.csv** ファイルの要件が表示されます。
ログの表示	ユーザーインターフェイスログを表示します。
閉じる	クリックすると、**デバイス固有属性のインポート / エクスポート** ウィンドウが表示されます。

関連リンク

テンプレートの導入ウィザード
デバイス固有属性のインポート
デバイス固有属性のエクスポート

スケジュールの設定

スケジュールの設定 ページでは、タスクを導入する日付と時刻を設定できます。

次の表に **スケジュールの設定** ページの各フィールドが記載されています。

フィールド	説明
今すぐ実行	これを選択すると、導入タスクがすぐに実行されます。
実行時刻	これを選択すると、導入タスクがスケジュールされます。
実行の資格情報	
ユーザー名	タスクを実行するのに必要なユーザー名を入力します。
パスワード	タスクを実行するのに必要なパスワードを入力します。

関連リンク

テンプレートの導入ウィザード

概要

概要 ページには、導入タスク用に選択したオプションが表示されます。

次の表に **概要** ページの各フィールドが記載されています。

フィールド	説明
名前	タスク名を表示します。
テンプレートの導入	タスクが構成テンプレートを導入するかどうかを表示します。

フィールド	説明
ネットワーク ISO への起動	タスクがネットワーク ISO イメージを起動するかどうかを表示します。
選択したテンプレート	導入用に選択した構成テンプレートを表示します。
デバイス固有の属性	デバイス固有属性が設定されているかどうかが表示されます。
ISO ファイル名	ISO ファイルの名前を表示します。
共有 IP	ISO ファイルが利用可能なネットワーク共有の IP アドレスを表示します。
共有名	ISO ファイルが利用可能なネットワーク共有の名前を表示します。
ユーザー名の共有	ネットワーク共有にアクセスするために入力されたユーザー名を表示します。
関連するデバイス	選択したターゲットデバイスを表示します。
スケジュール	タスクに選択されたスケジュールを表示します。

関連リンク

テンプレートの導入ウィザード

自動導入のセットアップウィザード

自動導入のセットアップ ウィザードの指示に従うと、後に検出するターゲットデバイスで構成テンプレートを導入したり、さらに/またはネットワーク ISO イメージを起動する手順を実行できます。ウィザードに表示される手順は、選択した導入オプションによって異なる場合があります。ウィザードの各ページに表示されるフィールドは、次の項で説明されています。

関連リンク

導入オプション
テンプレートの選択
ISO の場所の選択
サービスタグ / ノード ID のインポート
属性の編集
実行の資格情報
概要

導入オプション

導入オプション ページでは、導入オプションを選択することができます。

自動導入のセットアップ ウィザードの **導入オプション** ページに表示されるフィールドを次の表で説明します。

フィールド	説明
テンプレートの導入	選択して、デバイス設定テンプレートを導入します。
ネットワーク ISO からの起動	選択して、ネットワーク ISO イメージから起動します。

テンプレートの選択

テンプレートの選択 ページでは、ターゲットデバイスで導入するテンプレートを選択できます。

メモ: テンプレートの選択 ページは、**名前および導入オプション** または **導入オプション** ページで **テンプレートの導入** オプションを選択する場合にのみ表示されます。

次の表に **テンプレートの選択** ページの各フィールドが記載されています。

フィールド	説明
サーバーテンプレート	作成またはクローンしたサーバー設定テンプレートを表示します。
シャーシテンプレート **メモ: 名前および導入オプション** または **導入オプション** ページで **テンプレートの導入** と **ネットワーク ISO からの起動** の両方を選択すると、**シャーシテンプレート** オプションが無効になります。	作成またはクローンしたシャーシ設定テンプレートを表示します。

関連リンク

テンプレートの導入ウィザード

ISO の場所の選択

ISO の場所の選択 ページで、ISO ファイルの詳細を指定できます。

メモ: ISO の場所の選択 ページは、**名前および導入オプション** または **導入オプション** ページで **ネットワーク ISO からの起動** オプションを選択する場合にのみ表示されます。

ISO の場所の選択 ページに表示されるフィールドを、以下の表で説明します。

フィールド	説明
ISO ファイル名	
ISO ファイル名	ISO ファイルの名前を指定します。
共有の場所	
共有 IP	ISO ファイルを使用できるネットワーク共有の IP アドレスを入力します。
共有名	ISO ファイルを使用できるネットワーク共有の名前を入力します。
共有の資格情報	

フィールド	説明
共有のユーザー名	ネットワーク共有にアクセスするために必要なユーザー名を入力します。
共有のパスワード	ネットワーク共有にアクセスするために必要なパスワードを指定します。

関連リンク

テンプレートの導入ウィザード

サービスタグ / ノード ID のインポート

自動導入のセットアップ ウィザードの **サービスタグ / ノード ID のインポート** ページに **インポート** ボタンが表示されます。**インポート** をクリックして、後ほど検出するデバイスのサービスタグまたはノード ID が含まれる **.csv** ファイルをインポートします。

メモ: ノード ID は、複数の計算ノードで構成されているデバイスの識別子です。例えば、PowerEdge FM120x4 スレッドには、4 台の計算ノードがあります。 .csv ファイルでは、自動展開したい特定の計算ノードのノード ID を含める必要があります。

メモ: インポートするサービスタグまたはノード ID は、次の条件を満たす必要があります。

- 「サービスタグ」「サービスタグ」、「ノード ID」というタイトルの列にある .csv ファイルにリストされている。
- 有効なノード ID またはサービスタグである。
- 既に検出されているデバイスのサービスタグまたはノード ID ではない。

次の例は、サービスタグおよびノード ID を含む **.csv** ファイル形式の例です。

	A
1	Service Tag
2	ABCD123
3	1DSZF23
4	HY3912B
5	GFEDCBAa
6	GFEDCBAb
7	GFEDCBAc
8	GFEDCBAd

図 5. サンプル CSV ファイル

属性の編集

属性の編集 ページでは、選択した設定テンプレートの属性、およびデバイス固有の属性を編集することができます。

メモ: 属性の編集 ページは、**名前および導入オプション** または **導入オプション** ページで **テンプレートの導入** オプションを選択する場合にのみ表示されます。

テンプレート属性

属性の編集 ページの **テンプレート属性** タブに表示されるフィールドは、次の表に記載されています。

フィールド	説明
グループ化基準	グループとしての属性表示を選択した場合に表示されます。
合計	属性の合計数を表示します。
変更済み	変更した属性の数を表示します。
属性	選択したデバイス設定テンプレートの名前を表示します。
デバイス固有属性対象	次が表示されます： • 導入タスクの場合 — デバイス名、サービスタグ、およびデバイスモデル。 • 自動導入タスクの場合 — 後ほど検出されるデバイスのサービスタグ。
導入	これを選択して属性を導入します。属性を選択しない場合、属性値はターゲットデバイスに導入されず、ターゲットデバイスでは現在の値が維持されます。**導入** 列見出しのチェックボックスを選択することにより、テンプレートの全属性を選択できます。
変更済み	属性の値が変更されているかどうかが表示されます。
セクション	属性が属するコンポーネントが表示されます。たとえば、iDRAC、BIOS、NIC などです。
インスタンス	属性が属するコンポーネントのインスタンスが表示されます。
属性名	属性の名前を表示します。
値	属性の値を表示します。
依存関係	属性が他の属性に依存しているかどうかが表示されます。依存関係がある属性を編集するには、まず主要属性を設定する必要があります。
破壊的	属性の導入が、パフォーマンス、接続性、およびデバイスを起動させる能力を含む、デバイス設定に対する破壊的な変更を生じるす可能性があるかどうかを示します。
元に戻す	クリックして、設定テンプレートに加えられた変更を元に戻します。
保存	クリックして、設定テンプレートに加えられた変更を保存します。

デバイス固有属性

属性の編集 ページの **デバイス固有属性** タブに表示されるフィールドは、次の表に記載されています。

フィールド	説明
デバイスの選択	導入することを選択したデバイスが表示されます。デバイスを選択すると、そのデバイスに固有の属性が表示されます。
デバイス固有属性対象	選択したデバイスのモデル番号およびサービスタグを表示します。
グループ化基準	グループとしての属性表示を選択した場合に表示されます。
合計	属性の合計数を表示します。
変更済み	変更した属性の数を表示します。
導入	選択すると属性が導入されます。属性が選択されていない場合、ターゲットデバイスに属性が導入されず、ターゲットデバイスで現行値が維持されます。**導入** 列見出しのチェックボックスを選択することにより、テンプレートの全属性を選択できます。
変更済み	属性の値が変更されているかどうかが表示されます。
セクション	属性が属するコンポーネントが表示されます。たとえば、iDRAC、BIOS、NIC などです。
インスタンス	属性が属するコンポーネントのインスタンスが表示されます。
属性名	属性の名前を表示します。
値	属性の値を表示します。
依存関係	属性が他の属性に依存しているかどうかが表示されます。依存関係がある属性を編集するには、まず主要属性を設定する必要があります。
破壊的	属性の導入が、パフォーマンス、接続性、およびデバイスを起動させる能力を含む、デバイス設定に対する破壊的な変更を生じるす可能性があるかどうかを示します。
元に戻す	クリックして、設定テンプレートに加えられた変更を元に戻します。
保存	クリックして、設定テンプレートに加えられた変更を保存します。
インポート / エクスポート	**デバイス固有属性のインポート / エクスポート** ウィンドウが表示されます。

次の表に **デバイス固有属性のインポート / エクスポート** ページの各フィールドが記載されています。

フィールド	説明
選択したデバイスのエクスポート	クリックすると、選択したデバイスのデバイス固有の属性が **.csv** ファイルにエクスポートされます。
すべてのデバイスのエクスポート	クリックすると、すべてのデバイスのデバイス固有の属性が **.csv** ファイルにエクスポートされます。
インポート	クリックすると、デバイス固有の属性がインポートされます。
ファイル要件および情報	デバイス固有の属性をインポートするために必要な **.csv** ファイルの要件が表示されます。
ログの表示	ユーザーインターフェイスログを表示します。
閉じる	クリックすると、**デバイス固有属性のインポート / エクスポート** ウィンドウが表示されます。

関連リンク

テンプレートの導入ウィザード
デバイス固有属性のインポート
デバイス固有属性のエクスポート

実行の資格情報

実行の資格情報 ページでは、ターゲットデバイスで自動導入タスクを実行するのに必要な資格情報を追加および/または割り当てることができます。**自動導入のセットアップ** ウィザードの **実行の資格情報** ページに表示されるフィールドは、次の項で説明します。

資格情報

資格情報 セクションには、後に検出するターゲットデバイスに構成した資格情報を含む表が表示されます。資格情報の表に表示されるフィールドは次の通りです。

フィールド	説明
新しい資格情報の追加	クリックすると、**資格情報の入力**ウィンドウが開き、ターゲットデバイスに資格情報を入力できます。
説明	資格情報に入力された説明を表示します。
ユーザー名	ユーザー名を表示します。
パスワード	マスクされたフォーマットでパスワードを表示します。
デフォルトです	選択可能なチェックボックスを表示し、新しいターゲットデバイスに資格情報を関連付けることができます。
アップデート	クリックすると資格情報を編集できるアイコンが表示されます。
削除	クリックすると資格情報を削除できるアイコンが表示されます。

デバイス

デバイス セクションには、**サービスタグのインポート** ページで選択したターゲットデバイスを含む表が表示されます。デバイスの表に表示されるフィールドは次の通りです。

フィールド	説明
デバイス名	デバイスのサービスタグを表示します
デバイスモデル	システムのモデル名を表示します（該当する場合）。
実行の資格情報	導入タスクを実行するためにデバイスに割り当てられている資格情報が表示されます。

関連リンク

資格情報の追加

資格情報の追加

資格情報の入力 ウィンドウでは、ターゲットデバイスでの自動導入タスク実行に必要な資格情報を入力できます。

次の表に **資格情報の入力** ウィンドウの各フィールドが記載されています。

フィールド	説明
説明	資格情報の説明を入力します。
ユーザー名	ターゲットデバイスでタスクを実行するのに必要なユーザー名を入力します。
パスワード	ターゲットデバイスでタスクを実行するのに必要なパスワードを入力します。
デフォルト	選択すると、新しいターゲットデバイスに資格情報を関連付けることができます。

概要

概要 ページには、自動導入タスク用に選択したオプションが表示されます。

次の表に **概要** ページの各フィールドが記載されています。

フィールド	説明
名前	タスク名を表示します。
テンプレートの導入	タスクが構成テンプレートを導入するかどうかを表示します。
ネットワーク ISO への起動	タスクがネットワーク ISO イメージを起動するかどうかを表示します。
選択したテンプレート	導入用に選択した構成テンプレートを表示します。
ISO ファイル名	ISO ファイルの名前を表示します。

フィールド	説明
共有 IP	ISO ファイルが利用可能なネットワーク共有の IP アドレスを表示します。
共有名	ISO ファイルが利用可能なネットワーク共有の名前を表示します。
ユーザー名の共有	ネットワーク共有にアクセスするために入力されたユーザー名を表示します。
関連付けられたサービスタグ	ターゲットデバイスのサービスタグを表示します。
デバイス固有の属性	デバイス固有属性が設定されているかどうかが表示されます。

自動導入資格情報の管理

自動導入資格情報の管理 ページでは、ターゲットデバイスで自動導入タスクを実行するのに必要な資格情報を追加および/または割り当てることができます。**自動導入資格情報の管理** ページに表示されるフィールドは、次の項で説明します。

資格情報

資格情報 セクションには、自動導入タスクに構成した資格情報を含む表が表示されます。資格情報の表に表示されるフィールドは次の通りです。

フィールド	説明
新しい資格情報の追加	クリックすると、**資格情報の入力**ウィンドウが開き、ターゲットデバイスに資格情報を入力できます。
説明	資格情報に入力された説明を表示します。
ユーザー名	ユーザー名を表示します。
パスワード	マスクされたフォーマットでパスワードを表示します。
デフォルトです	選択可能なチェックボックスを表示し、新しいターゲットデバイスに資格情報を関連付けることができます。
アップデート	クリックすると資格情報を編集できるアイコンが表示されます。
削除	クリックすると資格情報を削除できるアイコンが表示されます。

デバイス

デバイス セクションには、**自動導入のセットアップ**ウィザードの**サービスタグのインポート** ページで選択したターゲットデバイスを含む表が表示されます。デバイスの表に表示されるフィールドは次の通りです。

フィールド	説明
デバイス名	デバイスのサービスタグを表示します
デバイスモデル	システムのモデル名を表示します（該当する場合）。
実行の資格情報	導入タスクを実行するためにデバイスに割り当てられている資格情報が表示されます。このフィールドを使って、自動導入タスクを実行するために必要な資格情報を割り当てることができます。

関連リンク

自動導入資格情報の管理

11

サーバー設定ベースラインの管理

実働環境内のサーバーまたはシャーシ設定は、サーバーの可用性を確保するために適切に維持される必要があります。これらのサーバー設定設定は、さまざまな理由により、次第にベースラインから外れてしまう傾向にあります。**デバイスコンプライアンスポータル** では、ベースラインとして機能するデバイス設定テンプレートに対する複数のサーバーおよびシャーシのコンプライアンスを検証して確認することができます。コンプライアンス状態は、現在の設定設定とそれに対応するベースライン設定テンプレートの間に違いがあるかどうかを示します。また、**デバイスコンプライアンスポータル** では、ベースラインテンプレートを作成し、複数の実稼働サーバーに希望のテンプレートを割り当ててベースラインを確立することができます。

メモ: デバイスに関連するテンプレートで定義されたすべての設定と一致する場合、デバイスは順守（コンプライアンス）の状態にあるとみなされます。追加のハードウェア（例：追加の NIC カードなど）があるデバイスも順守の状態にあるとされます。デバイスインベントリまたは関連するテンプレートに変更がある場合に、デバイスは非順守の状態になることがあります。関連するテンプレートが変更された場合は、そのテンプレートを関連するデバイスに再導入する必要があります。

デバイスコンプライアンスポータル を使用することにより、次の操作が可能になります。

- サーバーまたはシャーシ設定ファイルからの設定テンプレートの作成
- サーバーまたはシャーシからの設定テンプレートの作成
- 設定テンプレートの編集
- サーバーまたはシャーシへの設定テンプレートの関連付け
- ターゲットデバイスのデバイス設定インベントリのスケジュールと資格情報の設定
- 作成済みのタスクとその状態の表示
- ファイル共有導入の設定

メモ: *デバイス設定導入*および*設定コンプライアンス*機能は、対応サーバー（iDRAC 装備の PowerEdge 12G 以上）に対してライセンス付与（有料）されています。ただし、対応 Dell シャーシ上でのこれらの機能の使用は無料で、ライセンスは必要ありません。サーバーまたはシャーシからのデバイス設定テンプレートの作成にもライセンスは不要です。詳細については、OpenManage Essentials — サーバー設定管理ライセンスを参照してください。

関連リンク

導入ファイル共有の設定
デバイス設定テンプレートの作成
資格情報およびデバイス設定インベントリスケジュールの設定
設定テンプレートへのターゲットデバイスの関連付け
デバイスのコンプライアンス状態の表示
コンプライアンスタスクの表示
追加情報

デバイスコンプライアンスポータルの表示

デバイスコンプライアンスポータルを表示するには、**管理 → 設定 → デバイスコンプライアンスポータル** の順にクリックします。

デバイス設定コンプライアンス入門

デバイス設定テンプレートへのデバイスのコンプライアンス状態を確認する前に、次の手順を実行する必要があります。

1. OpenManage Essentials を実行しているサーバー上で導入ファイル共有を設定します。
2. ターゲットデバイスの資格情報およびインベントリのスケジュールを設定します。

関連リンク

導入ファイル共有の設定
資格情報およびデバイス設定インベントリスケジュールの設定
デバイス設定コンプライアンスの概要

デバイス設定コンプライアンスの概要

デバイスのコンプライアンス状態の確認、またはデバイスをデバイス設定テンプレートに順守させるのに必要な手順は次の通りです。

1. **デバイス設定テンプレートの作成** – **共通タスク** ペインの **テンプレートの作成** タスクを使用してデバイス設定テンプレートを作成します。設定ファイルまたはリファレンスデバイスから選んでテンプレートを作成することができます。
2. **デバイス設定テンプレートのターゲットデバイスへの関連付け** – テンプレートを選択し、そのテンプレートを該当するデバイスに関連付けてコンプライアンスの状態を表示します。
3. **コンプライアンス状態の表示** – **デバイスコンプライアンスポータル** には、テンプレートに関連付けられたすべてのデバイスのコンプライアンスのサマリが表示されます。デバイスとそれに関連づけられたテンプレートのコンプライアンス状態を表示するには、**テンプレート** ペインでテンプレートを選択します。各デバイスの詳細なコンプライアンス状態を表示するには、**デバイスコンプライアンス** のグラフまたは表をダブルクリックします。またはデバイスツリーでデバイスを選択して（**管理 → デバイス**）、右ペインで **設定** タブをクリックしてコンプライアンスステータスを表示します。
4. **関連するデバイス設定テンプレートにデバイスを適合させる（オプション）** – デバイスを関連するデバイス設定テンプレートに適合させるには、**導入ポータル** 経由でデバイス設定テンプレートを導入する必要があります。

関連リンク

デバイス設定コンプライアンス入門

資格情報およびデバイス設定インベントリスケジュールの設定

設定インベントリのスケジュール タスクでは、定期的に該当するデバイスからデバイス設定属性のインベントリを収集できます。インベントリ情報は、特定のデバイス設定テンプレートへのデバイスのコンプライアンス状態を確認するために使用されます。
デバイスインベントリのスケジュールを設定する前に、次を確認します。

- ターゲットデバイスが 導入およびコンプライアンスタスクのデバイス要件を満たしている。
- *OpenManage Essentials — サーバー設定管理*ライセンスがすべてのターゲットサーバーにインストールされている。詳細に関しては、OpenManage Essentials — サーバー設定管理ライセンスを参照してください。

デバイス設定インベントリのスケジュールを設定するには、次の手順を実行します。

1. **管理** → **設定** の順にクリックします。
2. 次のいずれかの手順を実行してください。
   - **共通タスク** ペインで、**設定インベントリのスケジュール** をクリックします。
   - **デバイス設定コンプライアンスポータル** ペインで、**コンプライアンスを開始する前に** → **ターゲットデバイスの資格情報とインベントリのスケジュールを設定する** の順にクリックします。

   設定インベントリのスケジュール ウィザードが表示されます。
3. **インベントリ資格情報** ページで次の手順を実行します。
   a. **新しい資格情報の追加**）をクリックします。
   資格情報の追加 ウィンドウが表示されます。
   b. 内容、ユーザー名、パスワードを入力します。

   メモ: システム管理者またはオペレーターの権限のいずれかがある iDRAC 資格情報を入力する必要があります。
   c. 資格情報を新しいターゲットデバイスすべてのデフォルト資格情報として設定したい場合は、**デフォルト** を選択して **終了** をクリックします。
   d. **デバイス** の項で、各ターゲットデバイス用の **実行の資格情報** を設定します。
   e. **次へ** をクリックします。
4. **スケジュール** ページで次の手順を実行します。
   a. **設定インベントリを有効にする** を選択します。
   b. 設定インベントリを今すぐ実行したい場合は、**終了時にインベントリを実行する** を選択します。
   c. 希望のスケジュールパラメータを選択します。
   d. （オプション） より高速なタスク実行のために **インベントリポーリング速度** スライダを調整することができますが、より多くのシステムリソースを消費することになります。
   e. **終了** をクリックします。

タスクのステータスが **タスク実行履歴** に表示されます。**タスク実行履歴** 内のタスクをダブルクリックして、タスク実行の詳細を表示することができます。

関連リンク

OpenManage Essentials — サーバー設定管理ライセンス
導入およびコンプライアンスタスクのデバイス要件
設定インベントリスケジュールウィザード

設定テンプレートへのターゲットデバイスの関連付け

テンプレートへのデバイスの関連付け タスクでは、ターゲットデバイスのコンプライアンス状態の確認に使用するテンプレートを指定することができます。

メモ: デバイスが所有できる関連付けられたデバイス設定テンプレートは 1 つのみです。2 つ目のテンプレートをデバイスに関連付けると、2 つ目のテンプレートがデバイスに関連付けられた唯一の設定テンプレートになります。

ターゲットデバイスをテンプレートに関連付けるには、次の手順を実行します。

1. **管理** → **設定** の順にクリックします。
2. 次のいずれかの手順を実行してください。
   - **共通タスク** ペインで、**デバイスをテンプレートに関連付ける** をクリックします。
   - **デバイス設定コンプライアンスポータル** ペインで **コンプライアンスを開始する前に** → **ターゲットデバイスへのテンプレートの関連付け** の順にクリックします。

   テンプレートへの関連付け ウィザードが表示されます。
3. **テンプレートの選択** ページで次の手順を実行します。
   a. ターゲットデバイスタイプに基づいて、**サーバーテンプレート** または **シャーシテンプレート** のいずれかをクリックしてテンプレートを選択してください。

      メモ: 作成済みまたはクローン化が完了している設定テンプレートのみを選択することができます。
   b. リストからデバイス設定テンプレートを選択します。
   c. **次へ** をクリックします。
4. **デバイスの選択** ページで、**該当するすべてのデバイス** ツリーからターゲットデバイスを選択してから **終了** をクリックします。

関連リンク

テンプレートの関連付け
テンプレートへのデバイスの関連付けウィザード

インベントリ構成詳細の表示

デバイスのインベントリ構成詳細は、 **デバイス** ポータルで見ることができます。
開始する前に、インベントリ構成詳細を表示するデバイスが導入とコンプライアンスタスクのデバイス要件で指定された要件を満たす必要があります。
インベントリ構成詳細を表示するには、次の手順を実行します。

1. **デバイス**をクリックします。
   デバイス ポータルが表示されます。
2. デバイスツリーで、インベントリ構成詳細を表示したいデバイスを選択します。
3. 右ペインで、**インベントリ** をクリックします。
   インベントリ構成詳細が表示されます。その場合、デバイスにインベントリ構成タスクが実行されていない場合、**インベントリ構成の実行**ボタンが表示されます。 **インベントリ構成の実行**ボタンをクリックすると、**インベントリ構成スケジュール**でデバイスの資格情報を設定していれば、構成詳細が表示されます。

関連リンク

導入およびコンプライアンスタスクのデバイス要件

デバイスのコンプライアンス状態の表示

関連付けられた構成テンプレートに対するデバイスのコンプライアンスステータスを表示する前に、デバイス構成インベントリタスクを実行する必要があります。デバイス構成インベントリタスクを実行するには、インベントリ構成スケジュールを作成するか、またはデバイスツリーでデバイスを選択して、右側ペインの **構成** タブで **設定インベントリの実行** をクリックします。

デバイスと関連する設定テンプレートのコンプライアンス状態を表示するには、次の手順を実行します。

1. **管理** → **設定** → **デバイスコンプライアンスポータル** の順にクリックします。
   デバイスのコンプライアンス のグラフとグリッドにデバイスのコンプライアンス状態が表示されます。
2. コンプライアンス状態ごとにデバイスを表示するには、**デバイスのコンプライアンス** のグラフをクリックします。
3. 特定のデバイスのコンプライアンス状態を表示するには、**デバイスのコンプライアンス** のグリッドでデバイスをクリックします。

メモ: また、デバイスツリーにあるデバイスを選択し（**管理** → **デバイス**）、右側のペインで **構成** タブをクリックしても、コンプライアンスステータスが表示されます。

コンプライアンスタスクの表示

作成済みのコンプライアンスタスクを表示するには、次の手順を実行します。

1. **管理** → **設定** をクリックします。
2. 左側の **タスク** ペインでタスクの種類を選択します。
   右ペインの **タスク** タブに作成済みのタスクが表示されます。

関連リンク

タスク

12

設定 - リファレンス

次の項目に **管理 → 設定** ページからアクセスできます。

- デバイス設定コンプライアンスポータル
  - コンプライアンスを開始する前に — デバイス設定コンプライアンス機能のセットアップ、使用、および開始に必要な情報を表示します。
  - デバイスコンプライアンスポータル — **デバイスコンプライアンスポータル**のデフォルトビューを表示します。
- 一般タスク — 設定コンプライアンスのセットアップタスク、および作成可能なタスクを表示します。
  - テンプレートの作成
  - テンプレートへのデバイスの関連付け
  - 設定インベントリスケジュール
  - ファイル共有の設定
- テンプレートごとのコンプライアンス - サンプルのデバイス設定テンプレート、および作成またはクローンしたテンプレートを表示します。
  - サーバーテンプレート
    * 例 - iDRAC SNMP 管理設定
    * 例 - iDRAC 自動アップデート設定
    * 例 - Broadcom パーティションの有効化
    * 例 - BIOS セットアップシステムパスワード
    * 例 - iDRAC 静的 IP アドレス
    * 例 - iDRAC システムの場所
    * 例 - iDRAC 熱アラート監視
    * 例 - iDRAC タイムゾーン NTP
    * 例 - iDRAC ユーザーの設定
    * 例 - iDRAC 初期化済み仮想ディスク
    * 例 - 仮想ディスクの起動ディスクとしての設定
    * 例 - BIOS システムセットアップパスワードの削除
    * 例 - PXE 起動の有効化
    * 例 - ワンタイム BIOS 起動デバイス
    * 例 - ワンタイム HD 起動デバイス
    * 例 - ワンタイム UEFI 起動デバイス

    * 例 - BIOS 起動順序の設定
    * 例 - HD 起動順序の設定
    * 例 - iDRAC 電力上限の設定
    * 例 - UEFI 起動順序の設定
    * 例 - SNMP E-メールアラートの設定
  – シャーシテンプレート
    * 例 - VRTX シャーシ
    * 例 - M1000e シャーシ
- タスク — 右側のペインの **タスク** タブに、選択したカテゴリのタスクを表示します。
  – 設定タスク
    * シャーシ設定導入 — シャーシ用に作成した **テンプレートの作成** タスクを表示します。
    * デバイス設定インポート — サーバー用に作成した **テンプレートの作成** タスクを表示します。

メモ: サンプルのデバイス設定テンプレートについての情報は、**dell.com/support/manuals** で iDRAC マニュアルを参照してください。

関連リンク

デバイスコンプライアンス
タスク
タスクの実行履歴
テンプレートへのデバイスの関連付けウィザード
設定インベントリスケジュールウィザード

デバイスコンプライアンス

デバイスのコンプライアンス のグラフと表では、デバイスのコンプライアンス状態を表示できます。

デバイスコンプライアンスのグラフ

デバイスコンプライアンスグラフは、コンプライアンスステータスの円グラフ分布を表示します。円グラフのセグメントをクリックして、システムについての詳細情報を表示します。円グラフには、デバイスコンプライアンスステータスを示す次のセグメントが表示されます。

- 適合 — 関連付けられている設定テンプレートに適合するデバイス。
- 非適合 — 関連付けられている設定テンプレートに適合していないデバイス。
- インベントリ未施行 — 設定インベントリが完了されていないデバイス。
- 関連付けなし — 設定テンプレートに関連付けられていないデバイス。
- ライセンスなし — *OpenManage Essentials* — *サーバー設定管理*ライセンスがインストールされていないデバイス。

デバイスコンプライアンスの表

デバイスコンプライアンス ポータルの **デバイスコンプライアンス** 表に表示されるフィールドは、次の表に記載されています。

フィールド	説明
コンプライアンス状態	関連する設定テンプレートに対するデバイスのコンプライアンス状態を示すアイコンを表示します。
デバイス名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
サービスタグ	システムに割り当てられた固有の識別子を表示します。
モデル	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
コンプライアンステンプレート	デバイスに関連付けられたデバイス設定テンプレートを表示します。
前回実行されたインベントリ	最後に行われたデバイス設定インベントリの日付と時間を表示します。

タスク

タスク タブには、作成されたすべてのタスクが表示されます。

デバイスコンプライアンスポータル の **タスク** タブに表示されるフィールドを次の表で説明します。

フィールド	説明
スケジュール	タスクのスケジュールが有効または無効かを表示します。
タスク名	タスクの名前を表示します。
種類	タスクの種類を表示します。
説明	タスクに関する簡単な説明が表示されます。
アップデート日	タスクがアップデートされた日付と時刻が表示されます。
アップデート者	タスクをアップデートしたユーザーの名前を表示します。
作成日	タスクが作成された日付と時刻が表示されます。
作成者	タスクを作成したユーザーの名前を表示します。

関連リンク

コンプライアンスタスクの表示

タスクの実行履歴

タスクの実行履歴 タブにはタスクのステータスが表示されます。

タスク実行履歴 タブに表示されるフィールドは、次の表に記載されています。

フィールド	説明
状態	タスクの状態を示すアイコンを表示します。  – 実行中または保留中  - 完了  – 停止  – 失敗  – 警告
タスク名	タスクの名前を表示します。
開始時刻	タスクの開始時間を表示します。
% 完了	タスクの進捗状況の情報を表示します。
タスク状況	タスクの状態を表示します。 • 実行中 • 完了 • 停止 • 失敗 • 警告
終了時刻	タスクの終了時間を表示します。
ユーザーにより実行済み	タスクを実行したユーザーの名前を表示します。

テンプレートへのデバイスの関連付けウィザード

テンプレートへのデバイスの関連付けウィザード では、デバイスをデバイス構成テンプレートに関連付けることができます。**テンプレートへのデバイスの関連付けウィザード**に表示されるフィールドは、次の項で説明します。

関連リンク

テンプレートの選択
デバイスの選択
設定テンプレートへのターゲットデバイスの関連付け

テンプレートの選択

テンプレートの選択 ページでは、ターゲットデバイスに関連付けるテンプレートを選択できます。

次の表に **テンプレートの選択** ページの各フィールドが記載されています。

フィールド	説明
サーバーテンプレート	作成またはクローンしたサーバー構成テンプレートを表示します。
シャーシのテンプレート	作成またはクローンしたシャーシ構成テンプレートを表示します。

デバイスの選択

デバイスの選択 ページでは、ターゲットデバイスを選択して構成コンプライアンスを検証できます。

デバイスの選択 ページには、ターゲットデバイスを含む **適用可能なすべてのデバイス** ツリービューが表示されます。1 つ以上のターゲットデバイスをデバイス構成テンプレートに関連付けることができます。

設定インベントリスケジュールウィザード

設定インベントリのスケジュール ウィザードでは、検出済みデバイスに資格情報を関連付け、構成インベントリのスケジュールを設定できます。ウィザードのページに表示されるフィールドは、次の項で説明されています。

関連リンク

- インベントリ資格情報
- スケジュール
- 資格情報およびデバイス設定インベントリスケジュールの設定

インベントリ資格情報

インベントリ資格情報 ページでは、ターゲットデバイスに資格情報を追加したり、関連付けたりすることができます。**インベントリ資格情報** ページに表示されるフィールドを、以下の表で説明します。

資格情報

資格情報 セクションには、構成インベントリタスクに構成した資格情報を含む表が表示されます。資格情報の表に表示されるフィールドは次の通りです。

フィールド	説明
新しい資格情報の追加	クリックすると、**資格情報の入力**ウィンドウが開き、ターゲットデバイスに資格情報を入力できます。
説明	資格情報に入力された説明を表示します。
ユーザー名	ユーザー名を表示します。
パスワード	マスクされたフォーマットでパスワードを表示します。
デフォルトです	選択可能なチェックボックスを表示し、新しいターゲットデバイスに資格情報を関連付けることができます。
アップデート	クリックすると資格情報を編集できるアイコンが表示されます。

フィールド	説明
削除	クリックすると資格情報を削除できるアイコンが表示されます。

デバイス

デバイス セクションには、構成インベントリタスクのターゲットデバイスを含む表が表示されます。デバイスの表に表示されるフィールドは次の通りです。

フィールド	説明
デバイス名	デバイスのサービスタグを表示します
デバイスモデル	システムのモデル名を表示します（該当する場合）。
実行の資格情報	構成インベントリタスクを実行するためにデバイスに割り当てられている資格情報が表示されます。このフィールドを使って、構成インベントリタスクを実行するために必要な資格情報を割り当てることができます。

スケジュール

スケジュール ページでは、構成インベントリについてスケジュールを設定することができます。

次の表に **スケジュール** ページの各フィールドが記載されています。

フィールド	説明
設定インベントリを有効にする	これを選択して、構成インベントリをスケジュールします。
終了時にインベントリを実行する	これを選択して、インベントリ構成が完了した後に構成インベントリを実行します。
グローバルインベントリポーリング間隔の設定	インベントリの頻度を毎週または毎日に設定します。 **メモ:** OpenManage Essentials は、すでに検出済みのデバイスに対しては構成インベントリのみを実行します。 • **毎週の曜日** — インベントリ をスケジュールする曜日（1 日または複数日）と、 インベントリ を開始する時刻を設定します。 • **<n> 日 <n> 時間ごと** — 検出サイクル間の間隔を指定します。最大検出間隔は 365 日 / 23 時間です。
インベントリポーリングの速度	インベントリポーリングの速度を速めるために使用できるリソース量を指定します。インベントリポーリングの速度を早くするほど、必要なリソース量が増えますが、インベントリの実行時間は短縮されます。

フィールド	説明
	速度の変更後、OpenManage Essentials が新しい速度に適応するまで数分かかる場合があります。

13

インベントリリポートの表示

OpenManage Essentials は、検出およびインベントリされたすべてのデバイスに事前定義されたレポートを提供します。これらのレポートを使用して、次のことができます。

- 環境内にあるデバイスについての情報を統合する
- **次によってフィルタ：** ドロップダウンリストをクリックすることにより、デバイスに基づいてレポートデータのフィルタします。また、**次によってフィルタ：** ドロップダウンリストから **新規グループの追加** をクリックすることにより、ダッシュボードからデバイスの新グループを追加することもできます。
- 別のアプリケーションで使用するデータは **XML** ファイルフォーマットでエクスポートします。

メモ: デフォルトでは、レポートはユーザーがレポートにアクセスする際に最新のデバイス情報を表示します。レポートが開いている状態で、レポートを操作していない場合は、更新ボタンを押してレポートで最新のデバイス情報を表示する必要があります。

メモ: 新しいレポートは作成できません。

事前定義されたレポートの選択

事前定義されたレポートを表示するには、**レポート** をクリックします。

管理下システムレポートには事前定義されたレポートが表示されます。表示されたレポートのいずれかを選択して、お使いの環境でのデバイスについての情報を表示します。**フィルタ基準:** ドロップダウンリストをクリックすることにより、デバイスに基づいてレポートをフィルタできます。**フィルタ基準:** ドロップダウンリストから**新規グループの追加**をクリックすることにより、新しいデバイスのグループを追加することもできます。

事前定義されたレポート

レポート	説明
エージェントおよびアラート概要	環境内のデバイスにインストールされている OpenManage Server Administrator バージョンを識別し、最も多くのアラートを生成しているデバイスを識別できます。Server Administrator がサーバーにインストールされていない場合は、**なし** が表示されます。 • 左上のウェブパーツで環境内にある OpenManage Server Administrator のバージョンが識別されます。 • 右上のウェブパーツで OpenManage Server Administrator の円グラフ内の OpenManage Server Administrator バージョンをクリックすると、そのバージョンがインストールされたサーバーのリストが表示されます。

レポート	説明
	• 左下のウェブパーツには、初回の検出とインベントリ以降のアラート生成数が多い順にデバイスが表示されます。 • イベント生成数上位 5 に入るデバイスは、右下のウェブパーツに表示されます。特定のデバイスをクリックして、そのデバイスに関連するイベントを表示します。
デバイスコンプライアンス	サーバーまたはシャーシのコンプライアンスに関する情報を、関連付けられたデバイス構成テンプレートに提供します。
サーバーの概要	システム名、サーバーにインストールされたオペレーティングシステム、プロセッサ、およびメモリなどのサーバーに関する情報を提供します。
サーバーコンポーネントとバージョン	検出およびインベントリが行われたすべてのサーバー上の BIOS、ドライバ、およびファームウェアバージョンを識別します。
資産取得情報	デバイスの取得情報を表示します。
資産メンテナンス情報	デバイスのメンテナンス情報を表示します。
資産サポート情報	デバイスのサポート情報を表示します。
ハードドライブ情報	ハードディスクドライブのシリアル番号、リビジョン、製造元および、バスタイプを特定します。
ESX 情報	ESX および ESXi 仮想マシンのホストと、それに関連する仮想マシンを識別します。
HyperV 情報	HyperV 仮想マシンのホストと、それに関連する仮想マシンを識別します。
FRU 情報	交換可能サーバーコンポーネントの詳細を示します。
ライセンス情報	デバイスに関するライセンス情報を表示します。
デバイス位置の情報	データセンター内のデバイスの位置に関する情報を提供します。
メモリ情報	DIMM に関する詳細を提供し、サーバー内で特定の DIMM が専有するスロットを特定します。
モジュラーエンクロージャ情報	エンクロージャの種類、ファームウェアバージョン、エンクロージャのサービスタグなどに関する情報を提供します。
NIC 情報	NIC モデルの IP アドレス、MAC アドレス、製造元とパーツ、NIC のシリアル番号を特定します。

レポート	説明
PCI デバイス情報	各サーバー内の PCI および PCIe コントローラのモデル、製造元および、スロットを特定します。
ストレージコントローラ情報	サーバー上のストレージコントローラを特定し、コントローラ名、ベンダー、コントローラタイプおよびコントローラの状態を特定します。 • **準備完了 :** ストレージコントローラの使用準備ができています。 • **劣化 :** コントローラに潜在的な問題があります。調査が必要です。
仮想ディスク情報	サイズ、レイアウト、ストライプサイズなどの仮想ディスクに関する情報を提供します。
保証情報	保証レポートの実行と、そのレポートが提供する情報の詳細については、「保証レポートの表示」を参照してください。
BIOS 設定	システムの BIOS 設定情報を提供します。
ライセンス情報	iDRAC の IPMI オーバー LAN、SSH、および Telnet のステータスを提供します。
テンプレートの関連付け	デバイス構成テンプレートおよびテンプレートに関連付けられたデバイスに関する情報を提供します。

レポートデータのフィルタリング

行のヘッダーをレポート上にドラッグ & ドロップして、結果をフィルタできます。表示を必要に応じて変更する場合、1 つ、または複数の属性を選択できます。

例えば、NIC 情報レポートでは、**システムの種類** および **システム名** をレポートの最上部にドラッグします。表示は、このプリファランスに基づいた表示内容に瞬時に変化します。この例では、NIC IP アドレス、MAC アドレス、および NIC の説明といった NIC の入れ子データを表示できます。

