Dell EMC OpenManage Essentials バージョン 2.3
ユーザーズガイド

DELL EMC

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

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

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

2017 - 10

Rev. A02

目次

1

OpenManage Essentials について

OpenManage Essentials は、企業ネットワーク内のシステム、デバイス、およびコンポーネントの包括的な表示を提供するハードウェア管理アプリケーションです。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
- サーバー、シャーシ、または I/O アグリゲータ（IOA）を導入または再プロビジョニングします。
- サーバーまたはシャーシの設定ベースラインの管理
- サーバーの仮想 I/O ID の管理

本リリースの新機能

- 展開テンプレートと設定ベースラインを分割することで簡素化されたデバイス設定展開および設定コンプライアンス機能をサポートしました。
- コンプライアンス、展開、エクスポート機能に設定を追加して、シャーシ設定ベースラインと導入テンプレートを強化しました。
- サーバおよびシャーシのベースラインに対する設定ドリフトの修正を用意しました。
- OpenManage Essentials のステートレス機能によって管理されていないサーバに対して、バックアップのプロビジョニングとプロファイルの復元を行います。
- SNMPv3 ベースの検出とイベントをサポートします。
- シャーシと IOA 設定を組み合わせた、簡素化されたモジュラーインフラストラクチャ設定管理機能。
- 起動設定の導入テンプレート、ネットワークインタフェース設定、または IOA VLAN 属性の編集をサポートします。
- 次のデバイスがサポートされました。
  - 第 14 世代 PowerEdge サーバ
  - ネットワーク、ストレージ、およびディスクバックアップデバイスの追加モデル
  - VxRail および XC コンバージドインフラストラクチャ
- 拡張機能 ：
  - **アラート無視処置** では、重複アラートを無視する間隔を最長 24 時間まで延ばしました。
  - アラートログの最大サイズに達した後、パージされたアラートを保存する機能。
  - インベントリおよびハードドライブ情報レポートの両方でハードドライブが自己暗号化対応か、自己暗号化ドライブ（SED）かを表示するようになりました。
  - ICMP（Internet Control Message Protocol）ping がブロックされているデータセンターで、OpenManage Essentials の使用が可能。
  - ガイド付きウィザードで、デバイスタイプベースの検出が可能。
  - 設定導入タスクの中に、静的 IPv4 アドレスを設定することにより、サーバまたはシャーシの再検出が可能。
  - IOA の VLAN 設定および VLAN 導入機能のためのプログラム可能 MUX（PMUX）モードのサポートが可能。
  - 検出範囲をエクスポートする機能。

- 仮想 I/O プールの作成中に、I/O 識別情報のタイプの仮想 I/O プールサイズを表示する機能。
- 制限超過時に以前のタスク実行履歴レコードをパージする機能。
- REST インタフェースの新しい機能と強化。

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『*Dell EMC OpenManage Essentials Version 2.3 Support Matrix*』(Dell EMC OpenManage Essentials バージョン 2.3 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：

表 1. その他の情報

文書	説明	可用性
Dell EMC OpenManage Essentials サポートマトリックス	OpenManage Essentials がサポートするデバイスのリストです。	1. **dell.com/OpenManageManuals** にアクセスします。 2. **OpenManage Essentials** をクリックし、必要なバージョンの OpenManage Essentials を選択します。 3. **マニュアルおよび文書** をクリックして、該当のドキュメントにアクセスします。
Dell EMC OpenManage Essentials Readme	OpenManage Essentials の既知の問題とその回避策を提供します。	
Dell EMC 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 EMC 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。	
Dell EMC 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 EMC 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 EMC SupportAssist Enterprise User's Guide（*Dell EMC SupportAssist Enterprise* ユーザーズガイド）	SupportAssist Enterprise 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。アイコンをクリックします。
Dell EMC 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。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 EMC OpenManage Essentials Support Matrix*』（Dell EMC 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、ローカルシステム管理者権限が必要であり、使用しているシステムが、**dell.com/OpenManageManuals** にある『*Dell EMC OpenManage Essentials Version 2.3 Support Matrix*』（Dell EMC OpenManage Essentials バージョン 2.3 サポートマトリクス）の「**Minimum Requirements for OpenManage Essentials**」（OpenManage Essentials の最小要件）セクション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

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。

表 2. Microsoft SQL Server の最小ログインロール

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。**	OpenManage Essentials データベースの db_owner アクセス。
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 を以前のバージョンから最新バージョン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、8000 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。

表 3. データベースのサイズと拡張性

イベント	データベースサイズ
初期データベースサイズ	113.38 MB
8000 台のデバイスの検出とインベントリ後	846.97 MB
20,000 件のアラート生成後	851.85 MB
20,000 件のアラート削除後	847.6 MB

毎日のメンテナンス時に、OpenManage Essentials は、データベースを圧縮して最適化します。OpenManage Essentials は管理下サーバ用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、OpenManage Essentials がインストールされたローカルファイルシステムに保存されます（データベースには保存されません）。

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保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 の起動に問題が発生することがあります。タスク設定 → 維持するタスク実行履歴の記録で設定した制限を超えると、それまでのタスク実行履歴レコードがパージされます。いくつかのタスクのタスク実行履歴詳細はパージされません。詳細については、「タスク設定」を参照してください。不要になったタスク実行履歴詳細を定期的に削除するか、タスク実行履歴詳細のパージ設定を変更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。
   OpenManage インストール 画面が表示されます。次のオプションがあります。

   - **Dell EMC OpenManage Essentials** — このオプションを選択して、OpenManage Essentials、およびトラブルシューティングツールをインストールします。
   - **Dell EMC Repository Manager** — このオプションを選択して、Repository Manager をインストールします。Repository Manager を使用することにより、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 EMC License Manager** — このオプションを選択して、License Manager をインストールします。License Manager は、integrated Dell Remote Access Controller（iDRAC）、Chassis Management Controller（CMC）、OpenManage Essentials および PowerEdge のストレージスレッドライセンスに対応する 1 対多のライセンス導入およびレポートツールです。
   - **Dell EMC SupportAssist Enterprise** — このオプションを選択して、SupportAssist Enterprise をインストールします。SupportAssist Enterprise は、対応しているサーバ、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. **OpenManage インストール** で、**Dell EMC OpenManage Essentials** を選択し、**インストール** をクリックします。
   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。また、インストール後半では、機能の選択にセットアップ種類の **カスタム** インストールを使用します。
   - **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のインストール** をクリックして、他に操作を行うことなくすべての重要な必要条件のインストールをすぐに開始します。**すべての重要な必要条件のインストール** では、設定に応じて再スタートが必要な場合があり、必要条件のインストールは再スタート後、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: OpenManage Essentials 2.3 を実行するには、KB2919355 アップデートが Windows 2012 R2 システムにインストールされていることを確認します。KB2919355 アップデートをインストールするには、support.microsoft.com で Microsoft の技術情報（ID 2919355）を参照してください。

   メモ: 最新の iDRAC およびシャーシファームウェアでは、Windows 2008 R2、および Windows 2012 システムで TLS 1.1 および TLS 1.2 プロトコルを有効にする必要があります。WinHTTP で TLS 1.1 および TLS 1.2 をデフォルトのセキュアプロトコルとして有効にするには、support.microsoft.com で Microsoft の技術情報（ID 3140245）を参照してください。

   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。
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」のステップ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. **セットアップタイプ** 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。

     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ーは、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。

メモ: カスタムインストールオプションを選択した場合は、データベース名をカスタマイズすることができます。データベース名 フィールドに、任意の名前を入力することができます。データベース名を入力しない場合は、デフォルトで OMEssentials が選択されます。通常、複数の OpenManage Essentials インスタンスをインストールするために使用する専用のリモート SQL Server があるシナリオではデータベース名フィールドを使用することができます。たとえば、対応する OpenManage Essentials インスタンスをインストールして、データベース名を DB_OME_Site1、DB_OME_Site2、DB_OME_Site3 として割り当てることができます。

メモ: データベース名は、先頭を英字で開始する必要があり、最大 80 文字です。角括弧（ [] ）、アポストロフィ（ ' ）、および中括弧（ {} ）を除く特殊文字も使用できます。

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。

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。

OpenManage Essentials データベースの再ターゲット

リモートシステム上で使用可能な OpenManage Essentials データベースへ接続するために、OpenManage Essentials コンソールをセットアップすることができます。例えば、ローカルデータベースを使用した OpenManage Essentials をインストールした後で、リモートシステム上に OpenManage Essentials データベースをバックアップおよび復元できます。リモートシステム上にデータベースを復元した後は、リモートシステム上で使用できる復元されたデータベースへ接続するために、OpenManage Essentials をセットアップすることができます。

OpenManage Essentials データベースを再ターゲットする手順は、次のとおりです。

1. OpenManage Essentials データベースをバックアップします。
2. OpenManage Essentials データベースを復元します。
3. SQL Server で新しいユーザーを作成します。
4. OpenManage Essentials データベースへ接続します。

次の項で、OpenManage Essentials データベースを再ターゲットする手順を示してます。

OpenManage Essentials データベースのバックアップ

OpenManage Essentials データベースのバックアップを始める前に：

- **一般的** なインストール方法を使用して、OpenManage Essentials システム がシステムにインストールされていることを確認してください。
- OpenManage Essentials がインストールされているシステムに Microsoft SQL Server Management Studio がインストールされていることを確認します。
- Internet Information Services（IIS）およびすべての OpenManage Essentials サービスを停止していることを確認します。

OpenManage Essentials データベースをバックアップするには：

1. SQL Server Management Studio を開きます。
2. **オブジェクトエクスプローラ** で、**データベース** ノードを展開します。
3. **OMEssentials** データベースを右クリックし、**タスク** → **バックアップ** をクリックします。
   バックアップデータベース - OMEssentials ウィンドウが表示されます。
4. バックアップデータベースを起動するには **OK** をクリックします。

データベースが完了した後に、確認のメッセージが表示されました。OpenManage Essentials データベースのバックアップファイル OMEssentials.bak は C:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESSOME\MSSQL\Backup で保存されます。

OpenManage Essentials データベースの復元

OpenManage Essentials データベースの復元を開始する前に：

- OpenManage Essentials データベースのバックアップファイル OMEssentials.bak が、システムで利用可能かどうかを確認します。必要に応じて、バックアップファイルを作成したシステムから OpenManage Essentials データベースのバックアップファイルをコピー&ペーストする必要があります。
- システム上に Microsoft SQL Server Management Studio がインストールされていることを確認します。
- SQL Server の sysadmin アクセス権を持っていることを確認します。

OpenManage Essentials データベースを復元するには：

1. OpenManage Essentials データベースを復元したいシステム上で SQL Server Management Studio を開きます。
2. **オブジェクトエクスプローラ** で、**データベース** → **データベースの復元** を右クリックします。
   データベースの復元 ウィンドウが表示されます。
3. **ソース** の下の、**デバイス** を選択し、ブラウズボタンをクリックします。
   バックアップデバイスの選択 ウィンドウが表示されます。
4. **追加** をクリックし、ブラウズして OpenManage Essentials データベースのバックアップファイルを選択します。
5. **OK** をクリックして、**バックアップデバイスの選択** ウィンドウを閉じます。
6. **データベースの復元** ウィンドウで **OK** をクリックしてデータベースの復元を開始します。

確認のメッセージが、データベースが復元された後で表示されます。復元された **OMEssentials** データベースが **オブジェクトエクスプローラ** 内の **データベース** の下に表示されます。

メモ: バックアップファイル OMEssentials.bak の複数のインスタンスがシステム上で使用可能であると、データベースの復元に失敗する場合があります。この問題を解決するには、両方のファイルの名前（OMEssentials および OMEssentials_log）を データベースの復元 ウィンドウの データベースファイルを別名で復元 セクションで名前を変更し、データベースの復元を行います。

SQL Server で新規ユーザの作成

SQL Server で新規ユーザーを作成するには：

1. OpenManage Essentials データベースを復元したシステム上で SQL Server Management Studio を開きます。
2. **オブジェクトエクスプローラ** で、**セキュリティ** ノードを展開します。
3. **ログイン** → **新規ログイン** をクリックします。
   ログイン - 新規 ウィンドウが表示されます。
4. **一般的な** ページで：
   a. **ログイン名** フィールドに名前を入力します。
   b. プリファランスに基づいて、**Windows 認証** または **SQL Server 認証** を選択します。
   c. 該当するフィールドにパスワードを入力および再確認します。
   d. オプション：複雑性のパスワードポリシーオプションを強制実行する場合は、**ポリシーパスワードの強制実行** を選択します。
   e. **デフォルトのデータベース** リストから、**OMEssentials** を選択します。
   f. **デフォルト言語** リストから、ログインのデフォルト言語を選択します。

5. **サーバーロール** ページで、**パブリック** を選択します。
6. **ユーザーマッピング** ページで：
   a. **このログインでマップされたユーザー** の下の **OMEssentials** を選択します。
   b. **OMEssentials のデータベース役割メンバーシップ**の下の **db_owner** および **パブリック** を選択します。
7. **OK** をクリックします。

作成した新規ユーザーは、**オブジェクトエクスプローラ** の **セキュリティ** → **ログイン** の下に表示されます。

OpenManage Essentials データベースへの接続

OpenManage Essentials データベースへ接続するには：

1. OpenManage Essentials がインストールされている システムでは、コマンドプロンプトを開き、次のコマンドを実行します。`sqlcmd -E -S ".\SQLEXPRESSOME" -Q "ALTER LOGIN [OMEService] WITH PASSWORD='DummyPassword'"`

   メモ: 標準インストール中で作成された OpenManage Essentials データベースインスタンスが SQLEXPRESSOME であることを確認します。

   メモ: このコマンドをコピー&ペーストすると、正しくない文字となる場合があります。したがって、このコマンドを手入力することをお勧めします。
2. OpenManage Essentials を開きます。
   データベースログインエラーウィンドウが表示されます。
3. データベースログインエラーウィンドウで **OK** をクリックします。
   データベース接続エラー ウィンドウが表示されます。
4. **データベース接続でエラー**では：
   a. **サーバー名** フィールドに、OpenManage Essentials を復元したシステムの名前を入力します。
   b. **認証** リストから、データベースの認証方式を選択します。
   c. 適切なフィールドで作成した新しいユーザーのユーザー名とパスワードを入力します。
   d. SQL Server で作成済みのデータベース名を入力します。
   e. **接続** をクリックします。
5. OpenManage Essentials をいったん終了して、再起動します。
6. インターネットインフォメーションサービス（IIS）のメタベーを再起動します。
7. OpenManage Essentials サービスを再起動またはサーバーを再起動します。

データベースの再ターゲットが正常に完了した後（必要であれば)、OpenManage Essentials がインストールされているシステムから OpenManage Essentials データベース システム を削除することができます。

ドメインコントローラ上の OpenManage Essentials のインストール

ドメインコントローラ上に OpenManage Essentials をインストールする場合は、リモートデータベースと一緒に OpenManage Essentials をインストールすることをお勧めします。ドメインコントローラ上で SQL Server を実行する場合、特定の制限があり、ドメインコントローラのリソース要求を考慮に入れると、SQL Server のパフォーマンスが低下し、OpenManage Essentials のパフォーマンスに影響を及ぼす場合があります。ドメインコントローラ上で SQL Server を実行する場合の制限の詳細については、**support.microsoft.com** で Microsoft Knowledge Base の記事 ID 2032911 を参照してください。

メモ: 安全のために、ドメインコントローラ上には SQL サーバー 2012 をインストールしないことをお勧めします。SQL Server セットアップは、ドメインコントローラに SQL Server をインストールしますが、次の制限事項が適用されます。

- ローカルサービスアカウントを使って SQL Server サービスをドメインコントローラ上で実行することはできません。
- SQL Server がシステムにインストールされた後、システムをドメインメンバーからドメインコントローラへ変更することはできません。ホストシステムをドメインコントローラへ変更する前に、SQL Server をアンインストールする必要があります。
- SQL Server フェールオーバークラスタインスタンスは、クラスタノードがドメインコントローラであるところではサポートされていません。
- SQL Server セットアップでは、読み取り専用ドメインコントローラ上ではセキュリティグループまたはプロビジョニング SQL Server サービスアカウントを作成できません。この場合、セットアップは失敗します。

ドメインコントローラ上の OpenManage Essentials を設定する場合は、次の前提条件を満たしていることを確認します

- OpenManage Essentials がインストールされているシステムとリモートデータベースシステム間のネットワーク通信が機能していることを確認します。
- SQL Server ユーザーは、データベースをバックアップ、作成、設定する許可を持っていることを確認します。
- SQL Server 認証を使用している場合は、SQL Server および Windows 認証モードが SQL Server 内で有効になっていることを確認します。「SQL Server での SQL Server 認証と Windows 認証の有効化」を参照してください。
- TCP / IP が SQL Server で有効になっていることを確認します。「SQL Server の TCP/IP ステータスの確認」を参照してください。

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。

以下のセクションでは、リモートまたはローカルデータベースのあるドメインコントローラ上で OpenManage Essentials をインストールしてセットアップする手順を示しています。

リモートデータベースを使用したドメインコントローラへの OpenManage Essentials インストール

ドメインコントローラへの OpenManage Essentials のインストールを開始する前に、管理者権限によってドメインコントローラにログインしていることを確認してください。
リモーとデータベースでドメインコントローラへ OpenManage Essentials をインストールするには：

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。
   OpenManage インストール ウィンドウが表示されます。
3. **Dell EMC OpenManage Essentials** を選択して、**インストール** をクリックします。
   OpenManage Essentials の 開始する前に ウィンドウが表示されます。
4. **すべての重大な前提条件をインストール** をクリックします。

   メモ: SQL Server が、ドメインコントローラ上にインストールされていない 場合は、作業を開始する前に ウィンドウに、リンクとともに警告メッセージが表示されます。このリンクを使用すると、OpenManage Essentials 固有の SQLEXPRESSOME データベースインスタンスを使用して、ドメインコントローラ（ローカル）上に SQL Express をインストールすることができます。この警告メッセージを無視して、OpenManage Essentials のインストールを開始したとき、ローカルデータベースまたはリモートデータベースで OpenManage Essentials をインストールするかどうかの確認を求めるメッセージが表示されます。

5. データベースの場所の確認メッセージが表示されたら、**いいえ** をクリックし、リモートデータベースに OpenManage Essentials をインストールします。
   Custom Setup（カスタムセットアップ）ウィンドウが表示されます。
6. **次へ** をクリックします。
   OpenManage Essentials カスタム設定 ウィンドウが表示されます。
7. 必要であれば、要件に応じて、デフォルトのポート番号を変更し、**次へ** をクリックします。
   サーバーマネージャ ウィンドウが表示されます。
8. 次のいずれかの手順を実行してください。
   - **参照する** をクリックし、リモートデータベースを選択します。
   - **データベースサーバ** フィールドに、ホスト名とデータベースインスタンス名を入力します。
9. **Windows 認証** または **SQL Server 認証** をクリックします。

   メモ: Windows 認証の場合、ドメイン以外の Windows アカウントを使用している場合は、資格情報がドメインコントローラとリモートシステムの両方に存在している必要があり、識別できなければなりません。Windows ユーザーアカウントは、SQL Server でデータベースを作成するために必要な権限を持っている必要があります。

10. 該当するフィールドにユーザー名とパスワードを入力し、**次へ** をクリックします。
    プログラムのインストール準備完了 ウィンドウが表示されます。

11. **Install**（インストール）をクリックします。

OpenManage Essentials のインストールが完了すると、ログインしている管理者を OMEAdministrators ユーザーグループに追加します。「OpenManage Essentials グループへのユーザーの追加」を参照してください。

メモ: OpenManage Essentials データベースがリモート システムにセットアップされた後、データベースが移動または変更された場合は、新しいデータベース接続を使用して、再ターゲットする OpenManage Essentials を開きます。

ローカルデータベースを使用したドメインコントローラへの OpenManage Essentials のインストール

ドメインコントローラへの OpenManage Essentials のインストールを開始する前に、管理者権限によってドメインコントローラにログインしていることを確認してください。
ローカルデータベースを使用してドメインコントローラ上に OpenManage Essentials をインストールするには：

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。
   OpenManage インストール ウィンドウが表示されます。
3. **Dell EMC OpenManage Essentials** を選択して、**インストール** をクリックします。
   OpenManage Essentials の 開始する前に ウィンドウが表示されます。

   メモ: SQL Server が、ドメインコントローラ上にインストールされていない 場合は、作業を開始する前に ウィンドウに、リンクとともに警告メッセージが表示されます。このリンクを使用すると、OpenManage Essentials 固有の SQLEXPRESSOME データベースインスタンスを使用して、ドメインコントローラ（ローカル）上に SQL Express をインストールすることができます。
4. **作業を開始する前に** ウィンドウにあるリンクをクリックし、ドメインコントローラ上の SQL Express をインストールします。
5. ドメインコントローラ上の SQL Server を実行するために必要なドメインサービスアカウントを作成します。「ドメインサービスアカウントの作成」を参照してください。
6. ドメインサービスアカウントを使用して、実行する SQLEXPRESSOME インスタンスを設定します。「データベースインスタンスの設定」を参照してください。
7. **作業を開始する前に** ウィンドウの **Essentials をインストール**をクリックし、画面の指示に従って、OpenManage Essentials のインストールを完了してください。

OpenManage Essentials のインストールが完了すると、ログインしている管理者を OMEAdministrators ユーザーグループに追加します。「OpenManage Essentials ユーザーグループへのユーザーの追加」を参照してください。

サービスアカウントの作成

ドメインサービスアカウントは、ドメインコントローラ上の SQL Server を実行するために必要です。
ドメインサービスアカウントを作成するには：

1. **スタート** → **管理ツール** をクリックします。
2. **Active Directory ユーザーとコンピュータ** を選択します。
3. 左ペインで、**管理サービスアカウント** → **新規** → **ユーザー** を右クリックします。
   新しいオブジェクト - ユーザー ウィンドウが表示されます。
4. 該当するフィールドに名前とユーザーログイン名を入力し、**次へ** をクリックします。
5. 該当するフィールドで、パスワードを入力、および再確認し、**完了** をクリックします。

データベースインスタンスの設定

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は、SQL Server サービスは開始されません。このため、ドメインサービスアカウントを使用して実行されるように SQLEXPRESSOME データベースインスタンスを設定する必要があります。
SQLEXPRESSOME データベースインスタンスを設定するには：

1. Microsoft SQL Server Configuration Manager を開きます。
2. 左ペインで、**SQL Server サービス** をクリックします。
3. 右ペインでは、**SQL Server（SQLEXPRESSOME）** を右クリックし、**プロパティ** をクリックします。
   SQL Server （ SQLEXPRESSOME ）プロパティ ウィンドウが表示されます。
4. **ログオン** タブで、**このアカウント** を選択します。

5. ドメインサービスアカウント名、パスワードを入力し、該当するフィールドでパスワードを確認します。
6. **再起動** をクリックします。
7. **適用** をクリックします。

OpenManage Essentials ユーザーグループへのユーザーの追加

OpenManage Essentials ユーザーグループにユーザーを追加するには：

メモ: また、OpenManage Essentials ユーザーグループに追加するユーザーは、ビルトインローカル管理者グループに属している必要があります。グループへの Windows ユーザーアカウントの追加については、support.microsoft.com で「グループへのユーザーアカウントの追加」を参照してください。