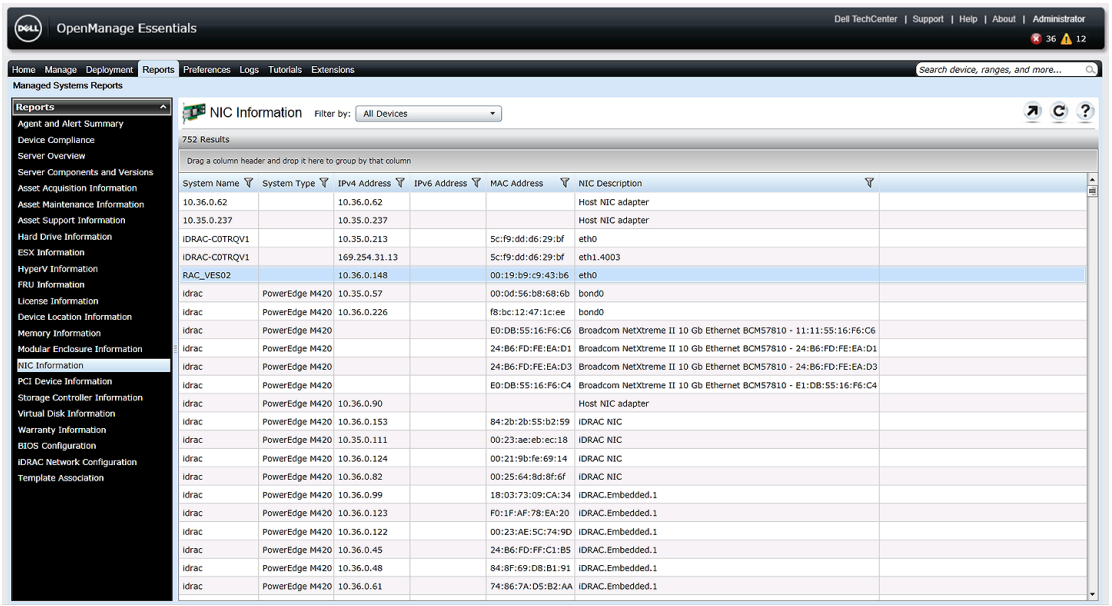


図 6. NIC 情報レポート

レポートのエクスポート

レポートのエクスポートでは、データの変更や再フォーマットが可能になります。レポートをエクスポートするには、次の手順を行います。

1. レポートリストで、任意のレポートを右クリックし、**エクスポート** オプションを表示します。
2. **エクスポート** オプションをスクロールして、対応フォーマットを表示します。
3. フォーマット（CSV、HTML、または XML）を選択して、エクスポートするレポートのファイル名を入力します。

14

レポート — リファレンス

レポートでは、次の内容を表示できます。

- エージェントおよびアラート概要
- デバイスコンプライアンス
- サーバーの概要
- サーバーコンポーネントとバージョン
- 資産取得情報
- 資産メンテナンス情報
- 資産サポート情報
- ハードドライブ情報
- ESX 情報
- HyperV 情報
- FRU 情報
- ライセンス情報
- デバイス位置の情報
- メモリ情報
- モジュラーエンクロージャ情報
- NIC 情報
- PCI デバイス情報
- ストレージコントローラ情報
- 仮想ディスク情報
- 保証情報
- BIOS 設定
- iDRAC ネットワーク設定
- テンプレートの関連付け

フィルタ基準 をクリックしてデバイスまたはグループを選択することにより、デバイスまたはグループに基づいて情報をフィルタリングすることもできます。

関連リンク

エージェントおよびアラート概要
デバイスコンプライアンス
サーバーの概要
サーバーコンポーネントとバージョン
資産取得情報
資産メンテナンス情報
資産サポート情報
ハードドライブ情報

ESX 情報
HyperV 情報
フィールドで交換可能なユニット（FRU）に関する情報
ライセンス情報
デバイス位置の情報
メモリ情報
モジュラーエンクロージャ情報
NIC 情報
PCI デバイス情報
ストレージコントローラ情報
仮想ディスク情報
保証情報
BIOS 設定
iDRAC ネットワーク設定
テンプレートの関連付け

エージェントおよびアラート概要

エージェントとアラート概要 には、次の内容が表示されます。

- **エージェント概要**
- **iDRAC サービスモジュール概要**
- **1 デバイス当たりの警告**
- **最多警告生成**

エージェント概要

エージェント概要 ペインは、エージェントの概要情報を表およびグラフで表示します。

フィールド	説明
特定の Server Administrator エージェントを使用しているシステムの数	
エージェント詳細	エージェントの名前とバージョンを表示します。
このエージェントを利用するシステム数	特定バージョンのエージェントを利用するシステムの数を表示します。

iDRAC サービスモジュール概要

iDRAC サービスモジュール概要 ペインには iDRAC Service Module の概要情報が表およびグラフで表示されます。

フィールド	説明
特定の iDRAC サービスモジュールを使用しているシステムの数	
エージェント詳細	エージェントの名前とバージョンを表示します。
このエージェントを利用するシステム数	特定バージョンのエージェントを利用するシステムの数を表示します。

iDRAC サービスモジュール概要 チャートには、次のようにデバイスが表示されます。

- 対応 Linux
- 導入可能 Linux
- 対応 Windows
- 導入可能 Windows
- 非対応

1 デバイス当たりの警告

フィールド	説明
アラート発生に基づいた最もアクティブな検出済みシステム	
デバイス名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
関連イベント数	デバイスからの警告数を表示します。
最終検出場所	IP アドレス範囲またはホスト名を表示します。
インベントリ日時	最後に実行されたインベントリの時間および日付情報を表示します。

最多警告生成

最多警告生成 ペインには最大警告数の上位 5 システムが表示されます。

デバイスコンプライアンス

フィールド	説明
コンプライアンス状態	構成テンプレートに関連するデバイスのコンプライアンスステータスを表示します。
デバイス名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
サービスタグ	システムに割り当てられた固有の識別子を表示します。
モデル	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
コンプライアンステンプレート	デバイスに関連付けられたデバイス構成テンプレートを表示します。
前回実行されたインベントリ	最後に行われたデバイス設定インベントリの日付と時間を表示します。

サーバーの概要

フィールド	説明
システム名	システムのホスト名を表示します
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
オペレーティングシステム	システムにインストールされているオペレーティングシステムを表示します。
プロセッサ数	システムに取り付けられたされたプロセッサの数です。
プロセッサシリーズ	システムに取り付けられたプロセッサの種類を表示します。
プロセッサコア	プロセッサのコア数を表示します。
プロセッサ速度	プロセッサの速度を表示します。
コア合計	システム内にあるコアの合計数を表示します。
メモリ合計	システムに取り付けられたメモリの合計を表示します。

サーバーコンポーネントとバージョン

フィールド	説明
システム名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
サービスタグ	システムに割り当てられた固有の識別子を表示します。
モデルタイプ	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
説明	ソフトウェアの情報を表示します。
ソフトウェアの種類	システムで使用可能なソフトウェアの種類を表示します。例えば、ファームウェアなどです。
ソフトウェアバージョン	システムで使用可能なソフトウェアのバージョン番号を表示します。

資産取得情報

フィールド	説明
システム名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
サービスタグ	システムに割り当てられた固有の識別子を表示します。
購入コスト	所有者が支払ったシステム代金を表示します。
購入日	所有者がシステムを購入した日付を表示します。
納品書番号	受け取った商品の貨物受領書を表示します。
注文書番号	システム代金支払いを承認した文書の番号を表示します。
インストール日	システムの稼働開始日を表示します。
経費清算済み	システム代金が特定目的、または研究開発部門や販売部門などの部署に請求されるかどうかを表示します。
コストセンター	システムを取得したビジネス組織の名前またはコードを表示します。
署名責任者名	システムの購入またはサービスコールを承認した人物の名前を表示します。
ベンダー	システムのサービスを提供する企業体を表示します。
減価償却期間	システムが減価償却される年数または月数を表示します。
減価償却期間の単位	単位を、月または年で表示します。
減価償却率	資産の価値切り下げまたは減価償却率（百分率）を表示します。
減価償却方法	システム減価償却の計算に使用する手順と仮定を表示します。
所有者コード	このシステムの所有者コードを定義します。
所有企業名	システムを所有する企業体を表示します。
保険会社	システムの保証契約を行った保険会社名を表示します。

資産メンテナンス情報

フィールド	説明
システム名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
サービスタグ	システムに割り当てられた固有の識別子を表示します。
複数スケジュール	リースに複数のスケジュールがあるかどうかを表示します。
買取額	システムの買取残額を表示します。
リースのレート係数	システムリース用のレート係数を表示します。
リース終了日	システムリースの終了日を表示します。
適正市場価格	システムの市場適性価格を表示します。
賃貸者	システムの賃貸者の名称を表示します。
メンテナンスプロバイダ	メンテナンスプロバイダの名前を表示します。
メンテナンス制限	メンテナンス契約の制限事項を表示します。
メンテナンス開始日	システムのメンテナンス開始日を表示します。
メンテナンス終了日	システムのメンテナンス終了日を表示します。
アウトソーシング問題の説明	アウトソーシングサービスプロバイダで生じた問題を表示します。
アウトソーシングサービス料金	アウトソーシングベンダーがサービスに対して請求する金額を表示します。
アウトソーシングプロバイダ料金	サービスに関する追加のアウトソーシング料金を表示します。
アウトソーシングプロバイダのサービスレベル	システムのサービスレベル契約を表示します。
アウトソーシング署名責任者	サービスの承認に署名することができる人物の名前を表示します。

資産サポート情報

フィールド	説明
システム名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
サービスタグ	システムに割り当てられた固有の識別子を表示します。
保証コスト	システムの延長保証コストの日付を表示します。
保証期間	保証の期間を表示します。
保証期間タイプ	システムの保証期間のタイプを表示します。
保証終了日	システムの保証終了日を表示します。
延長保証コスト	システムの保証コストを表示します。
延長保証開始日	システムの延長保証開始日を表示します。
延長保証終了日	システムの延長保証終了日を表示します。
延長保証プロバイダ名	システムの延長保証プロバイダの名称を表示します。
更新された契約	システムのサービス契約が更新されたかどうかを表示します。
契約タイプ	システムのサービス契約タイプの名前を表示します。
契約ベンダー	システムのサービス契約プロバイダの名前を表示します。
アウトソース	システムのサポートがアウトソーシングされているかどうかを表示します。
サポートタイプ	発生したコンポーネント、システム、またはネットワーク問題のタイプを表示します。
ヘルプデスク	提供されるヘルプデスクの情報を表示します。
自動修復	問題を修正するために使用される方法を表示します。

ハードドライブ情報

フィールド	説明
システム名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
サービスタグ	システムに割り当てられた固有の識別子を表示します。
エンクロージャ ID	Storage Management によってエンクロージャに割り当てられたエンクロージャ ID を表示します。Storage Management はコントローラに接続されているエンクロージャに 0 から順に番号を付けます。
チャネル	チャネルの数を表示します。
ターゲット ID	バックプレーン（サーバーに対して内部）の SCSI ID またはコントローラコネクタが接続されているエンクロージャを表示します。値は通常 6 です。
LUN ID	LUN の ID を表示します。コンピュータストレージでは、SCSI プロトコルまたはファイバチャネルや iSCSI など同様のプロトコルによってアドレス指定されるデバイスである論理ユニットの識別に使用される、論理ユニット番号または LUN 番号です。
サイズ（GB）	ハードディスクドライブのサイズをギガバイト単位で表示します。
バスのタイプ	使用されているバス接続の種類を表示します。コンピュータでは、バスとはシステムのコンポーネント間の伝送経路情報のことです。
シリアル番号	製造元によってデバイスに割り当てられたロール番号を表示します。
リビジョン	ハードディスクドライブのリビジョン履歴を表示します。
メディアの種類	メディアの種類を表示します。例えば HDD などです。
ベンダー	ハードディスクドライブを供給する組織の名前を表示します。
モデル番号	物理デバイスのモデル番号を表示します。
パーツ番号	特定の OEM ベンダーのドライブおよびドライブ容量に関連付けられた固有の番号を表示します。

フィールド	説明
残留書き込み耐久率	PERC に接続されているソリッドステートドライブ（SSD）の、% 単位での消耗レベルまたは残りの寿命を表示します。ドライブがこのプロパティをサポートしない場合、該当なしと表示されます。

ESX 情報

フィールド	説明
ホスト名	ネットワーク上でシステムを識別するためのシステムの固有の名前を表示します。このシステムには、組み込みのベアメタル製品がインストールされています。
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
VM の種類	システムにインストールされた組み込みのベアメタル製品のタイプを表示します。例えば、VMware ESX などです。
バージョン	システムにインストールされている組み込みのベアメタルのバージョンを表示します。
ゲスト名	ゲスト仮想マシンの名前を表示します。
ゲスト OS の種類	仮想マシンにインストールされているオペレーティングシステムを表示します。
ゲストメモリサイズ（MB）	仮想マシンの RAM のサイズを表示します。
ゲスト状況	仮想マシンの電源がオンになっているかまたはオフになっているかを表示します。

HyperV 情報

フィールド	説明
ホスト名	HyperV がインストールされているシステムのホスト名を表示します。
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
ゲスト名	ゲスト仮想マシンの名前を表示します。
ゲストメモリサイズ（MB）	仮想マシンの RAM のサイズを表示します。
ゲスト状況	仮想マシンの電源がオンになっているかまたはオフになっているかを表示します。

フィールドで交換可能なユニット（FRU）に関する情報

フィールド	説明
システム名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
モデルタイプ	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
サービスタグ	システムに割り当てられた固有の識別子を表示します。
FRU デバイス名	デバイスに割り当てられた標準 FRU 名を表示します。
FRU メーカー	FRU メーカーの名前を表示します。
FRU シリアル番号	製造元が指定した FRU の識別番号を表示します。
FRU パーツ番号	FRU のタイプを識別する、業界固有の番号を表示します。

ライセンス情報

フィールド	説明
システム名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
モデルタイプ	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
ライセンスの説明	このライセンスで有効にされている機能のレベルを表示します。
ライセンス期間	ライセンスの期間を表示します。
資格 ID	ライセンス固有の ID を表示します。
残り時間	ライセンスが期限切れになるまでの残りの日数を表示します。

デバイス位置の情報

フィールド	説明
システム名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。

フィールド	説明
サービスタグ	システムに割り当てられた固有の識別子を表示します。
場所	システムの場所を表示します。
データセンター	システムがあるデータセンターを表示します。
部屋	システムがある部屋の名前を表示します。
アイル	システムがあるアイルを表示します。
ラック	システムがあるラックを表示します。

メモリ情報

フィールド	説明
システム名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
サービスタグ	システムに割り当てられた固有の識別子を表示します。
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
メモリデバイス名	製造元によってデバイスに割り当てられた名前を表示します。例えば、DIMMI_A などです。
メモリデバイスのサイズ（MB）	メモリデバイスのサイズをギガバイト単位で表示します。
メモリデバイスメーカー	デバイス製造元の名前を表示します。
メモリデバイスのパーツ番号	デバイスに割り当てられた業界固有の番号を表示します。
メモリデバイスのシリアル番号	製造元によってデバイスに割り当てられたロール番号を表示します。

モジュラーエンクロージャ情報

フィールド	説明
エンクロージャモデルタイプ	エンクロージャのモデル名を表示します。例えば、PowerEdge M1000e などです。
スロット番号	エンクロージャ上のスロット番号を表示します。
スロット名	エンクロージャのスロット名を表示します。
スロット可用性	モジュラエンクロージャのスロットが使用可能か使用中かを表示します。

フィールド	説明
ファームウェアバージョン	エンクロージャにインストールされたファームウェアのバージョンを表示します。
エンクロージャのサービスタグ	エンクロージャに割り当てられた固有の識別子を表示します。
エンクロージャ名	ネットワークでエンクロージャを識別する、固有のエンクロージャの名前を表示します。
ブレードのモデルタイプ	ブレードサーバーのモデル名です。例えば、PowerEdge M710 などです。
ブレードのサービスタグ	ブレードサーバーに割り当てられた固有の識別子を表示します。
ブレードのホスト名	ブレードサーバーのホスト名を表示します。
ブレードの OS	ブレードサーバーにインストールされているオペレーティングシステムを表示します。

NIC 情報

フィールド	説明
システム名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
IPv4 アドレス	NIC デバイスに割り当てられた固有の IPv4 アドレスを表示します。
IPv6 アドレス	NIC デバイスに割り当てられた固有の IPv6 アドレスを表示します。
MAC アドレス	物理ネットワークセグメントでの通信用にネットワークインタフェースに割り当てられた固有のメディアアクセス制御アドレス（MAC アドレス）を表示します。
NIC の説明	NIC デバイスに関する情報を表示します。

PCI デバイス情報

フィールド	説明
システム名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。

フィールド	説明
サービスタグ	システムに割り当てられた固有の識別子を表示します。
デバイスカードの説明	使用されている PCI（Peripheral Component Interconnect）カードの種類を表示します。例えば、82546GB Gigabit Ethernet Controller などです。
デバイスカードの製造元	製造元情報を表示します。
デバイスカードのスロットタイプ	カードが挿入されるマザーボードのスロットタイプを表示します。

ストレージコントローラ情報

フィールド	説明
システム名	ネットワーク上でシステムを識別するためのシステムの固有の名前を表示します。このシステムには、ストレージコントローラが存在します。
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
コントローラ名	ストレージコントローラの名前を表示します。例えば、オンボード SAS 6/iR などです。
ベンダー	供給業者の情報を表示します。例えば、オンボード SAS 6/iR はデルによって供給されます。
コントローラタイプ	コントローラの種類を表示します。例えば、オンボード SAS 6/iR は SAS タイプです。
コントローラ状況	コントローラの状態を表示します。例えば、使用可能などです。

仮想ディスク情報

フィールド	説明
システム名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
サービスタグ	システムに割り当てられた固有の識別子を表示します。
ターゲット ID	バックプレーン（サーバーに対して内部）の SCSI ID またはコントローラコネクタが接続されているエンクロージャを表示します。

フィールド	説明
名前	仮想ディスクの名前を表示します。
デバイス名	仮想ディスクが存在するデバイスの名前を表示します。
サイズ（GB）	仮想ディスクのサイズをギガバイト単位で表示します。
レイアウト	RAID レベルを表示します。
キャッシュポリシー	ストレージで使用されるキャッシュポリシーを表示します。
読み取りポリシー	ストレージで使用される読み取りポリシーを表示します。
書き込みポリシー	ストレージで使用される書き込みポリシーを表示します。
ストライプサイズ（バイト）	ストライプのサイズをバイト単位で表示します。

保証情報

フィールド	説明
保証事項の表示と更新	デルのウェブサイトを開く際にクリックするリンクを表示します。このサイトでは、デバイスの保証を表示または更新できます。
システム名	ネットワーク上でシステムを識別する固有のシステム名を表示します。該当する場合は、 **dell.com/support** から保証のデータを取得するためにプロキシの設定を行う必要があります。
デバイスモデルの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
デバイスタイプ	デバイスの種類を表示します。例えば、サーバー、Remote Access Controller などです。
出荷日	デバイスが工場から発送された日付を表示します。
サービスタグ	システムに割り当てられた固有の識別子を表示します。
サービスレベルコード	特定のシステムに対するパーツのみの保証（POW）、翌営業日オンサイト（NBD）、その他のサービスレベルコードを表示します。
サービスプロバイダ	デバイスへの保証サービスサポートを提供する組織の名前を表示します。
開始日	保証が開始する日付を表示します。

フィールド	説明
終了日	保証が失効する日付を表示します。
残りの日数	デバイスの保証を使用可能な日数を表示します。
保証の説明	デバイスに適用される保証の詳細を表示します。

BIOS 設定

フィールド	説明
システム名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
サービスタグ	システムに割り当てられた固有の識別子を表示します。
仮想化テクノロジ	Virtualization Technology によって提供される追加のハードウェア機能が有効または無効になっているかを表示します。
システムプロファイル	選択したシステムプロファイルを表示します。 ワットあたりのパフォーマンス（DAPC）、ワットあたりのパフォーマンス（OS）、パフォーマンス、高密度の構成、カスタムがあります。
ユーザーのアクセスが可能な USB ポート	ユーザーアクセス可能 USB ポートオプションの状態を表示します。
プロセッサごとのコア	プロセッサごとに有効になっているコア数を表示します。
ノードインターリーブ	ノードインターリーブオプションが有効または無効になっているかを表示します。
論理プロセッサ	倫理プロセッサオプションが有効または無効になっているかを表示します。
内蔵 RAID コントローラ	内蔵 RAID コントローラが有効または無効になっているかを表示します。
SR-IOV グローバル有効	シングルルート I/O 仮想化（SR-IOV）デバイスの設定が有効または無効になっているかを表示します。
無効化を実行する	メモリ保護機能無効化の実行が有効または無効になっているかを表示します。

iDRAC ネットワーク設定

フィールド	説明
システム名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
サービスタグ	システムに割り当てられた固有の識別子を表示します。
IPMI オーバー Lan	IPMI オーバー Lan インタフェースオプションが有効または無効になっているかを表示します。
IPMI コミュニティ	トラップの SNMP コミュニティ名を表示します。
SSH	SSH 接続が有効または無効になっているかを表示します。
SSH ポート	iDRAC が SSH 接続に使用しているポート番号を表示します。
SSH タイムアウト	SSH 接続がアイドル状態でいられる期間を表示します。
Telnet	Telnet 接続が有効または無効になっているかを表示します。
Telnet ポート	iDRAC が Telnet 接続に使用しているポート番号を表示します。
Telnet タイムアウト	Telnet 接続がアイドル状態でいられる期間を表示します。

テンプレートの関連付け

フィールド	説明
システム名	ネットワーク上でシステムを識別するシステムの固有の名前を表示します。
システムの種類	システムのモデル名を表示します。例えば、PowerEdge R710 となります。
サービスタグ	システムに割り当てられた固有の識別子を表示します。
関連付けられたテンプレート	システムに関連付けられているデバイス設定テンプレートを表示します。

関連リンク

設定テンプレートへのターゲットデバイスの関連付け

15

保証レポートの表示

保証情報は、有効なサービスタグのあるデバイス（クライアント、サーバー、スイッチ、ストレージなどを含む）で利用することができます。保証情報はデバイス検出時に自動的に取得されます。

保証情報レポートは、保証情報を Dell 保証データベースから取得するためにインターネットアクセスが必要であることから、OpenManage Essentials のレポートの中では特殊なものです。インターネットアクセスがない場合は、保証情報は投入されません。保証情報は、次回インターネットに接続し、保証レポートを開く時にダウンロードされます。

メモ: 特定のサービスタグに対して OpenManage Essentials に表示された保証情報（失効および更新情報を含む）が、**support.jp.dell.com** に表示される保証記録と一致しない場合があります。**support.jp.dell.com** に表示された保証記録のサービスレベルコードとモデル名は、OpenManage Essentials の保証レポートと完全に一致しないことがあります。

延長保証

デバイスのサポートを延長するには 、**レポート → 保証情報** ページで **保証の表示および更新** をクリックするとデルの保証サイトが開きます。会社のアカウントで保証サイトにログインし、すべてのデバイスとその保証情報を表示することができます。

16

アラートの管理

メモ: OpenManage Mobile アプリケーションをインストールしてセットアップすることにより、Android モバイルデバイスで OpenManage Essentials からのアラート通知を受信することができます。詳細に関しては、「OpenManage Mobile 設定」、および **dell.com/OpenManageManuals** の『OpenManage Mobile ユーザーズガイド』を参照して下さい。

OpenManage Essentials について

- アラートおよびアラートカテゴリの表示
- アラート管理処置
- アラートログ設定

アラートおよびアラートカテゴリの表示

アラートページを表示するには、OpenManage Essentials で、**管理 → アラート** をクリックします。

メモ: 削除したデバイスのアラートはコンソールに表示されません。しかし、これらのアラートはパージ制限に達するまでデータベースから削除されません。

アラートログの表示

アラートログを表示するには、**管理 → アラート → アラートログ** の順にクリックします。

アラートタイプについて

次のアラートログの種類が表示されます。

表 2. アラートの種類

アイコン	アラート	説明
	正常アラート	電源装置がオン、またはセンサーの測定値が正常に戻ったなど、ユニットの正しい動作を示すサーバーまたはデバイスからのイベントです。
	警告アラート	イベントは必ずしも重要ではありませんが、警告しきい値を超えたなど、発生する可能性のある問題があることを示します。
	重要アラート	障害しきい値を超えた、またはハードウェアの障害など、データまたは機能が実際に失われるあるいは喪

アイコン	アラート	説明
		失が差し迫っていることを示す重要なイベントです。
	不明アラート	イベントが発生しましたが、分類するための十分な情報がありません。
	情報アラート	情報のみを提供します。

内部アラートの表示

内部アラートを表示する前に、**プリファランス** タブの **アラート設定** で内部正常性アラートが有効になっていることを確認してください。「アラート設定」を参照してください。
内部アラートを表示するには、**管理 → アラート → アラートログ → すべての内部アラート** の順にクリックします。
すべての内部アラート フィルタは、管理下デバイスのグローバル正常性または接続状態で変更が生じるときに OpenManage Essentials が生成する内部アラートの参照です。

アラートカテゴリの表示

アラートカテゴリを表示するには、**管理 → アラート → アラートカテゴリ** の順にクリックします。
事前定義されたアラートカテゴリはアルファベット順にリストされています。

アラートソースの詳細の表示

アラートカテゴリを表示するには、アラートカテゴリリストでアラートカテゴリを展開し、アラートソースを選択します。

メモ: イベントソースを新しく作成することはできません。

例えば、**環境** アラートカテゴリを展開して **alertCoolingDeviceFailure** アラートソースを選択します。

alertCoolingDeviceFailure アラートソースの値と説明

フィールド名	値	説明
名前	alertCoolingDeviceFailure	
タイプ	snmp	SNMP アラートベースのソースです。
カタログ	MIB - 10892	
重大度	重要	このアラートを受信したら、システムは重要な状態にあり、迅速な処置が必要です。
文字列のフォーマット	$3	
SNMP Enterprise OID	.1.3.6.1.4.1.674.10892.1	

フィールド名	値	説明
SNMP 一般トラップ OID	6	
SNMP 指定トラップ OID	1104	

以前に設定されたアラート処置の表示

本項では、以前に設定されたアラート処置を表示する方法が記載されています。

アプリケーションの起動アラート処置の表示

アプリケーションの起動アラート処置を表示するには、次の手順を実行します。

1. **管理** → **アラート** → **アラート処置** を選択します。
2. **アラート処置** で **アプリケーションの起動** を選択します。

電子メールアラート処置の表示

電子メールアラート処置を表示するには、次の手順を実行します。

1. **管理** → **アラート** → **アラート処置** の順に選択します。
2. **アラート処理** で **電子メール** を選択します。

アラート無視処置の表示

アラートの無視処置を表示するには、次の手順を実行します。

1. **管理** → **アラート** → **アラート処置** の順に選択します。
2. **アラート処置** で **無視** を選択します。

トラップ転送処置の表示

トラップ転送処置を表示するには、次の手順を実行します。

1. **管理** → **アラート** → **アラート処置** の順に選択します。
2. **アラート処置** で **トラップ転送** を選択します。

アラートへの対処

アラートのフラグ付け

アラートで処置が完了した後、確認済みとしてアラートをフラグ付けします。アラートの承認は、自分のためのリマインダーとして、解決済みであるかさらに処置が必要であるかを示します。アラートを確認済みにするには、次の手順を行います。

1. **管理** → **アラート** → **アラートログ** の順に選択します。
2. 確認したいアラートをクリックします。

   メモ: 複数のアラートを同時に承認できます。<Ctrl> または <Shift> を使用して、複数のアラートを選択します。

3. 右クリックして、**確認 → 設定 → 選択されたアラートまたはフィルタされたアラート**をクリックします。
   選択されたアラート を選択すると、ハイライト表示されたアラートが確認されます。

   フィルタされたアラート を選択すると、現在フィルタ / 表示されているアラートが確認されます。

新規ビューの作成と編集

アラートの表示方法を好みに合わせて変更するには、新規ビューを作成するか、既存のビューを変更します。新規ビューを作成するには、次の手順を行います。

1. **管理 → アラート → 一般タスク → 新規アラート表示フィルタ**を選択します。
2. **名前と重大度の関連** で、新規フィルタの名前を入力し、1 つまたは複数の重大度にチェックを付けます。**次へ** をクリックします。
3. **カテゴリとソースの関連** で、この新規フィルタに関連付けたいアラートカテゴリまたはソースを割り当て、**次へ** をクリックします。
4. **デバイスの関連** で、このビューフィルタに関連付けたいデバイスの検索クエリを作成するか、デバイスまたはデバイスグループを割り当て、**次へ** をクリックします。
5. （オプション）デフォルトでは、アラート表示フィルタは常にアクティブです。アクティビティを制限するには、**日付 / 時刻の関連** で、日付範囲、時間範囲、または日数を入力して、**次へ** をクリックします。
6. （オプション）**承認済み関連性** で、このアラート処置がアクティブである期間を設定し、**次へ** をクリックします。デフォルトは常にアクティブです。
7. **概要** で入力を確認して **終了** をクリックします。

アラート処置の設定

アラート処置は、OpenManage Essentials コンソールが受信したすべてのアラートで実行されます。OpenManage Essentials がデバイスの SNMP トラップ転送宛先リストにリストされている限り、OpenManage Essentials がデバイスを検出しているかどうかにかかわらず、アラートは OpenManage Essentials コンソールによって受信および処理されます。これを回避するには、デバイスの SNMP トラップ転送宛先リストから OpenManage Essentials を削除してください。

電子メール通知の設定

アラートを受信したときの電子メール通知を作成できます。例えば、サーバーから重要な温度アラートを受信すると電子メールが送信されます。

アラートを受信した際の電子メール通知を設定するには、次の操作を実行します。

1. **管理 → アラート → 一般タスク → 新しいアラート電子メール処置**を選択します。
2. **名前と説明** で電子メールアラート処理名と説明を入力し、**次へ** をクリックします。
3. **電子メール設定** で次を実行し **次へ** をクリックします。
   a. **宛先：** と **発信元：** の受信者の電子メール情報を入力して、代替情報を入力します。それぞれの受信者と配布リストはセミコロンで区切ってください。
   b. 次の代替パラメータで電子メールメッセージをカスタマイズします。
      - $n = デバイス
      - $ip = デバイス IP
      - $m = メッセージ
      - $d = 日付
      - $t = 時刻

- $sev = 重大度
- $st = サービスタグ
- $e = エンタープライズ OID
- $sp = 指定のトラップ OID
- $g = 一般トラップ OID
- $cn = アラートカテゴリ名
- $sn = アラートソース名
- $pkn = パッケージ名
- $at = 管理タグ

c. **電子メール設定** をクリックして SMTP サーバー名または IP アドレスを提供し、電子メール設定をテストして **OK** をクリックします。

d. **テスト処置** をクリックしてテストの電子メールを送信します。

4. **重大度の関連** で、この電子メールアラートに関連付けたいアラートの重大度を割り当て、**次へ** をクリックします。
5. **カテゴリおよびソースの関連** で、この電子メールアラートに関連付けたいアラートカテゴリまたはアラートソースを割り当て、**次へ** をクリックします。
6. **デバイスの関連** で、この電子メールアラートに関連付けたいデバイスまたはデバイスグループを割り当て、**次へ** をクリックします。
7. デフォルトでは、電子メールの通知は常にアクティブです。アクティビティを制限するには、**日付 / 時刻の関連** で、日時範囲、時間範囲、または日数を入力して、**次へ** をクリックします。
8. **概要** で入力を確認して **終了** をクリックします。

関連リンク

アラートログ
アラートログフィールド
アラートログ設定
重大度

アラートの無視

無視したいアラートを受信することがあります。例えば、管理下ノード上の SNMP サービス内で **認証トラップの送信** が選択されているときに生成される複数の警告を無視したいなどです。

メモ: デバイスツリーのデバイス、または **アラート** ポータルのアラートのどちらかを右クリックすると使用できる **デバイスからのすべてのアラートを無視** オプション使用することで、特定のデバイスからのアラートをすべて無視できます。

アラートを無視するには、次の手順を実行します。

1. OpenManage Essentials で、**管理 → アラート → 一般タスク → 新しいアラート無視処置**を選択します。
2. **名前と重大度の関連** で名前を入力し、このアラート無視処理に関連付けたいアラートの重大度を割り当て、**次へ** をクリックします。
3. **カテゴリとソースの関連** で、このアラート無視処理に関連付けたいアラートカテゴリソースを割り当て、**次へ** をクリックします。
4. **デバイスの関連** で、このアラート無視処理に関連付けたいデバイスまたはデバイスグループを割り当て、**次へ** をクリックします。
5. デフォルトでは、アラートの無視は常にアクティブです。アクティビティを制限するには、**日付け / 時刻の関連** で、日時範囲、時間範囲、または日数を入力して、**次へ** をクリックします。
6. **重複アラートの相関性** で、設定された時間制限内での重複アラートの受信を除外するために **はい** を選択し、次に **次へ** をクリックします。

7. **概要** で入力を確認して **終了** をクリックします。

カスタムスクリプトの実行

特定のアラートを受信したときに、カスタムスクリプトを実行するか、特定のアプリケーションを起動することができます。このファイルは、クライアントブラウザシステム上ではなく、OpenManage Essentials サービス層システム（OpenManage Essentials がインストールされているシステム）上に存在する必要があります。例えば、

- 温度警告を受信した場合、カスタムスクリプトを使用して社内ヘルプデスク用のインシデントチケットを作成できます。
- MD アレイストレージアラートを受信した場合、Modular Disk Storage Manager（MDSM）アプリケーションを起動してアレイのステータスを表示できます。

カスタムスクリプトの作成

1. **管理 → アラート → アラート処置** の順に選択します。
2. **アラート処置** で、**アプリケーションの起動** を右クリックし、**新規アラートアプリケーションの起動処置** を選択します。
3. **名前および説明** でアプリケーションの起動名と説明を入力し、**次へ** をクリックします。
4. **アプリケーション起動の設定** で、実行可能ファイル名を指定し（ファイルへの絶対パス、例えば、**C:\ProgramFiles\Dell\Application.exe**）、代替情報を入力して **次へ** をクリックします。
5. **重大度の関連付け** で、このアラートアプリケーションの起動に関連付けたいアラートの重大度を割り当て、**次へ** をクリックします。
6. **カテゴリとソースの関連付け** で、このアラートアプリケーションの起動に関連付けたいアラートカテゴリまたはアラートソースを割り当て、**次へ** をクリックします。
7. **デバイスの関連付け** で、このアラートアプリケーションの起動に関連付けたいデバイスまたはデバイスグループを割り当て、**次へ** をクリックします。
8. デフォルトでは、アプリケーションの起動処置は常にアクティブです。アクティビティを制限するには、**日時の関連付け** で、日付範囲、時間範囲、または日数を入力して、**次へ** をクリックします。
9. **サマリ** で入力を確認して **終了** をクリックします。

関連リンク

アラートログ
アラートログフィールド
アラートログ設定
重大度

アラートの転送

複数の管理ステーションからのアラートを 1 つの管理ステーションにまとめることができます。例えば、複数の場所に管理ステーションがあり、1 つの中央の場所から状態を表示してアクションを実行できます。転送アラートの動作の詳細に関しては、「アラート転送使用事例」を参照してください。アラート転送を作成するには、次の手順を実行します。

1. **管理 → アラート → 一般タスク → 新しいトラップ転送のアラート処置**を選択します。
2. **名前と説明** でトラップ転送名と説明を入力し、**次へ** をクリックします。
3. **トラップ転送の設定** で、テストトラップを送信先の管理ステーションに送信するため、送信先のホスト名または IP アドレス、コミュニティ情報を入力し、**処置のテスト** をクリックします。設定された送信先に同じフォーマットでトラップを転送するには、**オリジナルフォーマットでのトラップの転送** をクリックし、**次へ** をクリックします。

4. **重要度の関連** で、このトラップ転送アラートに関連付けたいアラートの重大度を割り当て、**次へ** をクリックします。
5. **カテゴリおよびソースの関連** で、このトラップ転送アラートに関連付けたいアラートカテゴリソースを割り当て、**次へ** をクリックします。
6. **デバイスの関連** で、このトラップ転送アラートに関連付けたいデバイスまたはデバイスグループを割り当て、**次へ** をクリックします。
7. デフォルトでは、トラップ転送処置は常にアクティブです。アクティビティを制限するには、**日時の関連付け** で、日付範囲、時間範囲、または日数を入力して、**次へ** をクリックします。
8. **概要** で入力を確認して **終了** をクリックします。

   すべてのトラップの状態重大度は正常に設定されており、アラート処理を成功させるためには、重大度、カテゴリ、およびデバイスの組み合わせには、先行の手順で選択したものを参照する必要があります。

アラートの転送使用事例シナリオ

本項は、SNMP v1 および SNMP v2 プロトコルを使用してアラートを転送するシナリオについて説明します。シナリオは次のコンポーネントで構成されます。

- MNv1 と呼ばれる、SNMP v1 エージェントがインストールされた管理下ノード
- MNv2 と呼ばれる、SNMP v2/v2c エージェントがインストールされた管理下ノード
- MS1 と呼ばれる、OpenManage Essentials がインストールされた管理下ステーション 1
- MS2 と呼ばれる、OpenManage Essentials がインストールされた管理下ステーション 2
- MS3 と呼ばれる、サードパーティソフトウェアがインストールされた管理下ステーション 3

シナリオ 1 — SNMP v1 プロトコルを使用したオリジナルフォーマットでのアラート転送

このシナリオでは、SNMP v1 アラートは MNv1 から MS1 に送信され、次に MS1 から MS2 に転送されます。転送アラートのリモートホストを取得しようとすると、アラートが MNv1 から発生していることから、MNv1 の名前が表示されます。SNMP v1 アラート標準では、SNMP v1 アラートでエージェント名を設定することができるので、MNv1 が表示されます。

シナリオ 2 — SNMP v2/v2c プロトコルを使用したオリジナルフォーマットでのアラート転送

このシナリオでは、SNMP v2 アラートは MNv2 から MS1 に送信され、次に MS1 から MS3 に転送されます。MS3 から転送アラートのリモートホストを取得しようとすると、MS1 として表示されます。

SNMP v2 アラートには、エージェント名を指定するフィールドがないので、アラートを送信するホストがエージェントと想定されます。SNMP v2 アラートが MS1 から MS3 に転送されると、MS1 は問題の発生源とみなされます。この問題を解決するには、SNMP v2 または v2c アラートを転送するときに、OID を .1.3.6.1.6.3.18.1.3.0 として varbind（変数は **エージェントアドレス**）が追加されます。これは、RFC2576-MIB で指定された標準 OID に基づいて設定されています。MS3 から **エージェントアドレス** を取得しようとすると、MNv2 と表示されます。

メモ: SNMP v2 アラートが MS1 から MS2 に転送される場合、MS1 は転送されたトラップと一緒に追加の OID も解析するため、リモートホストは MNv2 と表示されます。

シナリオ 3 — SNMP v1/v2 プロトコルを使用した OMEssentials フォーマットでのアラート転送

このシナリオでは、SNMP v1 アラートは MNv1 から MS1 に送信され、その後 MS2 に転送されます。転送されたアラートのリモートホストを取得すると、MS1 と表示されます。アラートの重要度とメッセージも MS1 に定義され、MNv1 によって定義されたオリジナルの重要度とメッセージは表示されません。

メモ: SNMPv2 トラップでも同様の動作になります。

サンプルアラート処置の使用事例での作業

サンプルアラート処置は、**アプリケーションの起動、電子メール、無視、**および **トラップ転送** のアラート処置で使用できます。サンプルアラート処置の使用事例はデフォルトで無効になっています。サンプルアラート処置をクリックして、サンプルアラート処置を有効にします。

サンプル使用事例を有効にするには、使用事例を右クリックして **有効** を選択します。

アラート処置の使用例

アプリケーションの起動

例 - サーバーの重要アラートでのスクリプトの実行 — 重要アラートを受信した場合にこの使用例を有効にして、カスタムスクリプトを実行します。

電子メール

- **例 - サービスデスクへの電子メールアラート** — アラートの基準がマッチした場合にこの使用例を有効にして、OpenManage Essentials サーバーから、サービスデスクアカウントに電子メールを送信します。
- **例 - 管理者への電子メール重要サーバーアラート** — アラートの基準がマッチした場合にこの使用例を有効にして、OpenManage Essentials サーバーから、管理者に電子メールを送信します。

無視

- **例 - メンテナンス時間帯の間アラートを無視** — 指定した時間の間アラートを無視する場合にこの使用例を有効にします。
- **例 - 15 秒間の重複アラートを無視** — 同一システムからの重複アラートを無視する場合にこの使用例を有効にします。
- **例 - プリンタからの非重要アラートを無視** — プリンタに関連した非重要アラートを無視する場合にこの使用例を有効にします。

トラップ転送

例 - 重要なサーバーアラートを他の監視コンソールに転送 — SNMP アラートを他の監視コンソールに転送する場合にこの使用例を有効にします。

アラートログ設定

アラートログが設定されたしきい値に達した場合、およびアラートログをパージする場合に、警告アラートが生成されるようにアラートログ設定でアラートログの最大サイズを設定できます。デフォルト設定を変更するには、次の手順を行います。

1. **管理 → アラート → 一般タスク → アラートログ設定**を選択します。
2. 値を入力するか、増 / 減の矢印ボタンを使用して値を増大または減少させます。