1. Server Manager を開きます。
2. **ツール** → **コンピュータの管理** をクリックします。
3. 左ペインで、**ローカルユーザーとグループ** → **グループ** をクリックします。
4. 右ペインで、**OmeAdministrators** を右クリックし、**グループに追加** を選択します。
5. **OmeAdministrator プロパティ** ウィンドウで、**追加** をクリックします。
   リポジトリの選択 ウィンドウが表示されます。
6. **選択するオブジェクト名を入力** フィールドで、ユーザー名を入力します。
7. **名前をチェック** をクリックしてから **OK** をクリックします。
   ユーザー名は **OmeAdministrator のプロパティ** ウィンドウ内の **メンバー** リストに表示されます。
8. **OK** をクリックします。

SQL Server での SQL Server および Windows 認証モードの有効化

SQL Server および Windows 認証モードを有効にするには：

1. SQL Server Management Studio を開きます。
2. **オブジェクトエクスプローラ** で、上部レベル の SQL Server オブジェクトをクリックし、**プロパティ** をクリックします。
   ストレージのプロパティ ウィンドウが表示されます。
3. 左ペインの **セキュリティ** をクリックします。
4. 右のペインの **サーバー認証** の下で、**SQL Server 認証モードと Windows 認証モード** をクリックします。
5. **OK** をクリックします。
6. **オブジェクトエクスプローラ** で、上部レベルの SQL Server オブジェクトをクリックし、**再起動** をクリックします。

SQL Server TCP または IP ステータスの確認

SQL サーバーの TCP/IP ステータスを確認するには：

1. **スタート** → **すべてのプログラム** → **SQL Server 設定マネージャ** をクリックします。

   メモ: 複数のバージョンの SQL Server 構成マネージャをがインストールされている場合は、最新バージョンが選択されていることを確認してください。
2. 左ペインで、**SQL SQL Native Client 11.0 設定** をクリックして展開します。
3. **クライアントプロトコル** をクリックします。
4. 右ペインで、TCP/IP のステータスが **有効** になっていることを確認します。
5. TCP/IP が有効になっていない場合は、TCP/IP を右クリックし、**有効** を選択します。

SupportAssist Enterprise のインストール

SupportAssist Enterprise は、エンタープライズサーバ、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、デル EMC 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 Enterprise 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 Dell EMC SupportAssistSetup.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。

   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 2.3 がシステムにインストールされていない場合は、**Dell EMC OpenManage Essentials** が選択されていることを確認してください。
4. **Dell EMC SupportAssist Enterprise** を選択して、**インストール** をクリックします。

   Dell EMC OpenManage Essentials と **Dell EMC SupportAssist Enterprise** 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 Enterprise がインストールされます。SupportAssist Enterprise 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 Enterprise 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 Enterprise 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 EMC 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 EMC 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。

   システムをプロキシサーバー経由でインターネットに接続する場合は、**プロキシ設定** ウィンドウが表示されます。**SupportAssist Enterprise 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: プロキシサーバ資格情報が指定されないと、SupportAssist Enterprise は匿名のユーザーとしてプロキシサーバに接続します。
   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** - パスワードを再入力します。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. **Install**（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 Enterprise 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. `Finish`（終了）をクリックします。

SupportAssist Enterprise を起動すると、**SupportAssist Enterprise のセットアップウィザード** が表示されます。SupportAssist Enterprise を使用する前に、**SupportAssist Enterprise 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 EMC SupportAssist Enterprise User's Guide**』（Dell EMC SupportAssist Enterprise 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

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. **OpenManage インストール** で **Dell EMC Repository Manager** を選択して、**インストール** をクリックします。
3. **Dell EMC 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. **Ready to Install the Program（プログラムインストールの準備完了）** で、**Install（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。

License Manager のインストール

License Manager は、integrated Dell Remote Access Controller（iDRAC）、Chassis Management Controller（CMC）、OpenManage Essentials および PowerEdge のストレージスレッドライセンスに対応する 1 対多のライセンス導入およびレポートツールです。

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. **OpenManage インストール** で、**Dell EMC 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、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 のアップグレード

バージョン 2.0、2.0.1、2.1 および 2.2 の OpenManage Essentials を、バージョン 2.3 にアップグレードできます。
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。次のオプションがあります。
   - **Dell EMC OpenManage Essentials** — このオプションを選択して、OpenManage Essentials、およびトラブルシューティングツールをインストールします。

- **Dell EMC Repository Manager** — このオプションを選択して、Repository Manager をインストールします。Repository Manager を使用することにより、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 EMC License Manager** — このオプションを選択して、License Manager をインストールします。License Manager は、integrated Dell Remote Access Controller（iDRAC）、Chassis Management Controller（CMC）、OpenManage Essentials および PowerEdge のストレージスレッドライセンスに対応する 1 対多のライセンス導入およびレポートツールです。
- **Dell EMC SupportAssist Enterprise** — このオプションを選択して、SupportAssist Enterprise をインストールします。SupportAssist Enterprise は、対応しているサーバ、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 Enterprise がすでにシステムにインストールされている場合は、デフォルトで Dell EMC SupportAssist Enterprise オプションが選択され、無効になっています。OpenManage Essentials のアップグレード後、SupportAssist Enterprise もアップグレードされます。該当する場合は、SupportAssist Enterprise 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 EMC SupportAssist User's Guide』(Dell EMC 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. **OpenManage インストール** 画面で、**Dell EMC OpenManage Essentials** を選択し、**インストール** をクリックします。

   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。
7. **OK** をクリックします。
8. **Install**（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、最新のカタログを取得するようにしてください。

OpenManage Essentials 2.3 へのアップグレード後

このセクションでは、導入ポータルのテンプレートの変更、設定ポータルのベースライン、OpenManage Essentials 2.3 へのアップグレード後に実行する必要があるタスクについて説明します。OpenManage Essentials のアップグレードバージョンの機能は次のとおりです。

- シャーシテンプレートおよびユーザーフレンドリーな属性名を含むベースラインの拡張設定を提供します。
- シャーシ導入で変更された属性に関する拡張された詳細を提供します。

- 以前のバージョンの OpenManage Essentials で使用可能だった対応するサーバまたはシャーシのテンプレートから、サーバおよびシャーシのベースラインを作成します。新たに作成したサーバおよびシャーシのベースライン名には、Baseline の接尾語が付きます。

  メモ: ベースラインは、デバイスコンプライアンスのために使用されます。

- 導入用のシャーシテンプレートと、コンプライアンス関連のタスク用のシャーシのベースラインを再作成するためのオプションを提供します。

  メモ: OpenManage Essentials 2.3 へのアップグレード後に、テンプレートの導入タスクは、導入 → タスク 下で使用できるようになります。

アップグレードが完了したら、次のタスクを実行する必要があります。

- **導入** ポータルから、シャーシテンプレートを再作成します。詳細については、「シャーシテンプレートの再作成」を参照してください。
- **管理** → **ポータルの構成** は、シャーシベースラインを再作成します。詳細については、シャーシのベースラインの再作成を参照してください。
- 以前のバージョンの OpenManage Essentials で作成したスケジュール済みシャーシ導入タスクを再作成します。これは、スケジュール済みシャーシ導入タスクは、OpenManage Essentials バージョン 2.3 へのアップグレード後に、編集または再実行できないためです。ユーザーは、アップグレード後に、作成されたスケジュール済みタスクを編集できます。

  メモ: 再作成されたシャーシテンプレートとベースラインについて確認し、属性値に必要な変更と選択を行います。

- 特定のデバイスタイプと特定のプロトコルに基づいて、デバイスを検出するオプションを提供します。詳細については、dell.com/support で 検出ウィザードの設定

シャーシテンプレートの再作成

OpenManage Essentials の最新バージョンにアップグレードした後、以前のバージョンの OpenManage Essentials で作成した既存のシャーシテンプレートが破損している旨が示されます。
シャーシテンプレートを再作成するには

1. **導入** → **テンプレート** をクリックします。
2. **シャーシテンプレート** から、テンプレートを選択します。
3. **テンプレートのアクション** ウィンドウで、**このテンプレートの再作成** ボタンをクリックし、シャーシテンプレートを再作成します。
4. **タスク認証** ウィンドウに、テンプレートの資格情報を入力し、**OK** をクリックします。
5. テンプレートの作成タスクが実行のために送信されます。**OK** をクリックします。

   選択したシャーシのテンプレートが再作成されます。

   メモ: 再作成されたシャーシテンプレートの名前は変更されません。
6. 再作成されたシャーシテンプレートをクリックし、**属性** タブをクリックして、目的のテンプレートの属性を変更します。

   メモ: コンプライアンスと導入に関連するタスクの場合、シャーシにエンタープライズライセンスがあること、ファームウェアバージョンがサポートされていること、および WSMAN プロトコルを使用して検出されたことを確認します。詳細については、dell.com/support で 導入およびコンプライアンスタスクのデバイス要件

   メモ: ファイルから作成されたシャーシのテンプレートで このテンプレートの再作成 ボタンが表示されない場合は、シャーシ設定ファイルから手動で再作成する必要があります。

シャーシのベースラインの再作成

アップグレード後、OpenManage Essentials 2.3 では、以前のバージョンの OpenManage Essentials で作成されたシャーシテンプレートに対応するシャーシのベースラインが自動的に作成されます。アップグレード後に作成されたシャーシのベースラインの名前には、**Baseline** の接尾語が付きます。**設定** ポータルでシャーシのベースラインが破損している旨が示される場合は、再作成する必要があります。
シャーシのベースラインを再作成するには

1. **管理** → **設定** → **ベースラインによるコンプライアンス** → **シャーシのベースライン** をクリックします。
2. **シャーシのベースライン** から、ベースラインを選択します。
3. **ベースラインの処置** ウィンドウで、**このベースラインの再作成** ボタンをクリックして、シャーシのベースラインを再作成します。
4. **タスク認証** ウィンドウに、シャーシの資格情報を入力し、**OK** をクリックします。
5. ベースラインの作成タスクが実行のために送信されます。**OK** をクリックします。

   選択したシャーシのベースラインが再作成されます。

メモ: 再作成されたベースラインの名前は変更されません。

メモ: シャーシのベースラインの再作成時に、OpenManage Essentials では、以前のバージョンとコンプライアンス関連のタスクに関連するすべてのデバイスに自動的に反映されます。

6. 再作成されたベースラインをクリックし、**属性** タブをクリックして、ベースラインの属性をチェックします。

メモ: コンプライアンスと導入に関連するタスクの場合、シャーシにエンタープライズライセンスがあること、ファームウェアバージョンがサポートされていること、および WSMAN プロトコルを使用して検出されたことを確認します。詳細については、dell.com/support で 導入およびコンプライアンスタスクのデバイス要件

メモ: ファイルから作成されたシャーシのベースラインで このテンプレートの再作成 ボタンが表示されない場合は、シャーシ設定ファイルから手動で再作成する必要があります。

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、OpenManage Essentials MIB Import Utility と SupportAssist Enterprise（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 EMC OpenManage Essentials** を選択して、**アンインストール** をクリックします。
3. メッセージ `Are you sure you want to uninstall OpenManage Essentials?` が表示されたら、**はい** をクリックします。
4. メッセージ `Uninstalling OpenManage Essentials removes the OpenManage Essentials database. Do you want to retain the database?` が表示されたら、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。
5. **Finish**（終了）をクリックします。