   メモ: アラートログのデフォルトの最大サイズは 20,000 アラートです。この値に達すると、古いアラートはパージされます。

アラートカテゴリおよびアラートソースの名前の変更

1. **管理** → **アラート** → **アラートカテゴリ** の順にクリックします。
2. **アラートカテゴリ** で、ラートカテゴリのいずれか（左ペインのアラートカテゴリ見出し下）を右クリックして、**名前の変更** を選択します。
3. アラートカテゴリの名前を入力して **OK** をクリックします。

アラートポップアップ通知

アラートポップアップ通知は、**重要** または **警告** アラートが受信されるときに、OpenManage Essentials コンソールの右下角に表示されます。アラートポップアップ通知に表示される情報は、受信されたアラートの数に応じて異なります。

受信されたアラートが 1 件だけの場合は、次の情報が表示されます。

- アラートタイプ — 警告または重要。
- アラートを生成したデバイスの名前。
- アラートの説明。
- **アラートの表示** — アラート詳細ウィンドウを表示します。
- **デバイスに移動** — デバイスツリー内のデバイスに移動します。
- **無効** — アラートポップアップ通知を無効化します。

受信されたアラートが 2 件以上の場合は、次の情報が表示されます。

- アラートタイプと頻度。
- デバイスツリー内のデバイスに移動するための、各デバイスのリンク化された名前。

  メモ: デバイスリンクは最初 3 件のアラートにのみ表示されます。
- **アラートの表示** — **すべての直近警告および重要アラート** ウィンドウを表示します。
- **アラートコンソールに移動** — アラートポータルに移動します。
- **無効** — アラートポップアップ通知を無効化します。

アラートポップアップ通知はデフォルトで有効です。アラートポップアップ通知を無効化、または各アラートポップアップ通知間の時間間隔を設定するために OpenManage Essentials を設定することができます。

メモ: アラートポップアップ通知設定 はユーザー固有です。あるユーザーが設定する設定が他のユーザーに適用されることはありません。

関連リンク

アラートポップアップ通知の設定
アラートポップアップ通知の有効化または無効化

アラートポップアップ通知の設定

アラートポップアップ通知を設定するには、次の手順を実行します。

1. **プリファランス** → **アラート設定**をクリックします。

アラート設定 ページが表示されます。

2. **アラートポップアップ通知設定** で **アラートポップアップ通知の有効化** を選択または選択解除して、アラートポップアップ通知を有効化または無効化します。
3. **ポップアップ通知間の秒数** ボックスで、各ポップアップ通知間の時間間隔を選択します。
4. **適用** をクリックします。

関連リンク

アラートポップアップ通知

アラートポップアップ通知の有効化または無効化

アラートポップアップ通知を有効化または無効化するには、次の手順を実行します。

メモ: アラートポップアップ通知を素早くを無効化するには、アラートポップアップ通知に表示されている **無効** リンクをクリックします。**アラートポップアップ通知の無効化** プロンプトが表示されたら、**はい** をクリックします。

1. **プリファランス → アラート設定**をクリックします。
   アラート設定 ページが表示されます。
2. **アラートポップアップ通知設定** で次を行います。
   - **アラートポップアップ通知の有効化** オプションを選択して、**警告** または **重要** アラートが受信されるときのアラートポップアップ通知を有効化します。
   - **アラートポップアップ通知の有効化** オプションの選択をクリアして、アラートポップアップ通知を無効化します。
3. **適用** をクリックします。

関連リンク

アラートポップアップ通知

17

アラート - 参照

このページは次の情報を提供します。

- 一般タスク
  - アラートログ設定
  - 新しいアラート表示フィルタ
  - 新しいアラートアプリケーションの起動処置
  - 新しいアラート電子メール処置
  - 新しいアラート無視処置
  - 新しいアラートのトラップ転送処置
- アラートログ
  - アラート表示フィルタ
    - すべてのアラート
    - すべての内蔵アラート
    - 重要アラート
    - 情報アラート
    - 正常アラート
    - 不明アラート
    - 警告アラート
- アラート処置
  - アプリケーションの起動
  - 電子メール
  - 無視
  - トラップ転送
- アラートカテゴリ

アラートログ

アラートログ からアラートを表示できます。アラートログでは、アクティブな表示フィルタでフィルタリングしたすべてのアラートを表示できます。

表示フィルタにおけるアラートの一致基準には、次の基準が挙げられます。

- アラートの重大度。「重大度」を参照してください。
- アラートカテゴリまたはソース。「カテゴリおよびソースの関連性」を参照してください。

- アラートデバイスまたはデバイスグループソース。「デバイスの関連性」を参照してください。
- アラート日時、曜日。「日時範囲」を参照してください。
- アラート確認済みフラグ。「確認」を参照してください。

関連リンク

アラートログ設定
アラート処置の設定
電子メール通知の設定
カスタムスクリプトの作成
アラートログフィールド
アラートログ設定
重大度

事前定義されたアラート表示フィルタ

次の表に、事前定義されたアラート表示フィルタを示します。

フィールド	説明
すべてのアラート	これを選択して、すべてのアラートを表示します。
重要アラート	これを選択して、重要なシステムすべてを表示します。
情報アラート	これを選択して、情報アラートを表示します。
正常アラート	これを選択して、正常アラートを表示します。
不明アラート	これを選択して、OpenManage Essentials が分類できないアラートを表示します。
警告アラート	これを選択して、すべての警告を表示します。

連続的アップデート を選択して、新たなアラートが受信されるたびにユーザーインタフェースが自動的に更新されるようにします。

アラートログフィールド

フィールド	説明
重大度	アラートの重大度
確認済み	アラートがユーザーによって承認されたかどうかです。
時間	アラートの生成日時です。
デバイス	アラートを生成したデバイスです。
詳細	アラートに含まれるメッセージです。

フィールド	説明
カテゴリ	アラートのカテゴリ化です。
ソース	アラートソース定義の名前です。

列によるグループ分け

すべてのアラート でグループ分けを行うには、グループ分けの基準にするすべてのアラートの列をドラッグし、**列のヘッダをドラッグしてここにドロップし、その列でグループ化する** にドロップします。

例えば、**すべてのアラート** で、重大度ごとにグループ分けする場合は、**重大度** を選択し、それをドラッグして **列のヘッダーをドラッグしてここにドロップし、その列でグループ化する** バーにドロップします。

アラートが重大度ごとに表示されます。

アラート詳細

フィールド	説明
重大度	アラートの重大度です。
確認済み	アラートがユーザーによって承認されたかどうかです。
デバイス	アラートを生成したデバイスです。
時間	アラートの生成日時です。
カテゴリ	アラートのカテゴリ化です。
ソース	アラートソース定義の名前です。
説明	アラートに含まれるメッセージです。
SNMP Enterprise OID	監視するイベントソースを定義する管理情報ベース（MIB）ファイルのエンタープライズ OID（SNMP OID のプレフィックス）を提供します。
SNMP 一般トラップ OID	目的のイベントソースから監視する SNMP トラップの汎用トラップ ID を提供します。SNMP トラップの詳細については、**dell.com/OpenManageManuals** で『Dell OpenManage Server Administrator SNMP リファレンスガイド』を参照してください。
SNMP 指定トラップ OID	目的のイベントソースから監視する SNMP トラップの特定のトラップ ID を提供します。SNMP トラップの詳細については、**dell.com/OpenManageManuals** で『Dell OpenManage Server Administrator SNMP リファレンスガイド』を参照してください。

アラートログ設定

アラートログのサイズ、メッセージ、およびパージに関する設定の制御を設定します。

フィールド	説明
アラートログの最大サイズ	パージが発生する前にアラートログで許容されるアラートの最大数を決定します。
警告が発行されるアラートログの最大サイズ	このサイズに達すると、警告アラートがアプリケーションログに送信されます。
アラートログが最大容量に達した時にパージする	最大サイズに達すると、指定数のアラートをパージします。

アラート表示フィルタ

メモ: Dell OpenManage Mobile アプリケーションをインストールしてセットアップすることにより、Android モバイルデバイスで OpenManage Essentials からのアラート通知を受信することができます。詳細に関しては、「OpenManage Mobile 設定」、および **dell.com/OpenManageManuals** の『Dell OpenManage Mobile ユーザーズガイド』を参照して下さい。

アラートフィルタ名

OpenManage Essentials では、アラート処置に関連付けられたアラートフィルタを使用してアラート機能を実装します。例えば、

- アラートの条件を満たした時に電子メールを送信する等の処置をトリガするよう、アラート処置の関連付けを作成することができます。
- 無視、除外、または両方の関連付けを作成して、SNMP トラップおよび CIM 表示を受け取った時にこれらを無視することができます。らの関連付けは、アラートの氾濫を抑制するために使用します。
- アラート表示フィルタを作成すると、**アラートログ** ビューをカスタマイズできます。

アラート処置の関連付けの作成の詳細については、「アラートの管理」を参照してください。

このウィンドウでは次のタスクを実行できます。

- 新しいアラート処置の関連付け、無視 / 除外フィルタ、およびアラート表示の関連付けの作成。
- アラート処置の関連付け、無視 / 除外フィルタの関連付け、およびアラート表示フィルタの概要情報の表示。
- アラート処置の関連付け、無視 / 除外の関連付け、およびアラート表示フィルタの編集、削除、名前の変更、コピー。

重大度

このページはアラートの重大性のリストを提供します。

フィールド	説明
名前	アイテムの名前（無視処置および表示フィルタの場合のみ適用可能）。
有効	選択してアラート処置を有効にします（無視処置のみに適用）。
重大度	使用可能なアラートの種類です。
すべて	これを選択して、すべてのアラートタイプを含めます。
不明	これを選択して、不明アラートを含めます。
情報	これを選択して、情報アラートを含めます。
正常	これを選択して、正常アラートを含めます。
警告	これを選択して、警告アラートを含めます。
重要	これを選択して、重要アラートを含めます。

確認

フィールド	説明
確認フラグに基づいてアラートを制限してください。	アラートが確認されたかどうかに基づいてアラートを表示するためにアラートビューフィルタを設定するには、このオプションを選択します。このオプションはデフォルトでは無効になっています。
確認済みアラートのみを一致させる	確認済みアラートを表示するには、このオプションを選択します。
未確認アラートのみを一致させる	確認されていないアラートを表示するには、このオプションを選択します。

概要 - アラート表示フィルタ

概要 ページは、**アラート表示フィルタ** ウィザードの最終ページに表示されるか、ツリーで **概要の表示** 右クリックオプションをクリックすると表示されます。

フィールド	説明
名前	アラート処置の名前です。
種類	アラート処置の種類（アプリケーションの起動、電子メール、無視、トラップ、および転送）です。
説明	アラート処置の説明です。

フィールド	説明
関連する重大度	アラートを一致させる際に使用されるアラートの重大度基準です。
関連するアラートカテゴリ	アラートを一致させる際に使用されるアラートのカテゴリ基準です。
関連するアラートソース	アラートを一致させる際に使用されるアラートのソース基準です。
関連するデバイスグループ	アラートを一致させる際に使用されるアラートのソースデバイスグループ基準です。
関連するデバイス	アラートを一致させる際に使用されるアラートのソースデバイス基準です。
関連付けられた日付範囲	アラートを一致させる際に使用されるアラートの日付範囲基準です。
関連付けられた時間範囲	アラートを一致させる際に使用されるアラートの時間範囲基準です。
関連付けられた日数	アラートを一致させる際に使用されるアラートの日数基準です。
関連性確認	有効の場合には、アラートに一致した際にアラート確認フラグを使用します。

アラート処置

アラート処置は、着信アラートがアラート処置で定義された特定の基準に一致するとトリガされます。アラートの一致基準には、次の基準が挙げられます。

- アラートの重大度。「重要度の関連付け」を参照してください。
- アラートカテゴリまたはソース。「カテゴリおよびソースの関連付け」を参照してください。
- アラートデバイスまたはデバイスグループソース。「デバイスの関連性」を参照してください。
- アラート日時、曜日。「日時範囲」を参照してください。

4 つのタイプのアラート処置があります。

- **アラートアプリケーションの起動処置** – アラート処置基準に一致すると、スクリプトまたはバッチファイルを起動します。
- **アラート電子メール処置** – アラート処置基準に一致すると、電子メールを送信します。
- **アラート無視処置** – アラート処置基準に一致すると、アラートを無視します。
- **アラートトラップ転送処置** – アラート処置基準に一致すると、SNMP トラップを別の管理コンソールに転送します。

新しい処置はデフォルトで有効になっています。アラート処置を削除せずにオフにする場合は、右クリックメニューまたはそのアラート処置の編集ウィザードを使用して無効にできます。

一般的な使用例を説明するために、複数の一般的なアラート処置の使用例が無効状態で事前にインストールされています。これらの事前にインストールされた処置を使用する場合には、この例のクローンを作成して、

ニーズに合った新しい処置を作成することを推奨します。この処理中に、新しい処置を有効にして、テストするようにしてください。

名前と説明

フィールド	説明
名前	アラート処置の名前です。
説明	電子メール処置の説明です。
有効	これを選択して、アラート処置を有効にします。

重要度の関連

フィールド	説明
重大度	使用可能なアラートの種類です。
すべて	これを選択して、すべてのアラートタイプを含めます。
不明	これを選択して、不明アラートを含めます。
情報	これを選択して、情報アラートを含めます。
正常	これを選択して、正常アラートを含めます。
警告	これを選択して、警告アラートを含めます。
重要	これを選択して、重要アラートを含めます。

アプリケーションの起動設定

このウィンドウでは、起動するアプリケーションや、起動をテストするアプリケーションを設定します。

メモ: アラート処置は、一致アラートが受信されたときに実行されます。したがってアラートアプリケーションの起動処置は、ユーザー操作を必要としないスクリプトまたはバッチファイルです。

フィールド	説明
実行ファイル名	アプリケーションプログラムを起動する実行ファイルの完全修飾パス名とファイル名を指定します。
引数	アプリケーションプログラムを起動するために必要、または使用したいコマンドラインパラメータを指定または編集します。次の変数置換を使用して引数フィールドに情報を指定できます。 • $n = システム名 • $ip = IP アドレス • $m = メッセージ

フィールド	説明
	• $d = 日付 • $t = 時刻 • $sev = 重大度 • $st = サービスタグ • $e = エンタープライズ OID • $sp = 指定のトラップ ID • $g = 一般トラップ ID • $cn = アラートカテゴリ名 • $sn = アラートソース名 • $pkn = パッケージ名 • $at = 管理タグ **実行可能ファイル**：実行可能ファイル（例えば、createTroubleTicket.exe）がある場合は、トラブルチケットをパラメーター –arg1、-arg2 などを付けて作成するには、アラートアプリケーションの起動を次のように設定します。 • 実行可能ファイル（フルパス）：C:\temp \createTroubleTicket.exe • 引数：-arg1 –arg2 アラート処置がトリガされると、コマンド C:\temp \createTroubleTicket.exe –arg1 -arg2 が実行され、関連付けられたアプリケーション起動アラート処置が実行されます。 **バッチファイル**：バッチファイル（例えば、createTroubleTicket.bat）がある場合は、トラブルチケットをパラメーター –arg1、-arg2 などを付けて作成するには、アラートアプリケーションの起動を次のように設定します。 • 実行可能ファイル（フルパス）：C:\temp \createTroubleTicket.bat • 引数：-arg1 –arg2 アラート処置がトリガされると、コマンド C:\temp \createTroubleTicket.bat –arg1 -arg2 が実行され、関連付けられたアプリケーション起動アラート処置が実行されます。 **VB スクリプト**：VB スクリプトファイルをアラート処置として設定するときは、実行可能ファイルと引数を次のように指定します。例えば、スクリプト（createTroubleTicket.vbs）がある場合、トラブルチケットをパラメーター arg1 を付けて作成するには、アプリケーション起動を次のように設定します。 • 実行可能ファイル名：cscript.exe または C:\Windows\System32\cscript.exe（フルパス） • 引数：C:\temp\createTroubleTicket.vbs arg1 アラート処置がトリガされると、コマンド cscript.exe C:\temp\ createTroubleTicket.vbs arg1

フィールド	説明
	が実行され、関連付けられたアプリケーション起動アラート処置が実行されます。 **メモ:** アラート処置が機能していない場合は、コマンドプロンプトで完全なコマンドを入力したことを確認してください。 詳細については、アプリケーションの起動 アラート処置のサンプルアラート処置を参照してください。
テスト処置	アプリケーションの起動をテストできます。 **メモ:** アラート処置は、一致アラートが受信されたときに実行されます。したがってアラートアプリケーションの起動処置は、ユーザー操作を必要としないスクリプトまたはバッチファイルです。

電子メール設定

お使いのデバイスのアラート関連性が特定のアラート条件を満たすたびに電子メールを受け取るように Essentials を設定できます。たとえば、警告アラートと重要アラートすべてについて電子メールメッセージを受け取りたい場合があります。

このウィンドウでは、電子メールのアラート処置を設定するパラメータを指定します。

フィールド	説明
宛先	会社の SMTP サーバーがサービス提供している電子メール受取人の有効な電子メールアドレスを指定します。
差出人	電子メールの発信元アドレスを指定します。
件名	テキストまたは使用可能なアラートトークンリンクを使用して電子メールの件名を指定します。
メッセージ	テキストまたは使用可能なアラートトークンリンクを使用して電子メールのメッセージを指定します。
電子メール設定	これを選択して、SMTP サーバー名前（または IP アドレス）を指定します。
テスト処置	電子メールの処置をテストできます。 **メモ:** テストメールを送信したら、その電子メールが正常に受信され、予期された内容であることを確認します。

メモ: アラートトークンは、アラート処置の発生時に置換されます。テスト処置については、置換されません。

メモ: 一部のポケットベルベンダーは、電子メールを使用した英数字の呼び出しをサポートしています。OpenManage Essentials も電子メールによる呼び出しオプションをサポートしています。

トラップ転送

簡易ネットワーク管理プロトコル（SNMP）トラップは、管理下デバイスでのセンサーや他の監視対象パラメーターのステータスに変化が生じたときに生成されます。これらのトラップを正しく転送するために、IP アドレスまたはホスト名で定義された SNMP トラップ宛先を設定する必要があります。オリジナルフォーマットと OMEssentials フォーマットの両方で SNMPv1 と SNMP v2 トラップを転送する方法の詳細に関しては、「アラートの転送使用事例シナリオ」を参照してください。

例えば、OpenManage Essentials を使用してアソシエーションを作成したり、トラップを Enterprise Manager に転送しているマルチティアの企業環境には、トラップ転送が適切な場合があります。

トラップをローカルで処理してから宛先に転送したり、単に宛先に転送したりします。

このウィンドウで、トラップ転送の設定でのパラメータを指定します。

フィールド	説明
送信先	エンタープライズ管理アプリケーションをホストしているシステムの IP アドレスまたはホスト名を指定します。
コミュニティ	宛先 IP アドレスまたはホスト名が属する SNMP コミュニティを指定します。
オリジナルフォーマットでのトラップの転送	このチェックボックスを選択して、OpenManage Essentials が受信したものと同じフォーマットでトラップを転送します。
テスト処置	指定のコミュニティ文字列を使用して、指定の送信先にテストトラップを転送します。

カテゴリおよびソースの関連性

OpenManage Essentials には、Dell 管理エージェント用に事前定義されて実装済みのアラートカテゴリおよびソースが多数あります。任意の事前定義されたアラートカテゴリまたはソースを選択して、アラート処置やフィルタに関連付けます。 カテゴリとアラートソースの詳細および完全なリストについては、「アラートカテゴリ」を参照してください。

デバイスの関連性

事前定義されたグループ（デバイスの種類）、カスタムグループ、特定のデバイス、またはデバイスクエリを選択できます。デバイスの関連は、現在、事前定義されたグループのみを対象にしています。

カスタムグループの場合、**カスタムグループの新規作成ウィザード** を使用してカスタムグループを作成します。作成したカスタムグループはツリーに表示されます。

デバイスクエリを使用するには、リストからクエリを選択します。

新規 をクリックして、デバイスを検索し、アラート処置に割り当てるための新規デバイスクエリを作成します。

クエリロジックを変更するには、**編集** をクリックします。

ツリーからグループまたはデバイスを選択すると、クエリオプションを使用して、選択内容に対する特有の基準を作成できます。

デバイスクエリオプション

フィールド	説明
クエリの選択	ドロップダウンリストからクエリを選択します。
新規	新しいクエリを追加します。
編集	既存のクエリを編集します。
すべてのデバイス	これを選択して、OpenManage Essentials で管理されているデバイスすべてを含めます。
クライアント	これを選択して、デスクトップ、ポータブル、ワークステーションなどのクライアントデバイスを含めます。
HA クラスタ	これを選択して、高可用性サーバークラスタを含めます。
KVM	これを選択して、KVM（キーボード、ビデオ、マウス）デバイスを含めます。
Microsoft 仮想化サーバー	これを選択して、Microsoft 仮想化サーバーを含めます。
モジュラーシステム	これを選択して、モジュラーシステムを含めます。
ネットワークデバイス	これを選択して、ネットワークデバイスを含めます。
OOB 分類されていないデバイス	これを選択して、Lifecycle コントローラ対応デバイスなど、帯域外の分類されていないデバイスを含めます。
電源デバイス	これを選択して、PDU および UPS サーバーを含めます。
プリンタ	このオプションを選択して、プリンタを含めます。
RAC	これを選択して、Remote Access controller を備えたデバイスを含めます。
サーバー	これを選択して、Dell サーバーを含めます。

フィールド	説明
ストレージデバイス	これを選択して、ストレージデバイスを含めます。
不明	これを選択して、不明デバイスを含めます。
VMware ESX サーバー	これを選択して、VMware ESX サーバーを含めます。

日時範囲

フィールド	説明
日付範囲を制限する	アラートに一致させる特定の日付範囲を指定します。
時間範囲を制限する	アラートに一致させる特定の時間範囲を指定します。
日付を制限する	これを選択して、アラートの関連付けを有効にする日付を指定します。このオプションを有効にしなかった場合、指定された期間中、関連付けが継続的に適用されます。 これらのフィールドはそれぞれ、相互に排他的です。したがって、8/1/11～10/1/11 の日付、午前 1 時～午前 4 時、金曜日を選択すると、この日付範囲の金曜日の午前 1 時～午前 4 時だけにアラートを一致させます。 **メモ:** 結果をもたらさない日付範囲および日付を入力することも可能です。例えば、9/1/11 と月曜日など（9/1/11 は木曜日なので、決して一致しません）。 これらのいずれもが選択されない場合、アラート選択には日付 / 時刻フィルタが設定されていないことを意味します。

アラート処置 - 重複アラートの相関性

フィールド	説明
このフィルタに一致する重複アラートのみが実行されます。	このオプションを有効にすると、指定された時間間隔内で受信された重複アラート（ID が同じで、送信元デバイスも同じ）は削除されます。このオプションを使用して、デバイスからコンソールにアラートが過剰に送信されるのを防ぎます。
期間中（1～600 秒）に受信した重複アラートの無視	これを選択して、時間を設定します。
なし	延長した期間内で重複アラートが実行されることを防ぐには、このオプションを選択します。

サマリ - アラート処置の詳細

選択内容を表示して、編集します。

アラート処置の詳細画面は、アラート処置ウィザードの最終ページに表示されるか、ツリーで任意のアラート処置をクリックすると表示されます。

アラート処置には、アラート処置の種類および選択したフィルタ基準に応じて、次のプロパティの一部が含まれます（多くの場合は表です）。

フィールド	説明
名前	アラート処置の名前です。
処置有効	アラート処置が有効か、無効かを指定します。
種類	アラート処置の種類（アプリケーションの起動、電子メール、無視、およびトラップ転送）です。
説明	アラート処置の説明です。
宛先	電子メール送信先の電子メールアドレスです。
差出人	電子メール発信元の電子メールアドレスです。
件名	電子メールの件名（アラートトークンを含む場合があります）です。
メッセージ	電子メールのメッセージです（アラートトークンを含む場合があります）。
送信先	トラップ転送に使用される送信先名または IP アドレスです。
コミュニティ	トラップ転送に使用されるコミュニティ文字列です。
実行ファイル名	アラート処置で使用される、実行可能ファイル、スクリプト、またはバッチファイルの名前です。
引数	アラート処置の呼び出しに使用されるコマンドライン引数です。
関連する重大度	アラートを一致させる際に使用されるアラートの重大度基準です。
関連するアラートカテゴリ	アラートを一致させる際に使用されるアラートのカテゴリ基準です。
関連するアラートソース	アラートを一致させる際に使用されるアラートのソース基準です。

フィールド	説明
関連するデバイスグループ	アラートを一致させる際に使用されるアラートのソースデバイスグループ基準です。
関連するデバイス	アラートを一致させる際に使用されるアラートのソースデバイス基準です。
関連付けられた日付範囲	アラートを一致させる際に使用されるアラートの日付範囲基準です。
関連付けられた時間範囲	アラートを一致させる際に使用されるアラートの時間範囲基準です。
関連付けられた日数	アラートを一致させる際に使用されるアラートの日数基準です。
最低限の繰り返し時間	有効の場合、同じデバイスからの 2 つの同じアラートの最低限の間隔を秒単位で指定します。

アラートカテゴリ

OpenManage Essentials には、Dell 管理エージェント用に事前定義されて実装済みのアラートカテゴリおよびソースが多数あります。

アラートカテゴリは **アラートカテゴリ** ツリーの組織レベルです。アラートソースは、各アラートの低レベルの詳細を指定します。アラートカテゴリとソースをモニタするには、アラート処置の関連付けをアラートソースまたはその親カテゴリに適用する必要があります。

このページは、カテゴリと、そのカテゴリ内のアラートソースを一覧表示します。このページを使用して、カテゴリに基づいたアラートを設定してください。

アラートカテゴリオプション

フィールド	説明
Brocade スイッチ	このカテゴリを選択して、Brocade スイッチに関するアラートを含めます。
Compellent	このカテゴリを選択して、Compellent ストレージデバイスに関するアラートを含めます。
Dell 高度インフラストラクチャ管理	このカテゴリを選択して、高度インフラストラクチャ管理に関するアラートを含めます。
環境	このカテゴリを選択して、温度、ファンエンクロージャ、ファン速度、サーマル、および冷却に関するアラートを含めます。
EqualLogic ストレージ	このカテゴリを選択して、EqualLogic ストレージに関するアラートを含めます。

フィールド	説明
FC スイッチ	このカテゴリを選択して、ファイバチャネルスイッチに関するアラートを含めます。
一般冗長性	このカテゴリを選択して、一般冗長性に関するアラートを含めます。
HyperV サーバー	このカテゴリを選択して、HyperV サーバーに関するアラートを含めます。
iDRAC	このカテゴリを選択して、iDRAC に関するアラートを含めます。
Juniper スイッチ	このカテゴリを選択して、Juniper スイッチに関するアラートを含めます。
キーボード - ビデオ - マウス（KVM）	このカテゴリを選択して、KVM に関するアラートを含めます。
メモリ	このカテゴリを選択して、メモリに関するアラートを含めます。
ネットワーク	このカテゴリを選択して、Dell Networking スイッチに関するアラートを含めます。
その他	このカテゴリを選択して、他のデバイスに関するアラートを含めます。
PDU	このカテゴリを選択して、PDU に関するアラートを含めます。
物理ディスク	このカテゴリを選択して、物理ディスクに関するアラートを含めます。
電源	このカテゴリを選択して、電源に関するアラートを含めます。
Power Center	このカテゴリを選択して、パワーセンターに関するアラートを含めます。
プリンタ	このカテゴリを選択して、プリンタに関するアラートを含めます。
プロセッサ	このカテゴリを選択して、プロセッサに関するアラートを含めます。
リムーバブルフラッシュメディア	このカテゴリを選択して、リムーバブルフラッシュメディアに関するアラートを含めます。
セキュリティ	このカテゴリを選択して、セキュリティに関するアラートを含めます。

フィールド	説明
ストレージエンクロージャ	このカテゴリを選択して、ストレージエンクロージャに関するアラートを含めます。
ストレージ周辺機器	このカテゴリを選択して、ストレージ周辺機器に関するアラートを含めます。
ストレージソフトウェア	このカテゴリを選択して、ストレージソフトウェアに関するアラートを含めます。
システムイベント	このカテゴリを選択して、システムイベントに関するアラートを含めます。
テープ	このカテゴリを選択して、テープドライブに関するアラートを含めます。
テストイベント	このカテゴリを選択して、テストイベントに関するアラートを含めます。
不明	このカテゴリを選択して、不明アラートに関連した状態を含めます。
UPS	このカテゴリを選択して、UPS に関するアラートを含めます。
仮想ディスク	このカテゴリを選択して、仮想ディスクに関するアラートを含めます。
VMware ESX サーバー	このカテゴリを選択して、VMware ESX サーバーに関するアラートを含めます。

アラートソース

各アラートカテゴリには、アラートソースが含まれています。アラートソースを表示するには、アラートカテゴリをクリックしてください。カテゴリを展開してアラートソースのリストを表示し、アラートソースを選択します。

フィールド	説明
名前	新しいアラートソースの名前です（例：myFanAlert）。
種類	プロトコル情報です。
カタログ	カタログ情報を提供します。
重大度	アラートソースが指定の SNMP トラップを生成する場合にトリガされるアラートに割り当てられた重大度を指定します。

フィールド	説明
文字列のフォーマット	アラートソースがアラートをトリガするのに十分な重大度があるアラートを生成する場合に、アラートログ に表示されるメッセージ文字列を提供します。フォーマットコマンドを使うと、一部のメッセージ文字列を指定できます。SNMP で有効なフォーマットコマンドは次のとおりです。 $n = システム名 $d = 日付 $t = 時刻 $s = 重大度 $e = エンタープライズオブジェクト識別子（OID） $sp = 指定のトラップ OID $g = 一般トラップ OID $1 - $# = varbind 値
SNMP Enterprise OID	監視するイベントソースを定義する管理情報ベース（MIB）ファイルのエンタープライズ OID（SNMP OID のプレフィックス）を提供します。
SNMP 一般トラップ OID	目的のイベントソースから監視する SNMP トラップの汎用トラップ ID を提供します。SNMP トラップの詳細については、**dell.com/OpenManageManuals** で『Dell OpenManage Server Administrator SNMP リファレンスガイド』を参照してください。
SNMP 指定トラップ OID	目的のイベントソースから監視する SNMP トラップの特定のトラップ ID を提供します。SNMP トラップの詳細については、**dell.com/OpenManageManuals** で『Dell OpenManage Server Administrator SNMP リファレンスガイド』を参照してください。

18

サーバーの BIOS、ファームウェア、ドライバ、およびアプリケーションのアップデート

OpenManage Essentials のシステムアップデート機能によって、次のことが可能です。

- ファームウェアドライバ、BIOS、アプリケーション、および OpenManage Server Administrator のアップグレードおよびダウングレード。
- インベントリされたサーバーおよびモジュラブレードエンクロージャのドライバおよびファームウェアのソースカタログとの比較、および必要に応じたアップデート。

  メモ: システムアップデートは、LAN 上でのみサポートされており、WAN 上ではサポートされていません。データセンター外のデバイスにシステムアップデートを適用するには、そのエリアでローカルとなる別の OpenManage Essentials インスタンスをインストールしてください。ターゲットサーバーにアップデートが適用されるとインベントリが自動的に開始されます

  メモ: OpenManage Essentials は、Lifecycle Controller 搭載の iDRAC を使用した Dell PowerEdge 11 世代、12 世代、13 世代のサーバーでのシステムアップデートをサポートします。
- **フィルタ基準** オプションをクリックしてデバイスをフィルタリングします。クエリを選択するか、デバイスツリーからデバイス / グループを選択することもできます。

システムをアップデートする前に、次の必要条件をチェックしてください。

- オンラインカタログソースを使用する場合は、インターネットがアクセス可能で、**dell.com**（ポート 80）および **ftp.dell.com**（ポート 21）にアクセスできること。
- DNS が解決されていること。

メモ: システム資格情報を入力する際に、ユーザー名にスペースまたはピリオドが含まれる場合は、ユーザー名を引用符で囲む必要があります（例："localhost\johnny marr" または "us-domain\tim verlaine"）。スペースとピリオドは、OpenMange System Administrator タスク、一般的なコマンドラインタスク（ローカルシステム）、OpenManage Systems Administrator 導入タスクのユーザー名で使用可能です。システムアップデート（帯域内、OpenManage System Administrator 経由）もスペースとピリオドをサポートしています。帯域外アップデート（RAC デバイス経由）または RACADM などのコマンドではユーザー名のスペースとピリオドをサポートしていません。

メモ: 導入タスクが BIOS システムパスワードで構成されているターゲットサーバーで実行されている場合、タスク実行中に、iDRAC 仮想コンソールを起動し、プロンプトが表示されたら、システムパスワードを入力してください。表示されない場合、タスク実行状態がしばらく表示されて最終的にはタイムアウトする可能性があります。

システムアップデートページの表示

システムアップデートページを表示するには、**管理 → システムアップデート** をクリックします。

デフォルトでは、システムアップデートページにすべての検出済みサーバーが表示されます。**フィルタ基準:** リンクをクリックしてデバイスをフィルタし、デバイスまたはデバイスグループを表示することができます。

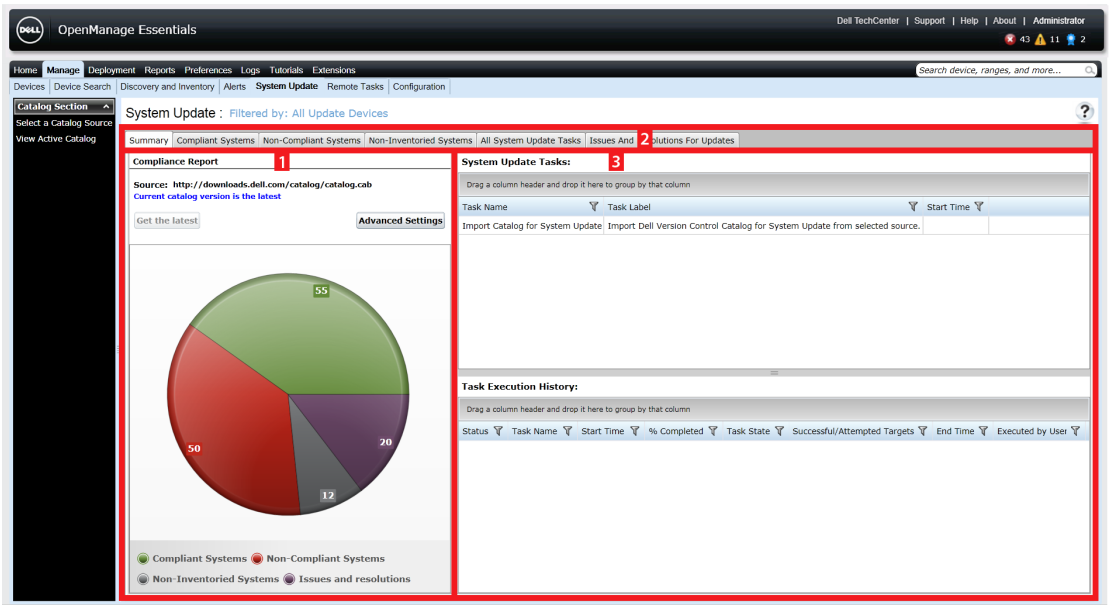


図 7. システムアップデートページ

1. 準拠レポート。「準拠レポート」を参照してください。
2. タブ化されたシステム情報です。「対応システム」、「非対応システム」、「インベントリ未施行システム」、および「問題と解決策」を参照してください。
3. システムアップデートタスク。「すべてのシステムアップデートタスク」を参照してください。

サーバー BIOS ファームウェアとドライバソースについて

サーバー用のファームウェアおよびドライバを取得するためのソースは複数あります。

- **オンラインソース** — 最新バージョンのドライバおよびファームウェアを **ftp.dell.com** から取得するデフォルトオプションです。

  メモ: OpenManage Essentials は、自動的にアップデートをチェックし、新しいバージョンが使用可能な場合、メッセージを表示します。
- **ファイルシステムのソース** — Dell OpenManage Server Update Utility（SUU）メディアのドライバおよびファームウェアです。
- **Repository Manager ファイル** — Dell Repository Manager ツールから生成された、特定のドライバとファームウェアのカスタマイズされた選択です。

アップデートのための正しいソースの選択

- **推奨オプション** — オンラインソースを使用して、デルから提供されている最新のドライバおよびファームウェアバージョンを常時維持するようにするか、ドライバとファームウェアの適合セットには、Dell Server Update Utility（SUU）オプションを使用します。
- **カスタムカタログの作成** — このオプションを使用すると、SUU メディア、または Dell Repository Manager を使用したオンラインソースからドライバとファームウェアを個別に選択することができるため、お使いの環境内のドライバとファームウェアのリビジョンに対する最大限の管理が可能になります。独立したツールである Repository Manager は、OpenManage Essentials インストールパッケージからインストールすることができます。

カタログソースのアップデートの選択

1. OpenManage Essentials で、**管理** → **システムアップデート** → **カタログソースの選択** の順にクリックします。
2. **カタログソースの選択** でオプションを選択し、次に **今すぐインポート** をクリックします。

比較結果の表示

この項では、デバイスとソースカタログの比較結果を表示するのに必要な情報が記載されています。

対応サーバーの表示

対応サーバーを表示するには、次の手順を行います。

1. **管理** → **システムアップデート** をクリックします。
2. **システムアップデート** で、**対応システム** タブを選択します。

非対応サーバーの表示

非対応サーバーを表示するには、次の手順を行います。

1. **管理** → **システムアップデート** をクリックします。
2. **システムアップデート** で、**非対応システム** タブを選択します。
   ドライバとファームウェアのバージョンが、カタログと異なるサーバーが表示されます。

インベントリ未施行サーバーの表示

インベントリ未施行サーバーを表示するには、次の手順を行います。

1. **管理** → **システムアップデート** をクリックします。
2. **システムアップデート** で、**インベントリ未施行システム** タブを選択します。
   インベントリ未施行サーバーが表示されます。

   メモ: CMC ファームウェアのアップデート（CMC アクティブコントローラのみ）もこれらの結果に表示されます。

サーバーの問題と解決策の表示

サーバーの問題と解決策を表示するには、次を実行します。

1. **管理** → **システムアップデート** をクリックします。
2. **システムアップデート** で、**アップデートの問題と解決策** タブを選択します。
   サーバーの問題と解決策が表示されます。詳細に関しては、「問題と解決策の使用事例シナリオ」を参照してください。

システムアップデート使用例シナリオ

下記の表は、異なるプロトコルとアップデートモードに基づいた、システムアップデートの発生のしくみに関する使用例シナリオの一覧です。

メモ: 詳細設定 で選択された優先システムアップデート方法が、**帯域内（オペレーティングシステム）** になっており、OpenManage Server Administrator（OMSA）がターゲットサーバーにインストールされている場合は、コンポーネントは OMSA を使用してアップデートされます。OMSA がターゲットサーバーにインストールされていない場合は、コンポーネントはオペレーティングシステムを通じてアップデートされます。

サーバー IP 検出とインベントリに使用するプロトコル	iDRAC IP 検出とインベントリに使用するプロトコル	詳細設定で選択した優先システムアップデートモード	システムアップデートの資格情報	実際のアップデートモード
snmp	snmp	帯域内（オペレーティングシステム）	サーバー	すべてのコンポーネントは OpenManage Server Administrator を使ってアップデートされます。 **メモ:** iDRAC IP の検出に SNMP が使用された場合、iDRAC ソフトウェアインベントリは取得されず、すべてのコンポーネントは選択された優先システムアップデートモードに関係なく Server Administrator を使ってアップデートされます。
snmp	snmp	帯域外（iDRAC）	サーバー	
WMI	snmp	帯域内（オペレーティングシステム）	サーバー	すべてのコンポーネントは OpenManage Server Administrator を使ってアップデートされます。
WMI	snmp	帯域外（iDRAC）	サーバー	iDRAC 検出とインベントリに使用されたプロトコルが SNMP であるため、すべてのコンポーネントの更新には Server Administrator が使用されます。
WMI	snmp	帯域内（オペレーティングシステム）	サーバー	すべてのコンポーネントは、オペレーティングシステムを使用してアップデートされます。
SSH	WS-Man/SNMP	帯域内（オペレーティングシステム）	サーバー	すべてのコンポーネントは、オペレーティングシステム