IT Assistant から OpenManage Essentials への移行

IT Assistant から OpenManage Essentials バージョン 2.3 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 2.3 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 EMC OpenManage Essentials User's Guide*』（Dell EMC 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 EMC 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、次のいずれかを入力します。
  - **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での 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とき、または夏時間変更が発生したときは、コンソールにおける時刻が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することができます。次の表に **検出ウィザードの設定** ウィンドウの各オプションが記載されています。

表 4. 検出ウィザードの設定

オプション	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（デフォルト）	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、ストレージアレイの検出はサポートされていません。**
検出時に ICMP ping をスキップ	選択した場合、**デバイスの検出** ウィザードからは **ICMP 設定** の設定は無効になります。このオプションを選択すると、デバイスの検出とインベントリ作成、システムのアップデート、設定、および導入タスク時に ICMP ping がスキップされます。
選択されたデバイスタイプのみ検出	OpenManage Essentials 2.3 では、このオプションはデフォルトで有効に設定されています。選択した場合、ガイド付きウィザードで、このオプションによりデバイスタイプの検出が可能になります。 **メモ: 以前のバージョンの OME で検出されたデバイス範囲には、WS-MAN プロトコルを使用してシャーシと iDRAC の両方が検出されている場合があります。OpenManage Essentials 2.3 では、検出設定で 選択されたデバイスタイプのみ検出 オプションが有効である場合、ガイド付きウィザードで選択した特定のデバイスのみが検出され、その他のデバイスは不明なデバイスとして分類されます。例えば、WS-MAN プロトコルと iDRAC デバイスタイプを選択すると、WS-MAN プロトコルを使用して iDRAC デバイスのみが検出されます。**

ウィザードのタイプを選択して **終了** をクリックすると、設定が **設定** → **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することができます。

検出設定を指定するには、次の手順を実行します。

1. **設定** → **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、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。

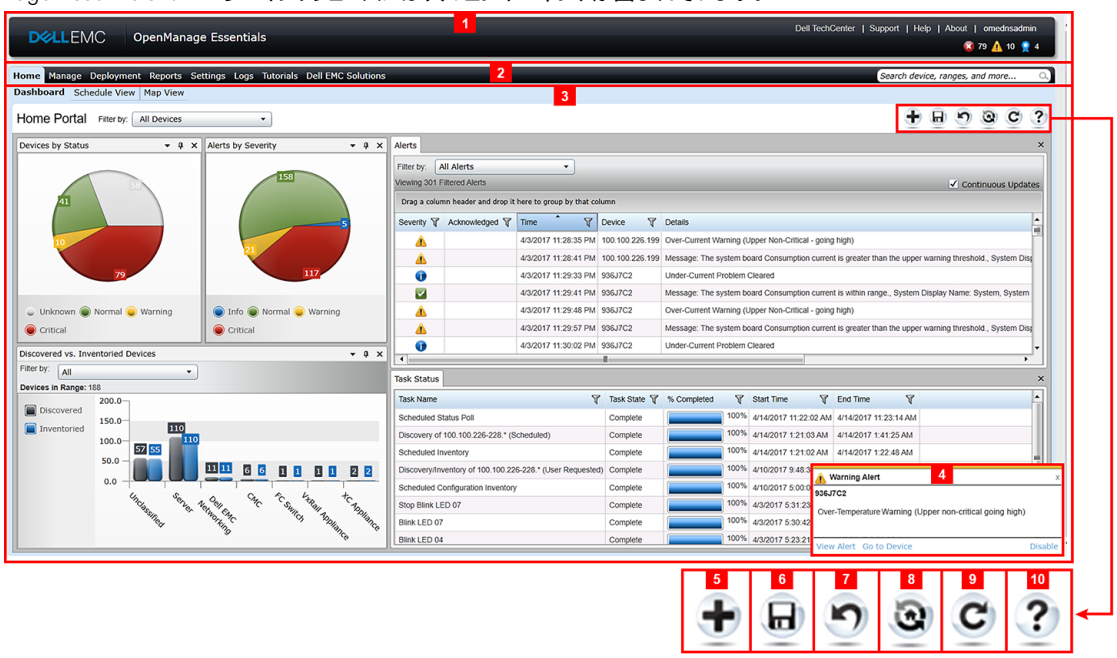

図 1. OpenManage Essentials ホームポータル

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 の新しい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、現在インストールされていて、OpenManage Essentials の新たに利用できるバージョンを表示する、**新しいバージョンが使用可能** ウィンドウを開きます。
- 保証スコアボード通知アイコン には、保証が *x* 日以下のデバイスの数が含まれています。アイコンまたは数字をクリックして、保証期間が特定の日数以下のデバイスをリストする **デバイス保証レポート** を表示することができます。保証スコアボード通知アイコンは、**設定** → **保証通知設定** で **保証スコアボード通知を有効にする** を選択した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名を表示します。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」。

。

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、

図 2. 追加のレポートとグラフの追加アイコンをクリックします。

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**
- **資産取得情報**
- **資産メンテナンス情報**
- **資産サポート情報**
- **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。

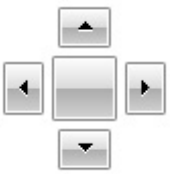

図 3. ドッキングアイコン

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、

図 4. 保存アイコン

アイコンで識別できます。
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、

図 5. 以前のポータルのレイアウトのロードアイコンをクリックします。

アイコンで識別できます。

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、

図 6. Refresh（更新）アイコン

アイコンで識別できます。
ポータルのデフォルトレイアウトをロードするには、

図 7. デフォルトレイアウトアイコン

アイコンで識別できます。

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、

図 8. 非表示にするアップデートの横にある非表示アイコン

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、

図 9. 移動アイコン

アイコンで識別できます。

グラフおよびレポートの配置変更およびサイズ変更 - コンポーネント

 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。

次のアイコン

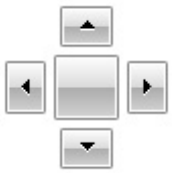

図 10. ドッキング アイコン

の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、

図 11. 移動アイコン

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、

図 12. 復元アイコン

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、

図 13. フィルタアイコン

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：

表 5. 選択処置

選択されたアイテム	Action
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、WS-Man プロトコルを使用して Enterprise ライセンスのある PowerEdge VRTX または PowerEdge FX2/FX2s デバイスを検出した場合にのみ利用可能です。SNMP プロトコルを使用してライセンスのあるデバイスが 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
マップビューインタフェース - ホーム ポータル

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、新しいバージョンの OpenManage Essentials が使用できるときに OpenManage Essentials ヘッダバナーに表示されます。  アイコンをクリックすると、**新しいバージョンが使用可能** ウィンドウが開き、現在インストールされていて、新しく使用

可能なバージョンの Openmanage Essentials が表示されます。**もっと詳しく知る** をクリックすると、OpenManage Essentials の Web サイトでのダウンロードの詳細が表示されます。アップデート使用可能通知を設定またはキャンセルするには、**後で通知する** をクリックします。

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、**設定** → **保証通知設定** で設定した基準に基づいて OpenManage Essentials ヘッダ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
マップビューインタフェース - ホーム ポータル

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。

表 6. 状態ごとのデバイス

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。
接続が失われました	これらのデバイスに到達できません。

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。

表 7. 重大度ごとのアラート

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サーバの数を表示します。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サーバを確認できます。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を選択します。

表 8. 検出済み対インベントリ済みデバイス

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作成
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作成
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

表 9. 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。

フィールド	説明
	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

OpenManage Essentials 見出しバナーの保証スコアボード通知アイコン をクリックすると、**デバイス保証レポート** が表示されます。**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。

表 10. デバイス保証レポート

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。
期限切れの保証を含む	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。
Device Name（デバイス名）	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。
モデル	システムのモデル情報を表示します。
Device Type（デバイスタイプ）	デバイスタイプを表示します。例えば、サーバーまたは Remote Access Controller です。
Service Tag	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。
保証タイプ	保証タイプを表示します。例えば、初期、拡張など。
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。
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。
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。
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。
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。

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

マップビューインタフェース - ホーム ポータル

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作成
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 - SNMP、WMI、および Ws-Man

対応デバイス、プロトコル、および機能マトリックス - SNMP、WMI、および Ws-Man

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。

表 11. 対応デバイス、プロトコル（ SNMP、WMI、Ws-Man ）、および機能マトリックス

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サーバ	Windows / Hyper-V	検出 相関 Classification（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 • RAC • リモートデスクトップ • システムアップデート	検出 相関 Classification（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 • システムアップデート	非対応
	Linux/VMware ESX	検出 相関 Classification（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 • RAC	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	トラップ / アラート	非対応	検出 相関 Classification（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） アプリケーション起動 — RAC
OpenManage Server Administrator をインストールしていないサーバ	Windows / Hyper-V	非対応	検出 相関 Classification（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
	VMware ESXi	非対応	非対応	検出 相関 Classification（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） アプリケーションの起動
iDRAC/DRAC/BMC		検出 相関 Classification（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 相関 Classification（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 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。** アプリケーションの起動 • RAC • コンソール
ハイパーコンバージドインフラストラクチャ（VxRail、XC Series）		検出 相関 Classification（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	非対応	検出 相関 Classification（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

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）
	アプリケーションの起動 • RAC • コンソール		ハードウェアインベントリ アプリケーションの起動 • RAC • コンソール • VxRail マネージャ • PRISM **メモ: OpenManage Essentials は、VxRail および XC Series のデバイスでのリモートタスクの実行、サーバ設定、およびシステムアップデートをサポートしていません。**
モジュールエンクロージャ（PowerEdge M1000e）	検出 相関 Classification（分類） エンクロージャ正常性 トラップ システムアップデート アプリケーション起動 — CMC	非対応	検出 相関 Classification（分類） エンクロージャ正常性 トラップ システムアップデート アプリケーション起動 — CMC **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。**
PowerEdge VRTX	検出 相関 Classification（分類） エンクロージャ正常性 トラップ アプリケーション起動 — CMC	非対応	検出 相関 Classification（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 アプリケーション起動 — CMC マップビュー（PowerEdge VRTX のみ）
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 Classification（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
SonicWALL ファイアウォールアプライアンス	検出 Classification（分類） アプリケーションの起動	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）
	トラップ / アラート		
Networking イーサネットスイッチ	検出 相関 Classification（分類） アプリケーションの起動 トラップ / アラート Health（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 Classification（分類） アプリケーションの起動 トラップ / アラート Health（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。

メモ: OpenManage Essentials は、PowerEdge C シリーズサーバ（PowerEdge C4130、PowerEdge C6320、PowerEdge C6320p、PowerEdge C6420）のみのインバンド（OMSA）およびアウトバンド（iDRAC）検出をサポートします。

メモ: OpenManage Essentials は、他のクライアントデバイスの検出と同様に、WMI プロトコルを使用して Dell Precision ラックの 7910 および 7920 のクライアントの検出をサポートします。Dell Precision ラック 7910 および 7920 のクライアントが iDRAC（帯域外検出）を使用して検出された場合、これらのデバイスは、管理 → デバイス → すべてのデバイス → RAC でサーバとして分類されます。

メモ: 読み取り専用 権限を持つ iDRAC ユーザーアカウントの資格情報を使用して、サーバの帯域外（iDRAC）の検出およびインベントリを実行することもできます。ただし、システムアップデートやデバイス設定導入など、昇格された権限を必要とする操作は実行できません。

対応デバイス、プロトコル、および機能マトリックス - IPMI、CLI、および SSH

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。

表 12. 対応デバイス、プロトコル（IPMI、CLI、SSH）、および機能マトリックス

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 をインストールしたサーバ	Windows/Hyper-V	非対応	OpenManage Server Administrator CLI OpenManage Server Administrator の展開 サーバーアップデート • BIOS • ファームウェア • ドライバ	非対応
	Linux/VMware ESX	非対応	OpenManage Server Administrator CLI OpenManage Server Administrator の展開	検出 相関 Classification（分類）

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）
			サーバーアップデート • BIOS • ファームウェア • ドライバ	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 Classification（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 をインストールしていないサーバ	Windows/Hyper-V	非対応	OpenManage Server Administrator の展開	非対応
	Linux/VMware ESX	非対応	OpenManage Server Administrator の展開	検出 相関 Classification（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	非対応
	PowerEdge C	検出 Classification（分類）	RACADM CLI IPMI CLI	非対応
iDRAC/DRAC/BMC		検出 Classification（分類） 相関 iDRAC の正常性	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
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
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
Networking イーサネットスイッチ		非対応	非対応	非対応
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。

メモ: ホストシャーシの下の PowerEdge FC430、FC630、または FC830 スレッド間の相互関係は、以下のサポートではサポートされていません。

- スレッドは WMI プロトコルを使用して検出されますが（帯域内）、OMSA はインストールされていません。
- スレッドは、IPMI プロトコルを使用して検出されます（帯域外）。
- スレッドは ESXi を実行していますが、OMSA はインストールされています（インストールしないでください）。

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。

表 13. 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

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 Classification（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 **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。**	検出 Classification（分類） トラップ / アラート	非対応	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 — EMC Navisphere Manager
	PowerVault	トラップ / アラート	検出 Classification（分類） ハードウェアインベントリ 監視 アプリケーション起動 - Modular Disk Storage Manager (a)	非対応
	Compellent	検出 Classification（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	非対応	非対応
	テープ	検出 Classification（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ソール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。

メモ: PowerEdge M1000e シャーシによってホストされているストレージデバイスは、PowerEdge M1000e シャーシがインベントリされるまで、シャーシの ストレージ ノードの下に分類されません。

メモ: NAS アプライアンスに関連付けられた EqualLogic グループが検出されると、EqualLogic グループは NAS クラスタ および ストレージデバイス → Dell EqualLogic グループ の下のデバイスツリーに表示されます。ただし、Dell EqualLogic グループ 下に表示されるのは EqualLogic グループのメンバーのみです。

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 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 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. SNMP で、ESXi 5 ホストでのハードウェアアラートに対して、SNMP トラップを OpenManage Essentials に送信するよう設定します。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 と ESXi ホストをグループ化するには、ESXi ホストと VM で SNMP が有効になっ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。

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。
  - サーバー、スイッチ、RAC、およびストレージ装備の CMC
  - 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**：デバイスの正常性ステータスおよび接続ステータスを取得する機能。
- **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。

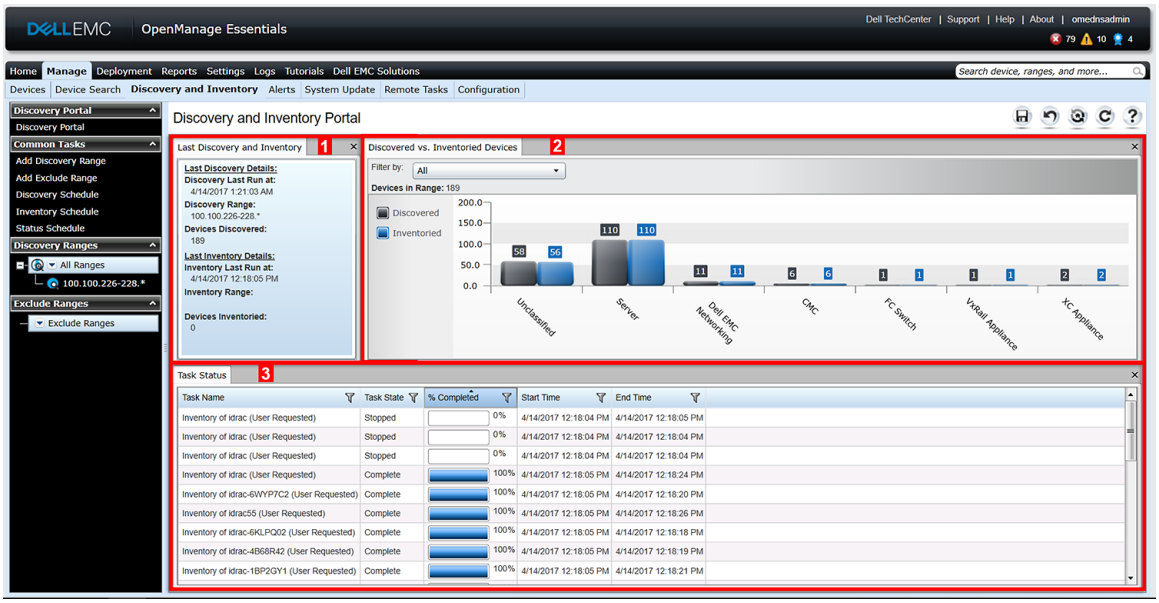

図 14. 検出とインベントリポータル

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、デバイスの検出でサポートされる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、**イタリック**のテキストで示されています。

表 14. 検出用のプロトコルサポートマトリックス

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）
iDRAC6 以降	対応	**対応**	該当なし	対応	非対応
Linux	**対応** [1]	該当なし	該当なし	該当なし	対応
Windows	**対応** [1]	該当なし	対応 [2]	該当なし	該当なし
ESXi	対応 [1]	**対応**	該当なし	該当なし	非対応
Citrix XenServer	**対応** [1]	該当なし	該当なし	該当なし	対応 [2]
PowerEdge（CMC）	対応	**対応**	該当なし	該当なし	非対応
PowerEdge C*	対応	対応	該当なし	**対応**	非対応
クライアントシステム	対応 [3]	該当なし	**対応** [3]	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

* PowerEdge C4130、PowerEdge C6320、PowerEdge C6320p、PowerEdge C6420 の検出は、C シリーズ以外の PowerEdge サーバを検出するために使用されるプロトコルと同じプロトコルを使用して実行することができます。

[1] OpenManage Server Administrator（OMSA）がインストール済みの場合に対応。

[2] OMSA をインストール済みの場合に対応、OMSA が未インストールの場合は正常性情報なし。

[3] Dell Command | Monitor がインストール済みの場合に対応、Dell Command | Monitor が未インストールの場合は正常性情報なし。

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サポートされる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、***イタリック***のテキストで示されています。

表 15. 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

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）
iDRAC6 以降	非対応	**対応**	該当なし	該当なし	該当なし
Linux	**対応** [1]	該当なし	該当なし	該当なし	対応 [2]
Windows	**対応** [1]	該当なし	対応 [1,2]	該当なし	該当なし
ESXi	非対応	**対応** [3]	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（CMC）	対応 [4]	**対応** [4]	該当なし	該当なし	該当なし

[1] OpenManage Server Administrator（OMSA）がインストール済みの場合に対応。

[2] インベントリの収集方法を使用している場合に対応。

[3] 対応、帯域外チャネルを通して iDRAC を検出およびアップデートする必要があります。

[4] 対応、RACADM ツールが必要です。

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作成

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タイプは、**設定** → **検出設定** の設定に基づきます。「検出設定の指定」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追加することもできます (例えば、ホスト名 1、ホスト名 2、ホスト名 3 など)。
   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。また、.csv ファイルに行項目として含まれたホスト名および IP アドレスをインポートできます。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。

      メモ: 検出範囲は、すべての範囲 または所定の検出範囲を右クリックして、.csv ファイルとしてエクスポートできます。ホスト名と IP アドレスによりエクスポートされた .csv ファイルは、同じまたは別の OpenManage Essentials インスタンスでインポートできます。
   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を指定したら、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、修正することを推奨します。

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

   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: Open Manage Essentials 2.3 では、ICMP ping はオプションです。ICMP パラメータは、検出時に ICMP ping をスキップ設定の選択に応じて適用されます。

   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。

メモ: 設定 → 検出設定 の下で 検出時に ICMP ping をスキップ 設定が選択されている場合、ICMP 設定 ウィンドウは表示されません。

- 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。検出用に、SNMP V1/V2c または SNMP V3 を選択できます。**Get コミュニティ**で指定した SNMP コミュニティ文字列が、SNMP V1/V2c を使用して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。SNMP V3 を使用したデバイスの検出とインベントリ作成では、デバイスの検出時に使用した同じユーザー名とパスワード、認証プロトコル、暗号化プロトコルの資格情報でデバイスが設定されていることを確認します。

  メモ: ユーザーが SNMPv1/v2c および SNMPv3 オプションの両方を選択した場合は、SNMPv3 を使用したデバイスの検出が SNMPv1/v2C を使用した検出よりも優先度は高くなります。検出範囲設定の詳細 には、特定の検出範囲について選択した検出プロトコルが表示されます。

  メモ: iDRAC では、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 ポートが変更された場合、iDRAC では検出されないことがあります。

- 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 パラメーターを入力して PowerEdge VRTX、iDRAC 6、iDRAC 7、および ESXi がインストールされたサーバ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、サーバでの 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。**デバイスタイプフィルタリング** 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、システム上のローカルサービスファイルで設定を変更することができます。

メモ: このセクションでは、設定 → アラート設定 の SNMP リスナー設定 で V1/V2c トラップのサポート が選択されている必要があります。

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、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、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。

ガイド付きウィザードを使用したシャーシとそのコンポーネントの検出

ガイド付きウィザード 内で、**シャーシ（CMC）検出 - すべてのコンポーネント** デバイスタイプフィルタを使用してシャーシを検出したときに、OpenManage Essentials は、自動的にシャーシ内のコンポーネント（ブレードサーバーと IOA スイッチ）を自動的に検出します。シャーシとそのコンポーネントを検出するには、CMC のホスト名 /IP アドレスおよび WS-Man 資格情報を入力する必要があります。

シャーシ内のブレードサーバー (iDRAC) はデフォルトで、CMC 向けに入力した WS-Man 資格情報を使用して検出されます。CMC と iDRAC の資格情報が同じではない場合、iDRAC を検出するために代替 WS-Man 資格情報を入力することができます。

メモ: 必要に応じて、シャーシのみを検出するために ガイド付きウィザード を使用することができます。

メモ: シャーシ内のブレードサーバーの自動検出は、デルの第 11 世代以降の PowerEdge サーバー（iDRAC 6 以降）に対してのみサポートされています。

メモ: PowerEdge M1000e シャーシとそのコンポーネントを検出するには、CMC ファームウェアのバージョン 5.0 以降がインストールされているようにしてください。インストールされているファームウェアが 5.0 より前のバージョンである場合、標準ウィザード を使ってシャーシとそのコンポーネントを個別に検出する必要があります。

メモ: IOA スイッチの自動検出は、PowerEdge M1000e に CMC ファームウェアバージョン 5.1 以降がインストールされている場合、および PowerEdge FX2/Fx2s に CMC ファームウェアバージョン 1.3 以降がインストールされている場合のみサポートされます。

ガイド付きウィザード を使用してシャーシとそのコンポーネントを検出するには、次の手順を実行します。

1. **管理** → **検出とインベントリ** をクリックします。
検出とインベントリポータル が表示されます。
2. **共通タスク** で **検出範囲の追加** をクリックします。
検出デバイス ウィザードの **検出範囲設定** ページが表示されます。
3. **グループとして保存** オプションを選択し、該当するフィールドにそのグループの名前を入力します。