サーバー IP 検出とインベントリに使用するプロトコル	iDRAC IP 検出とインベントリに使用するプロトコル	詳細設定で選択した優先システムアップデートモード	システムアップデートの資格情報	実際のアップデートモード
				を使用してアップデートされます。
snmp	WS-MAN	帯域内（オペレーティングシステム）	サーバー	すべてのコンポーネントは OpenManage Server Administrator を使ってアップデートされます。
snmp	WS-MAN	帯域外（iDRAC）	iDRAC	BIOS、ファームウェア、およびアプリケーションは iDRAC を使ってアップデートされます。 **メモ:** iDRAC IP の検出に WS-Man が使用された場合、iDRAC ソフトウェアインベントリが取得され、コンポーネントは iDRAC を使用してアップデートされます。 ただし、BIOS、ファームウェア、およびアプリケーションに加えてドライバも存在する場合、すべてのコンポーネントのアップデートには iDRAC ではなく Server Administrator が使用されます。
WMI	WS-MAN	帯域内（オペレーティングシステム）	サーバー	すべてのコンポーネントは OpenManage Server Administrator を使ってアップデートされます。
WMI	WS-MAN	帯域外（iDRAC）	iDRAC	BIOS、ファームウェア、およびアプリケーションは iDRAC を使ってアップデートされます。 **メモ:** iDRAC IP の検出に WS-Man が使用された場合、iDRAC ソフトウェアインベントリが取得され、コンポーネントは iDRAC を使用してアップデートされます。

サーバー IP 検出とインベントリに使用するプロトコル	iDRAC IP 検出とインベントリに使用するプロトコル	詳細設定で選択した優先システムアップデートモード	システムアップデートの資格情報	実際のアップデートモード
				ただし、BIOS、ファームウェア、およびアプリケーションに加えてドライバも存在する場合、すべてのコンポーネントのアップデートには iDRAC ではなく Server Administrator が使用されます。
WS-Man（ESXi ベースのサーバー）	WS-Man（ESXi ベースのサーバー）	帯域内（オペレーティングシステム）	iDRAC	すべてのコンポーネントは iDRAC を使用してアップデートされます。ESXi ベースのサーバーについては、選択された優先システムアップデートモードに関係なく iDRAC によってアップデートされます。
WS-Man（ESXi ベースのサーバー）	WS-Man（ESXi ベースのサーバー）	帯域外（iDRAC）	iDRAC	
適用できません。サーバー IP が検出されません。	WS-MAN	帯域内（オペレーティングシステム）	iDRAC	すべてのコンポーネントは iDRAC を使ってアップデートされます。
適用できません。サーバー IP が検出されません。	WS-MAN	帯域外（iDRAC）	iDRAC	

システムアップデートの適用

メモ: システムアップデートを適用する際に、次の事項を考慮する必要があります。

- システムの検出に WS-Man プロトコルが使用された場合、iDRAC6 以降でのみアップデートできます。
- システムアップデートの帯域外（iDRAC）の適用は、32 ビット Dell アップデートパッケージ（DUP）に対してのみサポートされています。帯域外システムアップデートの適用に対して 32 ビット DUP のないカタログを選択した場合、OpenManage Essentials の **適用するアップデートの選択** にアップデートが表示されません。
- 帯域内のシステムアップデート帯域内（オペレーティングシステム）を適用するには、選択したターゲット上で **Windows Management Instrumentation** サービスが実行されている必要があります。
- システムアップデートを適用するには、デフォルトの **Temp** フォルダ （**C:\Users\<username>\AppData\Local\Temp**）が使用可能になっている必要があります。**Temp** が削除されたり移動されたりしていないことを確認してください。
- 帯域外システムアップデートについては、OpenManage Essentials がインストールされているシステムと iDRAC が同じネットワークドメイン上にある必要があります。異なるネットワークドメイン上にある場合は、システムアップデートタスクを正常に実行できません。

システムアップデートを適用するには、以下の手順を実行します。

1. **管理 → システムアップデート** をクリックします。
2. **システムアップデート** で、**非対応システム** タブを選択します。

   メモ: フィルタ基準 : リンクをクリックすることにより、グループまたはデバイスに基づいてシステムをフィルタできます。**システムアップデートターゲットデバイスおよびデバイスグループの選択** ウィンドウでデバイスを選択してから、**適用** をクリックします。
3. **非対応システム** で、アップデートしたいシステムを選択します。

   メモ: 同時に複数のシステムをアップデートできます。

   メモ: システムアップデートに 64 ビットの DUP を使用する際には、次の内容を考慮します。

   - 帯域内のアップデートの場合（オペレーティングシステム）– 選択したターゲットが、Windows の 64 ビットオペレーティングシステムを実行しているサーバーの場合は、アップデートに該当するすべての 64 ビットパッケージが利用可能です。カタログにコンポーネント用の 64 ビットパッケージが含まれていない場合は、対応する 32 ビットパッケージがアップデートに利用可能です。
   - 帯域外のアップデートの場合（iDRAC）- 選択したターゲットが、Dell PowerEdge 12 世代または 13 世代サーバーの iDRAC であり、iDRAC のファームウェアバージョンが 1.40.40 以降である場合は、アップデートに該当するすべての 64 ビットパッケージが利用可能です。カタログにコンポーネント用の 64 ビットパッケージが含まれていない場合は、対応する 32 ビットパッケージがアップデートに利用可能です。
   - 帯域内または帯域外のアップデートの場合 - 選択した PowerEdge 12 世代または 13 世代のサーバーが 32 ビットのオペレーティングシステムを実行しており、iDRAC のファームウェアバージョンが 1.40.40 以降である場合、iDRAC のみに対応し OMSA には非対応のパッケージがない限り、デフォルトで 32 ビットのパッケージのみがアップデートに利用可能です。
4. **選択したアップデートを適用** をクリックします。

アップデートをスケジュールするためのウィンドウが表示されます。

メモ: シャーシおよびブレードは、アップデートに関連付けられません。これらは、個々のコンポーネントとして扱われるので、手動で選択する必要があります。

メモ: シャーシ、ブレードサーバー BIOS、および iDRAC バージョンの相互依存管理機能はありません。

5. タスク名を入力します。
6. 選択したアップデートを確認します。
7. タスクスケジュールを **今すぐ実行** に設定するか、特定の日時に設定します。
8. 変更をただちに適用しない場合は、**アップデート後は、必要に応じてデバイスを再起動します** をクリアします。変更は、次回再起動するまで有効になりません。
9. システムアップグレードパッケージで署名とハッシュのチェックをスキップする場合は、**署名とハッシュのチェックをスキップ** を選択します。
10. 管理対象サーバーに、オペレーティングシステムのシステム管理者または iDRAC 資格情報を入力します。

    メモ: ユーザーアカウント制御（UAC）機能が有効になっている Windows オペレーティングシステムを実行しているターゲットシステム上でシステムアップデートを適用する場合：

    - ターゲットシステムがドメインの一部である場合は、ドメイン管理者または管理者グループ内メンバーの資格情報を入力する必要があります。アカウントが管理者グループ内にある場合でも、ターゲットシステムのローカル、非ドメインアカウントの資格情報を入力しないでください。
    - ターゲットシステムがドメインの一部でない場合、管理者の資格情報を入力する必要があります。非デフォルトの管理者アカウントの資格情報を入力したい場合は、そのユーザーアカウントでリモート WMI 許可が有効になっていることを確認してください。

    例：Windows ドメイン環境では、<ドメイン\システム管理者> およびパスワードを入力します。
    Windows ワークグループ環境では、<ローカルホスト\システム管理者> およびパスワードを入力します。

    Linux 環境では、ルートおよびパスワードを入力します。sudo を使用してシステムアップデートを適用するには、**Sudo を有効にする** を選択して **SSH ポート番号** をアップデートします。

    メモ: sudo を使用してシステムアップデートを適用する前に、新しいユーザーアカウントを作成し、`visudo` コマンドを使用して **sudoers** ファイルを編集し、以下を追加します。

    32 ビットオペレーティングシステムを実行するターゲットシステム：

    ```
    Cmnd_Alias OMEUPDATE = /bin/tar,/opt/dell/srvadmin/bin/omexec,/tmp/
    LinuxPreInstallPackage/runbada,/tmp/LinuxPreInstallPackage/omexec,/tmp/
    invcol.bin <sudo_username> ALL=OMEUPDATE,NOPASSWD:OMEUPDATE
    ```

    64 ビットオペレーティングシステムを実行するターゲットシステム：

    ```
    Cmnd_Alias OMEUPDATE = /bin/tar,/opt/dell/srvadmin/bin/omexec,/tmp/
    LinuxPreInstallPackage64/runbada,/tmp/LinuxPreInstallPackage64/
    omexec,/tmp/invcol64.bin <sudo_username>
    ALL=OMEUPDATE,NOPASSWD:OMEUPDATE
    ```

    メモ: SUSE Linux Enterprise Server ターゲットでは、sudo を使用したシステムアップデートの適用はサポートされていません。
11. **終了** をクリックします。

メモ: Windows と Linux のアップデートを、同じタスクを使用してスケジュールすることはできません。それぞれに個別のタスクを作成してください。

アップデート状態の表示

アップデートが正常に適用されたことを表示および確認するには、**管理 → システムアップデート → サマリ** をクリックします。**タスクの実行履歴** ペインは、アップデートが正常に適用されたかどうかを表示します。

OMSA を使用しないファームウェア、BIOS、ドライバのアップデート

OMSA がインストールされていないシステムでファームウェア、BIOS、ドライバをアップデートするには、次の操作を実行します。

1. ソフトウェアのインベントリをサーバーから収集します。「ソフトウェアインベントリの収集」を参照してください。
2. システムアップデートポータルを介してシステムをアップデートします。「システムアップデートの適用」を参照してください。

アクティブなカタログの表示

ソフトウェアアップデートを適用するために現在使用されているカタログファイルを表示するにはこのオプションを選択します。

フィールド	説明
ソース	ソースを表示します。ソースは、Server Update Utility、FTP、または Repository Manager のいずれかです。
ソースタイプ	カタログファイルが取得されるソースの種類です。例えば、Dell ftp サイトなどです。
リリース ID	リリースされたカタログファイルに割り当てられた固有の識別番号です。
リリース日	カタログファイルがリリースされた日です。
新しいバージョンが利用可能	新しいバージョンが利用可能かどうか表示します。

問題と解決の使用事例シナリオ

以下の表は、**アップデートの問題と解決策** タブに表示される問題の詳細情報を示しています。

問題	解決策
SNMP または IPMI を使用して PowerEdge VRTX のインベントリが実行された。	PowerEdge VRTX の検出とインベントリは、WS-Man を使用して実行してください。
SNMP または IPMI を使用して iDRAC のインベントリが実行された。	WS-Man を使用して iDRAC の検出とインベントリを実行してください。
iDRAC が最低バージョン要件を満たしていない。	モジュラーサーバーでサポートされている iDRAC の最低バージョンは 2.20 で、モノリシックサーバーの場合は 1.4 です。続行するには、必要な iDRAC バージョンを手動でインストールしてください。
iDRAC に必要なライセンスがない。	iDRAC には、Dell License Manager を使用して取得できるシステムアップデートを実行するためのライセンスが必要です。
サーバーに Server Administrator がインストールされていないか、SSH を使用して検出された。この問題は以下の場合に発生します。 • Server Administrator がインストールされていない Windows ベースのサーバーが WMI を使用して検出された。 • Server Administrator がインストールされている、またはインストールされていない Linux ベースのサーバーが SSH を使用して検出された。	インベントリ収集タスクをスケジュールしてください。定期的なインベントリ収集タスクのスケジュールが推奨されます。

19

システムアップデート - 参照

次にアクセスすることが可能です。

- システムアップデートページ
  - 概要
    - 準拠レポート
    - システムのアップデートタスク
    - タスク実行の履歴
  - 対応システム
  - 非対応システム
  - インベントリ未施行システム
  - すべてのシステムアップデートタスク
  - アップデートの問題と解決策
- カタログセクション
  - カタログソースの選択
  - アクティブなカタログの表示

関連リンク

サーバーの BIOS、ファームウェア、ドライバ、およびアプリケーションのアップデート
システムアップデートページの表示
準拠レポート
非準拠システム
システムアップデートタスク
インベントリ未施行システム
すべてのシステムアップデートタスク
問題と解決策

フィルタオプション

フィルタオプション	説明
と同じ	これを選択して、*同等*ロジックを作成します。
と異なる	これを選択して、不一致ロジックを作成します。
で開始	これを選択して、テキスト群の文頭にある英数字に基づいたフィルタ検索を行います。フィールドに開始英数文字を入力します。

フィルタオプション	説明
で終わる	これを選択して、テキスト群の文末にある英数字に基づいたフィルタ検索を行います。フィールドに終了英数文字を入力します。
を含む	これを選択して、テキスト群に現在含まれている英数文字に基づいたフィルタ検索を行います。フィールドに英数文字を入力します。
を含まない	これを選択してテキスト群に存在する英数文字に基づいた検索に*未存在*ロジックを含めます。
に含まれる	これを選択して、英数文字列に*存在*ロジックを含めます。
に含まれない	これを選択して、英数文字列に*未存在*ロジックを含めます。
より小記号 (<)	入力した値*より小さい*値を探して選択します。
より小か等しい記号 (< =)	入力した値*以下の*値を探して選択します。
より大記号 (>)	入力した値*より大きい*値を探して選択します。
より大か等しい記号 (< =)	入力した値*以上の*値を探して選択します。

システムアップデート

このページは次の情報を提供します。

- 概要
- 対応システム
- 非対応システム
- インベントリ未施行システム
- すべてのシステムアップデートタスク
- アップデートの問題と解決策

関連リンク

準拠レポート
非準拠システム
インベントリ未施行システム
すべてのシステムアップデートタスク

準拠レポート

準拠レポートは、ソフトウェアアップデートタスクの円グラフ分布を提供します。円グラフの一部分をクリックして、そのシステムについての詳細情報を表示します。

関連リンク

システムアップデート

準拠レポートオプション

フィールド	説明
ソース	レポートソース
最新を取得	このオプションは、カタログバージョンが最新の場合は無効になります。そうでない場合は、有効になります。このオプションをクリックして最新のカタログバージョンを取得します。
詳細設定	これらのオプションを使用することで、ファームウェア、BIOS、ドライバおよびアプリケーションのバージョンのアップグレードおよびダウングレードに対するプリファランスを設定することができます。 • **ダウングレードの有効化** – このオプションを選択して、システムにインストールされているファームウェアおよび BIOS、ドライバおよびアプリケーションのバージョンより前のバージョンをインストールします。 • **ダウングレードの無効化** – このオプションはデフォルトで設定されており、これを選択すると、システムにインストールされているファームウェアおよび BIOS、ドライバ、およびアプリケーションのバージョンより新しいバージョンをインストールできます。 また、次のアップデートモードのいずれかをデフォルトに設定できます。 • OpenManage Server Administrator—システムの全コンポーネントをアップデートできます。 • iDRAC—BIOS、ファームウェア、およびアプリケーションのみをアップデートできます。 **メモ:** アップデートモードのいずれかをデフォルトモードに設定できますが、実際のアップデートモードは使用するプロトコルとアップデートするコンポーネントによって異なります。詳細に関しては「システムアップデート使用事例シナリオ」を参照してください。
システム情報 - 円グラフフォーマット	円グラフは、既存のカタログファイルと比較したシステムの状態をリストします。次のシステムがリストされます。 • 準拠システム • 非準拠システム • インベントリ未施行システム • 問題と解決策
準拠システム	ソフトウェアアップデートを示したアクティブなカタログで使用可能なバージョンと比較して、ソフトウェアが最新のシステムです。対応システムの部分をクリックし、**対応システム** タブに詳細情報を表示します。

フィールド	説明
非準拠システム	ソフトウェアアップデートを示したアクティブなカタログで使用可能なバージョンと比較して、アップデートが必要なソフトウェアのあるシステムです。対応システムの部分をクリックし、**非準拠システム** タブに詳細情報を表示します。
インベントリ未施行システム	アクティブなカタログで使用可能なバージョンと比較して、インベントリ保留中が検出されたシステムです。インベントリ未施行部分をクリックして、**インベントリ未施行システム** タブに詳細情報を表示します。

準拠システム

システムシステム タブでは、この情報が提供されます。

フィールド	説明
システム名	システムのドメイン名です。
モデルタイプ	デバイスモデル情報です。
オペレーティングシステム	サーバーで実行されているオペレーティングシステムです。
サービスタグ	サービスライフサイクルを提供する固有の識別子です。
検出された時間	検出された日付と時間です。
インベントリ日時	インベントリされた日付と時間です。
サーバーサブネットの位置	IP アドレスの範囲情報です。

非準拠システム

非準拠システムタブでは、次の情報が提供されます。

フィールド	説明
システム名	システムのドメイン名です。
モデルタイプ	システムのモデル名です。例えば、Dell PowerEdge があります。
オペレーティングシステム	システムにインストールされているオペレーティングシステムです。
サービスタグ	サービスライフサイクル情報を提供する固有の識別子です。

フィールド	説明
アップデート方法	OpenManage Server Administrator および iDRAC などのアップデート方法を表示します。
検出された時間	検出された日付と時間です。
インベントリ日時	インベントリされた日付と時間です。

非準拠システムを選択して適用するアップデートを選択し、**選択したアップデートを適用** をクリックします。

フィールド	説明
システム名	システムのドメイン名です。
重要	システム用のソフトウェアアップデートの要件です。
アップデート方法	OpenManage Server Administrator および iDRAC などのアップデート方法を表示します。
コンポーネント	ソフトウェア情報です。
種類	ソフトウェアアップデートの種類です。
インストールされたバージョン	インストールされたバージョン番号です。
アップグレード / ダウングレード	緑の矢印は、およびアップグレードを示します。
使用可能なバージョン	使用可能なバージョン番号です。
パッケージ名	ソフトウェアアップデートの名前です。

関連リンク

システムアップデート

システムアップデートタスク

フィールド	説明
タスク名	ソフトウェアアップデートタスクに名前を付けます。
アップデートするシステムの選択	アップデートするシステムを選択します。
システム名	システムのドメイン名です。
重要性	システム用のソフトウェアアップデートの要件です。

フィールド	説明
配信モード	OpenManage Server Administrator および iDRAC などの配信方法を表示します。
コンポーネント	ソフトウェア情報です。
種類	ソフトウェアアップデートの種類です。
インストールされたバージョン	インストールされたバージョン番号です。
アップグレード / ダウングレード	緑の矢印は、およびアップグレードを示します。
使用可能なバージョン	使用可能なバージョン番号です。
パッケージ名	ソフトウェアアップデートの名前です。
タスクスケジュールの設定	
今すぐ実行	**終了** をクリックする時にこのタスクを実行する場合は、このオプションを選択します。
アップデート後は、必要に応じてデバイスを再起動します。	ソフトウェアのアップデートタスクが完了してからシステムを再起動する場合は、このオプションを選択します。
スケジュールの設定	これを選択し、必要な日時にタスクをスケジュールします。このアイコンをクリックして、日付および時間を設定します。
署名とハッシュのチェックをスキップ	システムアップグレードパッケージで署名とハッシュのチェックをスキップするには、このオプションを選択します。
タスク実行のための資格情報入力	
Sudo を有効にする	sudo を使ってシステムをアップデートするには、このオプションを選択します。
SSH ポート番号	SSH ポート番号を設定します。
サーバーユーザー名	選択したターゲットのサーバーユーザー名を設定します。
サーバーパスワード	選択したターゲットのサーバーパスワードを設定します。
iDRAC ユーザー名	選択したターゲットの iDRAC ユーザー名を設定します。
iDRAC パスワード	選択したターゲット iDRAC パスワードを設定します。

インベントリ未施行システム

インベントリ未施行システム タブは、インベントリが必要なシステムの一覧を提供します。システムのインベントリを行うには、システムを選択して **インベントリ** をクリックします。

フィールド	説明
システム名	システムのドメイン名です。
検出された時間	検出された日付と時間です。
インベントリ日時	インベントリされた日付と時間です。
サーバーサブネットの位置	IP アドレスの範囲情報です。

関連リンク

サーバーの BIOS、ファームウェア、ドライバ、およびアプリケーションのアップデート
システムアップデートページの表示
システムアップデート - 参照
システムアップデート

システムのインベントリ

システムをインベントリするには、**インベントリを行うシステム** を選択し、**インベントリの実行** をクリックします。

すべてのシステムアップデートタスク

このページは、ソフトウェアアップデートタスクに関する追加情報を提供します。

フィールド	説明
タスク名	タスクの名前です。
タスクラベル	タスクが何を行うかについての情報を提供します。
開始時刻	インベントリされた日付と時間です。

関連リンク

システムアップデート

問題と解決策

フィールド	説明
システム名	システムのドメイン名を表示します
理由	サーバーに関連付けられた問題を表示します。

フィールド	説明
推奨	問題を解決するための解決策を表示します。

関連リンク

サーバーの BIOS、ファームウェア、ドライバ、およびアプリケーションのアップデート
システムアップデートページの表示
システムアップデート - 参照

タスクの実行履歴

システムアップデートタスクまたはリモートタスクの詳細をリストします。

フィールド	説明
状態	タスクの状態を示すアイコンを表示します。  – 実行中または保留中  – 完了  – 停止  – 失敗  – 警告
タスク名	タスクの名前です。
開始時刻	システムのアップデートタスクが開始される時間と日付です。
% 完了	タスクの進捗情報です。
タスク状況	これらのタスクの状況を提供します。 • 実行中 • 完了 • 停止 • 失敗 • 警告  **メモ:** システムのアップデートタスクの **アップデート後は、必要に応じてデバイスを再起動します** のオプションが選択されていない場合、タスクのステータスに警告が表示されます。
成功 / 試行対象ターゲット	タスクが正常に実行されたターゲットシステムの数です。

フィールド	説明
終了時刻	システムのアップデートタスクが終了する時間と日付です。
ユーザーにより実行済み	ユーザー情報です。

カタログソースの選択

ソフトウェアのアップデートには、これらのオプションを選択して Dell FTP サイトにあるデフォルトのカタログファイルを使用するか、代替となるソフトウェアアップデートパッケージファイルを提供します。

フィールド	説明
ファイルシステムソースを使用（SUU）	これを選択し、Server Update Utility を使用してソフトウェアをアップデートします。**参照** をクリックしてファイルの場所にトラバースします。**catalog.cab** ファイルは、リポジトリフォルダ内にあります。
Repository Manager ファイルを使用	これを選択し、Repository Manager ファイルを使用してソフトウェアをアップデートします。**参照** をクリックしてファイルの場所にトラバースします。**catalog.cab** ファイルは、リポジトリフォルダ内にあります。
オンラインソースを使用	これを選択し、Dell FTP サイトにあるソフトウェアアップデートパッケージを使用してソフトウェアをアップデートします。

メモ: SUU または Repository Manager を使用してカタログをインポートする場合、カタログファイルへのパスが画面に表示されることがあります。ただし、**参照** をクリックしてカタログファイルを手動で選択することをお勧めします。

Dell Update Package

Dell Update Package（DUP）は、システム上にある単一のソフトウェア要素をアップデートする、標準パッケージフォーマットでの自己完結型実行ファイルです。DUP は、Dell PowerEdge システム、Dell デスクトップ、および Dell ノートブック上の特定のソフトウェアコンポーネントをアップデートするために Dell が提供するソフトウェアユーティリティです。カスタム化されたバンドルおよびリポジトリは、サポートされるオペレーティングシステム、アップデートの種類、フォームファクタおよび業務に基づいた DUP で構成されます。

Dell OpenManage Server Update Utility

Dell OpenManage Server Update Utility（SUU）は、システム用のアップデートを識別し、それを適用する DVD ベースのアプリケーションです。SUU は、バージョンの比較レポートを表示し、コンポーネントをアップデートするための多様なオプションを提供します。

Repository Manager

Repository Manager は、サポートされる Microsoft Windows または Linux オペレーティングシステムを実行するシステムのために、カスタム化されたバンドルおよびアップデートのリポジトリと、関連アップデートのグループを作成することが可能になるアプリケーションです。これにより、比較レポートの生成、およびリポジトリのアップデートベースラインの確立が容易になります。Repository Manager を使用することによって、お使いの Dell PowerEdge システム、Dell デスクトップ、または Dell ノートブックに最新の BIOS、ドライバ、ファームウェアおよびソフトウェアアップデートが搭載されていることを確実にすることができます。

アクティブなカタログの表示

ソフトウェアアップデートを適用するために現在使用されているカタログファイルを表示するにはこのオプションを選択します。

フィールド	説明
ソース	ソースを表示します。ソースは、Server Update Utility、FTP、または Repository Manager のいずれかです。
ソースタイプ	カタログファイルが取得されるソースの種類です。例えば、Dell ftp サイトなどです。
リリース ID	リリースされたカタログファイルに割り当てられた固有の識別番号です。
リリース日	カタログファイルがリリースされた日です。
新しいバージョンが利用可能	新しいバージョンが利用可能かどうか表示します。

20

リモートタスクの管理

リモートタスクについて

OpenManage Essentials のリモートタスク機能によって、次のことが可能です。

- ローカルおよびリモートシステムでのコマンドの実行、ローカルシステムでのバッチファイルおよび実行可能ファイルの実行、およびローカルとリモートタスクのスケジュール。

  メモ: このファイルは、リモートシステム上ではなく、OpenManage Essentials がインストールされたシステムにある必要があります。
- システムの電源状態の変更。
- システムへの OpenManage Server Administrator の導入 。
- iDRAC サービスモジュールをシステムに導入します。
- Dell OpenManage Server Administrator（OMSA）がインストールされていないサーバーからファームウェアとドライバインベントリ情報を収集します。
- リモートタスクの表示。
- 右クリックによる任意のタスクの変更。

メモ: 実行中のタスクを停止する場合、タスクが正常に停止し、アップデートされたタスク状態がコンソールに反映されるまでに 3～4 分かかることがあります。

メモ: **タスクの実行履歴** には、作成または削除したリモートタスクが、わずか数秒以内に反映されます。

メモ: システム資格情報を入力する際に、ユーザー名にスペースまたはピリオドが含まれる場合は、ユーザー名を引用符で囲む必要があります（例："localhost\johnny marr" または "us-domain\tim verlaine"）。スペースとピリオドは、OpenMange System Administrator タスク、一般的なコマンドラインタスク（ローカルシステム）、OpenManage Systems Administrator 導入タスクのユーザー名で使用可能です。システムアップデート（帯域内、OpenManage System Administrator 経由）もスペースとピリオドをサポートしています。帯域外パッチ（RAC デバイス経由）または RACADM などのコマンドではユーザー名のスペースとピリオドをサポートしていません。

コマンドラインタスクの管理

カスタムコマンドを作成して、ローカルおよびリモートシステムで CLI コマンドを実行し、ローカルシステムでバッチファイルおよび実行可能ファイルを実行できます。

例えば、セキュリティ監査を実行してシステムのセキュリティ状態に関する情報を収集するカスタムコマンドラインのタスクを作成できます。

メモ: **リモート Server Administrator コマンド** タスクには、選択したターゲット上で **Windows Management Instrumentation** サービスが実行されている必要があります。

コマンドラインタスクを作成するには、次の手順を行います。

1. OpenManage Essentials から、**管理 → リモートタスク → 一般タスク → コマンドラインタスクの作成**をクリックします。
2. **一般** で、タスク名を入力します。
3. 次のオプションのいずれかを選択します。
   - **リモート Server Administrator コマンド** — これを選択して、リモートサーバーで Server Administrtor コマンドを実行します。
   - **一般コマンド** — これを選択して、コマンド、実行可能ファイル、またはバッチファイルを実行します。
   - **IPMI コマンド** — これを選択して、リモートシステムで IPMI コマンドを実行します。
   - **RACADM コマンドライン** — これを選択して、リモートシステムで RACADM コマンドを実行します。
4. 前手順での選択に基づいて、次を入力します。
   - **リモート Server Administrator コマンド** を選択した場合は、コマンド、SSH ポート番号を入力し、信頼済みキーを生成する場合は **Linux 用の信頼済みキーの生成** を選択します。
   - **一般コマンド、RACADM コマンドライン、**または **IPMI コマンド** を選択した場合は、コマンドと追記出力情報を入力します。追記出力情報の入力はオプションです。
5. **タスクのターゲット** で、次のいずれかを実行します。
   - ドロップダウンリストでクエリを選択するか、**新規** ボタンをクリックして新規クエリを作成します。
   - コマンドを実行するためのサーバーターゲットを選択します。該当するターゲットはデフォルトで表示されます。詳細に関しては、「デバイス機能マトリクス」を参照してください。
6. **スケジュールと資格情報** では、ユーザー資格情報を入力し、利用可能なオプションからタスクのスケジュールを設定して、**終了** をクリックします。

   コマンドラインタスクの作成 ウィザードのフィールドの詳細については、「コマンドラインタスク」を参照してください。

関連リンク

リモートタスク
リモートタスク - 参照
リモートタスクのホーム
コマンドラインタスク
すべてのタスク
デバイス機能マトリクス

RACADM コマンドラインタスクの管理

RACADM コマンドラインタスクは、リモート DRAC および iDRAC でコマンドを実行するために使用します。たとえば、帯域外（OOB）チャネルを介した iDRAC の設定を行うため、RACADM タスクを実行します。RACADM コマンドラインタスクを管理するには、次の手順を実行します。

1. OpenManage Essentials から、**管理 → リモートタスク → 一般タスク → コマンドラインタスクの作成** をクリックします。
2. **一般** で、**RACADM コマンドライン** を選択してタスクの名前を入力します。
3. RACADM サブコマンド（たとえば、**getsysinfo**）を入力します。RACADM コマンドのリストは、**dell.com/support** にアクセスしてください。
4. （オプション）**ファイルへ出力** を選択して、複数のターゲットからタスクの出力をキャプチャします。パスおよびファイル名を入力します。
   - 選択したターゲットすべてからの情報をログするには、**追加** を選択します。

- 検知されたエラーのすべてをログファイルに書き込むには、**エラーを含める** を選択します。

5. **タスクのターゲット** で、次のいずれかを実行します。
   - ドロップダウンリストでクエリを選択するか、**新規** ボタンをクリックして新規クエリを作成します。
   - ターゲットサーバーまたは DRAC / iDRAC を選択します。該当するターゲットはデフォルトで表示されます。詳細に関しては、「デバイス機能マトリクス」を参照してください。
6. **スケジュールと資格情報** でスケジュールパラメータを設定し、ターゲット資格情報を入力してから **終了** をクリックします。

関連リンク

リモートタスク
リモートタスク - 参照
リモートタスクのホーム
コマンドラインタスク
すべてのタスク
デバイス機能マトリクス

一般的なコマンドラインタスクの管理

一般的なコマンドラインタスクを使用して、バッチファイルや Powershell または VBS スクリプトなどのスクリプトファイル、実行可能ファイル、コマンドなど、さまざまなタスクをローカル OpenManage Essentials システムで実行できます。タスクは常にローカル OpenManage Essentials システムで実行されますが、ローカルタスクを構成して、多くのリモートデバイスまたはサーバー上で実行したり連携したりすることができます。

コマンドラインタスクにトークン（代替パラメーター）を入力して、スクリプトファイル、実行可能ファイル、コマンド、またはバッチファイルに渡し、OpenManage Essentials で検出されるデバイス上でローカルスクリプトを実行できます。

一般的なコマンドラインタスクを管理するには、次の手順を実行します。

1. OpenManage Essentials から、**管理 → リモートタスク → 一般タスク → コマンドラインタスクの作成** をクリックします。
2. **一般** タブで、**一般コマンド** を選択します。
3. 必要に応じて、タスク名を更新します。
4. ローカルシステムで実行するためのパスとコマンド（バッチ、スクリプト、または実行可能ファイル）を入力します。
5. （オプション）コマンドの引数を入力します。$USERNAME および $PASSWORD を **引数** で使用すると、**スクリプト資格情報** で資格情報を入力することにより、コマンドに資格情報を渡すことができます。$IP または $RAC_IP を **引数** で使用すると、各ターゲットの IP アドレスをコマンドに渡すことにより、選択されたターゲットに対してコマンドを実行できます。

   メモ: 引数 フィールドに入力するトークンは、すべて大文字または小文字にする必要があります。例えば、$HOSTNAME または $hostname にします。

   メモ: トークンまたは引数を必要としないコマンドを実行している場合は、**スクリプト資格情報** の項と **タスクのターゲット** タブは表示されません。
6. （オプション）最初にデバイスに対して ping を実行する場合は、**デバイスの ping** を選択します。
7. （オプション）**ファイルへ出力** を選択して、複数のターゲットからタスクの出力をキャプチャします。パスおよびファイル名を入力します。
   - 選択したターゲットすべてからの情報をログするには、**追加** を選択します。
   - 検知されたエラーのすべてをログファイルに書き込むには、**エラーを含める** を選択します。
8. **タスクのターゲット** で、次のいずれかを実行します。

- ドロップダウンリストでクエリを選択するか、**新規** ボタンをクリックして新規クエリを作成します。
- コマンドを実行するターゲットを選択します。

9. **スケジュールと資格情報** で、OpenManage Essentials システムでコマンドを実行するための権限を持つローカル管理者の資格情報を入力します。タスクのスケジュールを設定して、**終了** をクリックします。

関連リンク

トークンについて
一般コマンド

トークンについて

バッチ、スクリプト、または実行可能ファイルに値を渡すときに使用できるトークンは以下のとおりです。

- **$IP** および **$RAC_IP** — これらの引数を使用すると、**コマンドラインタスクの作成** 画面に **タスクのターゲット** タブが表示されます。**タスクのターゲット** タブでは、引数を渡すターゲットを選択できます。$IP はサーバー IP の代わりに使用され、$RAC_IP は RAC (iDRAC) IP の代わりに使用されます。**タスクのターゲット** タブから、グループまたはデバイスを選択するか、動的クエリを使用できます。
- **$USERNAME** および **$PASSWORD** — 一部のインスタンスでは、バッチファイルまたはスクリプトファイルでリモートシステムに対する資格情報を指定する必要があります。$USERNAME または $PASSWORD が引数で使用されると、これらの値に対する **スクリプト資格情報** の項が表示されます。**スクリプト資格情報** の項に入力された資格情報はコマンドラインに渡されます。いずれかの値または両方の値を渡すことができます。

  メモ: スクリプト資格情報 の項には両方の値を入力する必要があります。1 つの値を使用する必要がない場合は、フィールドに任意のテキストを入力すると、トークンが使用されない場合に無視されます。
- **$NAME** — このトークンは、OpenManage Essentials **デバイスツリー** で見つかったシステムの名前を渡します。多くの場合、この名前はシステムのホスト名ですが、一部のインスタンスでは、IP アドレスか、`Dell Rack System - SVCTAG1` などの文字列になることがあります。

スクリプトへのトークンの受け渡し

バッチファイルまたはスクリプトを使用している場合は、%1、%2、%3 の形式を使用して OpenManage Essentials から渡される値を受け取ってください。値は **引数** フィールドの左から右に入力された順番に渡されます。

例えば、引数として $USERNAME $PASSWORD $IP $RAC_IP $NAME を使用する場合、バッチファイルとそれに続く Echo %1 %2 %3 %4 %5 により、以下の結果が表示されます。

```
C:\Windows\system32>echo scriptuser scriptpw 10.36.1.180 10.35.155.111 M60505-
W2K8x64 scriptuser scriptpw 10.36.1.180 10.35.155.111 M60505-W2K8x64
```

メモ: 資格情報はプレーンテキストでコマンドラインに渡されます。タスクを後で実行するようにスケジューリングしている場合は、資格情報は暗号化され、データベースに保存されます。資格情報は、タスクがスケジューリングされた時間に実行されたときに解読されます。ただし、前に作成されたタスクで **RUN** オプションを使用している場合は、システムの管理者資格情報とスクリプト資格情報の両方を入力してください。

サーバー電源オプションの管理

サーバーの電源を管理するためのタスクを作成することができます。

メモ: 電源タスクには、選択したターゲット上で **Windows Management Instrumentation** が実行されている必要があります。

リモートタスクを作成するには、次の手順を実行します。

1. OpenManage Essentials から、**管理 → リモートタスク → 一般タスク → 電源タスクの作成**をクリックします。
2. **電源タスクの作成** の **一般** で、次を行います。
   - タスク名を入力します。
   - 電源オプションを選択します。必要に応じて、**OS を最初にシャットダウンする** を選択して、電源タスクを開始する前にオペレーティングシステムをシャットダウンします。
3. **タスクのターゲット** で、次のいずれかを実行します。
   - ドロップダウンリストでクエリを選択するか、**新規** ボタンをクリックして新規クエリを作成します。
   - コマンドを実行するサーバーターゲットを選択します。
4. **スケジュールと資格情報** でスケジュールパラメータを設定し、ターゲット資格情報を入力してから **終了** をクリックします。

電源タスクの作成 ウィザードのフィールドの詳細については、「サーバーの電源オプション」を参照してください。

関連リンク

リモートタスク
リモートタスク - 参照
リモートタスクのホーム
コマンドラインタスク
すべてのタスク
デバイス機能マトリクス

Server Administrator の導入

OpenManage Server Administrator の展開タスクには、選択したターゲットで次が必要となります。

- **Windows Management Instrumentation** サービスが実行されていること。
- デフォルトの **Temp** フォルダ（**C:\Users\<username>\AppData\Local\Temp**）を使用可能なこと。**Temp** が削除されたり移動されたりしていないことを確認してください。

Windows または Linux オペレーティングシステムがインストールされたサーバーに OpenManage Server Administrator（OMSA）を導入するタスクを作成することができます。OMSA 導入タスクをスケジュールするための日付と時刻を計画することも可能です。

OpenManage Server Administrator の導入タスクを作成するには、次の手順を実行します。

1. **管理 → リモートタスク → 一般タスク → 導入タスクの作成**をクリックします。
2. **一般** で、**Server Administrator** を選択しタスク名を入力します。Windows ベースのサーバーに OpenManage Server Administrator を導入する場合は、**Windows** を選択して、インストーラパスを入力し、必要に応じて、引数を指定します。Linux ベースのサーバーに OpenManage Server Administrator を導入する場合は、**Linux** を選択して、インストーラーパスを入力し、必要に応じて、引数を指定します。サポートされているパッケージと引数のリスト（Windows または Linux で動作しているサーバー用）については、「サポートされる Windows および Linux パッケージ」と「引数」を参照してください。**信頼できるキーの作成** を選択して、**再起動の許可** を選択します。

   メモ: Linux に Server Administrator を導入する前に、Server Administrator の必要条件をインストールします。
3. **タスクのターゲット** で、次のいずれかを実行します。
   - ドロップダウンリストでクエリを選択するか、**新規** ボタンをクリックして新規クエリを作成します。

- このタスクを実行するサーバーを選択し、**次へ** をクリックします。

4. タスクを有効化するには、**スケジュールと資格情報** でスケジュールパラメータを設定し、ユーザー資格情報を入力します。
5. sudo ユーザーとして Server Administrator を導入する場合は、**Sudo の有効化** を選択し、**SSH ポート** 番号をアップデートします。

   メモ: sudo を使用して OMSA を導入する前に、新しいユーザーアカウントを作成し、**sudoers** ファイルを `visudo` コマンドを使って編集して、以下を追加します。

   - 32 ビットのオペレーティングシステムを実行しているターゲットシステムの場合：
     `Cmnd_Alias OMEUPDATE = /bin/tar,/bin/cat,/opt/dell/srvadmin/bin/omexec,/tmp/LinuxPreInstallPackage/runbada,/tmp/LinuxPreInstallPackage/omexec <sudo_username> ALL=OMEUPDATE, NOPASSWD:OMEUPDATE`。
   - 64 ビットのオペレーティングシステムを実行しているターゲットシステムの場合：
     `Cmnd_Alias OMEUPDATE = /bin/tar,/bin/cat,/opt/dell/srvadmin/bin/omexec,/tmp/LinuxPreInstallPackage64/runbada,/tmp/LinuxPreInstallPackage64/omexec <sudo_username> ALL=OMEUPDATE, NOPASSWD:OMEUPDATE`。

   メモ: root ユーザーによって OMSA がシステムからアンインストールされた場合は、sudo を使用して OMSA をそのシステムに導入する前に、**tmp** フォルダからすべての OMSA プレインストールパッケージファイルが削除されていることを確認してください。

   メモ: SUSE Linux Enterprise Server および ESX ターゲットでは、sudo を使用した OMSA の導入はサポートされていません。
6. **終了** をクリックします。

導入タスクの作成 ウィザードのフィールドの詳細については、「導入タスク」を参照してください。

関連リンク

リモートタスク
リモートタスク - 参照
リモートタスクのホーム
コマンドラインタスク
すべてのタスク
デバイス機能マトリクス

サポートされる Windows および Linux パッケージ

Windows パッケージ

パッケージタイプ	クリーンインストール	メジャーバージョンアップグレード（5.x → 6.x → 7.x）	マイナーバージョンアップグレード（6.x → 6.y）
.msi	対応	対応	対応
.msp	非対応	非対応	対応
.exe	非対応	対応	対応

Linux パッケージ

オペレーティングシステム	パッケージ
SUSE Linux Enterprise Server 10	OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.SLES10.x86_64_A01.6.tar.gz OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.SLES10.x86_64_A01.6.tar.gz.sign
SUSE Linux Enterprise Server 11	OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.SLES11.i386_A01.14.tar.gz OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.SLES11.i386_A01.14.tar.gz.sign
VMware ESX 4	OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.ESX41.i386_A01.tar.gz OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.ESX41.i386_A01.tar.gz.sign
Red Hat Enterprise Linux 5	OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.RHEL5.x86_64_A01.4.tar.gz OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.RHEL5.x86_64_A01.4.tar.gz.sign
Red Hat Enterprise Linux 6	OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.RHEL6.x86_64_A01.5.tar.gz OM-SrvAdmin-Dell-Web-LX-6.5.0-2247.RHEL6.x86_64_A01.5.tar.gz.sign