   メモ: ガイド付きウィザード を使用したシャーシ検出のためには、検出範囲をグループとして保存することが必須です。
4. 適切なフィールドに CMC の IP アドレスを入力し、**追加** をクリックします。
5. **次へ** をクリックします。
デバイスタイプフィルタリング ページが表示されます。
6. **シャーシ (CMC) 検出 - すべてのコンポーネント** を選択し、**次へ** をクリックします。
ICMP 設定 ページが表示されます。
7. 必要に応じて、**タイムアウト** と **再試行** を希望の値に変更します。
8. **次へ** をクリックします。
WS-Man 設定 ページが表示されます。
9. 該当するフィールドに CMC ユーザー名 と パスワードを入力します。
10. シャーシコンポーネントの自動検出を無効にする、または iDRAC の検出のために代替資格情報を入力する場合は、**iDRAC のための代替 WS-Man 設定** をクリックします。
    - iDRAC とスイッチの自動検出を無効にするには、**CMC で iDRAC とスイッチを自動検出する** オプションをクリアします。
    - iDRAC 検出のための代替資格情報を入力するには、**iDRAC の検出に同じ CMC 資格情報を使用する** オプションをクリアし、該当するフィールドに iDRAC のユーザー名とパスワードを入力します。
11. **次へ** をクリックします。
サマリ ページが表示されます。

12. **終了** をクリックします。
    シャーシとそのコンポーネント（iDRAC と IOA スイッチ）の検出が開始されました。

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

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速くなり、ネットワーク全体の輻輳やレイテンシが回避されます。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 % のとき、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

タスクポップアップ通知

タスクポップアップ通知は、タスクが完了したときに、OpenManage Essentials コンソールの右下角に表示されます。タスクポップアップウィンドウに表示される情報は、完了したタスクの数に応じて異なります。

メモ: タスクポップアップ通知は、タスク実行履歴を作成するタスクについてのみ表示されます。

完了したタスクが 1 件だけの場合は、次の情報が表示されます。

- タスクのステータス — タスクが成功したか失敗したかどうかを示します。
- クリックすると「タスク実行詳細」（使用可能な場合）を表示できるタスク名。
- そのタスクに関連するポータルを開くためのリンク。
- タスクポップアップ通知を無効化できるタスクポップアップ通知設定にアクセスするためのリンク。

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。

- 完了したタスクの数。
- クリックすると「タスク実行詳細」（使用可能な場合）を表示できるリンクになったタスク名。

  メモ: タスク名リンクは、最初の 3 つのタスクにのみに表示されます。
- **アラートコンソールに移動** — アラートポータルにアクセスします。
- **無効** — タスクポップアップ通知設定にアクセスします。

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。

タスクポップアップ通知の設定

タスク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. **設定** → **タスク通知設定** をクリックします。

   タスク通知設定 ページが表示されます。
2. **タスクポップアップ通知設定** で、**タスクポップアップ通知の有効化** を選択または選択解除して、タスク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。

タスクポップアップ通知の有効化または無効化

タスク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: タスク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。タスク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. **設定** → **タスク通知設定** をクリックします。
   タスク通知設定 ページが表示されます。
2. **タスクポップアップ通知設定** で、次の手順を実行します。
   - タスクポップアップ通知を有効にするには、**アラートポップアップ通知の有効化** を選択します。
   - **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、タスク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。

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サーバのグラフィックレポートを表示。
- デバイスおよびサーバの検出範囲を管理。
- デバイスおよびサーバの検出、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作成
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

表 16. 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作成
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サーバの数を表示します。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サーバを確認できます。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を選択します。

表 17. 検出済み対インベントリ済みデバイス

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作成
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作成
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

表 18. 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、またはサーバを選択します。	これを選択して、オプション、デバイス、またはサーバ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： • **点灯**

フィールド	説明
	• **消灯**

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。詳細に関しては、「検出とインベントリタスクの作成」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。
   - 検出範囲の設定
   - デバイスタイプのフィルタリング
   - 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

表 19. 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。
Group Name（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。**

フィールド	説明
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。**
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。次の表は、**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についての説明です。

メモ: 以前のバージョンの OpenManage Essentials で検出されたデバイス範囲には、WS-MAN プロトコルを使用してシャーシと iDRAC の両方が検出されている場合があります。OpenManage Essentials 2.3 では、検出設定で 選択されたデバイスタイプのみ検出 オプションが有効である場合、ガイド付きウィザードで選択した特定のデバイスのみが検出され、その他のデバイスは不明なデバイスとして分類されます。例えば、WS-MAN プロトコルと iDRAC デバイスタイプを選択すると、WS-MAN プロトコルを使用して iDRAC デバイスのみが検出されます。

表 20. デバイスタイプのフィルタリング

フィールド	説明
Device Type（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。

メモ: OpenManage Essentials 2.3 では、ICMP ping はオプションです。ICMP 設定 は、設定 → 検出設定 → 検出時に ICMP ping をスキップ での 検出時に ICMP ping をスキップ の選択内容に基づいて表示されます。

詳細については、ヘルプ（ ）アイコンをクリックしてください。

ICMP 設定オプション

表 21. 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

表 22. 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。
SNMP V1/V2c を有効にする	
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。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。
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小文字を区別します。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。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。**
SNMP V3 を有効にする	
認証プロトコル	デバイスの検出用の認証プロトコルを指定します。サポートされる認証プロトコルは、MD5 および SHA1 です。デバイスを正常に検出するには、同じ認証プロトコルを使用してデバイスを設定する必要があります。認証プロトコルを なし にした場合、暗号化オプションも無効になります。
ユーザー名	デバイス上で設定されたユーザー名を指定します。
認証パスワード	認証パスワードを指定します。
暗号化プロトコル	デバイスの検出用の暗号化プロトコルを指定します（オプション）。サポートされる暗号化プロトコルは、AES および DES です。デバイスを正常に検出するには、同じ暗号化プロトコルを使用してデバイスを設定する必要があります。
暗号化パスワード	認証パスワードを指定します。
汎用設定	
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。有効な範囲は、1 秒～15 秒です。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

表 23. 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。
Password (パスワード)	パスワードを入力します。

ストレージ設定

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。

ストレージ設定オプション

表 24. ストレージ設定オプション

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、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に対してのみ可能です。iDRAC6 バージョン 1.25 以前では、サーバ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

表 25. WS-Man 設定オプション

フィールド	説明
WS-Man 検出の有効化	これを選択して、PowerEdge FX、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。
Password（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、デフォルト値は 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、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 4 回です。
ポート	ポート情報を入力します。デフォルトのポート番号は 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。

iDRAC のための代替 WS-Man 設定（ガイド付きウィザードのみ）

表 26. iDRAC のための代替 WS-Man 設定（ガイド付きウィザードのみ）

フィールド	説明
CMC で iDRAC とスイッチを自動検出する	• これを選択して、シャーシ検出中に CMC で iDRAC とスイッチの自動で検出します。 • CMC での iDRAC とスイッチの自動検出を無効にするには、この選択をクリアします。シャーシのみが検出されます。
iDRAC の検出に同じ CMC 資格情報を使用する	• これを選択して、CMC 用に入力した資格情報を使用して CMC 内の iDRAC の検出します。 • シャーシ内の iDRAC を検出するために異なる資格情報を入力するには、この選択をクリアします。

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

表 27. 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。
Password (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

表 28. 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。**
Password (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。**
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

フィールド	説明
	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。

表 29. 検出範囲処置

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

表 30. 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
Name（ 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

ネットワークで新しいデバイスを検出するように OpenManage Essentials を設定します。設定は、すべての検出範囲に適用されます。OpenManage Essentials では、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。

表 31. 検出スケジュール設定

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。Open Manage Essentials 2.3 では、ICMP ping はオプションです。検出中に ICMP ping をスキップするには、**設定** → **検出設定** → **検出時に ICMP ping をスキップ** をクリックします。選択した場合、デバイスの検出およびインベントリ作成中に ICMP ping がスキップされます。 • **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（OpenManage Server Administrator、OpenManage Array Manager、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

フィールド	説明
	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 のデフォルトイン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

表 32. 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

表 33. 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** — デバイス状態ポ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** — デバイス状態ポ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 セクションには、検出用に設定した IP アドレスまたは IP アドレス範囲のすべてが表示されます。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タイプ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と、 アイコンが表示されます。
- **ガイド付きウィザード** を使用して検出範囲を設定すると、 アイコンが表示されます。
  - **ガイド付きウィザード** を使用してシャーシを検出すると、シャーシ範囲グループに アイコンが表示されます。動的に検出されたシャーシ範囲グループのメンバーには アイコンが表示されます。シャーシ範囲グループが無効化されていると、 アイコンが表示されます。範囲グループのメンバーが無効化されていると、 アイコンが表示されます。

検出範囲を右クリックして検出範囲で使用できるオプションを表示することもできます。右クリックオプションについての情報は、「包含範囲の管理」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、タイプ別にデバイスがリストされます。例えば、PowerEdge サーバは、**サーバ** というデバイスタイプにリストされています。OpenManage Essentials にはデバイスタイプ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、これらのデバイスタイプに分類されます。未分類のデバイスは、**不明** というデバイスタイプにリストされます。定義されたデバイスタイプ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、デバイスタイプ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を作成し、そのグループへのデバイスを含めます。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、PowerEdge VRTX および FX2/FX2s デバイスの表示と管理を行います。

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、デバイスタイプ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**
- **クラスタ**
  - **HA クラスタ**

  - NAS クラスタ
- ハイパーコンバージドインフラストラクチャ
  - VxRail
  - XC Series
- 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
  - ネットワーキングスイッチ
  - Fibre Channel 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 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 グループに表示されます。

  メモ: IPMI を使用して、PowerEdge C サーバ上で 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。デバイス設定を導入するには、このグループにデバイスを明示的に追加する必要があります。ベアメタル導入では、導入完了後に 再利用およびベアメタル グループからデバイスを削除することができます。詳細については、「サーバ導入と再プロビジョニング」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 34. ノードおよび記号の説明

ノード記号	説明
 **図 15. 重要デバイスアイコン**	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。
 **図 16. デバイス未検出アイコン**	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。
 **図 17. 期待される動作からの逸脱アイコン**	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。
 **図 18. デバイスが期待通りに動作中アイコン**	デバイスが期待どおりに動作していることを示します。
 **図 19. 不明デバイスアイコン**	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。
 **図 20. 接続が失われました**	デバイスが到達不能であることを示します。

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。

表 35. デバイス詳細

- 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
- 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

- 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
- 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ついて 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 に表示される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は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、PowerEdge M1000e、PowerEdge VRTX、VMware ESX サーバ 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. **設定** → **カスタム URL 設定** の順にクリックします。
2. 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、  アイコンで識別できます。
   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

OpenManage Essentials は、メールから定期的な間隔でお使いのデバイスの保証通知を送信するように設定できます。設定できる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. **設定** → **保証通知設定** をクリックします。
   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、**期限切れの保証を含む** 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** の詳細については、「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 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よう設定することができます。設定できる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. **設定** → **保証通知設定** をクリックします。
   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. 保証通知スコアボード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、**期限切れの保証を含む** 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. **設定** → **保証通知設定**をクリックします。
   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。

保証アップデート設定の構成

OpenManage Essentials は、サポートサイトで検出されたデバイスの保証情報を確認するように設定できます。設定できる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。

保証アップデート設定を構成するには、次の手順に従います。

1. **設定** → **保証通知設定** をクリックします。
   保証通知設定 ページが表示されます。
2. **保証アップデート設定** の下で **保証アップデートを有効にする** を選択します。
3. **保証アップデートの頻度** フィールドで日数を選択し、保証のアップデートを確認する頻度を設定します。

4. **次回の保証アップデート日** フィールドで、次に保証アップデートを確認する日時を選択します。
5. **適用** をクリックします。

メモ: デフォルトでは、保証アップデート設定 は無効にされています。保証情報は、デバイス保証レポート で表示できます。

マップビューの使用

メモ: マップビューで使用できる機能の詳細については、「マップビュー（ホーム）ポータル」を参照してください。

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：警告 – インターネットに接続できません!。

メモ: マップビュー機能には、有効なマッププロバイダ（MapQuest または Bing）キーが必要です。マッププロバイダキーを入力するには、「マップの設定」を参照してください。