引数

クリーンインストール

コンポーネントインストール	Linux 属性	Windows 属性
Server Administrator Web Server のみ	-w	ADDLOCAL=IWS
Server Administrator Instrumentation のみ	-d	ADDLOCAL=SA
Server Administrator Web Server および Server Instrumentation	-w –d	ADDLOCAL=ALL

アップグレード

- REINSTALL=ALL REINSTALLMODE=VOMUS — .msi パッケージを使用した Server Administrator マイナーバージョンアップグレードに必要な引数です。
- /qn — サイレントインストールおよび無人インストールに使用されるオプションの引数です。

iDRAC サービスモジュールの導入

メモ: iDRAC サービスモジュールは、次の条件を満たしているサーバーのみに導入できます。

- 64 ビットの Windows または Linux オペレーティングシステムを実行している Dell PowerEdge 12 世代以降のサーバー
- iDRAC ファームウェアバージョン 1.51.51 またはそれ以降
- iDRAC とサーバーは OpenManage Essentials 内で検出される必要があります。

iDRAC サービスモジュールの導入タスクは、ターゲットサーバーで次の条件を満たす必要があります。

- **Windows Management Instrumentation** サービスが実行されていること。
- デフォルトの **Temp** フォルダ（**C:\Users\<username>\AppData\Local\Temp**）を使用可能なこと。**Temp** が削除されたり移動されたりしていないことを確認してください。

Windows または Linux オペレーティングシステムを実行しているサーバーに iDRAC サービスモジュールを導入するタスクを作成することができます。また、iDRAC タスク導入タスクをスケジュールするための日付と時刻を計画することも可能です。

iDRAC サービスモジュール導入タスクを作成するには、次の手順を実行します。

1. **管理 → リモートタスク → 一般タスク → 導入タスクの作成** をクリックします。
2. **一般** で **iDRAC サービスモジュール** を選択してタスク名を入力します。Windows ベースのサーバーに iDRAC サービスモジュールを導入するには、**Windows** を選択し、インストールのパスを入力して、必要な場合は引数を入力します。Linux ベースのサーバーに iDRAC サービスモジュールを導入する場合は、**Linux** を選択し、インストールパスを入力して、**信頼済みキーの生成** および **再起動の許可** を選択します。.rpm パッケージを使用して iDRAC サービスモジュールを導入するには、**GPG キーのアップロードおよびインストール** を選択します。

   メモ: Linux での iDRAC サービスモジュールの導入は、iDRAC サービスモジュールの前提条件をインストールしてから実行します。
3. **タスクのターゲット** で、次のいずれかを実行します。
   - ドロップダウンリストでクエリを選択するか、**新規** ボタンをクリックして新規クエリを作成します。
   - このタスクを実行するサーバーを選択し、**次へ** をクリックします。

     メモ: iDRAC サービスモジュールの導入に該当しないデバイスは、**タスクターゲット** で選択することはできません。**タスクターゲット** でそのようなデバイスにマウスのポインタを置くと、iDRAC サービスモジュールを導入できない理由を示すツールヒントが表示されます。デバイス機能を上書きして、すべてのデバイスをタスクターゲットとして選択できるようにする場合は、**すべてを有効にする** を選択します。
4. タスクを有効化するには、**スケジュールと資格情報** でスケジュールパラメータを設定し、ユーザー資格情報を入力します。
5. Sudo ユーザーとして iDRAC サービスモジュールを導入する場合は、**Sudo の有効化** を選択して、**SSH ポート** 番号をアップデートします。

   メモ: Sudo を使用して iDRAC サービスモジュールを導入する前に、新しいユーザーアカウントを作成し、`visudo` コマンドを使用して **sudoers** ファイルを編集してから、以下を追加します。

   ```
   Cmnd_Alias OMEUPDATE = /bin/tar,/bin/cat,/bin/rpm,/opt/dell/
   srvadmin/bin/omexec,/tmp/LinuxPreInstallPackage64/runbada,/tmp/
   LinuxPreInstallPackage64/omexec <sudo_username> ALL=OMEUPDATE,
   NOPASSWD:OMEUPDATE
   ```

   メモ: root ユーザーによって iDRAC サービスモジュールがシステムからアンインストールされた場合は、Sudo を使用して iDRAC サービスモジュールをそのシステムに導入する前に、**tmp** フォルダからすべての iDRAC サービスモジュールプレインストールパッケージファイルが削除されていることを確認してください。

   メモ: Sudo を使用した iDRAC サービスモジュールの導入は、SUSE Linux Enterprise Server および ESX ターゲットではサポートされていません。
6. **終了** をクリックします。

導入タスクの作成 ウィザードのフィールドの詳細については、導入タスクを参照してください。

関連リンク

導入タスク

サポートされる Windows および Linux パッケージ

Windows パッケージ

パッケージタイプ	クリーンインストール	メジャーバージョンアップグレード（1.x から 2.x へ）
.msi **メモ:** iDRAC サービスモジュールバージョン 2.0 のみに適用されます。	対応	対応
.exe	非対応	対応

Linux パッケージ

オペレーティングシステム	パッケージ
• Red Hat Enterprise Linux 5 • Red Hat Enterprise Linux 6 • Red Hat Enterprise Linux 7 • SUSE Linux Enterprise Server 11 • Community Enterprise Operating System（CentOS）5.9 • CentOS 6.5	OM-iSM-Dell-Web-LX-100-429.tar.gz OM-iSM-Dell-Web-LX-100-429.tar.gz.sign Systems-Management_Application_NH7WW_LN64_1.0.0_A01 Systems-Management_Application_NH7WW_LN64_1.0.0_A01.BIN
SUSE Linux Enterprise Server 11	dcism-1.0.0-4.435.1.sles11.x86_64.rpm
Red Hat Enterprise Linux 5	dcism-1.0.0-4.435.1.el5.x86_64.rpm
Red Hat Enterprise Linux 6	dcism-1.0.0-4.435.1.el6.x86_64.rpm

ファームウェアおよびドライバインベントリの収集

ファームウェアおよびドライバのインベントリタスクの作成 により、ファームウェアおよびドライバインベントリ情報をサーバーから収集することができます。収集された情報は基準値として OpenManage Essentials が使用し、サーバでのアップデートの認識と適用を行います。このタスクでは、次の状況下で OpenManage Essentials では利用できないインベントリ情報を収集することができます。

- WMI または SSH プロトコルを使用して検出された Dell OpenManage Server Administrator（OMSA）がインストールされていないサーバー。
- OMSA がインストールされていない、デルまたは OEM のサーバー。
- サーバーは OMSA がインストールされている Linux を実行しているが、インベントリ収集コンポーネントはインストールされていない。

インベントリ情報が収集された後、**システムアップデート** を介して、サーバーのファームウェア、BIOS、またはドライバをアップデートすることができます。

ファームウェアとドライバのインベントリを収集するには、次の手順を実行します。

1. 次のいずれかの手順を実行してください。
   - **管理 → リモートタスク → ファームウェアおよびドライバのインベントリタスクの作成** の順にクリックします。
   - **管理 → システムアップデート → インベントリ未施行システム** の順にクリックします。

   a. インベントリを行うシステムを選択して **インベントリ** をクリックします。
   b. **インベントリを行うシステム** ウィンドウで **インベントリの実行** をクリックします。

   ファームウェアおよびドライバのインベントリタスクの作成 ウィンドウが表示されます。
2. **一般** で、タスクの名前を入力します。
3. オペレーティングシステムに応じて **タスクターゲット** 内に表示されるデバイスをフィルタしたい場合は、**オペレーティングシステムに基づいてデバイスをフィルタする** を選択します。
   a. **Windows** または **Linux** を選択します。
   b. 該当する場合は、 **64 ビットシステム** を選択します。
4. **タスクのターゲット** で、次のいずれかを実行します。
   - ドロップダウンリストからクエリを選択するか、**新規** をクリックして新規クエリを作成します。
   - このタスクを実行するサーバーを選択し、**次へ** をクリックします。
5. タスクを有効化するには、**スケジュールと資格情報** でスケジュールパラメータを設定し、ユーザー資格情報を入力します。
6. **終了** をクリックします。
   インベントリ収集のステータスが **リモートタスク** ポータルの **タスク実行履歴** に表示されます。

関連リンク

リモートタスク
リモートタスク - 参照
リモートタスクのホーム
コマンドラインタスク
すべてのタスク
デバイス機能マトリクス
ファームウェアおよびドライバインベントリ収集タスク

サンプルリモートタスクの使用例での作業

サンプルリモートタスクは、サーバーの電源オプション、Server Administrator の展開、およびコマンドラインで使用可能です。サンプルリモートタスクの使用例は、デフォルトでは無効になっています。サンプルの使用例を有効にするには、次の手順を実行します。

1. 使用例を右クリックして、**クローン** を選択します。
2. **クローンされたタスク名** を入力して、**OK** をクリックします。
3. クローンされたタスクを右クリックして、**編集** を選択します。
4. 必要な情報を入力して、タスクにターゲットを割り当てます。オプションの詳細については、「リモートタスク — 参照」を参照してください。

関連リンク

リモートタスク
リモートタスク - 参照
リモートタスクのホーム
コマンドラインタスク

すべてのタスク
デバイス機能マトリクス

リモートタスクの使用例

サーバーの電源オプション

Sample-Power On Device（サンプル-デバイスの電源投入） — この使用例を有効化して、サーバーの電源をオンにします。システムには、RAC/DRAC を設定する必要があります。

Server Administrator の展開

Sample-OMSA Upgrade Windows（サンプル-Windows での OMSA アップグレード） — この使用例を有効化して、Windows ベースのシステムで OpenManage Server Administrator をアップグレードします。

コマンドライン

- **Windows OMSA アンインストールサンプル** — この使用例を有効にして、Windows Server オペレーティングシステムを実行しているシステム上の OMSA をアンインストールします。
- **Linux OMSA アンインストールサンプル** — この使用例を有効にして、Linux オペレーティングシステムを実行しているシステム上の OMSA をアンインストールします。
- **サーバー XML 設定サンプル** — この使用例を有効にして、特定のサーバーの設定を複数の管理下ノードに適用します。詳細に関しては、「サーバー XML 設定サンプルコマンドラインタスクの使用」を参照してください。
- **汎用コマンドリモートサンプル** — この使用例を有効にして、インベントリシステムの IP アドレスまたは名前を受信するためのトークンを使用します。

  メモ: このコマンドを使用するには、ローカルシステムの資格情報を入力する必要があります。
- **汎用コマンドローカルサンプル** — この使用例を有効にして、OpenManage Essentials を使用するシステムでコマンドまたはスクリプトを実行します。

  メモ: このコマンドを使用するには、ローカルシステムの資格情報を入力する必要があります。
- **IPMI コマンドサンプル** — この使用例を有効にして、サーバーの電源状態の詳細を受信します。
- **リモートコマンドサンプル** — この使用例を有効にして、Server Administrator でシステム概要を表示します。
- **RACADM-SEL ログのクリアサンプル** — この使用例を有効にして、RAC の SEL ログをクリアします。
- **RACADM-リセットサンプル** — この使用例を有効にして、RAC をリセットします。

ファームウェアおよびドライバインベントリタスク

スケジュール済み S/W インベントリタスク — サーバーからファームウェアおよびドライバインベントリを収集するには、このユースケースを有効にします。

サーバー XML 設定サンプルコマンドラインタスクの使用

サーバー XML 設定サンプル コマンドラインタスクの使用の必要条件は次の通りです。

- Dell Lifecycle Controller 2 バージョン 1.2 以降
- RACADM バージョン 7.2 以降
- ファームウェアバージョン 1.30.30 以降
- Express または Enterprise ライセンス
- iDRAC7

サーバー XML 設定サンプル コマンドラインタスクでは、特定のサーバー設定を複数の管理下ノードに適用することができます。Dell Lifecycle Controller 2 バージョン 1.2 以降を使用すると、「サーバー設定のエクスポート」操作によって、サーバーの設定概要を iDRAC から XML 形式でエクスポートすることができます。

メモ: Lifecycle Controller 2 を使用したサーバー設定概要のエクスポートの詳細に関しては、**DellTechCenter.com/LC** にある、『*設定 XML ワークフロー*』ホワイトペーパーを参照してください。

サーバー設定概要 XML ファイルは、**サーバー XML 設定サンプル** コマンドラインタスクを使用して別の iDRAC に適用できます。

メモ: サーバー設定概要を 1 つの iDRAC から別の iDRAC に適用するには、これらの iDRAC 両方の世代、ライセンス状態などが同じである必要があります。必須条件の詳細については、**DellTechCenter.com/LC** にある『Lifecycle Controller（LC）XML スキーマガイド』、『サーバー設定 XML ファイル』、および『設定 XML ワークフロー』ホワイトペーパーを参照してください。

サーバー XML 設定サンプル コマンドラインタスクを使用するには、次の手順を実行します。

1. OpenManage Essentials **リモートタスク** ポータルで、**サーバー XML 設定サンプル** を右クリックして **クローン** をクリックします。

   新しくクローンされたタスクの情報を入力 ダイアログボックスが表示されます。
2. **クローンされたタスク名** を入力して、**OK** をクリックします。
3. 作成したクローンされたタスクを右クリックして、**編集** をクリックします。

   コマンドラインタスクの作成 ダイアログボックスが表示されます。
4. **コマンド** フィールドを編集し、OpenManage Essentials 管理ステーションのサーバー設定概要 xml ファイルの位置を入力します。例：`set -f c:\user1\server1.xml-t xml`。ここで `c:\user1\server1.xml` はサーバー設定概要 xml ファイルの位置です。
5. **ターゲット** タブで、サーバー設定を適用するための適切なターゲットを選択します。
6. **スケジュールと資格情報** タブで、タスクの実行またはスケジュールを選択して、必要な資格情報を入力します。
7. **終了** をクリックします。

デバイス機能マトリクス

以下のデバイス機能マトリクスは、**タスクのターゲット** タブに表示されるデバイスでサポートされるリモートタスクのタイプの情報について示しています。

リモートタスクタイプ	Server Administrator 装備の SNMP/WMI で検出されたすべてのサーバー（ESXi を除く）	Server Administrator 未装備の WMI で検出された Windows ベースのサーバー	Server Administrator 未装備の SSH で検出された Linux ベースのサーバー	IPMI で検出された DRAC/iDRAC	SNMP/WS-Man で検出された DRAC/iDRAC
	DRAC/iDRAC が検出されなかった			サーバーオペレーティングシステムが検出されなかった	
再起動 / パワーサイクル操作	対応	対応	非対応	非対応	非対応
電源オフ操作	対応	対応	非対応	非対応	非対応
電源オン操作	非対応	非対応	非対応	対応	非対応

リモートタスクタイプ	Server Administrator 装備の SNMP/WMI で検出されたすべてのサーバー（ESXi を除く）	Server Administrator 未装備の WMI で検出された Windows ベースのサーバー	Server Administrator 未装備の SSH で検出された Linux ベースのサーバー	IPMI で検出された DRAC/iDRAC	SNMP/WS-Man で検出された DRAC/iDRAC
	DRAC/iDRAC が検出されなかった			サーバーオペレーティングシステムが検出されなかった	
リモート Server Administrator コマンドタスク	対応	非対応	非対応	非対応	非対応
IPMI コマンドタスク	非対応	非対応	非対応	非対応	非対応
RACADM コマンドラインタスク	非対応	非対応	非対応	非対応	対応
ファームウェアおよびドライバのインベントリタスクの作成	非対応	対応	対応	非対応	非対応

次の表は、iDRAC サービスモジュール導入タスクのためのデバイス検出要件をリストしています。iDRAC サービスモジュールを導入するには、指定された適切なプロトコルを使用してサーバーおよび iDRAC を検出する必要があります。例えば、SNMP/WMI を使用して検出される Server Administrator を実行する Windows ベースのサーバーで iDRAC サービスモジュールを導入するには、SNMP/WS-Man を使用して iDRAC を検出する必要があります。

リモートタスクタイプ	サーバー / 帯域内検出				iDRAC/ 帯域外検出
	SNMP/WMI を使用して検出された Server Administrator 装備の全 Windows ベースサーバー	WMI を使用して検出された Server Administrator 装備の全 Windows ベースサーバー	SNMP/SSH を使用して検出された Server Administrator 装備の全 Linux ベースサーバー	SSH を使用して検出された Server Administrator 装備の全 Linux ベースサーバー	SNMP/WS-Man で検出された DRAC/iDRAC
iDRAC サービスモジュールの導入タスク	✔	該当なし	該当なし	該当なし	✔
	該当なし	✔	該当なし	該当なし	✔
	該当なし	該当なし	✔	該当なし	✔
	該当なし	該当なし	該当なし	✔	✔

サーバーまたは DRAC/iDRAC デバイスのデバイス機能は検出中に入力され、リモートタスクが各タスクタイプの使用可能なターゲットを判別するのに利用されます。機能は以下のパラメーターに基づいて入力されます。

- サーバーおよび DRAC/iDRAC を検出するために使用するプロトコル。例えば、IPMI、SNMP、など。
- Server Administrator がサーバーにインストールされている場合。
- DRAC/iDRAC で有効にされている設定。

すべて有効にする チェックボックスを選択すると、デバイス機能をオーバーライドでき、すべての使用可能なデバイスをタスクのターゲットとして選択できるようになります。

以下のデバイス機能マトリックスは、デバイス機能がオーバーライドされたときにデバイスでサポートされるリモートタスクのタイプの情報について示しています。

リモートタスクタイプ	**Server Administrator 装備の SNMP/WMI で検出されたすべてのサーバー（ESXi を除く）**	**Server Administrator 未装備の WMI で検出された Windows ベースのサーバー**	**Server Administrator 未装備の SSH で検出された Linux ベースのサーバー**	**IPMI で検出された DRAC/ iDRAC**	**SNMP/WS-Man で検出された DRAC/iDRAC**
	DRAC/iDRAC が検出されなかった			**サーバーオペレーティングシステムが検出されなかった**	
再起動 / パワーサイクル操作	対応	対応	非対応	非対応	非対応
電源オフ操作	対応	対応	非対応	非対応	非対応
電源オン操作	次の条件下で対応。 DRAC / iDRAC 情報が取得され、インベントリページに表示される。 IPMI オーバー LAN が DRAC / iDRAC デバイスで有効になっている。 **タスクのターゲット** タブで **すべてを有効にする** を選択している。	非対応	非対応	対応	次の条件下で対応。 IPMI オーバー LAN が DRAC / iDRAC デバイスで有効になっている。 **タスクのターゲット** タブで **すべてを有効にする** を選択している。
リモート Server Administrator コマンドタスク		非対応	非対応	非対応	
IPMI コマンドタスク	非対応	非対応	非対応	非対応	非対応
RACADM コマンドラインタスク	次の条件下で対応。 DRAC / iDRAC 情報が取得され、インベントリページに表示される。	非対応	非対応	非対応	対応

リモートタスクタイプ	Server Administrator 装備の SNMP/WMI で検出されたすべてのサーバー（ESXi を除く）	Server Administrator 未装備の WMI で検出された Windows ベースのサーバー	Server Administrator 未装備の SSH で検出された Linux ベースのサーバー	IPMI で検出された DRAC/iDRAC	SNMP/WS-Man で検出された DRAC/iDRAC
	DRAC/iDRAC が検出されなかった			サーバーオペレーティングシステムが検出されなかった	
	タスクのターゲット タブで **すべてを有効にする** を選択している。				

メモ: タスクのターゲット タブで **すべてを有効にする** オプションが選択されている場合、iDRAC サービスモジュール導入は検出されたすべてのサーバーまたは不明なデバイスに対して有効になります。

関連リンク

- コマンドラインタスクの管理
- RACADM コマンドラインタスクの管理
- サーバー電源オプションの管理
- Server Administrator の導入
- ファームウェアおよびドライバインベントリの収集
- サンプルリモートタスクの使用例での作業
- サーバー XML 設定サンプルコマンドラインタスクの使用
- iDRAC サービスモジュールの導入
- リモートタスク
- リモートタスク - 参照

21

リモートタスク - 参照

リモートタスク から、次を実行できます。

- ローカルとリモートのシステムでコマンドを実行、ローカルシステムでバッチファイルおよび実行可能ファイルを実行、およびローカルとリモートのタスクをスケジュール。
- システムの電源状態の変更。
- システムへの OpenManage Server Administrator の導入 。
- システムへの iDRAC サービスモジュールの導入。
- ファームウェアとドライバのインベントリの収集。
- リモートタスクの表示。

リモートタスク：

- 一般タスク
  - コマンドラインタスクの作成
  - 導入タスクの作成
  - 電源タスクの作成
  - ファームウェアおよびドライバのインベントリタスクの作成
- リモートタスク
  - サーバーの電源オプション
  - Server Administrator の導入
  - コマンドライン
- ファームウェアおよびドライバのインベントリタスク

関連リンク

コマンドラインタスクの管理
RACADM コマンドラインタスクの管理
サーバー電源オプションの管理
Server Administrator の導入
ファームウェアおよびドライバインベントリの収集
サンプルリモートタスクの使用例での作業
サーバー XML 設定サンプルコマンドラインタスクの使用
iDRAC サービスモジュールの導入
リモートタスクのホーム
コマンドラインタスク
すべてのタスク
デバイス機能マトリクス

リモートタスクのホーム

リモートタスクページを表示するには、OpenManage Essentials で、**管理 → リモートタスク** をクリックします。

関連リンク

コマンドラインタスクの管理
RACADM コマンドラインタスクの管理
サーバー電源オプションの管理
Server Administrator の導入
ファームウェアおよびドライバインベントリの収集
サンプルリモートタスクの使用例での作業
サーバー XML 設定サンプルコマンドラインタスクの使用
iDRAC サービスモジュールの導入
リモートタスク
リモートタスク - 参照

リモートタスク

リモートタスクページには、以下の情報が表示されます。

- すべてのタスク
- サーバーの電源オプション
- Server Administrator の展開
- コマンドライン
- ファームウェアとドライバのインベントリ

関連リンク

コマンドラインタスクの管理
RACADM コマンドラインタスクの管理
サーバー電源オプションの管理
Server Administrator の導入
ファームウェアおよびドライバインベントリの収集
サンプルリモートタスクの使用例での作業
サーバー XML 設定サンプルコマンドラインタスクの使用
iDRAC サービスモジュールの導入
リモートタスクのホーム
コマンドラインタスク
すべてのタスク
デバイス機能マトリクス

すべてのタスク

フィールド	説明
スケジュール状況	タスクが有効な場合に表示されます。
タスク名	タスクの名前です。
タスクラベル	実行されるタスクのタイプです。例えば、コマンドラインタスクの場合、表示されるオプションは、リモート Server Administrator コマンド、一般コマンド、IPMI コマンド、および RACADM コマンドラインです。
最終実行	タスクを実行した最終日時の情報です。
作成日	タスクを作成した日時です。
更新日	タスクを実行した日時の情報です。
更新者	ユーザーの名前です。

関連リンク

- コマンドラインタスクの管理
- RACADM コマンドラインタスクの管理
- サーバー電源オプションの管理
- Server Administrator の導入
- ファームウェアおよびドライバインベントリの収集
- サンプルリモートタスクの使用例での作業
- サーバー XML 設定サンプルコマンドラインタスクの使用
- iDRAC サービスモジュールの導入
- リモートタスク
- リモートタスク - 参照

タスクの実行履歴

システムアップデートタスクまたはリモートタスクの詳細をリストします。

フィールド	説明
状態	タスクの状態を示すアイコンを表示します。  – 実行中または保留中  – 完了  – 停止  – 失敗

フィールド	説明
	 — 警告
タスク名	タスクの名前です。
開始時刻	システムのアップデートタスクが開始される時間と日付です。
% 完了	タスクの進捗情報です。
タスク状況	これらのタスクの状況を提供します。 • 実行中 • 完了 • 停止 • 失敗 • 警告  **メモ:** システムのアップデートタスクの **アップデート後は、必要に応じてデバイスを再起動します** のオプションが選択されていない場合、タスクのステータスに警告が表示されます。
成功 / 試行対象ターゲット	タスクが正常に実行されたターゲットシステムの数です。
終了時刻	システムのアップデートタスクが終了する時間と日付です。
ユーザーにより実行済み	ユーザー情報です。

サーバーの電源オプション

このオプションを選択して、電源状態を変更したり、システムを再起動したりします。

フィールド	説明
一般	
タスク名	このサーバーの電源オプションに名前を指定します。
タイプを選択	次のオプションから選択します。 • 再起動 - 電源を切らずにシステムを再起動します。 • パワーサイクル — 電源を切ってから、システムを再起動します。

フィールド	説明
	メモ: このオプションを使用して正常なシャットダウンを実行する前に、オペレーティングシステムのシャットダウンオプションが設定されていることを確認してください。シャットダウンオプションを設定せずにオペレーティングシステムでこのオプションを使用すると、シャットダウン操作を実行せずに、管理下システムを再起動します。 • 電源オフ — システムの電源を切ります。 • 電源オン — システムの電源を入れます。このオプションは、RAC を搭載したターゲットシステム上でのみ機能します。
OS を最初にシャットダウンする	これを選択して、オペレーティングシステムをシャットダウンしてから、サーバーの電源オプションタスクを実行します。
タスクのターゲット	
クエリの選択	ドロップダウンリストからクエリを選択します。新しいクエリを作成するには、**新規** をクリックします。
このタスクのターゲットとなるデバイスの選択	このタスクを割り当てるデバイスを選択します。
すべて有効化	デバイス機能を上書きし、すべての利用可能デバイスをタスクのターゲットとして選択可能にします。
スケジュールと資格情報	
スケジュールの設定	次のオプションから選択します。 • **アクティブなスケジュール** — このオプションを選択して、タスクのスケジュールをアクティブにします。 • **今すぐ実行 —** このオプションを選択して、ただちにタスクを実行します。 • **スケジュールの設定** — このオプションを選択して、タスクを実行する日時を設定します。 • **1 度実行** — このオプションを選択して、計画したスケジュールを 1 度だけ実行します。 • **定期的** — このオプションを選択して、指定間隔でタスクを頻繁に実行します。 – **毎時** — このオプションを選択して、タスクを 1 時間に 1 度実行します。 – **毎日** — タスクを 1 日に 1 度実行します。 – **毎週** — タスクを週に 1 度実行します。 – **毎月** — タスクを月に 1 度実行します。 **反復の範囲**： • **開始** — タスクの開始日時を指定します。 • **終了日なし** — 選択した頻度に基づいてこのタスクを継続的に実行します。例えば、毎時を選択し

フィールド	説明
	た場合、このタスクは、開始時刻から 1 時間ごとに 1 回継続的に実行されます。 • **終了日** — タスクを指定した日時に停止します。
ユーザー名とパスワードを入力	**ユーザー名** — ドメイン\ユーザー名またはローカルホスト\ユーザー名の形式で入力します。 **パスワード** — パスワードを入力します。 **電源オン** は、iDRAC 搭載のターゲットシステムでのみ動作し、**電源オン** タスクの実行には IPMI 資格情報を使用します。 **電源オン** を選択した場合は、KG キーを入力します。 **KG キー** — KG キーを入力します。DRAC は IPMI KG キーもサポートしています。個々の BMC は、ユーザーの資格情報のほかにアクセスキーも要求するように設定されています。KG キーは、電源オンタスクの場合にのみ要求され、それ以外のタスクは IPMI タスクではないため要求されません。 **メモ:** KG キーは、ファームウェアとアプリケーション間で使用される暗号化キーを生成するために使用する公開キーで、Dell PowerEdge 9 世代以降のシステムでのみ利用できます。KG キーの値は、16 進数文字の偶数です。このフォーマット *yxxx* では、*y* は英数文字を示し、x は数字を示します。

関連リンク

サーバー電源オプションの管理
デバイス機能マトリクス

導入タスク

このオプションを選択して、選択したサーバーに Server Administrator または iDRAC サービスモジュールのいずれかを導入するタスクを作成します。

フィールド	説明
一般	
展開タイプ	次のオプションから導入のタイプを選択します。 • **サーバーシステム管理者** • **iDRAC サービスモジュール**
タスク名	タスクの名前を入力します。
タイプを選択	以下のオプションからターゲットタイプを選択します。 • **Windows**

フィールド	説明
	• **Linux**
インストーラパス	Server Administrator または iDRAC サービスモジュールインストーラを使用できる場所です。 Windows の場合、.**dup**、**.msi**、および **.msp** のファイル拡張子の付いたパッケージを使用できます。msi パッケージでは Server Administrator インストールとアップグレードが可能であり、dup パッケージと msp パッケージでは Server Administrator アップグレードのみが可能です。 • Linux に Server Administrator を導入する場合： – tar.gz ファイル拡張子の付いたパッケージが使用可能です。 – 検証には **.sign** ファイルが必須です。.sign ファイルは、tar.gz ファイルと同じフォルダ内に存在する必要があります。 • Linux に iDRAC サービスモジュールを導入する場合： – tar.gz ファイルおよび .bin ファイル拡張子の付いたパッケージが使用可能です。 – .rpm ファイルの導入には、RPM-GPG-KEY ファイルが、.rpm ファイルと同じフォルダ内に存在する必要があります。
引数のインストール **メモ:** Server Administrator の導入タスクのみに該当する作業となります。	（オプション）引数を指定します。 Windows では次のようなパラメータがあります。 • `ADDLOCAL` = IWS — Server Administrator Web サーバーのみ • `ADDLOCAL` = SSA — サーバー計装のみ Linux では次のようなパラメータがあります。 • `-w` - Server Administrator Web サーバーのみ • `-d` - サーバー計装のみ 引数の完全なリストについては、**dell.com/support/manuals** にある『Dell OpenManage インストールとセキュリティユーザーズガイド』を参照してください。
信頼できるキーの生成	Linux を選択した場合にこのオプションを使用できます。このオプションを選択して、信頼できるキーを生成します。
64 ビットシステム	Server Administrator の 64 ビットバージョンを管理対象ノードに導入する場合は、このオプションを選択します。

フィールド	説明
再起動の許可（必要な場合）	このオプションを選択して、サーバーに Server Administrator を導入したら、サーバーを再起動します。
GPG キーのアップロードおよびインストール（GPG キーが同じフォルダに必要） **メモ:** iDRAC サービスモジュール導入タスクのみに適用されます。	このオプションは、iDRAC サービスモジュールの導入用に .rpm ファイルを選択した場合に利用可能になります。このオプションを選択して、ターゲットデバイスの .rpm ファイルを検証します。
タスクのターゲット	
クエリの選択	ドロップダウンリストからクエリを選択します。新しいクエリを作成するには、**新規** をクリックします。
このタスクのターゲットとなるサーバーの選択	このタスクを割り当てるサーバーを選択します。
すべて有効化 **メモ:** iDRAC サービスモジュールの導入手順のみに適用されます。	デバイス機能をオーバーライドし、すべての利用可能デバイスをタスクのターゲットとして選択可能にします。
スケジュールと資格情報	
スケジュールの設定	次のオプションから選択します。 • **スケジュールのアクティブ化** — このオプションを選択して、タスクのスケジュールをアクティブにします。 • **今すぐ実行** — このオプションを選択して、ただちにタスクを実行します。 • **スケジュールの設定** — このオプションを選択して、タスクを実行する日時を設定します。
リモートターゲットの資格情報を入力	
ユーザー名	ドメイン\ユーザー名 または ローカルホスト\ユーザー名 の形式で入力します。
パスワード	パスワードを入力します。
Sudo を有効にする	Sudo を使用して Server Administrator または iDRAC サービスモジュールを導入するには、このオプションを選択します。
SSH ポート	SSH ポート番号を設定します。

関連リンク

Server Administrator の導入
デバイス機能マトリクス

コマンドラインタスク

このオプションを選択して、コマンドラインタスクを作成します。

フィールド	説明
タスク名	タスクの名前を入力します。
リモート Server Administrator コマンド	このオプションを選択して、選択したサーバーでリモート Server Administrator コマンドを実行します。
一般コマンド	このオプションを選択して、OpenManage Essentials が搭載されたシステム上で実行可能ファイルとコマンドを実行します。
IPMI コマンド	このオプションを選択して、選択したサーバーで IPMI コマンドを実行します。
RACADM コマンドライン	このオプションを選択して、選択したサーバーで RACADM コマンドを実行します。

関連リンク

コマンドラインタスクの管理
RACADM コマンドラインタスクの管理
サーバー電源オプションの管理
Server Administrator の導入
ファームウェアおよびドライバインベントリの収集
サンプルリモートタスクの使用例での作業
サーバー XML 設定サンプルコマンドラインタスクの使用
iDRAC サービスモジュールの導入
リモートタスク
リモートタスク - 参照
リモート Server Administrator コマンド
一般コマンド
IPMI コマンド
RACADM コマンドライン

リモート Server Administrator コマンド

フィールド	説明
コマンド	コマンドを指定します。例えば、`omereport system summary` があります。
デバイスの ping	このオプションは、デバイスにタスクを実行する前に、そのデバイスが到達可能かどうかを検証するための ping テストを実行します。このオプションは、$IP または $RAC_IP を使用しているときに使用で

フィールド	説明
	き、到達不能なデバイスをスキップするため、実行にかかる時間を削減できます。
ファイルへ出力	これを選択して、ログファイルに出力できるようにします。このオプションは、標準出力をキャプチャして、ログファイルに書き込みます。このオプションを選択する場合は、ログファイルのパス名とファイル名を入力します。このオプションは、デフォルトで無効になっています。
追加	これを選択して、完了したコマンドからの出力を指定したファイルに追加します。ファイルが存在しない場合は、ファイルが作成されます。
エラーを含める	これを選択して、すべての OpenManage Essentials の検出エラーをログファイルに書き込みます。たとえば、コマンド実行前の ping 要求に対して応答がなければ、ログファイルにエラーが書き込まれます。
SSH ポート番号	Linux 管理下システムにセキュアシェル（SSH）ポート番号を指定します。ポート番号のデフォルト値は 22 です。
Linux 用の信頼できるキーの生成	このオプションを選択して、デバイスとの通信用に信頼できるデバイスキーを生成します。このオプションは、デフォルトで無効になっています。 **メモ:** OpenManage Essentials は、Linux オペレーティングシステムを搭載したシステムと初めて通信するときに、両方のデバイスでキーを生成して保存します。このキーはデバイスごとに生成され、管理下デバイスとの信頼関係を可能にします。
タスクのターゲット	
クエリの選択	ドロップダウンリストからクエリを選択します。新しいクエリを作成するには、**新規** をクリックします。
このタスクのターゲットとなるサーバーの選択	このタスクを割り当てるサーバーを選択します。
すべて有効化	デバイス機能を上書きし、すべての利用可能デバイスをタスクのターゲットとして選択可能にします。
スケジュールと資格情報	
スケジュールの設定	次のオプションから選択します。 • **アクティブなスケジュール** — このオプションを選択して、タスクのスケジュールをアクティブにします。 • **今すぐ実行** — このオプションを選択して、ただちにタスクを実行します。

フィールド	説明
	• **スケジュールの設定** — このオプションを選択して、タスクを実行する日時を設定します。 • **1 度実行** — このオプションを選択して、計画したスケジュールを 1 度だけ実行します。 • **定期的** — このオプションを選択して、指定間隔でタスクを頻繁に実行します。 – **毎時** — このオプションを選択して、タスクを 1 時間に 1 度実行します。 – **毎日** — タスクを 1 日に 1 度実行します。 – **毎週** — タスクを週に 1 度実行します。 – **毎月** — タスクを月に 1 度実行します。 **反復の範囲**： • **開始** — タスクの開始日時を指定します。 • **終了日なし** — 選択した頻度に基づいてこのタスクを継続的に実行します。例えば、毎時を選択した場合、このタスクは、開始時刻から 1 時間ごとに 1 回継続的に実行されます。 • **終了日** — タスクを指定した日時に停止します。
リモートターゲットの資格情報を入力	**ユーザー名** — ドメイン\ユーザー名またはローカルホスト\ユーザー名の形式で入力します。 **パスワード** — パスワードを入力します。

関連リンク

コマンドラインタスク
コマンドラインタスクの管理
サーバー XML 設定サンプルコマンドラインタスクの使用

一般コマンド

フィールド	説明
タスク名	タスクの名前を入力します。デフォルトでは、タスク名が次のフォーマットで入力されています。 <タスク名>-<日時>。
コマンド	アプリケーションプログラムを起動する実行可能ファイル、コマンド、またはスクリプトファイルの完全修飾パス名およびファイル名を入力します。 • Tracert • C:\scripts\trace.bat • D:\exe\recite.exe
引数	コマンドまたは実行可能ファイルへのコマンドラインスイッチを入力するか、スクリプトまたはバッチファイルに値を渡します。例えば、-4 $IP です。この引数が tracert コマンドに渡されると、**タスクのタ**

フィールド	説明
	ーゲット タブで選択されたサーバーの IP に対して IPV4 のみの Traceroute が実行されます。実行されるコマンドは `tracert -4 10.35.0.55` になります。 詳細に関しては、「トークンについて」を参照してください。
デバイスの ping	このオプションは、デバイスにタスクを実行する前に、そのデバイスが到達可能かどうかを検証するための ping テストを実行します。このオプションは、$IP または $RAC_IP を使用しているときに使用でき、到達不能なデバイスをスキップするため、実行にかかる時間を削減できます。
ファイルへ出力	これを選択して、ログファイルに出力できるようにします。このオプションは、実行中のアプリケーションからの出力をキャプチャして、ログファイルに書き込みます。このオプションを選択する場合は、ログファイルのパス名とファイル名を入力する必要があります。このオプションは、デフォルトで無効になっています。
追加	タスクを複数回実行する場合、このオプションを選択して、同じファイルへの書き込みを続行します。
エラーを含める	これを選択して、すべての OpenManage Essentials の検出エラーをログファイルに書き込みます。たとえば、コマンド実行前の ping 要求に対して応答がなければ、ログファイルにエラーが書き込まれます。
スケジュールと資格情報	
スケジュールの設定	次のオプションから選択します。 • **アクティブなスケジュール** — このオプションを選択して、タスクのスケジュールをアクティブにします。 • **今すぐ実行** — このオプションを選択して、ただちにタスクを実行します。 • **スケジュールの設定** — このオプションを選択して、タスクを実行する日時を設定します。 • **1 度実行** — このオプションを選択して、計画したスケジュールを 1 度だけ実行します。 • **定期的** — このオプションを選択して、指定間隔でタスクを頻繁に実行します。 – **毎時** — このオプションを選択して、タスクを 1 時間に 1 度実行します。 – **毎日** — タスクを 1 日に 1 度実行します。 – **毎週** — タスクを週に 1 度実行します。 – **毎月** — タスクを月に 1 度実行します。 **反復の範囲**：

フィールド	説明
	• **開始** — タスクの開始日時を指定します。 • **終了日なし** — 選択した頻度に基づいてこのタスクを継続的に実行します。例えば、毎時を選択した場合、このタスクは、開始時刻から 1 時間ごとに 1 回継続的に実行されます。 • **終了日** — タスクを指定した日時に停止します。
このシステムのこのタスクを実行するために適切な権限を持つ資格情報を入力	**ユーザー名** — OpenManage Essentials ユーザー資格情報をドメイン\ユーザー名またはローカルホスト\ユーザー名の形式で入力します。 **パスワード** — パスワードを入力します。

関連リンク

コマンドラインタスク
コマンドラインタスクの管理
サーバー XML 設定サンプルコマンドラインタスクの使用

IPMI コマンド

フィールド	説明
コマンド	選択したターゲットで実行する IPMI コマンドを入力します。
デバイスの ping	このオプションは、デバイスにタスクを実行する前に、そのデバイスが到達可能かどうかを検証するための ping テストを実行します。このオプションは、$IP または $RAC_IP を使用しているときに使用でき、到達不能なデバイスをスキップするため、実行にかかる時間を削減できます。
ファイルへ出力	これを選択して、ログファイルに出力できるようにします。このオプションは、実行中のアプリケーションからの出力をキャプチャして、ログファイルに書き込みます。このオプションを選択する場合は、ログファイルのパス名とファイル名を入力する必要があります。このオプションは、デフォルトで無効になっています。
追加	これを選択して、完了したコマンドからの出力を指定したファイルに追加します。ファイルが存在しない場合は、ファイルが作成されます。
エラーを含める	これを選択して、すべての OpenManage Essentials の検出エラーをログファイルに書き込みます。たとえば、コマンド実行前の ping 要求に対して応答がなければ、ログファイルにエラーが書き込まれます。
タスクのターゲット	