マップビュー機能では、インタラクティブな地図上で Enterprise ライセンスを持つ PowerEdge VRTX および PowerEdge FX2/FX2s デバイスを表示および管理できます。Enterprise ライセンスを持つ PowerEdge VRTX および PowerEdge FX2/FX2s デバイスは、地図上では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 および PowerEdge FX2/FX2s 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。

マップビューには**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：

表 36. マップビューの使用

Action	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 および PowerEdge FX2/FX2s デバイスの追加を許可します。
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 および PowerEdge FX2/FX2s デバイスのインポートを許可します。
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。
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 21. 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
マップビューインタフェース - ホーム ポータル
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
マップビューインタフェース - デバイス タブ
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。

表 37. マップのプロバイダ

MapQuest	Bing
月あたりのトランザクションの数に基づいて購入しなければならない有効な MapQuest キー（ライセンス）キーが必要です。利用可能なトランザクションプランを表示するには、**developer.mapquest.com/plans/** に移動します。 有効な MapQuest 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。	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。**

MapQuest	Bing
	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。
マップのオンラインの部分のレンダリングおよびそのアドレス検索のためには、インターネット接続が必須です。	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経由でインターネットに接続している場合は、OpenManage Essentials の **設定** → **一般設定** ページで設定された **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: MapQuest マップおよび Bing マップのプロバイダは、マップをレンダリングするためにインターネットへの常時接続を必要とします。システムがプロキシサーバ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 MapQuest および Bing の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ステータスの通知の有効化 / 無効化と、Bing マップのプロバイダが要求する有効な Bing キーの指定および MapQuest マップのプロバイダが要求する MapQuest キーの指定が可能です。

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** をクリックします。
   - **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. 次のマップのプロバイダのいずれかを選択します。
   - **MapQuest**
   - **Bing**
6. **キー** フィールドに、適切なマップのプロバイダキーを入力します。
7. **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。

表 38. 正常性状態

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。

表 39. 接続ステータス

ピンの色	アイコン	接続ステータス
青色		点灯
灰色		消灯

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 PowerEdge VRTX および PowerEdge FX2/FX2s 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** フィールドにその位置のアドレスを入力します。（例：シカゴ）

   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 PowerEdge VRTX および PowerEdge FX2/FX2s 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 および PowerEdge FX2/FX2s 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。

   名前を付けて保存 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 設定 → 一般設定 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。
   インポートサマリ 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 および PowerEdge FX2/FX2s デバイスのインポート用テンプレートは .csv ファイルであり、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ます。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。

表 40. デバイスのインポート用テンプレート

フィールド	説明
Name（名前）	Enterprise ライセンスを持つ PowerEdge VRTX および PowerEdge FX2/FX2s 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。
Address（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 および PowerEdge FX2/FX2s 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
- Address（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。
- ライセンス済みの PowerEdge VRTX および PowerEdge FX2/FX2s デバイスは、検索ピンの場所に追加または移動することができます。

。

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 PowerEdge VRTX および PowerEdge FX2/FX2s 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** をクリックします。
   - **管理** → **デバイス** → **マップビュー** の順にクリックします。
2. ライセンスを持つ PowerEdge VRTX または PowerEdge FX2/FX2s デバイスのピンをマップ上で選択します。
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コンピュートスレッドは、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。

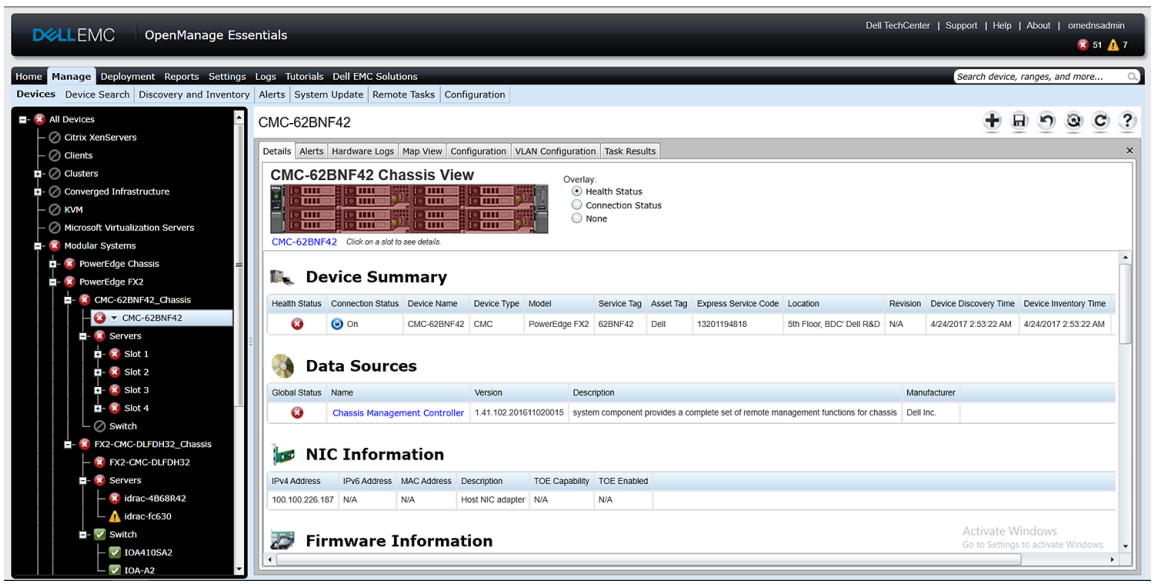

図 22. シャーシビュー

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状態に応じて異なります。複数の計算ノードを含むスレッド（例：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
- 接続ステータス

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
- Service Tag
- 資産タグ
- 正常性状態
- 接続ステータス

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。スロットが選択されると、スレッド周辺に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の説明です。

表 41. オーバーレイ

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
接続ステータス	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。例えば、1 つの計算ノードが **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。

VLAN 設定管理

VLAN 設定 タブでは、次の操作が可能です。

- ブレードサーバ、そしてブレードサーバ NIC ポート、関連する IOA ファブリックポート、および VLAN ID のような、IOA ファブリックの相互接続の詳細を表示します。

  メモ: IOA についての詳細情報がない場合でも、ファブリックのステータスは、グリッド内のデータや、スロットが空です や ファームウェアまたはモードがサポートされていません のような値として表示されます。
- シャーシ内で IOA に VLAN ID を割り当てます。

メモ: すでに検出されている IOA またはサーバを、別のシャーシに移動、シャーシから削除、またはシャーシ内でスワップする場合は、シャーシ、サーバ、および対応する IOA を削除して再検出する必要があります。この操作を行わないと、VLAN 設定インベントリで重複した、または誤ったデータが表示される場合があります。

VLAN 設定管理の要件

- VLAN 設定管理は、PowerEdge M1000e および PowerEdge FX2/FX2s でのみサポートされています。
- シャーシとそのコンポーネント（ブレードサーバと IOA）は、ガイド付きウィザードを使用して OpenManage Essentials で再検出されている必要があります。

- IOA はスタンドアロン、Virtual Link Trunk（VLT）、または Programmable MUX（PMUX）動作モードで設定されている必要があります。
- 最低限必要なファームウェアバージョンは次のとおりです。
  - PowerEdge M1000e — CMC ファームウェアバージョン 5.1 以降。
  - PowerEdge FX/FX2s — CMC ファームウェアバージョン 1.2 以降。
  - PowerEdge M および FN IOA
    * OpenManage Essentials バージョン 2.3 は、9.10.0.0、9.10.0.1P10、9.11.0.0 をサポートします。

メモ: VLAN 設定管理は、PowerEdge FM120x4 スレッドではサポートされていません。PowerEdge FM120x4 スレッドでは、サーバシャーシのスロットマッピングのみが VLAN 設定 タブに表示されます。サーバ名および NIC ポートの詳細は、PowerEdge FM120x4 スレッドの VLAN 設定 タブには表示されません。

VLAN 設定インベントリの表示

シャーシの VLAN 設定インベントリを表示するには、次の手順を実行します。

1. **管理 → デバイス** をクリックします。
2. デバイスツリーで、**Modular Systems**（モジュラーシステム） をクリックします。
3. **PowerEdge M1000e** または **PowerEdge FX2** をクリックし、シャーシ CMC ノードをクリックします。
4. 右ペインで **VLAN 設定** タブをクリックします。
   VLAN 設定インベントリが表示されます。

メモ: はじめて VLAN 設定 タブにアクセスするときは、更新アイコンをクリックしてください。  **は、VLAN 設定 タブの中央に表示されています。**

メモ: 表示されている VLAN 設定インベントリは、最新でない可能性があります。最新の VLAN 設定インベントリを表示するには、更新アイコンをクリックします。  **は、VLAN 設定 タブの右上に表示されています。**

メモ: IOA が検出または構成されていない場合は、VLAN 設定インベントリは表示されません。
VLAN 設定インベントリが表示されなくても、OpenManage Essentials によって取得可能な IOA 名およびモデル情報が表示されます。IOA 名およびモデル情報がない場合は、インベントリ情報を表示できない理由を示すステータスメッセージが表示されます。

次の表には、表示される可能性があるステータスメッセージを示します。
表 42. VLAN 設定インベントリの表示

ステータス	説明
デバイスが検出されません	IOA が OpenManage Essentials で検出されませんでした。
スロットが空です	シャーシのファブリックスロットが空です。
ファームウェアまたはモードがサポートされていません	操作モードまたは IOA のファームウェアのバージョンがサポートされていません。
データが取得できません	OpenManage Essentials が IOA から VLAN 設定インベントリを取得できません。
不明 / エラー	エラーが発生したか、ステータスが不明です。
モデルがサポートされていません	IOA モデルがサポートされていません。

VLAN ID の割り当て

作業開始前に、IOA の管理者権限があることを確認します。

VLAN の割り当てを適用するには、次の手順を実行します。

1. **VLAN 設定** タブの **シャーシ IOA** で、**タグ付き VLAN** および **タグなし VLAN** 行に適切なポートの VLAN ID を入力します。

   メモ: 有効な VLAN ID の範囲は 1 ~ 4094 です。コンマ (,) で各 VLAN ID を区切り、ID 範囲を指定するにはハイフン (-) を使用します。
2. **適用** をクリックします。

   VLAN 設定 ウィンドウに変更した IOA ポートが表示されます。

   メモ: VLAN 設定 ウィンドウでは、VLAN ID を変更することもできます。
3. タスクの一意的な名前を入力します。

   メモ: タスクには、一意の名前を入力することをお勧めします。
4. 必要に応じ、タスクのスケジュールを選択します。
5. ファブリック管理者権限のある IOA の資格情報を入力します。
6. **Finish**（終了）をクリックします。

タスク結果 タブに **VLAN 設定** タスクが表示されます。タスクが完了したら、OpenManage Essentials によって自動的にシャーシ内の IOA の VLAN 設定の一覧が作成されます。

メモ: 複数のポートに VLAN の割り当てを適用する際、VLAN の設定タスクが失敗することがあります。タスク結果 タブには、複数回再試行した結果タスクが失敗した、または、サーバのネットワーク接続が予期せず終了した、という内容のメッセージとともに VLAN の割り当てに失敗したポートが表示されます。そのような場合、正しく設定されなかったポートに対し、しばらく経ってから VLAN 設定を再試行することができます。