フィールド	説明
クエリの選択	ドロップダウンリストからクエリを選択します。新しいクエリを作成するには、**新規** をクリックします。
このタスクのターゲットとなるサーバーの選択	このタスクを割り当てるサーバーを選択します。
すべて有効化	デバイス機能を上書きし、すべての利用可能デバイスをタスクのターゲットとして選択可能にします。
スケジュールと資格情報	
スケジュールの設定	次のオプションから選択します。 • **アクティブなスケジュール** — このオプションを選択して、タスクのスケジュールをアクティブにします。 • **今すぐ実行** — このオプションを選択して、ただちにタスクを実行します。 • **スケジュールの設定** — このオプションを選択して、タスクを実行する日時を設定します。 • **1 度実行** — このオプションを選択して、計画したスケジュールを 1 度だけ実行します。 • **定期的** — このオプションを選択して、指定間隔でタスクを頻繁に実行します。 – **毎時** — このオプションを選択して、タスクを 1 時間に 1 度実行します。 – **毎日** — タスクを 1 日に 1 度実行します。**毎週** — タスクを週に 1 度実行します。 – **毎月** — タスクを月に 1 度実行します。 **反復の範囲**： • **開始** — タスクの開始日時を指定します。 • **終了日なし** — 選択した頻度に基づいてこのタスクを継続的に実行します。例えば、毎時を選択した場合、このタスクは、開始時刻から 1 時間ごとに 1 回継続的に実行されます。 • **終了日** — タスクを指定した日時に停止します。
ターゲットのリモートアクセスコントローラ資格情報を入力	
ユーザー名	RACADM タスクには IPMI 資格情報が必要です。このタスクを実行するには IPMI 資格情報を入力してください。
パスワード	パスワードを入力します。
KG キー	KG キー値を入力します。DRAC は IPMI KG キーもサポートしています。個々の BMC または DRAC は、ユーザーの資格情報のほかにアクセスキーも要求するように設定されています。

フィールド	説明
	メモ: KG キーは、ファームウェアとアプリケーション間で使用される暗号化キーを生成するために使用する公開キーです。KG キーの値は、16 進数文字の偶数です。

関連リンク

コマンドラインタスク
コマンドラインタスクの管理
サーバー XML 設定サンプルコマンドラインタスクの使用

RACADM コマンドライン

フィールド	説明
コマンド	サーバーで実行する RACADM コマンドを入力します。
デバイスの ping	このオプションは、デバイスにタスクを実行する前に、そのデバイスが到達可能かどうかを検証するための ping テストを実行します。このオプションは、$IP または $RAC_IP を使用しているときに使用でき、到達不能なデバイスをスキップするため、実行にかかる時間を削減できます。
ファイルへ出力	これを選択して、ログファイルに出力できるようにします。このオプションは、実行中のアプリケーションからの出力をキャプチャして、ログファイルに書き込みます。このオプションを選択する場合は、ログファイルのパス名とファイル名を入力する必要があります。このオプションは、デフォルトで無効になっています。
追加	これを選択して、完了したコマンドからの出力を指定したファイルに追加します。ファイルが存在しない場合は、ファイルが作成されます。
エラーを含める	これを選択して、すべての OpenManage Essentials の検出エラーをログファイルに書き込みます。たとえば、コマンド実行前の ping 要求に対して応答がなければ、ログファイルにエラーが書き込まれます。
タスクのターゲット	
クエリの選択	ドロップダウンリストからクエリを選択します。新しいクエリを作成するには、**新規** をクリックします。
このタスクのターゲットとなるサーバーの選択	このタスクを割り当てるサーバーを選択します。
すべて有効化	デバイス機能を上書きし、すべての利用可能デバイスをタスクのターゲットとして選択可能にします。

フィールド	説明
スケジュールと資格情報	
スケジュールの設定	次のオプションから選択します。 • **アクティブなスケジュール** — このオプションを選択して、タスクのスケジュールをアクティブにします。 • **今すぐ実行** — このオプションを選択して、ただちにタスクを実行します。 • **スケジュールの設定** — このオプションを選択して、タスクを実行する日時を設定します。 • **1 度実行** — このオプションを選択して、計画したスケジュールを 1 度だけ実行します。 • **定期的** — このオプションを選択して、指定間隔でタスクを頻繁に実行します。 – **毎時** — このオプションを選択して、タスクを 1 時間に 1 度実行します。 – **毎日** — タスクを 1 日に 1 度実行します。 – **毎週** — タスクを週に 1 度実行します。 – **毎月** — タスクを月に 1 度実行します。 **反復の範囲**： • **開始** — タスクの開始日時を指定します。 • **終了日なし** — 選択した頻度に基づいてこのタスクを継続的に実行します。例えば、毎時を選択した場合、このタスクは、開始時刻から 1 時間ごとに 1 回継続的に実行されます。 • **終了日** — タスクを指定した日時に停止します。
ターゲットのリモートアクセスコントローラ資格情報を入力	**ユーザー名** — RACADM タスクには IPMI 資格情報が必要です。このタスクを実行するには IPMI 資格情報を入力してください。 **パスワード** — パスワードを入力します。

関連リンク

コマンドラインタスク
コマンドラインタスクの管理
サーバー XML 設定サンプルコマンドラインタスクの使用

ファームウェアおよびドライバインベントリ収集タスク

このオプションを選択して、Dell OpenManage Server Administrator がインストールされていないサーバーからファームウェアとドライバのインベントリ情報を収集します。

フィールド	説明
一般	
タスク名	インベントリ収集タスクの名前を入力します。

フィールド	説明
オペレーティングシステムに基づいたデバイスのフィルタ	選択したオペレーティングシステムに基づいて **タスクのターゲット** に表示されるデバイスをフィルタするにはこのオプションを選択します。
オペレーティングシステムを選択します。	次のオプションから選択します。 • **Windows** • **Linux**
64 ビットシステム	ターゲットサーバーが 64 ビットのオペレーティングシステムを実行している場合は、このオプションを選択します。
タスクのターゲット	
クエリの選択	ドロップダウンリストからクエリを選択します。新しいクエリを作成するには、**新規** をクリックします。
このタスクのターゲットとなるサーバーを選択します。	タスクを割り当てるサーバーを選択します。
スケジュールと資格情報	
スケジュールの設定	次のオプションから選択します。 • **スケジュールのアクティブ化** — このオプションを選択して、タスクのスケジュールをアクティブにします。 • **今すぐ実行** — このオプションを選択して、ただちにタスクを実行します。 • **スケジュールの設定** — このオプションを選択して、タスクを実行する日時を設定します。 • **1 度実行** — このオプションを選択して、計画したスケジュールを 1 度だけ実行します。 • **定期的** — このオプションを選択して、指定間隔でタスクを頻繁に実行します。 – **毎時** — このオプションを選択して、タスクを 1 時間に 1 度実行します。 – **毎日** — このオプションを選択して、タスクを 1 日に 1 度実行します。 – **毎週** — このオプションを選択して、タスクを 1 週間に 1 度実行します。 – **毎月** — このオプションを選択して、タスクを 1 ヶ月に 1 度実行します。 **反復の範囲**： • **開始** — タスクの開始日時を指定します。 • **終了日なし** — 選択した頻度に基づいてこのタスクを継続的に実行します。例えば、毎時を選択した場合、このタスクは、開始時刻から 1 時間ごとに 1 回継続的に実行されます。 • **終了日** — タスクを指定した日時に停止します。

フィールド	説明
リモートターゲットの資格情報の入力	**ユーザー名** – ドメイン\ユーザー名またはローカルホスト\ユーザー名の形式で入力します。 **パスワード** – パスワードを入力します。

関連リンク

ファームウェアおよびドライバインベントリの収集

22

セキュリティ設定の管理

セキュリティの役割および許可の使用

OpenManage Essentials は、役割ベースのアクセス制御（RBAC）、認証、および暗号化を介してセキュリティを提供します。RBAC は、特定の役割を持つ人によって実行される操作を決定することにより、セキュリティを管理します。各ユーザーはそれぞれ、1 つ、または複数の役割を割り当てられ、各役割には、その役割でユーザーが許可される 1 つ、または複数のユーザー権限が割り当てられます。RBAC の使用により、セキュリティ管理は組織の構成に細かく対応します。

OpenManage Essentials の役割、およびそれらに関連付けられた許可は次のとおりです。

- **OmeUsers** は制限付きのアクセスと権限を持ち、OpenManage Essentials で読み取り限定の操作を実行できます。コンソールにログインでき、検出タスクとインベントリタスクの実行、設定の表示、イベントの承認を行うことができます。Windows ユーザーグループは、このグループのメンバーです。
- **OmeAdministrators** は OpenManage Essentials 内のすべての操作に対する完全なアクセス権を保有します。Windows 管理者グループは、このグループのメンバーです。
- **OmeSiteAdministrators** は、OpenManage Essentials 内のすべての操作に対する完全なアクセス権を持ちます。次の権限および制限があります。
  - デバイスツリーの **すべてのデバイス** に限り、カスタムデバイスグループの作成可能。**OmeAdministrators** によって割り当てられたカスタムデバイスグループに限り、リモートおよびシステムアップデートタスクの作成可能。
    - カスタムデバイスグループの編集不可。
    - カスタムデバイスグループの削除可能。
  - **OmeAdministrators** によって OmeSiteAdministrators に割り当てられたデバイスグループ上に限り、リモートおよびシステムアップデートタスクの作成可能。
  - 作成されたリモートおよびシステムアップデートタスクに限り実行および削除可能。
    - リモートタスクの編集不可。タスクスケジュールの有効化または無効化を含む。
    - リモートまたはシステムアップデートタスクのクローン不可。
    - 自身が作成したタスクのみが削除可能。
  - デバイスの削除可能。
  - デバイスクエリの編集またはターゲット不可。
  - **デバイスグループ許可** ポータルの編集不可、およびポータルへのアクセス不可。
  - デバイスクエリに基づいたリモートおよびシステムアップデートのタスクの作成不可。

  メモ: ユーザーの役割またはデバイスグループ権限に対する変更は、ユーザーがログアウトしてから再度ログインしないと有効になりません。
- **OmePowerUsers** は **OmeAdministraors** と同じ権限を保有しますが、プリファランスの編集はできません。

Microsoft Windows 認証

対応 Windows オペレーティングシステムでは、OpenManage Essentials 認証は Windows NT LAN Manager（NTLM v1 and NTLM v2）モジュールを使用するオペレーティングシステムのユーザー認証システムをベースとします。ネットワークでは、この基礎となる認証システムによって OpenManage Essentials のセキュリティを全体的なセキュリティスキームに統合することが可能になります。

ユーザー権限の割り当て

OpenManage Essentials をインストールする前にユーザー権限を OpenManage Essentials ユーザーに割り当てる必要はありません。次の手順は、OpenManage Essentials ユーザーの作成と Windows オペレーティングシステム用のユーザー権限を割り当てるための段階的な手順を説明します。

メモ: これらの手順を実行するには、システム管理者権限でログインしてください。

メモ: ユーザーの作成およびユーザーグループ権限の割り当てに関する質問、またはその他詳細手順については、オペレーティングシステムのマニュアルを参照してください。

1. Windows のデスクトップで、**スタート → すべてのプログラム → 管理ツール → コンピュータの管理** をクリックします。
2. コンソールツリーで、**ローカルユーザーとグループ** を展開して、**グループ** をクリックします。
3. **OmeAdministrators**、**OMEPowerUsers**、または **OmeUsers** グループをダブルクリックして、新規ユーザーを追加します。
4. **追加** をクリックして、追加するユーザー名を入力します。**名前をチェックして検証** をクリックしてから、**OK** をクリックします。

   新しいユーザーは、割り当てられたグループのユーザー権限で OpenManage Essentials にログインできます。

カスタム SSL 証明書の使用（オプション）

OpenManage Essentials デフォルト設定により、環境内でセキュアな通信が確立できるようになります。ただし、暗号化に自分の SSL 証明書を利用したいユーザーがいる場合もあります。

新規ドメインの証明書を作成するには、次の手順を実行します。

1. **スタート → すべてのプログラム → 管理ツール → IIS（インターネット情報サービス）マネージャ** の順に選択して、IIS（インターネット情報サービス）マネージャを開きます。
2. <サーバー名> を展開して、**サーバー証明書 → サイト** をクリックします。
3. **ドメイン証明書の作成** をクリックして、必要な情報を入力します。

   メモ: ドメイン管理者が証明書をクライアントに発行するまで、すべてのシステムが証明書エラーを表示します。

IIS サービスの設定

カスタム SSL 証明書を使用するには、OpenManage Essentials がインストールされているシステムに IIS サービスを設定する必要があります。

1. **スタート → すべてのプログラム → 管理ツール → IIS（インターネット情報サービス）マネージャ** の順に選択して、IIS（インターネット情報サービス）マネージャを開きます。
2. <サーバー名> **→ サイト** と展開します。

3. **DellSystemEssentials** で右クリックして、**バインドの編集** を選択します。
4. **サイトバインド** で **https バインド** を選択し、**編集** をクリックします。
5. **サイトバインドの編集** で、**SSL 証明書** ドロップダウンリストからお使いのカスタム SSL 証明書を選択し、**OK** をクリックします。

OpenManage Essentials でサポートされるプロトコルおよびポート

管理ステーションでサポートされるプロトコルおよびポート

ポート番号	プロトコル	ポートタイプ	最大暗号化レベル	方向	使用状況
21	FTP	TCP	なし	入力 / 出力	**ftp.dell.com** にアクセス。
25	SMTP	TCP	なし	入力 / 出力	オプションの電子メールアラート処置。
162	snmp	UDP	なし	入力	SNMP を使用したイベントの受信。
1278	HTTP	TCP	なし	入力 / 出力	Web GUI。Dell Lifecycle Controller にパッケージをダウンロード。
1279	専有	TCP	なし	入力 / 出力	タスクをスケジュール。
1433	専有	TCP	なし	入力 / 出力	オプションのリモート SQL Server アクセス。
2606	専有	TCP	なし	入力 / 出力	ネットワーク監視。
2607	HTTPS	TCP	128 ビット SSL	入力 / 出力	Web GUI。

管理下ノードでサポートされるプロトコルおよびポート

ポート番号	プロトコル	ポートタイプ	最大暗号化レベル	方向	使用状況
22	SSH	TCP	128 ビット	入力 / 出力	コンテキストアプリケーションの起動 — Server Administrator に対する SSH クライアントリモートソフトウェアアップデート — Linux システムにおける Linux オペレーティングシステムの パフォーマンス監視をサポートするシステム用。
80	HTTP	TCP	なし	入力 / 出力	コンテキストアプリケーションの起動 — Dell Networking コンソール。
135	RPC	TCP	なし	入力 / 出力	CIM を使用した Server Administrator からのイベントの受信 — Windows オペレーティングシステムをサポートするシステム用。 Server Administrator へのリモートソフトウエアアップデート転送 — Windows オペレーティングシステムのリモートコマンドラインをサポートす

ポート番号	プロトコル	ポートタイプ	最大暗号化レベル	方向	使用状況
					るシステム用 — Windows オペレーティングシステムをサポートするシステム用。
161	snmp	UDP	なし	入力 / 出力	SNMP クエリ管理。
623	RMCP	UDP	なし	入力 / 出力	LAN を使用した IPMI アクセス。
1443	専有	TCP	なし	入力 / 出力	オプションのリモート SQL Server アクセス。
443	専用 / WSMAN	TCP	なし	入力 / 出力	EMC ストレージ、iDRAC6、iDRAC7、および iDRAC8 検出とインベントリ。
3389	RDP	TCP	128 ビット SSL	入力 / 出力	コンテキストアプリケーションの起動 — Windows ターミナルサービスへのリモートデスクトップ。
6389	専有	TCP	なし	入力 / 出力	ストレージシステムでホストシステム（NaviCLI/NaviSec CLI または Navisphere ホストエージェント経由）と Navisphere アレイエージェント間の通信を有効にします。

23

トラブルシューティング

OpenManage Essentials トラブルシューティングツール

OpenManage Essentials トラブルシューティングツールは、OpenManage Essentials と共にインストールされるスタンドアローンツールです。トラブルシューティングツールは、検出およびアラートの問題の原因であることが多い、さまざまなプロトコル関連の問題に使用できます。

このツールでは、リモートノードに関する問題を特定するために、次のプロトコルに特有の診断を利用できます。

- データベース — リモートボックスに存在するユーザー定義データベースをすべて取得します。
- Dell|EMC — Dell|EMC ストレージデバイスへの接続を確認します。
- ICMP — ローカルボックスからリモートデバイスを ping できるかどうかを確認します。
- IPMI — BMC/iDRAC に接続するための IPMI プロトコルを確認します。
- 名前解決 — 解決された名前をローカルボックスから取得できるかどうかを確認します。
- OpenManage Server Administrator Remote Enablement — このテストは、Dell OpenManage Server Administrator の Remote Enablement 機能が管理下ノード（Remote Enablement コンポーネントがインストールされた Dell OpenManage Server Administrator）上で動作しているかどうかを確認するのに役立ちます。このツールは、Administrator Distributed Web Server（DWS）と同じように動作し、WSMAN プロトコルを使用して Server Administrator 管理ノード計装エージェントに接続します。

  接続に成功するには、管理ノードに OpenManage Server Administrator がインストールされていて Remote Enablement 機能が動作している必要があります。
- ポート — 指定したポートを管理ノードがリスニング中かどうかを確認します。1〜65、535 のポート番号を指定できます。
- PowerVault モジュラディスクアレイ — PowerVault ストレージデバイスへの接続に PowerVault モジュラーディスクストレージアレイプロトコルが使用されているかどうかを確認します。
- サービス — SNMP プロトコルを使用して、管理ノード上で実行中のサービスを取得します。
- SNMP — 必要な SNMP コミュニティ文字列を使用して、リモートノードへの SNMP 接続を確認し、再試行してタイムアウトになります。まず MIB-II エージェント、次に他のエージェントへの接続を試行してデバイスの種類を検出します。トラブルシューティングツール は、デバイスからのその他のエージェント固有情報の収集も行います
- SSH — 管理ノードへの接続に SSH プロトコルが使用されているかどうかを確認します。
- WMI — リモートノードへの WMI/CIM 接続を確認します。デフォルトの再試行回数およびタイムアウト値が内部で使用されます。
- WSMAN — リモートノード上の WSMAN クライアントへの接続を試行します。テストを使用して、WSMAN 仕様をサポートしている iDRAC、ESX、および他のデバイスの接続性に関する問題を検証できます。このテストはそれらのデバイスに接続し、リモートデバイス上で有効になっている公開された WSMAN プロファイルのリストも表示します。

トラブルシューティング手順

インベントリのトラブルシューティング

インベントリ済みの Linux サーバーがインベントリ未施行システムにリストされ、何度再試行してもこの状態が解決されない。

Red Hat Enterprise Linux 5.5、SUSE Linux Enterprise Server バージョン 10 およびバージョン 11 がインストールされたサーバーでこの問題を解決するには、次の手順を行います。

1. 『*Dell Systems Management Tools and Documentation DVD*』（Dell Systems Management ツールおよびマニュアル DVD）（バージョン 6.5 以降）を Linux サーバーにマウントします。
2. **srvadmin-cm** rpm をインストールします。
3. OpenManage Server Administrator 6.5 を再起動します。
4. OpenManage Server Administrator インベントリコレクタが機能していることを、**/opt/dell/srvadmin/sbin/invcol** から **/invcol -outc=/home/inv.xml** を実行して確認します。
5. サーバーのインベントリを実行します。

デバイス検出のトラブルシューティング

デバイス検出に失敗する場合は、次の手順を実行して問題をトラブルシュートし、修正します。

1. 検出対象のデバイスが Dell PowerEdge システムの場合は、Dell OpenManage Server Administrator がそのデバイス上にイストールされていることを確認します。
2. Windows デバイスを正常に検出するには、SNMP サービスを適切に設定します。Windows 上で SNMP サービスを設定する方法の詳細については、「Windows 上での SNMP サービスの設定」を参照してください。
3. Linux デバイスを正常に検出するには、SNMP サービスを適切に設定します。Linux 上で SNMP サービスを設定する方法の詳細については、「Linux 上での SNMP サービスの設定」を参照してください。
4. SNMP サービスを設定した後、SNMP サービスが正しく応答するかどうかを確認します。
5. 検出対象のデバイスが Microsoft Windows であり、検出に WMI を使用する場合は、WMI 資格情報として使用されるユーザー名とパスワードに、検出するマシンでのローカルな管理者特権が与えられていることを確認します。Microsoft **wbemtest** ユーティリティを使用して、Windows Server への WMI 接続が正しいことを確認できます。
6. 検出対象のデバイスが非サーバーネットワークデバイス（プリンタ、Dell Networking イーサネットスイッチなど）の場合は、そのデバイス上で SNMP が有効になっていることを確認します。この確認は、デバイスのウェブインタフェースにアクセスすることで実行できます。

Windows 上での SNMP サービスの設定

1. コマンド実行プロンプトを開き、**services.msc** と入力してサービス MMC を開きます。
2. **SNMP サービス** を右クリックし、**プロパティ** を選択します。SNMP サービスが見つからない場合は、**Windows コンポーネントの追加と削除** を使用してインストールします。
3. **セキュリティ** をクリックし、**すべてのホストから SNMP パケットを受け付ける** が選択されていることを確認します。
4. **受け付けるコミュニティ名** の下で、**public**（または自分で選択したコミュニティ文字列）が設定されていることを確認します。デフォルトで設定されていない場合は、**追加** をクリックし、コミュニティ文字列を **コミュニティ名** に入力します。さらに、コミュニティの権利として **読み取り専用** または **読み取り / 書き込み** を選択します。

5. **トラップ** をクリックし、コミュニティ文字列フィールドに有効な名前が設定されていることを確認します。
6. **トラップの送信先** で **追加** をクリックし、Open Manage Essentials コンソールの IP アドレスを入力します。
7. サービスを起動します。

Linux 上での SNMP サービスの設定

1. コマンド `rpm -qa | grep snmp` を実行し、**net-snmp** パッケージがインストールされていることを確認します。
2. `cd /etc/snmp` を実行して、snmp ディレクトリに移動します。
3. **snmpd.conf** を VI エディタで開きます（**vi snmpd.conf**）。
4. snmpd.conf 内で **# group context sec.model sec.level prefix read write notif** を検索し、read、write、および notif の各フィールドの値が **all** に設定されていることを確認します。
5. **snmpd.conf** ファイルの末尾において、Further Information の直前に、Open Manage Essentials コンソールの IP アドレスを次の形式で入力します。 `trapsink <OPEN MANAGE ESSENTIALS コンソールの IP> <コミュニティ文字列>` たとえば、trapsink 10.94.174.190 public と入力します。
6. SNMP サービスを起動します（service snmpd restart）。

SNMP トラップの受信に関するトラブルシューティング

SNMP トラップの受信に関する問題が発生した場合は、次の手順を実行して問題をトラブルシュートし、修正します。

1. 問題の発生した 2 つのシステム間のネットワーク接続を確認します。ping <IP アドレス> コマンドを使用して一方のシステムからもう一方のシステムへ Ping することにより接続を確認できます。
2. 管理ノード上の SNMP 設定を確認します。管理ノードの SNMP サービスに OpenManage Essentials コンソールの IP アドレスとコミュニティ文字列名が指定済みであることを確認します。

   Windows システム上での SNMP の設定方法の詳細については、「Windows 上での SNMP サービスの設定」を参照してください。

   Linux システム上での SNMP の設定方法の詳細については、『Linux 上での SNMP サービスの設定』を参照してください。
3. SNMP トラップサービスのサービスが OpenManage Essentials システム内で実行中であることを確認します。
4. ファイアウォール設定をチェックして、UDP 161、162 ポートを許可します。

Windows Server 2008 ベースのサーバーの検出に関するトラブルシューティング

サーバー検出も許可する必要があります。デフォルトでは、このオプションは Windows Server 2008 で無効になっています。

1. **スタート → コントロール パネル → ネットワークとインターネット → ネットワークと共有センター → 詳細な共有設定**の順にクリックします。
2. 該当するネットワークプロファイル（ホームまたはワーク / パブリック）のドロップダウン矢印を選択し、**ネットワーク検出**セクションの下にある**ネットワーク探索を有効にする**を選択します。

ESX または ESXi バージョン 3.5、4.x、5.0 の SNMP トラップに関するトラブルシューティング

詳細：ESX または ESXi 3.5 または 4.*x* ホストから仮想マシンおよび環境トラップを生成するには、組み込み SNMP エージェントを設定して有効化する必要があります。これらのトラップの生成に Net-SNMP ベースのエージェントは使用できませんが、GET トランザクションを受信したり、他の種類のトラップを作成することは可能です。

これは ESX 3.0.x から変更された動作を表すもので、3.0.x では Net-SNMP ベースのエージェント用設定ファイルが仮想マシントラップの生成を制御していました。

ソリューション：リモート CLI または vSphere CLI から `vicfg-snmp` コマンドを使用して、SNMP エージェントを有効化し、トラップ宛先を設定します。ターゲットを vicfg-snmp コマンドで指定するたびに、指定した設定によって以前指定した設定のすべてが上書きされます。複数のターゲットを指定するには、単一のコマンド毎にカンマで区切って指定してください。

Microsoft Internet Explorer の問題のトラブルシューティング

以下のいずれかが発生している場合は、本節の指示に従ってください。

- Internet Explorer を使用して OpenManage Essentials を開くことができない。
- Internet Explorer で証明書エラーが表示される。
- Internet Explorer で証明書の承認メッセージが表示される。
- Server Administrator とシステムアップデートの導入のためにファイルシステムを参照できない。
- デバイスのデバイスツリーを表示できない。
- アクティブなコンポーネントをインストールできない。

1. Internet Explorer を使用してクライアントサーバーで OpenManage Essentials を開きます。
2. **ツール → インターネットオプション → セキュリティ**の順にクリックします。
3. **ローカルイントラネット** を選択して **サイト** をクリックします。
4. **詳細設定** をクリックします。
5. OpenManage Essentials がインストールされているサーバーの完全修飾名を入力します。
6. **追加** をクリックします。

   問題が解消されない場合は、DNS サーバーでの OpenManage Essentials サーバー名の解決に問題がある可能性があります。「DNS サーバー問題の解決」を参照してください。

   証明書エラーが表示された場合：

   - 発行された OpenManage Essentials 証明書を、ドメインシステムの「信頼されたルート証明機関」と信頼された発行元に追加するようシステム管理者に連絡します。
   - OpenManage Essentials 証明書を「信頼されたルート証明機関」および「信頼された発行元」の証明書ストアに Internet Explorer を使用して追加します。

DNS サーバー問題の解決

DNS サーバー問題を解決するには、次の手順を実行してください。

1. システム管理者に連絡し、OpenManage Essentials を実行しているシステムの名前を DNS サーバーに追加します。
2. ホストファイルを編集して、OpenManage Essentials を実行しているシステムの IP を解決します。ホストファイルは **%windir%\System32\drivers\etc\hosts** にあります。

3. OpenManage Essentials を実行しているシステムの IP を Internet Explorer でローカルイントラネットサイトに追加します。

   メモ: OpenManage Essentials を実行しているサーバーの完全修飾名を使用しない限り証明書エラーは解消しません。

マップビューのトラブルシューティング

質問：**マップビュー** 機能が利用できないのはなぜですか?

回答：**マップビュー** 機能は、Enterprise ライセンス済みの Dell PowerEdge VRTX CMC を WS-Man プロトコルを使用して検出した場合にのみ利用可能です。Enterprise ライセンス済みの PowerEdge VRTX CMC を SNMP プロトコルを使用して検出した場合、**マップビュー** 機能は利用できません。Enterprise ライセンス済み Dell PowerEdge VRTX CMC のデバイス詳細ポータルに **マップビュー** タブが表示されない場合、WS-Man プロトコルを使用した PowerEdge VRTX CMC の再検出が必要です。

質問：特定のデバイスをマップに追加できないのはなぜですか?

回答：Enterprise ライセンスのある PowerEdge VRTX デバイスのみマップに追加可能です。

質問：MapQuest または Bing マッププロバイダでマップがロードされません。どうすればよいですか?

回答：これはインターネットの接続性の問題を示しています。

- ブラウザからインターネットに接続できるか確認してください。
- システムがプロキシ経由でインターネットに接続している場合、次の手順を実行します。
  - MapQuest マッププロバイダの場合 — OpenManage Essentials **プリファランス → コンソール設定** ページでプロキシ設定を設定します。
  - Bing マッププロバイダの場合 — プロキシサーバー設定を Internet Explorer で設定したことを確認してください。
- MapQuest ウェブサイトにアクセスできるか確認してください。

質問：マップのロードに時間がかかるのはなぜですか?

回答：マップのロードに時間がかかるのは、通常のブラウジングに比べて必要なネットワーク帯域幅とグラフィック処理機能が多いためです。また、マップ上でズームやパンを繰り返す場合にもマップのロードが遅くなります。

質問：検索バーまたは **デバイス位置の編集** ダイアログボックスを使って住所を検出できないのはなぜですか?

回答：インターネット接続に問題があるか、マップのプロバイダが住所を解決できない可能性があります。

- ブラウザからインターネットに接続できるか確認してください。
- システムがプロキシ経由でインターネットに接続している場合、次の手順を実行します。
  - MapQuest マッププロバイダの場合 — OpenManage Essentials **プリファランス → コンソール設定** ページでプロキシ設定を設定します。
  - Bing マッププロバイダの場合 — プロキシサーバー設定を Internet Explorer で設定したことを確認してください。
- 入力したアドレスの入力方法を変えてください。住所を完全に入力してみることもできます。州、国、空港コードなどの略語を入力すると期待通りの結果が得られない場合があります。

質問：**ホーム** ポータルではあるマッププロバイダが利用できず、**デバイス** ポータルでは別のマッププロバイダが利用できないのはなぜですか?

回答：**ホーム** ポータルおよび **デバイス** ポータルで利用可能な **マップビュー** は同期しています。**マップビュー** で **設定** またはデバイス位置を変更すると、両方のポータルに影響します。

質問：**マップビュー** の使い勝手を改善するにはどうすればよいですか?

回答：ネットワーク帯域幅を拡大させるとマップのロードが高速化します。より高性能なグラフィックカードを使用するとズームとパン機能が速くなります。MapQuest プロバイダを使用するときは、OpenManage Essentials が管理サーバーで起動されているとマップがより良くレンダリングされます。

24

よくあるお問い合わせ

インストール

質問：リモート SQL データベース名前付きインスタンスを使用して OpenManage Essentials をインストールするにはどのようにしますか?

回答：リモートで接続するには、名前付きインスタンスのある SQL Server で **SQL Server ブラウザ**サービスが実行されている必要があります。

質問：OpenManage Essentials は Microsoft SQL Server 評価版をサポートしていますか?

回答：いいえ、SQL Server 評価版はサポートされません。

質問：SQL Server の最小ログイン役割は何ですか?

回答：『Microsoft SQL Server の最小ログイン役割」および「Relational Database Management System の使用諸条件」を参照してください。

質問：OpenManage Essentials インストーラの起動時に、特定のライブラリのロード失敗（例：`OMIL32.DLL` のロードに失敗）、アクセス拒否、初期化エラーを示すエラーメッセージが表示されます。どのすればよいですか?

回答：これはおそらく、システム上の Component Object Model（COM）許可の不足が原因です。この状態を修正するには、**support.installshield.com/kb/view.asp?articleid=Q104986** を参照してください。以前の Systems Management Software またはその他ソフトウェア製品のインストールが正しく行われなかった場合にも、OpenManage Essentials インストーラの動作に失敗することがあります。Windows インストーラの一時レジストリ、**HKLM\Software\Microsoft\Windows\CurrentVersion\Installer\InProgress** がある場合は、これを削除してください。

アップグレード

質問：エラーメッセージ

`Https error 503. The service is unavailable` に対してどんなトラブルシューティングを行えばよいですか?

回答：この問題を解決するには、IIS リセットを行い、OpenManage Essentials を起動します。IIS リセットを行うには、コマンドプロンプトを起動し、`iisreset` と入力します。iisreset が完了すると、ウェブサーバーに対するすべての接続がリセットされます。また、同じ OpenManage Essentials サーバーでホストされているすべてのウェブサイトもリセットされます。

質問：OpenManage Essentials の最新バージョンへのアップグレードが大型の導入シナリオで失敗するのはなぜですか?

回答：この問題を解決するには、システムがハードウェアの最小要件を満たしていることを確認します。詳細については、**dell.com/openmanagemanuals** の『*Dell OpenManage Essentials User's Guide*』の「最小推奨ハードウェア」セクションを参照してください。

質問：SQL Server 2005 を使用するリモートデータベースに OpenManage Essentials バージョン 1.1 がインストールされているとき、OpenManage Essentials バージョン 2.0.1 へのアップグレードはどのようにすればよいですか?

回答：OpenManage Essentials バージョン 2.0.1 のインストールまたはアップグレードは、ローカルまたはリモートデータベースのいずれの場合も、Microsoft SQL Server 2005（全エディション）非対応です。リモート SQL Server 2005 と共にインストールされた OpenManage Essentials バージョン 1.1 を OpenManage Essentials バージョン 2.0.1 にアップグレードする際は、次のメッセージが表示されます。

```
Dell OpenManage Essentials cannot be installed or upgraded on SQL Server
versions prior to SQL Server 2008. Refer to the FAQ for information on possible
migration and additional details.
```

この場合、SQL Server 2005 からデータを手動で移行した後、OpenManage Essentials バージョン 2.0.1 にアップグレードすることができます。以下の手順を実行してください。

1. OpenManage Essentials バージョン 1.1 データベースのバックアップを作成します。
2. OpenManage Essentials バージョン 1.1 のデータを SQL Server 2005 から SQL Server 2008、2008 R2、または 2012 に移行します。詳細については、**http://en.community.dell.com/techcenter/systems-management/f/4494/t/19440364.aspx**. にある『*OpenManage Essentials データベース再ターゲットプロセス』を参照してください。*.
3. OpenManage Essentials バージョン 1.1 が移行されたデータベースに接続することができ、正常に機能することを確認してください。
4. OpenManage Essentials バージョン 2.0.1 インストーラを起動してアップグレードを完了します。

メモ: SQL Server 2012 との OpenManage Essentials バージョン 2.0.1 へのアップグレード後、SQLEXPRESSOME インスタンスが作成され、OpenManage Essentials バージョン 1.1 のデータが OpenManage Essentials バージョン 2.0.1 に移行されます。

タスク

質問：ソフトウェアアップデートタスクまたはリモートタスクの作成や実行に失敗した場合は、どのようなトラブルシューティングを実行できますか?

回答: Windows サービスで DSM Essentials Task Manager サービスが実行されていることを確認してください。

質問: OpenManage Server Administrator を展開するときにどのようにコマンドライン機能を使用しますか?

回答：無人インストールは次の機能を提供します。

- 無人インストールをカスタマイズするオプションのコマンドライン設定セット。
- 特定のソフトウェア機能のインストールを指定するカスタマイズパラメータ。

オプションのコマンドライン設定

次の表に、**msiexec.exe** MSI インストーラで使用可能なオプションの設定を示します。コマンドラインで、**msiexec.exe** の後に各設定の間にスペースを入れてオプションの設定を入力します。

メモ: Windows Installer Tool のすべてのコマンドラインスイッチに関する完全な詳細については、**support.microsoft.com** を参照してください。

表 3. MSI インストーラのコマンドライン設定

設定	結果
/i <Package|Product Code>	このコマンドを使用すると、製品がインストールまたは設定されます。 **/i SysMgmt.msi** – Server Administrator ソフトウェアがインストールされます。
/i SysMgmt.msi /qn	このコマンドを使用すると、バージョン 6.1 のフレッシュインストールが実行されます。
/x <Package|Product Code>	このコマンドを使用すると、製品がアンインストールされます。 **/x SysMgmt.msi** – Server Administrator ソフトウェアがアンインストールされます。
/q[n|b|r|f]	このコマンドを使用すると、ユーザーインタフェース（UI）レベルが設定されます。 **/q** または **/qn** – UI なし。このオプションは、サイレントおよび無人インストールに使用されます。**/qb** – 基本的な UI。このオプションは、サイレントインストールではなく無人インストールに使用されます。**/qr** – 簡易的な UI。このオプションは、無人インストールに使用され、インストールの進捗度を示すモーダルダイアログボックスを表示します。**/qf** – 完全な UI。このオプションは、標準的な有人インストールに使用されます。
/f[p|o|e|d|c|a|u|m|s|v]<Package| ProductCode>	このコマンドを使用すると、製品が修復されます。 **/fp** – このオプションを使用すると、ファイルが不在の場合にのみ製品が再インストールされます。 **/fo** – このオプションを使用すると、ファイルが欠落している場合や、ファイルの古いバージョンがインストールされている場合に、製品が再インストールされます。 **/fe** – このオプションを使用すると、ファイルが欠落している場合や、ファイルの同じバージョンまたは古いバージョンがインストールされている場合に、製品が再インストールされます。

設定	結果
	/fd – このオプションを使用すると、ファイルが欠落している場合や、ファイルの異なるバージョンがインストールされている場合に、製品が再インストールされます。 **/fc** – このオプションを使用すると、ファイルが欠落している場合や、保存されたチェックサム値が計算された値と一致しない場合に、製品が再インストールされます。 **/fa** – このオプションを使用すると、すべてのファイルが強制的に再インストールされます。 **/fu** – このオプションを使用すると、すべての必要なユーザー固有のレジストリエントリが書き換えられます。 **/fm** – このオプションを使用すると、すべての必要なシステム固有のレジストリエントリが書き換えられます。 **/fs** – このオプションを使用すると、すべての既存のショートカットが上書きされます。 **/fv** – このオプションを使用すると、ソースから実行し、ローカルパッケージを再キャッシュします。アプリケーションまたは機能の初めてのインストールには、**/fv** 再インストールオプションを使用しないでください。
INSTALLDIR=<path>	このコマンドを使用すると、製品が特定の場所にインストールされます。このスイッチで指定するインストールディレクトリは、CLI インストールコマンドを実行する前に手動で作成しておく必要があります。そうしないと、エラーメッセージを表示しないで失敗します。 **/i SysMgmt.msi INSTALLDIR=c:\OpenManage /qn** – **c:\OpenManage** をインストール場所として、製品をインストールします。

たとえば、**msiexec.exe /i SysMgmt.msi /qn** の実行によって、Server Administrator 機能が各リモートシステムに、システムのハードウェア設定に基づいてインストールされます。このインストールは、サイレントかつ無人で実行されます。

カスタマイズ用パラメータ

REINSTALL および **REMOVE** のカスタマイズ用 CLI パラメータを使用すると、サイレント状態で実行する場合や無人で実行する場合にインストール、再インストール、またはアンインストールするソフトウェア機能を正確にカスタマイズできます。 カスタマイズ用パラメータを使用すると、同じ無人インストールパッケージを使用してさまざまなシステムのソフトウェア機能を選択的にインストール、再インストール、またはアンインストールできます。たとえば、特定のサーバーグループに Server Administrator をインストールしても Remote Access Controller サービスはインストールしないように選択したり、別のサーバーグループへは Server Administrator をインストールして Storage Management サービスはインストールしないことを選択

することができます。 また、サーバーの特定のグループで 1 つまたは複数の機能のアンインストールを選択することもできます。

メモ: 大文字で REINSTALL パラメータと REMOVE の CLI パラメータを入力します（大文字と小文字が区別されます）。

メモ: 次の表に記載されるソフトウェア機能 ID は、大文字と小文字が区別されます。

表 4. ソフトウェア機能 ID

機能 ID	説明
すべて	すべての機能
BRCM	Broadcom NIC エージェント
INTEL	Intel NIC エージェント
IWS	Dell OpenManage Server Administrator Web サーバー
OMSM	Server Administrator Storage Management Service
RmtMgmt	Remote Enablement
RAC4	Remote Access Controller（DRAC 4）
RAC5	Remote Access Controller（DRAC 5）
iDRAC	Integrated Dell Remote Access Controller
SA	サーバーシステム管理者

メモ: xx1x システムでは iDRAC6 のみがサポートされています。

REINSTALL カスタマイズ用パラメータをコマンドラインに含め、再インストールするソフトウェア機能の機能 ID を割り当てることができます。以下に例を示します。

```
msiexec.exe /i SysMgmt.msi REINSTALL=BRCM /qb
```

このコマンドを使用すると、サイレントモードではなく無人モードで Dell OpenManage Systems Management のインストールが実行され、Broadcom エージェントだけが再インストールされます。

REMOVE カスタマイズ用パラメータをコマンドラインに含め、アンインストールするソフトウェア機能の機能 ID を割り当てることができます。以下に例を示します。

```
msiexec.exe /i SysMgmt.msi REMOVE=BRCM /qb
```

このコマンドを使用すると、無人モードで Dell OpenManage Systems Management のアンインストールが実行され、Broadcom エージェントだけがアンインストールされますが、サイレントモードではアンインストールされません。

また、**msiexec.exe** プログラムを 1 回実行するだけで、機能のインストール、再インストール、およびアンインストールを選択することもできます。以下に例を示します。

msiexec.exe /i SysMgmt.msi REMOVE=BRCM /qb

このコマンドを実行すると、管理下のシステムソフトウェアのインストールが実行され、Broadcom エージェントがアンインストールされます。これはサイレントモードではなく無人モードで実行されます。

メモ: グローバルに一意の識別子（GUID：Globally Unique Identifier）は、128 ビット長であり、GUID を生成するために使用されるアルゴリズムにより、各 GUID が一意であることが確実化されます。製品 GUID は、アプリケーションを一意に識別します。この場合、Server Administrator の製品 GUID は {54C04D53-C3C3-46EA-A75F-7AFF4BEB727C} です。

MSI 戻りコード

アプリケーションイベントログエントリは、**SysMgmt.log** ファイルに記録されます。表 3 には、**msiexec.exe** Windows インストーラエンジンにより返されるエラーコードの一部が示されています。

表 5. Windows インストーラの戻りコード

エラーコード	値	説明
ERROR_SUCCESS	0	処置が正常に完了しました。
ERROR_INVALID_PARAMETER	87	パラメータのひとつが無効です。
ERROR_INSTALL_USEREXIT	1602	ユーザーがインストールをキャンセルしました。
ERROR_SUCCESS_REBOOT_REQUIRED	3010	インストールを完了するためには再起動が必要です。このメッセージは正常なインストールを示しています。

メモ: msiexec.exe および **InstMsi.exe** Windows Installer 機能によって返されるすべてのエラーコードに関する完全な詳細については、**support.microsoft.com** を参照してください。

電子メールアラート処置

質問：電子メールアラート処置のセットアップ後に電子メールが受信されないのはなぜですか?

回答：システムにアンチウィルスクライアントがインストールされている場合は、電子メールを許可するように設定してください。

検出

質問：SSH プロトコルを使って検出した後、SUSE Linux Enterprise および Red Hat Enterprise Linux ベースのサーバーが **サーバー** カテゴリに表示されないのはなぜですか?

回答：OpenManage Essentials SSH プラグインは、sshlib2 を使用しています。sshlib2 は、**パスワードによる認証** オプションを無効にした Linux サーバーの認証には失敗します。このオプションを有効にするには、次の手順を行います。

1. 編集モードで **/etc/ssh/sshd_config** ファイルを開き、**PasswordAuthentication** キーを検索します。
2. 値をはいに設定し、ファイルを保存します。
3. sshd サービス **/etc/init.d/sshd restart** を再起動します。

これでサーバーが **デバイス** ツリーの **サーバー** カテゴリに表示されるようになります。

質問：検出タスクの作成や実行に失敗した場合は、どのようなトラブルシューティングを実行できますか?

回答：Windows サービスで DSM Essentials Task Manager サービスが実行されていることを確認してください。

質問：使用している ESX 仮想マシンが ESX ホストサーバーと相互に関連付けられていないのはなぜですか?

回答：SNMP および WSMan を使用して ESXi ホストサーバーを検出する必要があります。そうしなければ、SNMP を使用してゲスト仮想マシンが検出された時に正しく相互に関連付けられません。

質問：WMI で検出されたデバイスが不明と分類されるのはなぜですか?

回答：WMI 検出は、Administrators グループ（Administrator ではない）のユーザーアカウント用資格情報が検出範囲に提示されるとき、場合によってはデバイスを不明と分類します。

この問題が発生する場合は、**support.microsoft.com/?scid=kb;en-us;951016** の KB 記事を読み、説明されているとおりにレジストリ作業を適用してください。この解決方法は、Windows Server 2008 R2 で管理されるノードに適用されます。

質問：ルート CA 証明書付き WS-Man を使用して検出された Dell デバイスが「不明」に分類されるのはなぜですか ?

回答：WS-Man ターゲットの検出に使用したルート証明書に問題がある可能性があります。ルート CA 証明書を使用した WS-Man ターゲットの検出およびインベントリの方法については、「ルート証明書付き WS-Man プロトコルを使用した Dell デバイスの検出とインベントリ」を参照してください。

質問：SNMP 認証トラップとは何ですか?

回答：認証トラップは、SNMP エージェントが、認識しないコミュニティ名を含む要求を受け取ったときに送信されます。このコミュニティ名は、大文字と小文字が区別されます。

トラップは、誰かがシステムをプローブしているのを見つける場合に便利ですが、最近ではただパケットを盗聴してコミュニティ名を探し出す方が簡単です。

ネットワーク上で複数のコミュニティ名を使用していて、管理の一部が重複する可能性がある場合、誤検出（不便）につながることからこれらをオフにすることを考慮してください。

詳細については、**t**echnet.microsoft.com/en-us/library/cc959663.aspx を参照してください。

SNMP エージェントが、有効なコミュニティ名を含まない要求を受け取った場合や、メッセージを送信するホストが許容ホストのリストにない場合、エージェントは 1 つまたは複数のトラップ宛先（管理システム）に認証トラップメッセージを送信できます。トラップメッセージは SNMP リクエストが認証されなかったことを示します。これはデフォルトの設定です。

質問：OpenManage Essentials が、検出ウィザードでのアンダースコア付きのホスト名の入力をサポートしないのはなぜですか?

回答：RFC 952 で指定されているとおり、アンダースコアは DNS 名で無効です。*名前*（ネット、ホスト、ゲートウェイ、またはドメイン名）は、最長 24 文字の文字列であり、アルファベット（A〜Z）、数字（0〜9）マイナス記号（-）、およびピリオド（.）で構成されます。ピリオドは、ドメイン形式名の要素を区切る場合にのみ使用が許可されます。

詳細については、ietf.org/rfc/rfc952.txt および zytrax.com/books/dns/apa/names.html を参照してください。

質問：オンデマンドとは何ですか?

回答：オンデマンドとは、SNMP トラップの受信時に OpenManage Essentials によって管理下のシステムの状態をチェックする操作です。オンデマンド機能を有効にするために設定を変更する必要はありません。ただし、管理システムの IP アドレスが SNMP サービスのトラップ宛先で利用可能である必要があります。SNMP トラップは、サーバーコンポーネントに問題または不具合がある場合に管理下システムから受け取ります。これらのトラップは、アラートログで表示できます。

インベントリ

質問：インベントリタスクの作成または実行に失敗した場合は、どのようなトラブルシューティングを実行できますか?

回答：Windows サービスで DSM Essentials Task Manager サービスが実行されていることを確認してください。

質問：ファームウェアおよびドライバのインベントリ収集タスク、または検出 / インベントリ後に、ソフトウェアインベントリ情報表に、複数の「ベースシステムのデバイスドライバ」エントリが表示されます。どうすればよいですか?

回答：この問題を解決するには、チップセットドライバがサーバーにインストールされていることを確認します。チップセットドライバがインストールされていない場合は、最新のチップセットドライバをインストールしてからサーバーを再起動します。サーバーの再起動後、OpenManage Essentials でサーバーを再検出します。

システムアップデート

質問：OpenManage Essentials 管理者（OMEAdmin）として、デバイスにシステムアップデートを実行できない場合はどうすればよいですか?

回答：この問題を解決するには、次の手順のいずれかを実行します。

- サーバー管理者グループに OMEAdmin を追加します。
- **スタート → コントロールパネル → ユーザーアカウント → ユーザーアカウントコントロール設定の変更** をクリックすることにより、ユーザーコントロール設定を減らします。

質問：iDRAC がパッケージのダウンロードを行わない場合はどうしたらよいですか?

回答：この問題を解決するには、以下を確認します。

- デフォルトウェブサイトが IIS で有効になっている。
- 仮想フォルダ（**install_packages**）が存在し、**SystemUpdate** フォルダをポイントしている。

デフォルトウェブサイトが IIS で有効になっている。

質問：パッケージはどの順序でシステムにインストールされますか?

回答：パッケージは次の順序で適用されます。:

1. ドライバ
2. ファームウェア
3. ファームウェア ES
4. BIOS

質問: OpenManage Essentials が Dell オンラインからのリソースを使用するすべての機能を活用できるようにするには、Internet Explorer の Enhanced Security Configuration をどのように設定しますか?

回答：Internet Explorer の Enhanced Security Configuration が有効な環境で、これらの機能が Dell Open Manage Essentials コンソールで動作するようにします。 ユーザーは、***.dell.com** を **信頼済みサイト ゾーン** に追加する必要があります。

ユーザーが Dell オンラインをソースとして選択する場合は、*カタログのインポート* および *システムアップデート* にインターネットアクセスが必要です。

保証レポートも情報の取得に Dell オンラインリソースを使用し、インターネットアクセスなしではデータを返しません。

質問：BMC ユーティリティのインストール後に IPMI が無効な場合はどうしたらいいですか?

回答：DSM Essentials Network Monitor サービス、DSM Essentials Task Manager サービスを再起動し、IIS を再起動してください。

質問：Omremote とは何ですか?

回答：Omremote により、リモート Server Administrator コマンドラインタスク（inband）を実行したり、リモート Dell サーバーに Server Administrator を実装することができます。Omremote は C:\Program Files\Dell\SystMgt\Essentials\bin フォルダに入っている実行可能ファイルです。Windows ベースデバイスの場合は WMI 接続、Linux ベースデバイスの場合は SSH を使用します。必要なポートが解放されていることを確認してください。Omremote コマンドを使用するには、Server Administrator がサポートされているオペレーティングシステムにインストールされている必要があります。リモートシステムに Server Administrator をインストールおよびアップデートするには、オペレーティングシステムのプリインストールパッケージを使用する必要があります。

質問：ソフトウェアアップデートのために Dell カタログをどのようにロードしますか? また、ソフトウェアアップデートタスクの実行時にエラーが発生した場合は、どうしたらいいですか?
回答：

1. まず、カタログを直接 OpenManage Essentials システムにダウンロードするか、ローカルシステムのドライブで System Update Utility DVD を使用します。
2. ローカルシステムまたは DVD で **catalog.xml** ファイルを参照します（ファイル共有では行いません。ファイル共有を使用することも可能ですが、トラブルシューティングには使用しないでください）。
3. この時点で、ソフトウェアアップデートタスクを作成します。タスクが失敗する場合は、タスク詳細により多くの情報が記載されています。
4. タスクが実行されない場合は、Internet Explorer のすべてのセキュリティ設定を低に設定してみてください。

デバイス設定の管理

質問：デバイス設定ウィザードにサポートされていないデバイスグループが表示されるのはなぜですか？

回答：ユーザーが作成したすべてのカスタムグループはデバイス選択画面に表示されます。ウィザードではカスタムグループに無効なシステムグループが含まれていることがあります。無効なシステムグループは無視して構いません。

質問：属性をフィルタし、デバイス設定テンプレートを保存した場合、テンプレートにはフィルタ後の属性のみが含まれるのですか？

回答：いいえ、テンプレートにはすべての属性が含まれます。属性をフィルタしても、保存される属性には何も影響を及ぼしません。テンプレートから属性を削除するには、その属性の導入チェックボックスからチェックを外し、テンプレートを保存します。

質問：現在のテンプレートに既に関連付けられているデバイスがデバイス選択ページに表示されるのはなぜですか？

回答：デバイス選択ページには、現在テンプレートに関連付けられているデバイスを含むすべての該当するデバイスが表示されます。必要に応じて、現在関連付けられているデバイスは無視して、別のデバイスを選択することができます。

デバイスグループ許可

デバイスグループ許可ポータル

質問：**OmeSiteAdministrators** 役割にユーザーグループを追加できますか?

回答:できません。**OmeSiteAdministrators** 役割へのユーザーグループの追加は OpenManage Essentials バージョン 1.2 では対応していません。

質問：**OmeSiteAdministrators** 役割に OmeAdministrator を追加できますか?

解答：はい、OmeAdministrator は **OmeSiteAdministrators** 役割に追加することが可能です。ユーザーは OmeAdministrator の権限のすべてを持つことになります。ただし、デバイスグループ許可を効率的に管理するには、OmeSiteAdministrators 役割のメンバーを OmeAdministrators および OmePowerUsers 役割から削除することをお勧めします。

質問:OpenManage Essentials にログオンしていないユーザーを **OmeSiteAdministrators** 役割に追加できますか?

回答：できます。**OmeSiteAdministrators のメンバーの編集** ウィザードを使用して、OpenManage Essentials にログオンしていないユーザーを **OmeSiteAdministrators** 役割に追加できます。

質問：OmePowerUser を **OmeSiteAdministrators** 役割に追加するとどうなりますか?

回答:役割と権限が追加されます。ユーザーに OmeSiteAdministrator のすべての制限があるわけではありません（ただし一部の制限は残ります）。ユーザーは OmeSiteAdministrator では実行できなかった編集アクションを実行できます。ターゲットセキュリティはこのタイプのユーザー（割り当てられたデバイスグループを編集可能）には保証できません。

質問：OmeSiteAdministrator を OmeAdministrator に昇格できますか?

回答：できます。ユーザーにはすべての権限が与えられ、すべてのデバイスをターゲットにできます。ただし、ユーザーを **OmeSiteAdministrators** 役割から削除してから **OmeAdministrators** 役割に追加することをお勧めします（必須ではありません）。

質問：現在の OmeAdministrator を **OmeSiteAdministrators** 役割に追加するには、どうすればよいですか?

回答：

1. **OmeAdministrators** Windows ユーザーグループからユーザーを削除します。
2. **デバイスグループ許可** ポータルで、**OmeSiteAdministrators のメンバーの編集** オプションを使用してユーザーを選択し、**OmeSiteAdministrators** 役割に追加します。
3. ユーザーが再度ログインするとき、ユーザーは OmeSiteAdministrator になります。

質問：ユーザーが **OmeAdministrators** 役割から削除された後、**OmeSiteAdministrators** 役割に追加されました。ユーザーが OmeAdministrator であったときに作成されたタスクはどうなりますか?

回答：ユーザーが OmeAdministrator であったときに作成されたタスクは、タスク作成時に選択されたターゲットで引き続き実行可能です。

リモートおよびシステムアップデートタスク

質問：**OmeSiteAdministrators** デバイスグループ権限が変更された場合、リモートタスクのタスクターゲットはどうなりますか?

回答：リモートタスクのタスクターゲットはデバイスグループ権限の変更に影響されません。以前作成されたリモートタスクには、OmeSiteAdministrator が割り当てられていないタスクターゲットがある可能性があります。

質問：タスクの編集で OmeSiteAdministrator がしなければならないことは何ですか?

回答：OmeSiteAdministrator がタスクの所有者の場合、OmeSiteAdministrator は既存のタスクを削除して新しいタスクを作成する必要があります。

質問：OmeSiteAdministrator はタスクを再実行できますか?

回答：できます。OmeSiteAdministrator によって作成されたタスクであれば再実行できます。

質問：OmeSiteAdministrator は OmeSiteAdministrator のユーザー名の変更後にタスクを再実行できますか?

回答：できません。ユーザー名を変更した場合は、OmeSiteAdministrator はタスクを再作成する必要があります。

質問：2 名の **OmeSiteAdministrator** を同じカスタムデバイスグループに割り当てて、互いに作成したタスクを使用することはできますか?

回答：できません。**OmeSiteAdministrator** が使用できるのは自ら作成したタスクのみです。

カスタムデバイスグループ

質問：OmeSiteAdministrator はどのグループのデバイスでも削除できますか?

回答：できます。OmeSiteAdministrator は OmePowerUser または OmeAdministrator と同様に、どのグループのデバイスでも削除できます。

質問：**OmeSiteAdministrators** は作成したデバイスグループを編集できますか?

回答：できません。**OmeSiteAdministrators** はデバイスグループまたはクエリを編集できません。

質問：**OmeSiteAdministrators** はクエリとカスタムグループを削除できますか?

回答：できます。**OmeSiteAdministrators** はクエリとカスタムグループを削除できます。

質問：**OmeSiteAdministrators** はデバイスをカスタムデバイスグループに追加できますか?

回答：できません。**OmeSiteAdministrators** はカスタムデバイスグループを編集できません。

ログ

質問：OpenManage Essentials でログを有効にするにはどのようにしたらよいですか?

回答：ログを有効にするには、次の手順を実行します。

1. **C:\Program Files\Dell\SysMgt\Essentials\configuration** または OpenManage Essentials がインストールされているパスに移動します。
2. メモ帳で **dconfig.ini** ファイルを開きます。
3. [Logging] の項で、以下を変更します。
   - LOG_ENABLED=true を設定してログを有効にします。
   - LOG_TO_FILE=true を設定してファイルにログを書き込みます。
   - LOG_FILE_PREFIX のパスを入力します。例えば、LOG_FILE_PREFIX=**C:\windows\temp**。
   - 必要に応じて、LOG_FILE_SUFFIX=ome_log.txt のファイルの接尾辞を変更します。
   - LOG_LEVEL_MIN のログレベルを設定します。例えば、LOG_LEVEL_MIN=debug。

     メモ: デバッグまたはトレースの最小ログレベル（LOG_LEVEL_MIN）を設定すると OpenManage Essentials のパフォーマンスが低下します。
   - LOG_LEVEL_MAX のログレベルを設定します。例えば、LOG_LEVEL_MAX=output。

     メモ: 最大ログレベル（LOG_LEVEL_MAX）は必ず出力に設定します。

   メモ: ログの重大度レベルの詳細については、「ログレベル」の項を参照してください。
4. ファイルを閉じて **サービス** Microsoft 管理コンソールのすべての DSM サービスを再起動します。

ログレベル

ログレベルを設定すると、ログするメッセージ重大度タイプの範囲が決定されます。下表に LOG_LEVEL_MIN および LOG_LEVEL_MAX に割り当て可能なログメッセージの重大度レベルを示します。

重大度レベル	説明
トレース	コードフローに関連する詳細情報です。

重大度レベル	説明
	メモ: 技術サポートから指示のない限り、トレースの最小ログレベルを設定しないことを推奨します。
デバッグ	問題の診断時に役立つ詳細情報です。
情報	運用イベントに関連する情報です。
警告	予期しない事態が発生したこと、または近い将来に何らかの問題が発生することを示すインジケータです。ソフトウェアはまだ想定通りに機能しています。通常、設定またはネットワークの問題（タイムアウト、再試行など）に関連しています。
エラー)	ソフトウェアによる一部機能の実行不能の原因となる問題です。
致命的	重大なエラー。ソフトウェアの実行を継続できない可能性があることを示します。
出力	ロギングシステムが初期化されていない場合に、出力する必要のある情報です。

デフォルトでは、最小および最大ログメッセージ重大度レベルがそれぞれ以下のように設定されています。

- LOG_LEVEL_MIN=info
- LOG_LEVEL_MAX=output

デフォルト設定では、重大度が最小で「情報」、最大で「出力」 のメッセージがすべてログされます。

トラブルシューティング

質問：ESXi 5 ホストからの SNMP トラップが不明として OpenManage Essentials に表示されたらどうしたらよいですか?

答え：ESXi 5 ホストの SNMP config 内でハードウェアイベントソースを、CIM から IPMI に変更する必要があります。次のコマンドを実行します：

```
vicfg-snmp.pl --username root --password <yourpassword> --server <yourserver> --
hwsrc sensors
```

--show コマンドは以下を出力します：

Current SNMP agent settings:

Enabled : 1

UDP port : 161

Communities : public

Notification targets :

<myOMEservername>@162/public

Options :

EnvEventSource=sensors

25

デバイスグループ許可の管理

デバイスグループ許可 ポータルでは、**OmeAdministrators** がユーザーに対して、特定のデバイスグループ上でシステムアップデートおよびリモートタスクを実行する許可を付与することができます。

デバイスグループ許可 ポータルを使用して、**OmeAdministrators** は次の操作を行うことができます。

- **OmeSiteAdministrators** 役割にユーザーを追加する。
- **OmeSiteAdministrators** 役割の各ユーザーにデバイスグループを割り当て、ユーザーが、割り当てられたデバイスグループ上でのみシステムアップデートを実行してリモートタスクを実行できるようにします。

メモ: デバイスグループ許可を効率的に管理するには、**OmeSiteAdministrators** 役割のメンバーを **OmeAdministrators** および **OmePowerUsers** 役割から削除することをお勧めします。

メモ: デバイスグループがユーザーに割り当てられていない場合は、ユーザーによるそのデバイスグループでのシステムアップデートおよびリモートタスクの実行のみが制限されます。そのデバイスグループが **デバイス** ポータル内のデバイスツリーから非表示になったり削除されたりすることはありません。

一般タスク ペインには、**OmeSiteAdministrators** 役割へのユーザーの追加、またはこの役割からのユーザーの削除を行うために使用することができる **OmeSiteAdministrators のメンバーの編集** オプションが表示されます。

デバイスグループ許可の管理 ペインには、**OmeSiteAdministrators** がツリービュー形式で表示されます。ツリービューのルートで **OmeSiteAdministrators** を選択すると、**ユーザー概要** が右側ペインに表示されます。**OmeSiteAdministrators** ツリービューでユーザーを選択すると、右側ペインにユーザー名および **タスクとパッチ対象のデバイスグループ** セクションが表示されます。

メモ: OmeSiteAdministrators タスクのターゲットは、タスク作成時のままです。**OmeAdministrators** が **OmeSiteAdministrators** デバイスグループの権限を変更した場合、タスクのターゲットは変更されません。**OmeSiteAdministrators** デバイスグループの権限を変更しても、**OmeSiteAdministrators** が以前作成したタスクは変更されません。

メモ: OmeSiteAdministrators に割り当てられたサーバー、RAC、またはカスタムデバイスグループのみが **OmeSiteAdministrators** でリモートまたはシステムアップデートのタスクに利用可能です。他のデバイスグループを **OmeSiteAdministrators** でリモートまたはシステムアップデートのタスクに利用可能にするには、他のデバイスグループを含むカスタムデバイスグループを作成して **OmeSiteAdministrators** に割り当てる必要があります。

メモ: OmeSiteAdministrators 役割のユーザーが Windows ユーザーグループから削除された場合、このユーザーは **OmeSiteAdministrators** 役割からは自動的に削除されません。**OmeSiteAdministrators のメンバーの編集** オプションを使用して、**OmeSiteAdministrators** 役割からユーザーを手動で削除する必要があります。

関連リンク

デバイスグループ許可

OmeSiteAdministrators 役割へのユーザーの追加

メモ: **OmeSiteAdministrators** 役割にユーザーを追加することができるのは、**OmeAdministrators** のみです。

メモ: デバイスグループ許可を効率的に管理するには、**OmeSiteAdministrators** 役割のメンバーを **OmeAdministrators** および **OmePowerUsers** 役割から削除することをお勧めします。

OmeSiteAdministrators 役割へのユーザーの追加は、次の手順で行います。

1. **プリファランス → デバイスグループ許可** とクリックします。
   デバイスグループ許可 ポータルが表示されます。
2. 次のいずれかの手順を実行してください。
   - **一般タスク** ペインで、**OmeAdministrators のメンバーの編集** をクリックします。
   - **デバイスグループ許可の管理** ペインで、**OmeAdministrators** を右クリックし、**OmeAdministrators のメンバーの編集** をクリックします。

   OmeAdministrators のメンバーの編集 ダイアログボックスが表示されます。
3. 該当フィールドにドメイン名およびユーザー名を入力、またはそれらを選択して、**追加** をクリックします。
4. リストからユーザーを選択し、**OK** をクリックします。
   ユーザーが **デバイスグループ許可の管理** ペインの **OmeSiteAdministrators** ツリービューに表示されます。

   メモ: ユーザーが **OmeSiteAdministrators** 役割に追加されたら、デフォルトですべてのデバイスグループがそのユーザーに対して使用可能になります。ユーザーによる特定のデバイスグループでのシステムアップデートおよびリモートタスクの実行を制限するには、ユーザーにデバイスグループを割り当てる必要があります。「ユーザーへのデバイスグループの割り当て」を参照してください。

関連リンク

デバイスグループ許可

ユーザーへのデバイスグループの割り当て

メモ: ユーザーにデバイスグループを割り当てることができるのは、**OmeAdministrators** のみです。デバイスグループは、**OmeSiteAdministrators** 役割のメンバーになっているユーザーへの割り当てのみが可能です。

メモ: デバイスグループがユーザーに割り当てられていない場合は、ユーザーによるそのデバイスグループでのシステムアップデートおよびリモートタスクの実行のみが制限されます。そのデバイスグループが **デバイス** ポータル内のデバイスツリーから非表示になったり削除されたりすることはありません。

デバイスグループをユーザーに割り当てるには、次の手順を実行します。

1. **プリファランス → デバイスグループ許可** とクリックします。
   デバイスグループ許可 ポータルページが表示されます。
2. **デバイスグループ許可の管理** ペインで、デバイスグループを割り当てるユーザーを選択します。
   タスクとパッチ対象のデバイスグループ セクションが右側のパネルに表示されます。

3. デバイスグループのツリービューで、選択されたユーザーに割り当てる適切なデバイスグループのチェックボックスを選択します。以前に割り当てられたデバイスグループを削除するには、対象のデバイスグループのチェックボックスをクリアします。
4. **適用** をクリックします。

メモ: OmeSiteAdministrators タスクのターゲットは、タスク作成時のままです。**OmeAdministrators** が **OmeSiteAdministrators** デバイスグループの権限を変更した場合、タスクのターゲットは変更されません。**OmeSiteAdministrators** デバイスグループの権限を変更しても、**OmeSiteAdministrators** が以前作成したタスクは変更されません。

メモ: OmeSiteAdministrators に割り当てられたサーバー、RAC、またはカスタムデバイスグループのみが **OmeSiteAdministrators** でリモートまたはシステムアップデートのタスクに利用可能です。他のデバイスグループを **OmeSiteAdministrators** でリモートまたはシステムアップデートのタスクに利用可能にするには、他のデバイスグループを含むカスタムデバイスグループを作成して **OmeSiteAdministrators** に割り当てる必要があります。

関連リンク

デバイスグループ許可

OmeSiteAdministrators 役割からのユーザーの削除

メモ: OmeSiteAdministrators 役割からユーザーを削除することができるのは、**OmeAdministrators** のみです。

OmeSiteAdministrators 役割からのユーザーの削除、次の手順で行います。

1. **プリファランス → デバイスグループ許可** とクリックします。
   デバイスグループ許可 ポータルが表示されます。
2. 次のいずれかの手順を実行してください。
   - **一般タスク** ペインで、**OmeAdministrators のメンバーの編集** をクリックします。
   - **デバイスグループ許可の管理** ペインで、**OmeAdministrators** を右クリックし、**OmeAdministrators のメンバーの編集** をクリックします。

   OmeAdministrators のメンバーの編集 ダイアログボックスが表示されます。
3. **OmeSiteAdministrators** 役割から削除したいユーザーの隣にあるチェックボックスをクリアします。
4. **OK** をクリックします。
   ユーザーが **OmeSiteAdministrators** ツリービューの **デバイスグループ許可の管理** ペインから削除されます。

関連リンク

デバイスグループ許可

26

OpenManage Mobile 設定

Dell OpenManage Mobile は、お使いの Android を使用して、ひとつ、または複数の OpenManage Essentials コンソールおよび / または integrated Dell Remote Access Controller（iDRAC）におけるデータセンター監視のサブセットおよび修正タスクをセキュアに実行することを可能にするシステム管理アプリケーションです。OpenManage Mobile を使用して以下を実行することができます。

- OpenManage Essentials 管理システム / サーバーからのアラート通知の受信。
- グループ、デバイス、アラート、およびログ情報の表示。
- サーバー電源のオン / オフ、またはサーバーの再起動。

本章には、OpenManage Essentials コンソールを介して設定できる OpenManage Mobile 設定についての情報が記載されています。また、OpenManage Mobile のトラブルシューティングに必要な情報も説明されています。

メモ: OpenManage Mobile のインストールと使用についての情報は、**dell.com/OpenManageManuals** で『OpenManage Mobile ユーザーズガイド』を参照してください。

関連リンク

OpenManage Mobile 用アラート通知の有効化または無効化
OpenManage Mobile サブスクライバーの有効化または無効化
OpenManage Mobile サブスクライバーの削除
アラート通知サービス状態の表示
OpenManage Mobile サブスクライバー情報の表示
OpenManage Mobile のトラブルシューティング

OpenManage Mobile 用アラート通知の有効化または無効化

OpenManage Essentials は、デフォルトで OpenManage Mobile アプリケーションにアラート通知を送信するように設定されています。ただし、OpenManage Essentials からアラート通知が送信されるのは、OpenManage Mobile ユーザーが OpenManage Essentials コンソールを OpenManage Mobile アプリケーションに追加した場合のみです。**プリファランス → Mobile 設定** ページの **プッシュ通知を有効にする** オプションで、OpenManage Essentials コンソールからの OpenManage Mobile サブスクライバーに対するアラート通知の送信を有効または無効にすることができます。

メモ: OpenManage Mobile 用のアラート通知の有効化または無効化には、omeAdministrator 権限が必要です。

メモ: OpenManage Essentials による OpenManage Mobile へのアラート通知の送信のため、OpenManage Essentials サーバーにアウトバウンド（HTTPS）インターネットアクセスがあることを確認してください。詳細については、「コンソール設定」の「プロキシ設定」を参照してください。

OpenManage Mobile 用アラート通知を有効化または無効化するには、次の手順を実行します。

1. OpenManage Essentials で、**プリファランス → Mobile 設定**をクリックします。

Mobile 設定 ページが表示されます。

2. **プッシュ通知の有効化** を選択または選択解除して、OpenManage Mobile サブスクライバーへのアラート通知の送信を有効化または無効化します。
3. **適用** をクリックします。

関連リンク

OpenManage Mobile 設定

OpenManage Mobile サブスクライバーの有効化または無効化

Mobile サブスクライバー リスト内の **有効** 列にあるチェックボックスを使用して、OpenManage Mobile サブスクライバーに対するアラート通知の送信を有効化または無効化することができます。

メモ: OpenManage Mobile サブスクライバーの有効化または無効化には omeAdministrator 権限が必要です。

メモ: OpenManage Mobile サブスクライバーは、デバイスが恒久的に到達不可能であることをサブスクライバーのモバイルサービスプロバイダのプッシュ通知サービスが示す場合、OpenManage Essentials によって自動的に無効化される場合があります。

メモ: OpenManage Mobile サブスクライバーが **Mobile サブスクライバー** リストで有効化されていたとしても、サブスクライバーは OpenManage Mobile アプリケーション設定でアラート通知の受信を無効化することができます。

OpenManage Mobile サブスクライバーに対するアラート通知を有効化または無効化するには、次の手順を実行します。

1. OpenManage Essentials で、 **プリファランス → Mobile 設定**をクリックします。
   Mobile 設定 ページが表示されます。
2. **Mobile サブスクライバー** リストで **有効** チェックボックスを選択または選択解除して、該当する OpenManage Mobile サブスクライバーへのアラート通知を有効化または無効化します。
3. **適用** をクリックします。

関連リンク

OpenManage Mobile 設定

OpenManage Mobile サブスクライバーの削除

OpenManage Mobile サブスクライバーを削除すると、**モバイルサブスクライバー** リストからユーザーが削除され、ユーザーによる OpenManage Essentials コンソールからのアラート通信の受信が妨げられますが、OpenManage Mobile ユーザーは、後ほど OpenManage Mobile アプリケーションからアラート通知を再サブスクライブできます。

メモ: OpenManage Mobile サブスクライバーの削除には omeAdministrator 権限が必要です。

OpenManage Mobile サブスクライバーを削除するには、次の手順を実行します。

1. OpenManage Essentials で、 **プリファランス → Mobile 設定**をクリックします。
   Mobile 設定 ページが表示されます。
2. **Mobile サブスクライバー** リストで、削除するサブスクライバーに該当する削除アイコン をクリックします。
   サブスクリプション削除の確認 ダイアログボックスが表示されます。

3. **はい** をクリックします。

関連リンク

OpenManage Mobile 設定

アラート通知サービス状態の表示

OpenManage Essentials は、OpenManage Mobile サブスクライバーそれぞれのデバイスプラットフォームアラート通知サービスを介してサブスクライバーにアラート通知を転送します。OpenManage Mobile サブスクライバーがアラート通知の受信に失敗した場合は、**通知サービス状態** をチェックして、アラート通知配信をトラブルシューティングすることができます。

アラート通知サービスの状態を表示するには、**プリファランス → Mobile 設定** をクリックします。

関連リンク

OpenManage Mobile 設定

通知サービス状態

通知サービス状態

次の表では、**プリファランス → モバイル設定** ページに表示される **通知サービス状態** についての情報を説明しています。

ステータスアイコン	状態の説明
	サービスが稼働しており、正常に動作しています。  **メモ:** このサービス状態は、プラットフォーム通知サービスとの正常な通信のみを反映します。サブスクライバーのデバイスがインターネットまたはセルラーデータサービスに接続されていない場合、接続が回復されるまで通知は配信されません。
	サービスで、一時的な可能性のあるメッセージの配信エラーが発生しました。問題が解決されない場合は、トラブルシューティング手順に従うか、テクニカルサポートにお問い合わせください。
	サービスでメッセージの配信エラーが発生しました。トラブルシューティング手順に従うか、必要に応じてテクニカルサポートにお問い合わせください。

OpenManage Mobile サブスクライバー情報の表示

OpenManage Mobile ユーザーが OpenManage Essentials コンソールを正常に追加すると、そのユーザーは OpenManage Essentials コンソールの **Mobile サブスクライバー** 表に追加されます。**Mobile サブスクライバー** 表は、各 OpenManage Mobile サブスクライバーについての情報を提供します。

Mobile サブクスクライバー情報を表示するには、OpenManage Essentials で **プリファランス → Mobile 設定** とクリックします。

関連リンク

OpenManage Mobile 設定

Mobile サブスクライバー情報

Mobile サブスクライバー情報

次の表では、**プリファレンス → Mobile 設定** ページに表示される **Mobile サブスクライバー** 表についての情報が説明されています。

フィールド	説明
有効	OpenManage Mobile サブスクライバーへのアラート通知の送信を有効化または無効化するために選択または選択解除できるチェックボックスを表示します。
状態	OpenManage Essentials コンソールが Dell Alert Forwarding Service に対して正常にアラート通知を送信できるかどうかを示す、サブスクライバーの状態を表示します。
状態メッセージ	モバイルデバイスの状態を表示します。
ユーザー名	OpenManage Mobile ユーザーの名前を表示します。
デバイス ID	モバイルデバイス固有の識別子を表示します。
説明	モバイルデバイスの説明を表示します。
フィルタ	サブスクライバーがアラート通知のために設定したフィルタの名前を表示します。
最後のエラー	OpenManage Mobile ユーザーへのアラート通知の送信時に発生した最後のエラーの日付と時刻を表示します。
最後のプッシュ	Dell OpenManage Essentials から Dell Alert Forwarding Service に対して正常に送信された最後のアラート通知の日付と時刻を表示します。
最後の接続	ユーザーが最後に OpenManage Mobile 経由で OpenManage Essentials コンソールにアクセスした日付と時間を表示します。
登録	ユーザーが OpenManage Mobile に OpenManage Essentials コンソールを追加した日付と時間を表示します。
削除	サブスクライバーリストからサブスクライバーを削除するためにクリックできる削除アイコン を表示します。

OpenManage Mobile のトラブルシューティング

OpenManage Essentials が Dell Message Forwarding Service に登録できない、または通知を正常に転送できない場合は、次の解決方法を行うことができます。

問題	理由	解決策
OpenManage Essentials が Dell Message Forwarding Service に接続できない。[コード 1001/1002]	アウトバウンドインターネット（HTTPS）接続が失われています。	ウェブブラウザを使用して、アウトバウンドインターネット接続が使用可能かどうかを確かめます。 接続が失われている場合は、標準的なネットワークのトラブルシューティング手順を実行します。 • ネットワークケーブルが接続されているかどうかを確認します。 • IP アドレスと DNS サーバーの設定を確認します。 • ファイアウォールがアウトバウンドトラフィックを許可するように設定されているかどうかを確認します。 • ISP ネットワークが正常に動作しているかどうかを確認します。
	プロキシ設定が正しくありません。	プロキシホスト、ポート、ユーザー名、およびパスワードを必要通りに設定します。詳細については、「コンソール設定」の「プロキシ設定」を参照してください。
	Dell Message Forwarding Service が一時的に使用不可能になっている。	サービスが使用可能になるまでお待ちください。
Dell Message Forwarding Service がデバイスプラットフォーム通知サービスに接続できない。[コード 100-105、200-202、211-212]	プラットフォームプロバイダサービスが Dell Message Forwarding Service に対して一時的に使用不可能になっています。	サービスが使用可能になるまでお待ちください。
デバイス通信トークンがプラットフォームプロバイダサービスに登録されていない。[コード 203]	OpenManage Mobile アプリケーションがアップデート、復元、またはアンインストールされたか、デバイスのオペレーティングシステムがアップグレードまたは復元されています。	デバイスに OpenManage Mobile を再インストールするか、『OpenManage Mobile ユーザーズガイド』 で説明されている OpenManage Mobile トラブルシューティング手順に従って、デバイスを OpenManage Essentials に再接続します。 デバイスが OpenManage Essentials に接続されていない場

問題	理由	解決策
		合は、サブスクライバーを削除します。
Dell OpenManage Essentials 登録が Dell Message Forwarding Service によって拒否される。[コード 154]	古いバージョンの OpenManage Essentials が使用されています。	新しいバージョンの OpenManage Essentials にアップグレードしてください。

関連リンク

OpenManage Mobile 設定

27

プリファランス - 参照

プリファランス ページでは、OpenManage Essentials コンソールを設定できます。SMTP およびプロキシサーバーの情報の設定、セッションタイムアウト、データベースメンテナンススケジュールの調整、サービスの再起動、カスタム URL メニュー項目の作成、内部アラートの有効化または無効化、夏時間の監視、および ActiveX 機能の有効化または無効化を行うことができます。

メモ: コンソール設定の変更後に、**適用** をクリックして変更内容を保存する必要があります。**適用** をクリックせずにコンソールの別の部分に移動すると、以前に保存されたプリファランスにリセットされます。

関連リンク

- コンソール設定
- 電子メール設定
- アラート設定
- カスタム URL 設定
- 保証通知の設定
- デバイスグループ許可
- OpenManage Mobile 設定
- 検出設定
- 導入設定

コンソール設定

フィールド	説明
コンソールセッションのタイムアウト	コンソールがユーザーを自動的にログアウトするまでに経過するユーザー非アクティブ時間の長さです。
データベースメンテナンスの実行スケジュール	データベースメンテナンスアクティビティが開始される日時です。 **メモ:** データベースメンテナンス中はタスク（検出、インベントリ、状態ポーリングなど）を実行またはスケジュールしないことをお勧めします。データベースメンテナンス中はコンソールの反応が遅くなるためです。
全 OpenManage Essentials サービスを再開	OpenManage Essentials に関連付けられているサービスを再開します。
セキュリテイ設定（ActiveX）	

フィールド	説明
MIB Import Utility の起動を許可	MIB Import Utility を起動するため、クライアントマシンに ActiveX コンポーネントをインストールして実行します。
リモートデスクトップの起動の許可	リモートデスクトップセッションを起動するため、クライアントマシンに ActiveX コンポーネントをインストールして実行します。
トラブルシューティングツールの起動の許可	Dell トラブルシューティングツールを起動するため、クライアントマシンに ActiveX コンポーネントをインストールして実行します。
ActiveX ステータス	ActiveX の状態を表示します。**状態の更新** をクリックすると ActiveX の状態が更新されます。
タイムゾーン設定	
サーバー選択地域に夏時間を適用	このチェックボックスをクリックして、サーバーのタイムゾーンに基づいて、スケジューリングされた日時の値の調整を可能にします。サーバーのタイムゾーン設定の調整により、OpenManage Essentials 内の設定が変更されます。このオプションを有効にすると、夏時間が始まるときまたは終了するときに、スケジューリングされた項目の日時の値が調整されます。
クライアントのタイムゾーン	クライエントのタイムゾーンと UTC からのオフセット時間を表示します。
OME サーバーのタイムゾーン	サーバーのタイムゾーンのタイムゾーンと UTC オフセットを表示します。
OME サーバーの夏時間ステータス	サーバーのタイムゾーンの現在の夏時間ステータスと夏時間のオフセットを表示します。サーバーのタイムゾーンが、夏時間監視であるのか、標準のタイムゾーンの時刻であるのかも表示します。
プロキシ設定（システムアップデートおよび保証に使用）	
プロキシ設定の使用	システムアップデートおよび保証のためのインターネットアクセスに、プロキシ設定を使用できるようにします。
プロキシサーバーアドレスまたは名前	プロキシサーバーの IP アドレスまたはサーバー名です。不確かな場合は、ブラウザのプロキシ LAN 設定をチェックするか、ネットワーク管理者に問い合わせてください。
ドメイン\ユーザー名	プロキシユーザーのドメイン名とユーザー名です。
パスワード	ユーザーのプロキシパスワードです。

フィールド	説明
プロキシポート番号	プロキシサーバーにアクセスするためのポート番号です。不確かな場合は、ブラウザのプロキシ LAN 設定をチェックするか、ネットワーク管理者に問い合わせてください。
テスト接続	これをクリックして、プロキシ資格情報でのインターネットへの接続をテストします。
KACE アプライアンスの設定	
KACE アプライアンスの URL	KACE アプライアンスの URL
URL のテスト	これをクリックして、KACE アプライアンスへの接続をテストします。

電子メール設定

フィールド	説明
SMTP サーバー名または IP アドレス	SMTP サーバー名または IP アドレスを入力します。
資格情報を使用	ユーザー資格情報を有効にします。
ドメイン\ユーザー名	ドメインおよびユーザー名を入力します。
パスワード	ユーザーパスワードを入力します。
ポート	**デフォルトの使用** を選択してデフォルトのポート番号を使用するか、ポート番号を手動で入力します。
SSL の使用	SSL を使用する場合はこのチェックボックスを選択します。
ロギング	選択して、好みに応じてログを有効または無効にします。

アラート設定

フィールド	説明
内部正常性アラートの有効化	チェックボックスを選択して内部正常性アラートを有効にします。有効化されると、デバイスのグローバル正常性状態が変化するときに、OpenManage Essentials が内部アラートを生成します。
内部接続状態アラートの有効化	チェックボックスを選択して内部接続状態アラートを有効にします。有効化されると、デバイスのグローバル接続状態状態が変化するときに、OpenManage Essentials が内部アラートを生成します。

フィールド	説明
アラートポップアップ通知設定	
アラートポップアップ通知の有効化	チェックボックスを選択して、アラートが生成されたときにポップアップ通知が表示されるようにします。
ポップアップ通知間の時間（秒）	各アラートポップアップ通知の間の時間間隔を選択します。

カスタム URL 設定

フィールド	説明
名前	URL に割り当てられた名前が表示されます。
デバイスグループ	URL に関連付けられているデバイスグループが表示されます。
カスタム URL	URL が表示されます。
説明	カスタム URL に入力された説明が表示されます。
作成日	URL の作成日が表示されます。
アップデート日	URL のアップデート日が表示されます。

関連リンク

カスタム URL の作成
カスタム URL の起動

保証通知の設定

下表に **プリファランス → 保証通知の設定** ページに表示されるフィールドの情報を示します。

フィールド	説明
保証電子メール通知	
保証電子メール通知の有効化	保証電子メール通知の送信を有効または無効にします。
宛先	保証電子メール通知の受信者の電子メールアドレスです。各電子メールアドレスは、有効な電子メールアドレスであることが必要です。複数のアドレスはセミコロンで分離する必要があります。
差出人	保証電子メール通知の送信者の電子メールアドレスです。1 つの電子メールアドレスのみを使用します。電子メールアドレスは有効である必要があります。
保証残存期間が x 日またはそれ以下のすべてのデバイス	どのデバイスを保証電子メール通知に含むかを決定します。保証の残存期間が指定された日数またはそ

フィールド	説明
	れ以下のデバイスが保証電子メール通知に含まれます。
保証期限が切れたデバイスを含める	保証が切れた（0 日）または保証情報のないデバイスを保証電子メール通知に含めるかどうかを指定します。
電子メール送信間隔 *x* 日	連続した保証電子メール通知の送信間隔です。このフィールドへのアップデートは、次回の保証電子メール通知が送信された後でのみ適用されます。
次回の電子メールの送信日	次回の保証電子メール通知が送信される日時です。このフィールドで、次回に送信される保証電子メール通知の日時を設定することができます。 が正常に送信された後で、このフィールドは **電子メール送信間隔 *x* 日** フィールドの設定に基づいて、自動的にアップデートされます。
電子メール設定	SMTP 電子メールサーバーを設定できる **電子メール設定** ページを開きます。
保証スコアボード通知	
保証スコアボード通知の有効化	OpenManage Essentials ヘッダーバナーでの保証通知アイコンの表示を有効または無効にします。保証通知アイコンは、デバイスの保証が **保証残存期間が x 日またはそれ以下のすべてのデバイス** で指定された日数以下の場合にのみ表示されます。
保証残存期間が x 日またはそれ以下のすべてのデバイス	どのデバイスを保証電子メール通知に含むかを決定します。保証の残存期間が指定された日数またはそれ以下のデバイスが保証電子メール通知に含まれます。
保証期限が切れたデバイスを含める	保証が切れた（0 日）または保証情報のないデバイスを **デバイス保証レポート** に含めるかどうかを指定します。
保証ポップアップ通知の設定	
保証ポップアップ通知の有効化	コンソールでの保証ポップアップ通知の表示を有効または無効にします。保証ポップアップ通知は、デバイスの保証が **保証残存期間が x 日またはそれ以下のすべてのデバイス** で指定された日数以下の場合にのみ表示されます。

関連リンク

保証電子メール通知の設定
保証スコアボード通知の設定

デバイスグループ許可

次に、**デバイスグループ許可** ポータルに表示されるパネルおよびフィールドについて説明します。

一般タスク

一般タスク ペインには、**OmeSiteAdministrators** 役割へのユーザーの追加、またはこの役割からのユーザーの削除を行うために使用する **OmeSiteAdministrators のメンバーの編集** オプションが表示されます。

デバイスグループ許可の管理

デバイスグループ許可の管理 ペインには、**OmeSiteAdministrators** がツリービュー形式で表示されます。**デバイスグループ許可の管理** ペインの **OmeSiteAdministrators** をクリックすると、右ペインに**ユーザー概要**が表示されます。次に、**ユーザー概要** 内の各フィールドを示します。

フィールド	説明
ユーザータイプ	メンバーがユーザーかユーザーグループかを表示します。
ドメイン	ユーザーのドメインを表示します。
名前	ユーザーの名前を表示します。

タスクとパッチ対象のデバイスグループ

タスクとパッチ対象のデバイスグループ セクションは、**デバイスグループ許可の管理** ペイン内の*ユーザー名*をクリックすると、右側のペインに表示されます。このセクションはデバイスグループをツリービューフォーマットで表示します。

関連リンク

- デバイスグループ許可の管理
- OmeSiteAdministrators 役割へのユーザーの追加
- ユーザーへのデバイスグループの割り当て
- OmeSiteAdministrators 役割からのユーザーの削除

検出設定

検出設定 ページでは、デバイスの検出に使用するウィザードの種類を設定できます。**検出の設定** ページに表示されるフィールドは、次の表に記載されています。

フィールド	説明
標準ウィザード	これを選択すると、**デバイスの検出** ウィザードに、デバイス検出に用いるプロトコルの一覧が表示されます。
ガイド付きウィザード	選択した場合、**デバイスの検出** ウィザードに、デバイスタイプと、選択されたデバイスの検出と管理に必要なプロトコルの一覧が表示されます。必要なプログラムの設定が完了すると、デフォルトでは、このウィザードは検出とインベントリの両方を実行します。

フィールド	説明
	メモ: ガイド付きウィザードでは、Dell EMC ストレージアレイの検出はサポートされていません。

導入設定

次の表に **導入の設定** ページの各フィールドが記載されています。

フィールド	説明
ファイル共有の設定	
ドメイン\ユーザー名	ファイル共有にアクセスするためのユーザー名です。
パスワード	ファイル共有にアクセスするためのパスワードです。
ファイル共有の状態	導入ファイル共有設定の状態を示します。
自動導入設定	
デバイスが最近検出した自動導入を有効にします。	OpenManage Essentials が後に検出されるデバイスへの設定テンプレートを導入できるように許可するにはこのオプションを選択します。
XX 分ごとに自動導入を実行	後に検出されるデバイスへの設定導入を行う時間間隔を設定します。

28

ログ ー 参照

ツールから以下を実行できます。

- ユーザーインタフェースログの表示
- アプリケーションログの表示
- 
  検出ログのファイルシステムへのエクスポート ー デバイス検出中に生成されたログをエクスポートします。

ユーザーインタフェースログ

フィールド	説明
有効	ユーザーインタフェースのロギングを有効化または無効化します。無効化するとパフォーマンスが向上します。
ログの非同期呼び出し	スレッディングおよび非同期アップデートメソッドの呼び出しのロギングを有効化または無効化します。**同期呼び出しのログ** および **情報** の両方をオンにして、アップデートの呼び出しを表示します。
情報	重大度が **一般情報** となっている動作のログを有効化または無効化します。
警告	重大度が **警告** となっている動作のログを有効化または無効化します。
重要	重大度が **重要** となっている動作のログを有効化または無効化します。
クリア	ユーザーインタフェースロググリッドをクリアします。
エクスポート	ユーザーインタフェースログをファイルにエクスポートします（.CSV、.HTML、.TXT、および .XML 対応）。
重大度	ユーザーインタフェース動作における記録済み偏差の重大度です。

フィールド	説明
開始時刻	動作が発生した時間です。
ソース	動作に関するソースです。
説明	動作に関する追加情報です。

アプリケーションログ

フィールド	説明
重大度	アプリケーションの動作における記録済み偏差の重大度です。
時間	動作が発生した時間です。
メッセージ	動作に関する情報です。

29

拡張子

拡張子ページは、パートナー製品へのリンクのリストを表示します。このページには、製品に関する情報と、その製品がインストール済みかどうかが表示され、インストール済みの製品の場合はこのページから起動することもできます。

メモ: 一部の拡張子は、検出に ActiveX が必要な場合があります。ActiveX を有効にする方法については、**プリファランス** ページの「コンソール設定」を参照してください。

フィールド	説明
名前	ツールの名前を表示します。
説明	ツールの説明を表示します。
起動	製品がインストールされている場合はリンクを表示します。
追加情報	? アイコンをクリックすると製品についての詳細を表示できます。

30

右クリックアクション

次の表に、OpenManage Essentials で使用可能なすべての右クリックアクションを示します。

メモ: OpenManage Essentials で表示される右クリックオプションは、ユーザーのアクセス権限に応じて異なります。すべてのオプションを表示するには、管理者アクセス権限が必要です。

スケジュールビュー

フィールド	説明
新規タスクの作成	次のオプションを表示します。 • サーバーの電源オプション • Server Administrator の導入タスク • コマンドラインタスク
カレンダーのエクスポート	カレンダーを .ics ファイルフォーマットでエクスポートできます。ics ファイルは、Microsoft Outlook にインポートできます。

タスクの作成後、タスクを右クリックして次のオプションを表示できます。

フィールド	説明
編集	タスクの編集ができます。
削除	タスクの削除ができます。
今すぐ実行	タスクを今すぐ実行できます。
表示	タスクの詳細を表示できます。
タスクスケジュールをアクティブ解除	タスクスケジュールを非アクティブ化します。このフラグは、タスクが今後実行されるかどうかを決めます。 **メモ:** 非アクティブ化されたタスクを右クリックすると、**タスクスケジュールのアクティブ化**オプションが表示されます。
クローン	同じ詳細内容でタスクをコピーできます。

フィールド	説明
カレンダーのエクスポート	カレンダーを ics ファイルフォーマットでエクスポートできます。ics ファイルは、Microsoft Outlook にインポートできます。

デバイス状態

フィールド	説明
IP アドレスまたは CMC/iDRAC 名	IP アドレスまたは CMC/iDRAC 名を表示します。
アプリケーションの起動	これを選択して、アプリケーションを起動します。
トラブルシュート	Troubleshooting Tool がインストールされている場合、このオプションを選択してトラブルシューティングツールを起動します。 Troubleshooting Tool は、デフォルトでは無効になっています。Troubleshooting Tool の有効化は、「プリファランス - 参照」を参照してください。
インベントリの更新	これを選択して、デバイスでインベントリを実行します。
状態の更新	これを選択して、デバイスで状態チェックを行います。
新規グループに追加	これを選択して、デバイスをグループに追加します。
既存グループに追加	これを選択して、デバイスを既存のグループに追加します。
デバイスからのすべてのアラートを無視	これを選択して、デバイスからのすべてのアラートを無視します。
除外範囲	これを選択して、検出およびインベントリ範囲からデバイスを外します。
削除	これを選択して、デバイス情報を削除します。

検出範囲サマリ

包括範囲の管理

IP アドレスまたはグループを右クリックして、次のオプションを表示します。

フィールド	説明
編集	これを選択して検出範囲設定を編集します。
名前の変更	これを選択して検出範囲の名前を変更します。 **メモ:** このオプションは、IP アドレスを右クリックしたときのみ表示されます。
<グループ名> に **検出範囲を追加** する	このオプションを選択して、既存のグループに範囲を追加します。 **メモ:** このオプションは、グループを右クリックしたときのみ表示されます。
削除	これを選択して範囲を削除します。
無効	これを選択して範囲を無効化します。
今すぐ検出を実行	これを選択して検出を行います。
今すぐ検出とインベントリを実行	これを選択して検出とインベントリを行います。
状態ポーリングを今すぐ実行	これを選択して、検出済みのサーバーまたはデバイスに対する状態ポーリングタスクを開始します。
今すぐインベントリを実行	これを選択してインベントリを実行します。

表示フィルタ

フィールド	説明
編集	これを選択して、アラート処置またはアラートフィルタを編集します。
サマリの表示	これを選択して、重要なシステムすべてを表示します。
名前の変更	これを選択して、処置名またはアラートフィルタ名を変更します。
クローン	これを選択して、処置またはアラートフィルのコピーを作成します。
削除	アラートを選択して削除します。

アラート

フィールド	説明
詳細	これを選択して、アラートの詳細を表示します。
確認	これを選択して、アラートを設定するか、クリアします。
削除	これを選択して、アラートを削除します。
無視	これを選択して、選択したデバイスまたはすべてのデバイスでアラートフィルタ処置を無視します。このオプションを使用して、選択したデバイスからのすべてのアラートを無視することもできます。
エクスポート	これを選択して、アラート情報を CSV 形式または HTML 形式でエクスポートします。

リモートタスク

フィールド	説明
編集	これを選択して、タスクを編集します。
削除	これを選択して、タスクを削除します。
実行	これを選択して、タスクを今すぐ実行します。
表示	これを選択して、タスクを表示します。
タスクのスケジュールをアクティブ化	これを選択して、タスクのスケジュールをアクティブ化します。
クローン	これを選択して、タスクのコピーを作成します。

カスタム URL

フィールド	説明
編集	URL を編集するにはこのオプションを選択します。
削除	URL を削除するにはこのオプションを選択します。
エクスポート	URL に関する情報をエクスポートするにはこのオプションを選択します。

システムのアップデートタスク

フィールド	説明
削除	これを選択して、タスクを削除します。
実行	一部のコンポーネントがアップデートされていない完了済みタスクを再実行するには、このオプションを選択します。
表示	これを選択して、タスクを表示します。
エクスポート	これを選択して、システムアップデートタスクの情報をエクスポートします。
停止	これを選択して、タスクを停止します。

属性タブ

フィールド	説明
チェック	選択した属性を選択します。
チェック解除	選択した属性の選択を解除します。
エクスポート	**属性** タブに表示されるすべての属性をエクスポートします。

をクリックします。

テンプレート

フィールド	説明
導入	選択したデバイスの構成テンプレートを導入します。
クローン	選択したデバイスの構成テンプレートをクローンします。
名前の変更	選択したデバイスの構成テンプレートの名前を変更します。
削除	選択したデバイスの構成テンプレートを削除します。
テンプレートのエクスポート	選択したデバイスの構成テンプレートをエクスポートします。

をクリックします。

テンプレートによるコンプライアンス

フィールド	説明
デバイスの関連付け	選択したデバイスの構成テンプレートを導入します。
編集	編集のため、右ペインで選択したデバイス構成テンプレートの属性を表示します。
クローン	選択したデバイスの構成テンプレートをクローンします。
名前の変更	選択したデバイスの構成テンプレートの名前を変更します。
削除	選択したデバイスの構成テンプレートを削除します。
テンプレートのエクスポート	選択したデバイスの構成テンプレートをエクスポートします。

をクリックします。

デバイスコンプライアンス

フィールド	説明
コンプライアンス詳細の表示	選択したデバイスのコンプライアンスの詳細を表示します。
別のテンプレートへの関連付け	選択したデバイスを別の構成テンプレートに関連付けます。
今すぐインベントリを実行	選択したデバイスのデバイス構成インベントリを実行します。
エクスポート	デバイスのコンプライアンスレポートを HTML ファイルとしてエクスポートします。

。

31

チュートリアル

OpenManage Essentials の初回設定時には、完了する必要のあるセットアップオプションのためにチュートリアルを利用することができます。

チュートリアルで **初回セットアップ** をクリックし、次の設定情報を表示します。

- SNMP 設定
- SNMP - サービスコンソールを開く
- SNMP - SNMP プロパティを開く
- SNMP ツールのインストール（Windows Server 2012 以降）
- SNMP セキュリテイ設定
- SNMP トラップ設定
- OpenManage Server Administrator のインストール
- ネットワーク検出の有効化（Windows Server 2008 以降）
- ファイアウォール設定
- プロトコルサポートマトリクス
- デバイスの検出

以下に関するチュートリアルを表示できます。

- OpenManage Essentials 2.0.1 へのアップグレード
- OpenManage Server Administrator を使用しない 12G サーバーの検出と監視
- SNMP および OpenManage Server Administrator 用の Linux 設定
- グループポリシーを使用した SNMP の設定
- 検出およびインベントリ用 ESX 4.*x* の設定
- 検出およびインベントリ用 ESXi 4.*x* および 5.0 の設定
- デバイスグループ権限のチュートリアル

32

OpenManage Essentials コマンドラインインタフェースの使用

OpenManage Essentials コマンドラインインタフェースの起動

スタート → すべてのプログラム → OpenManage Applications → Essentials → Essentials コマンドラインインタフェース をクリックします。

検出プロファイル入力ファイルの作成

検出範囲または検出グループを作成する CLI コマンドには、SNMP、WMI、Storage、WS-Man、SSH および IPMI などの検出プロトコルのパラメータを定義する XML ベースのファイルが必要です。このファイルは、使用されるプロトコルと各プロトコルのパラメータを定義します。ファイルは XML エディタまたはテキストエディタを使って変更することが可能です。サンプル XML ファイル（DiscoveryProfile.xml）は、C:\Program Files (x86)\Dell\SysMgt\Essentials\Tools\CLI\Samples の Sample（サンプル）フォルダに含まれています。複数の検出プロファイルを作成するには、xml ファイルを編集して名前を変更します。XML ファイルに WMI、IPMI、WS-Man、EMC および SSH プロトコル用のパスワードを保存することはできません。OpenManage Essentials CLI コマンドでは、次のコマンドを使用してコマンドライン引数にパスワードを指定することができます。

- `-wmiPassword<secure password>`
- `-ipmiPassword<secure password>`
- `-wsmanPassword<secure password>`
- `-emcPassword<secure password>`
- `-sshPassword<secure password>`

メモ: クリアテキストのパスワードは許可されません。パスワード値へのクリアテキストの使用を試みても、CLI コマンドは正常に実行されません。

<セキュアパスワード > 引数は、セキュアパスワードである必要があります。PowerShell スクリプトで再利用できるセキュアパスワードを生成するには、PowerShell ウィンドウ内から次のコマンド（または同様のコマンド）を実行します。

ユーザーにパスワードを要求し、それを読み込んでセキュアな文字列に変換する：

```
PS> $password = Read-Host 'Enter password:' -AsSecureString
```

パスワードをセキュアな文字列としてファイルシステムに保存する：

```
PS> $password | ConvertFrom-SecureString | Set-Content c:\tmp\password.txt
```

上記 2 つの PowerShell コマンドは、パスワードをセキュアな文字列に変換してから、それをファイルに保存します。このセキュアパスワードは、その後 OpenManage Essentials CLI コマンドが関与する他の PowerShell スクリプトで使用することができます。次に例を示します。

ファイルからセキュアパスワードを読み込んで、それを変数に割り当てる：

```
PS> $passwordFile = convert-path c:\tmp\password.txt

PS> $wsmanpassword = Get-Content $passwordFile | ConvertTo-SecureString
```

OpenManage Essentials CLI コマンドのパスワード変数すべてでこのセキュア文字列を使用する：

```
PS> Add-DiscoveryRange -Range 10.36.0.48 -Profile samples\DiscoveryProfile.xml -
WSManPassword $wsmanpassword
```

プロファイル.xml ファイルの一例を以下に示します。

```
<?xml version="1.0" encoding="utf-8" ?> <DiscoveryConfiguration> <NetMask>
255.255.255.240 </NetMask> <ICMPConfiguration> <Timeout>400</Timeout>
<Retries>1</Retries> </ICMPConfiguration> <SNMPConfig Enable="True">
<GetCommunity>public</GetCommunity> <SetCommunity></SetCommunity> <Timeout>400</
Timeout> <Retries>2</Retries> </SNMPConfig> <WMIConfig Enable="False">
<UserName>Administrator</UserName> </WMIConfig> <StoragePowerVaultConfig
Enable="False"></StoragePowerVaultConfig> <StorageEMCConfig Enable="False">
<UserName>Administrator</UserName> <Port>443</Port> </StorageEMCConfig>
<WSManConfig Enable="False"> <Userid></Userid> <Timeout>2</Timeout> <Retries>4</
Retries> <Port>623</Port> <SecureMode Enable="False" SkipNameCheck="False"
TrustedSite="False"> <CertificateFile>Certificate.crt</CertificateFile> </
SecureMode> </WSManConfig> <IPMIConfig Enable="False"> <UserName></UserName>
<KGkey></KGkey> <Timeout>5</Timeout> <Retries>2</Retries> </IPMIConfig>
<SSHConfig Enabled="True"> <UserName>Administrator</UserName> <Timeout>5</
Timeout> <Retries>2</Retries> <Port>400</Port> </SSHConfig> </
DiscoveryConfiguration>
```

メモ: WS-Man を使って iDRAC を検出し、証明書ファイルがローカルシステムに存在することが必要なセキュアモードを使用している場合は、証明書ファイルへの完全なパス（例：**c:\192.168.1.5.cer**）を指定してください。

XML または CSV ファイルを使用した、IP、範囲、またはホスト名の指定

検出、インベントリ、およびステータスタスク中には、範囲を指定する必要があります。このインスタンスにおける範囲は、個別 IP アドレス、ホスト名、または 192.168.7.1～50 や 10.35.0.* などの実際の IP 範囲のいずれかに定義されます。範囲、IP、またはホスト名を xml と csv 入力ファイルのどちらかに追加し、次に -RangeList または -RangeListCSV 引数を使用してコマンドラインにファイルを指定し、入力ファイルを読み込みます。サンプル XML ファイル（**RangeList.xml**）および CSV ファイル（**RangeList.csv**）は、**C:\Program Files (x86)\Dell\SysMgt\Essentials\Tools\CLI\Samples** の **サンプル** フォルダにあります。複数の入力ファイルを作成するには、xml または csv ファイルを編集して名前を変更します。

メモ: 検出範囲グループを作成する場合、各グループは 1 つだけの対応サブネットを持つことができます。グループのサブネットは、**DiscoveryProfile.xml** ファイルから読み込まれ、**RangeList.xml** または **RangeList.csv** ファイルからは読み込まれません。必要に応じて、各サブネットに複数のグループを作成することができます。

RangeList.xml ファイルの一例を以下に示します。

```
<?xml version="1.0" encoding="utf-8" ?> <DiscoveryConfigurationRanges> <Range
Name="10.35.0.*"/> <Range Name="10.36.1.238"/> <Range Name="PE2850-
WebServer1A"/> </DiscoveryConfigurationRanges>
```

RangeList.csv の一例を以下に示します。

名前	SubnetMask
192.168.10.*	255.255.255.0
192.168.10.1～255	255.255.255.0
192.168.1～2.*	255.255.255.0
10.35.*.1～2	255.255.255.0
192.168.2.1	255.255.224.0
192.168.2.2	255.255.254.0
192.168.3.3	255.255.128.0
192.168.3.4	255.255.128.0

PowerShell における入力ファイルの指定

PowerShell で入力ファイルを使用するには、コマンドラインでファイルの場所を指定します。デフォルトで、OpenManage Essentials CLI は、以下のディレクトリから開始されます。

```
PS C:\Program Files (x86)\Dell\SysMgt\Essentials\Tools\CLI>
```

デフォルトの CLI ディレクトリからコマンドを実行しており、コマンドが 1 レベル下のディレクトリ（\samples）にある場合は、次の方法のどちらかを使用して入力ファイルのパスを指定することができます。

- 引用符の中にパス名全体を入力します。例:`Add-DiscoveryRange –Profile "C:\Program Files (x86)\Dell\SysMgt\Essentials\Tools\CLI\Samples\DiscoveryProfile.xml"`。
- 現在のディレクトリにあるファイルを取り出すには、ピリオド（.）を使用し、または現在のディレクトリから 1 つ下のレベルにあるファイルを取り出すには、.\directory を使用します。例：`Add-DiscoveryRange –Profile .\samples\DiscoveryProfile.xml`。

コマンドラインインタフェースコマンド

OpenManage Essentials における CLI コマンドへのアクセスは、お使いのアクセス権限に依存します。ユーザー ID が **OMEAdministrators** グループに属している場合、すべての CLI コマンドにアクセスできます。ユーザー ID が **OMEUsers** グループに属している場合、CLI を使ってデータを削除または変更することはできず、警告メッセージが表示されます。

検出範囲の作成

説明：`Add-DiscoveryRange` コマンドで、新しい検出範囲を作成することができます。コマンドは、検出範囲に関連したプロトコル定義である xml ファイル（**DiscoveryProfile.xml**）を参照します。xml ファイル、csv ファイルを使用、または範囲を指定して、範囲を入力します。**DiscoveryProfile.xml**、**RangeList.xml**、および **RangeList.csv** ファイルに関する詳細は、「検出プロファイル入力ファイルの作成」および「XML または CSV ファイルを使用した IP、範囲またはホスト名の指定」を参照してください。

コマンド：

- `PS> Add-DiscoveryRange –Profile <DiscoveryProfile.xml> -Range <range>`
- `PS> Add-DiscoveryRange –Profile <DiscoveryProfile.xml> -RangeList <RangeList.xml>`

- PS> Add-DiscoveryRange -Profile <DiscoveryProfile.xml> -RangeListCSV <RangeList.csv>

例：

- PS> Add-DiscoveryRange -Profile .\Samples\DiscoveryProfile.xml -Range 10.35.0.124
- PS> Add-DiscoveryRange -Profile .\Samples\DiscoveryProfile.xml -RangeList .\Samples\RangeList.xml
- PS> Add-DiscoveryRange -Profile .\Samples\DiscoveryProfile.xml -RangeListCSV .\Samples\RangeList.csv

検出範囲の削除

説明：Remove-DiscoveryRange コマンドで、検出範囲を削除することができます。xml ファイルを使用、または範囲を指定して、範囲を入力します。**RangeList.xml** ファイルの詳細は、「XML または CSV ファイルを使用した IP、範囲またはホスト名の指定」を参照してください。

コマンド：

- PS> Remove-DiscoveryRange -Range <range>
- PS> Remove-DiscoveryRange -RangeList <rangelist.xml>

例：

- PS> Remove-DiscoveryRange-Range 10.35.0.1, 10.120.1.2
- PS> Remove-DiscoveryRange -RangeList .\Samples\RangeList.xml

検出範囲グループの作成

説明：Add-DiscoveryRangeGroup コマンドによって、検出範囲グループを作成できます。検出範囲グループには、IP 範囲、個別の IP、またはその下のホスト名を含むことができます。これによって、そのグループのプロトコル設定や、それに含まれるすべての範囲を変更することができます。ネットワーク中のデバイスの異なるタイプに、異なるプロトコルセットを維持することができます。グループに含まれない範囲については、各範囲を個別に編集して、有効なプロトコル、タイムアウトまたは再試行値、各プロトコルで使用される資格情報を変更する必要があります。 各検出範囲グループは、それぞれ対応するサブネットを 1 つだけもつことができます。グループのサブネットは **DiscoveryProfile.xml** ファイルから読み込むことができますが、**Rangelist.xml** または **RangeList.csv** ファイルからは読み込めません。必要に応じて、各サブネットに複数のグループを作成します。**DiscoveryProfile.xml**、**Rangelist.xml**、および **RangeList.csv** ファイルに関する詳細は、「検出プロファイル入力ファイルの作成」および「SXML または CSV ファイルを使用した IP、範囲またはホスト名の設定」を参照してください。

コマンド：

- PS> Add-DiscoveryRangeGroup -Profile <DiscoveryProfile.xml> -GroupName <group name> -RangeList <Rangelist.xml>
- PS> Add-DiscoveryRangeGroup -Profile <DiscoveryProfile.xml> -GroupName <group name> -RangeListCSV <Rangelist.csv>

例：

- PS> Add-DiscoveryRangeGroup -Profile .\Samples\DiscoveryProfile.xml -GroupName Group1 -RangeList .\Samples\rangelist.xml

- PS> Add-DiscoveryRangeGroup -Profile .\Samples\DiscoveryProfile.xml -GroupName Group1 -RangeListCSV .\Samples\rangelist.csv

検出範囲グループの削除

説明： Remove-DiscoveryRangeGroup コマンドで、検出範囲グループを削除できます。

コマンド：

```
PS>Remove-DiscoveryRangeGroup -GroupName <groupname>
```

例：

```
PS>Remove-DiscoveryRangeGroup -GroupName Group1
```

検出範囲の編集

説明：Set-ModifyDiscoveryRange コマンドで、既存の検出範囲を編集することができます。このコマンドは、既存の指定済み検出範囲をターゲットとし、プロトコル情報を DiscoveryProfile.xml ファイルで指定された情報に置き換えます。DiscoveryProfile.xml および RangeList.xml ファイルに関する詳細は、「検出プロファイル入力ファイルの作成」および「XML または CSV ファイルを使用した IP、範囲またはホスト名の指定」を参照してください。

コマンド：

- PS> Set-ModifyDiscoveryRange -Profile <DiscoveryProfile.xml> -Range <range>
- PS> Set-ModifyDiscoveryRange -Profile <DiscoveryProfile.xml> -RangeList <RangeList.xml>

例：

- PS>Set-ModifyDiscoveryRange -Profile .\Samples\DiscoveryProfile.xml -Range 10.35.1.23
- PS> Set-ModifyDiscoveryRange -Profile .\Samples\DiscoveryProfile.xml -RangeList .\Samples\RangeList.xml

検出範囲グループの編集

説明：Set-ModifyDiscoveryRangeGroup コマンドで、既存の検出範囲グループの編集ができます。指定されたグループの現在のプロトコル設定を変更する DiscoveryProfile.xml ファイルを指定することで、検出範囲グループのプロトコルを変更できます。DiscoveryProfile.xml ファイルの詳細は、「検出プロファイル入力ファイルの作成」を参照してください。

コマンド：

```
PS> Set-ModifyDiscoveryRangeGroup -GroupName <グループ名> -Profile
<DiscoveryProfile.xml> -AddRangeList <rangelist .xml または .csv ファイル>
```

例：

- .xml ファイルを使用して検出範囲グループの検出プロファイルを変更し、新しい範囲を検出範囲グループに追加します。

  PS> Set-ModifyDiscoveryRangeGroup -GroupName WebServers-TX -Profile .\samples\snmp_only.xml -AddRangeList .\samples\new_ranges.xml

- .csv ファイルを使用して検出範囲グループの検出プロファイルを変更し、新しい範囲を検出範囲グループに追加します。

  ```
  PS> Set-ModifyDiscoveryRangeGroup -GroupName WebServers-TX -Profile .\samples
  \snmp_only.xml -AddRangeListCSV .\samples\new_ranges.csv
  ```

- .xml ファイルを使用して新しい範囲を検出範囲グループに追加します（以前検出したプロファイルを維持）。

  ```
  PS> Set-ModifyDiscoveryRangeGroup -GroupName WebServers-TX -AddRangeList .
  \samples\new_ranges.xml
  ```

- .csv ファイルを使用して新しい範囲を検出範囲グループに追加します（以前検出したプロファイルを維持）。

  ```
  PS> Set-ModifyDiscoveryRangeGroup -GroupName WebServers-TX -AddRangeListCSV .
  \samples\new_ranges.csv
  ```

検出範囲または検出範囲グループの有効化

説明：`Set-EnableDiscoveryRange` コマンドで、検出範囲または検出範囲グループを有効にできます。xml ファイルを使用、または範囲を指定することによって、範囲を入力します。**RangeList.xml** ファイルの詳細については、「XML または CSV ファイルを使用した IP、範囲またはホスト名の指定」を参照してください。

コマンド：

- `PS> Set-EnableDiscoveryRange -Range <range>`
- `PS> Set-EnableDiscoveryRange -RangeList <RangeList.xml>`
- `PS> Set-EnableDiscoveryRangeGroup -GroupName <groupname>`

例：

- `PS> Set-EnableDiscoveryRange -Range 10.35.1.3, 10.2.3.1`
- `PS> Set-EnableDiscoveryRange -RangeList .\Samples\RangeList.xml`
- `PS> Set-EnableDiscoveryRangeGroup -GroupName Group1`

検出範囲または検出範囲グループの無効化

説明：`Set-DisableDiscoveryRange` コマンドで、検出範囲または検出範囲グループを無効にできます。xml ファイルを使用、または範囲を指定することによって、範囲を入力します。**RangeList.xml** ファイルの詳細については、「XML または CSV ファイルを使用した IP、範囲またはホスト名の指定」を参照してください。

コマンド：

- `PS> Set-DisableDiscoveryRange -Range <range>`
- `PS> Set-DisableDiscoveryRange -RangeList <RangeList.xml>`
- `PS> Set-DisableDiscoveryRangeGroup -GroupName <groupname>`

例：

- `PS> Set-DisableDiscoveryRange -Range 10.35.1.3`
- `PS> Set-DisableDiscoveryRange -RangeList .\Samples\RangeList.xml`
- `PS> Set-DisableDiscoveryRangeGroup -GroupName Group1`

検出除外範囲の作成

説明：Add-DiscoveryExcludeRange コマンドで、除外範囲を追加することができます。xml ファイルを使用、または範囲を指定して、範囲を入力します。**RangeList.xml** ファイルの詳細については、「XML または CSV ファイルを使用した IP、範囲またはホスト名の指定」を参照してください。

コマンド：

- PS> Add-DiscoveryExcludeRange -Range <range>
- PS> Add-DiscoveryExcludeRange -RangeList <RangeList.xml>

例：

- PS> Add-DiscoveryExcludeRange -Range 10.35.12.1
- PS> Add-DiscoveryExcludeRange -RangeList .\Samples\RangeList.xml

検出除外範囲の削除

説明：Remove-DiscoveryExcludeRange コマンドで、除外範囲を除外することができます。xml ファイルを使用、または範囲を指定して、範囲を入力します。**RangeList.xml** ファイルの詳細については、「XML または CSV ファイルを使用した IP、範囲またはホスト名の指定」を参照してください。

コマンド：

- PS> Remove-DiscoveryExcludeRange -Range <range>
- PS> Remove-DiscoveryExcludeRange -RangeList <RangeList.xml>

例：

- PS> Remove-DiscoveryExcludeRange -Range 10.35.12.1
- PS> Remove-DiscoveryExcludeRange -RangeList .\Samples\RangeList.xml

検出、インベントリ、および状態ポーリングタスクの実行

説明：Set-RunDiscovery、Set-RunInventory、Set-RunDiscoveryInventory、および Set-RunStatusPoll コマンドは、検出範囲、検出範囲グループ、またはデバイスに対する、検出、インベントリ、および状態ポーリングタスクの実行を可能にします。範囲および範囲グループには、xml ファイルを使用するか範囲を指定することで、範囲を入力します。**RangeList.xml** ファイルの詳細は、「XML または CSV ファイルを使用した IP、範囲、またはホスト名の指定 」を参照してください。 デバイスには、デバイスツリーに表示されるデバイス名を入力します。複数のデバイス名はコンマで分離する必要があります。

コマンド：

- PS> Set-RunDiscovery -DeviceName <device 1>,<device 2>,...,<device N>
- PS> Set-RunDiscovery -Range <rangename>
- PS> Set-RunDiscovery -GroupName <rangeGroupName>
- PS> Set-RunDiscovery -RangeList <rangelist.xml>
- PS> Set-RunInventory -DeviceName <device 1>,<device 2>,...,<device N>
- PS> Set-RunInventory -Range <rangename>
- PS> Set-RunInventory -GroupName <rangeGroupName>

- PS> Set-RunInventory -RangeList <rangelist.xml>
- PS> Set-RunDiscoveryInventory -DeviceName <device 1>,<device 2>,...,<device N>
- PS> Set-RunDiscoveryInventory -Range <rangename>
- PS> Set-RunDiscoveryInventory -GroupName <rangeGroupName>
- PS> Set-RunDiscoveryInventory -RangeList <rangelist.xml>
- Set-RunStatusPoll -DeviceName <device 1>,<device 2>,...,<device N>
- PS> Set-RunStatusPoll -Range <rangename>
- PS> Set-RunStatusPoll -GroupName <rangeGroupName>
- PS> Set-RunStatusPoll -RangeList <rangelist.xml>

例：

- PS> Set-RunDiscovery -Range 10.23.23.1
- PS> Set-RunInventory -GroupName MyServers
- PS> Set-RunDiscoveryInventory -RangeList .\Samples\RangeList.xml
- PS> Set-RunStatusPoll -DeviceName MyZen

デバイスの削除

説明：Remove-Device コマンドで、デバイスツリーからデバイスを削除できます。

コマンド：

- PS> Remove-Device -DeviceName <device 1>,<device 2>,...,<device N>

例：

- PS> Remove-Device -DeviceName Server1,RAC1

検出範囲の状態実行進捗の取得

説明：Get-DiscoveryStatus コマンドで、検出範囲の進捗を取得することができます。xml ファイルを使用、または範囲を指定して、範囲を入力します。**RangeList.xml** ファイルの詳細については、「XML または CSV ファイルを使用した IP、範囲またはホスト名の指定」を参照してください。

コマンド：

- PS> Get-DiscoveryStatus –Range <rangeName>
- PS> Get-Discovery -RangeList <RangeList.xml>
- PS> Get-Discovery -GroupName <group name>

例：

- PS> Get-DiscoveryStatus –Range 10.35.2.1
- PS> Get-Discovery -RangeList .\Samples\RangeList.xml
- PS> Get-Discovery -GroupName Group1

実行中の検出範囲またはグループの停止

説明：どの範囲においても、一度に実行できるのは 1 タイプのタスク（検出、検出とインベントリ、または状態ポーリングなど）だけです。Set-StopTask コマンドによって、検出範囲に関連したタスク、または検出範囲グループに属する範囲に関連したタスクを停止することができます。

コマンド：

- PS> Set-StopTask -Range <rangename>
- PS> Set-StopTask -GroupName <groupname>

例：

- PS> Set-StopTask -Range 10.35.1.12
- PS> Set-StopTask -GroupName Group1

カスタムデバイスグループの作成

説明：Add-CustomGroup コマンドでは、デバイスツリーにカスタムデバイスグループを作成できます。必要に応じて、作成した後にグループにデバイスを追加することができます。

メモ: OpenManage Essentials CLI を使用して、有限のサーバーリストを含む静的なグループのみを作成することができます。動的グループは、OpenManage Essentials コンソールを使用して、クエリに基づいて作成することができます。詳細は、「新規グループの作成」を参照してください。

コマンド：

- PS> Add-CustomGroup -GroupName <groupName>
- PS> Add-CustomGroup -GroupName <groupName> -DeviceList <DeviceList.xml>
- PS> Add-CustomGroup -GroupName <groupName> -Devices <comma separated list of devices>

例：

- PS> Add-CustomGroup -GroupName MyServers -DeviceList .\Samples\devicelist.xml
- PS> Add-CustomGroup -GroupName MyServers -Devices PE2900-WK28-ZMD, PWR-CODE.US.DELL.COM, HYPERVISOR, M80504-W2K8

DeviceList.xml ファイルの例：

```
<DeviceList> <Device Name="PE2900-WK28-ZMD"/> <Device Name="PWR-
CODE.US.DELL.COM"/> <Device Name="HYPERVISOR"/> <Device Name="M80504-W2K8"/> </
DeviceList>
```

カスタムグループへのデバイスの追加

説明：Add-DevicesToCustomGroup コマンドで、既存グループにデバイスを追加することができます。デバイスをグループに追加するには、xml ファイルを使用するか、デバイスをリストし、それらをカンマで区切ります。

コマンド：

- PS> Add-DevicesToCustomGroup -GroupName <groupName> -DeviceList <devicelist.xml>

- PS> Add-DevicesToCustomGroup –GroupName <groupName> -Devices <comma separated list of devices>

例：

```
PS> Add-DevicesToCustomGroup –GroupName MyServers –DeviceList .\Samples
\DeviceList.xml
```

または

```
PS> Add-DevicesToCustomGroup –GroupName MyServers –Devices PE2900-WK28-ZMD, PWR-
CODE.US.DELL.COM, HYPERVISOR, M80504-W2K8
```

DeviceList.xml ファイルの例：

```
<DeviceList> <Device Name="PE2900-WK28-ZMD"/> <Device Name="PWR-
CODE.US.DELL.COM"/> <Device Name="HYPERVISOR"/> <Device Name="M80504-W2K8"/> </
DeviceList>
```

グループの削除

説明： Remove-CustomGroup コマンドによって、ルートノードからグループを削除することができます。

コマンド：

```
PS> Remove-CustomGroup –GroupName <groupName>
```

例：

```
PS> Remove-CustomGroup –GroupName MyServers
```