メモ: OpenManage Essentials では、IOA の CLI コマンドを使用して、IOA に VLAN を設定します。IOA への VLAN 設定は時間がかかり、リソースが集中的に必要となる操作であるため、IOA のパフォーマンスに影響を与える可能性があります。IOA の操作を安定させるため、OpenManage Essentials では、IOA に VLAN を設定するための十分な時間があるかを確認しながら、IOA の CLI コマンドを適切なタイミングで実行します。すでに IOA で複数の操作が実行されている場合は、VLAN 設定タスクの実行が遅延するか、またはタスクが失敗します。IOA ポートで VLAN 設定に失敗した場合は、該当する IOA で VLAN 設定タスクを再実行することができます。

すべての VLAN ID のリセット

作業開始前に、ファブリック管理者の権限があることを確認します。
VLAN ID に変更を加えた後、すべての変更を元に戻す場合は、次の手順を実行します。

1. **Reset All**（すべて元に戻す） をクリックします。
2. 確認を求められたら、**Yes**（はい） をクリックします。

   メモ: VLAN ID に加えた変更は、OpenManage Essentials のユーザーインタフェースのみに影響します。

デフォルト VLAN ID 値の設定

作業開始前に、ファブリック管理者の権限があることを確認します。
デフォルトの VLAN ID を設定する場合、次の手順を実行します。

1. デフォルト VLAN ID に設定する IOA ファブリックポートを選択します。
2. **Set to default value**（デフォルトの値に設定） をクリックします。

   タグ付けされた VLAN 行には **すべての VLAN** が表示され、タグなし VLAN の行には **1** が表示されます。

   メモ: タグ付けされた VLAN の場合、すべての VLAN のデフォルト値は 2 ~ 4094 の範囲内にあります。タグなし VLAN の場合は、デフォルト値は 1 です。
3. **適用** をクリックします。
4. タスクの一意的な名前を入力します。
5. 必要に応じ、タスクのスケジュールを選択します。

6. ファブリック管理者権限のある IOA の資格情報を入力します。
7. **Finish**（終了）をクリックします。

タスク結果 タブに **VLAN 設定** タスクが作成されます。タスクが完了したら、OpenManage Essentials によって自動的にシャーシ内にあるすべての IOA の VLAN 設定のインベントリが作成されます。

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。

表 43. Dell NAS アプライアンスサポート

	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。
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

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サーバおよび Compellent S8000 iDRAC）は、検出されると、デバイスツリー内の **OEM デバイス** に分類されます。タスク、レポート、およびフィルタなどのサーバで利用できる機能のほとんどが OEM サーバにも適用されます。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サーバ / 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。

メモ: WMI プロトコルを使用して検出された OEM サーバは、OMSA がインストールされている場合にのみ サーバ デバイスグループ下に分類されます。OMSA のない OEM サーバは、不明 デバイスグループ下に分類されます。

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

表 44. 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。
Acknowledged（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。
Device	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

表 45. ハードウェアログの詳細

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。
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。 例えば、電源の冗長性喪失などです。

VLAN 設定

VLAN 設定 タブでは、PowerEdge M1000e および PowerEdge FX2/FX2s シャーシ内で、IOA の VLAN 設定を表示および管理することができます。

VLAN 設定 タブに表示されるフィールドは次のとおりです。

表 46. VLAN 設定

フィールド	説明
最新インベントリ時間	最新の VLAN インベントリの時間を表示します。
ファブリックによるグループ分け	現在表示されているデータをグループ分けするのに使用される属性を表示します。デフォルトでは、VLAN 設定インベントリは **ファブリック** でグループ分けされています。
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。
シャーシブレード	シャーシに取り付けられているブレードサーバの詳細が表示されます。
変更済み	VLAN ID を変更した場合表示されます。
Server Name	ブレードサーバーのホスト名を表示します。

フィールド	説明
Service Tag	ブレードサーバのサービスタグを表示します。
モデル	ブレードサーバのモデル名を表示します。このフィールドが空白の場合、サーバは存在しません。
スロット	ブレードサーバが取り付けられているスロットを表示します。
サブスロット	ブレードサーバノードのサブスロットを表示します。
NIC	NIC の完全修飾デバイス記述子（FQDD）を表示します。
NIC ポート	ブレードサーバが接続されている NIC ポートが表示されます。
シャーシ IOA	シャーシに取り付けられている IOA の詳細が表示されます。
IOA 名	IOA 名を表示します。
IOA モデル	IOA のモデル名を表示します。
ファブリック	シャーシの特定のスロットに関連付けられたファブリックが表示されます。ファブリックは、グループ名（A、B、または C）およびスロット番号（1 または 2）の組み合わせで識別されます。
ポート	IOA に割り当てられたポートが表示されます。
Tagged VLAN(s)（タグ付き VLAN）	IOA のタグ付き VLAN ID が表示されます。
Untagged VLAN（タグなし VLAN）	IOA のタグなし VLAN ID が表示されます。
Set to default value（デフォルトの値に設定）	クリックすると、VLAN ID をデフォルト値に設定します。
すべてをリセット	クリックすると、すべての変更を元に戻します。
適用	クリックすると、VLAN 設定への変更が適用されます。

VLAN 設定タスク

Apply（適用） をクリックして VLAN ID を割り当てると、**VLAN Configuration Task**（VLAN 設定タスク） ウィンドウが表示されます。**VLAN Configuration Task**（VLAN 設定タスク） ウィンドウに表示されるフィールドは次のとおりです。

表 47. VLAN 設定タスク

フィールド	説明
タスク名	VLAN 設定タスクの名前が表示されます。
Selected IO Module Ports（選択した IO モジュールポート）	変更を適用する選択済みの IOA ポートを表示します。
ファブリックによるグループ分け	現在表示されているデータをグループ分けするのに使用される属性を表示します。デフォルトでは、VLAN 設定インベントリは **ファブリック** でグループ分けされています。
シャーシブレード	シャーシに取り付けられているブレードサーバの詳細が表示されます。
Server Name	ブレードサーバのホスト名を表示します。
Service Tag	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。
モデル	ブレードサーバのモデル名を表示します。
スロット	サーバが取り付けられているスロットを表示します。
サブスロット	サーバノードのサブスロットを表示します。
NIC	NIC の完全修飾デバイス記述子（FQDD）を表示します。

フィールド	説明
NIC ポート	サーバが接続されている NIC ポートが表示されます。
シャーシ IOA	シャーシに取り付けられている IOA の詳細が表示されます。
IOA 名	選択した IOA の名前を表示します。
IOA モデル	選択した IOA のモデル名を表示します。
ファブリック	シャーシの特定のスロットに関連付けられたファブリックが表示されます。ファブリックは、グループ名（A、B、または C）およびスロット番号（1 または 2）の組み合わせで識別されます。
ポート	IOA に割り当てられたポートが表示されます。
Tagged VLAN(s)（タグ付き VLAN）	選択した IOA のタグ付き VLAN のリストを表示します。
Untagged VLAN（タグなし VLAN）	選択した IOA のタグなし VLAN が表示されます。
タスクスケジュールの設定	
今すぐ実行	これを選択すると、設定タスクがすぐに実行されます。
スケジュールの設定	選択して、必要な日時にタスクをスケジュールします。
タスク実行のための IOA 資格情報入力	
User Name（ユーザー名）	タスクを実行するのに必要なファブリック管理者ユーザー名を入力します。
Password（パスワード）	タスクを実行するのに必要なファブリック管理者パスワードを入力します。
ヘルプ	クリックすると、オンラインヘルプが開きます。
キャンセル	クリックすると、タスクをキャンセルします。
完了	クリックすると、指定されたスケジュールでタスクを実行します。

タスク結果

タスク結果 タブにはタスクの状況が表示されます。

次の表は、**タスク結果** タブに表示されるフィールドについての説明です。

表 48. タスク結果

フィールド	説明
ステータス	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。

フィールド	説明
	• Running（実行中） • Complete（完了） • Stopped（停止） • Failed（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。

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。

表 49. アラートフィルタ

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。
Acknowledged（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。
Device	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。

表 50. 非準拠システム

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	システムモデル名です。例えば、PowerEdge です。
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。
Service Tag	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。

フィールド	説明
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。

表 51. 選択したアップデートを適用

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。
タイプ	ソフトウェアアップデートの種類です。
Installed Version（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

表 52. デバイスの検索

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。

表 53. クエリ結果

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。
接続ステータス	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。
Name（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。
Service Tag	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。
Asset Tag	デバイスに定義されているアセットタグを表示します。
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

表 54. デバイスグループ設定

フィールド	説明
Name（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

表 55. 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。

フィールド	説明
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。
ハイパーコンバージドインフラストラクチャ	VxRail および XC Series に含めるデバイスを選択します。
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 Controller 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、サーバを含めます。
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。

マップビューインタフェース - デバイス タブ

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。

表 56. マップビュー（ デバイス ）タブインタフェース

アイテム	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 **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**	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。
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。

アイテム	説明
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、およびマップのサービスプロバイダの選択ができます。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（ライセンス）** • **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。

表 57. この位置のデバイス

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、不明** です。
接続ステータス	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。
Device Name（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。
資産タグ	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。

フィールド	説明
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。
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。

表 58. マップ設定

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要求される有効な Bing キーを選択して指定します。
MapQuest キー	MapQuest マップのプロバイダに要求される有効な MapQuest キーを選択して指定します。
キー	マップビューのレンダリングに有効な Bing キーまたは MapQuest キーを入力できます。
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

導入と再プロビジョニング

サーバ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、サーバ用 NIC、およびシャーシ用 CMC の設定が含まれるサーバ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。

- 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編集
- シャーシインフラストラクチャ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
- **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変更または削除
- ベアメタルサーバーの導入
- 仮想 I/O 識別情報プールを作成する
- コンピュートプールを作成する
- 仮想 I/O ID を使用したサーバーの導入（ステートレスな導入）
- サーバーの交換
- 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: 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。デバイス設定を導入するには、再利用およびベアメタル グループにデバイスを明示的に追加する必要があります。ベアメタル導入では、導入完了後に再利用およびベアメタル グループからデバイスを削除することができます。

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、iDRAC を搭載した対応 PowerEdge サーバに対してライセンス付与 (有料)されています。PowerEdge VRTX および PowerEdge FX2/FX2s シャーシで設定コンプライアンスの検証を行うと同時にデバイス設定の作成と導入を行うには、CMC Enterprise ライセンスが必要です。ライセンスに関する詳細については、「OpenManage Essentials — サーバ設定管理ライセンス」を参照してください。

メモ: PowerEdge M1000e シャーシまたは IOA でデバイス設定の作成または導入を行う場合には、ライセンスは必要ありません。

関連リンク

導入ファイル共有の設定
デバイス導入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
デバイス導入テンプレートの管理
デバイス導入テンプレートの導入 - ベアメタル導入
デバイス設定テンプレートの導入 - ステートレス導入
ネットワーク ISO イメージの導入
デバイスの自動導入設定
導入タスクの表示
補足情報

OpenManage Essentials — サーバ設定管理ライセンス

メモ: *OpenManage Essentials* — サーバ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* — サーバ設定管理ライセンスがターゲットサーバにインストールされていることを必須とするのは、サーバ設定管理機能のみです。

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

メモ: *OpenManage Essentials* — サーバ設定管理ライセンスは、サーバ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。このライセンスは、サーバからデバイス設定テンプレートを作成する場合には必要ありません。

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 PowerEdge サーバ
- 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 PowerEdge サーバ

ライセンスの購入

OpenManage Essentials — サーバ設定管理ライセンスは、サーバの購入時、または営業担当者にお問い合わせの上で購入することができます。購入したライセンスは、**Dell.com/support/retail/lkm** のソフトウェアライセンス管理ポータルからダウンロードできます。

ライセンスの導入

サーバ購入後にライセンスを購入する場合は、License Manager を使用してライセンスをサーバ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できます。ライセンスの導入の詳細については、『Dell EMC License Manager ユーザーズガイド』（**Dell.com/OpenManageManuals**）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** ポータルの **管理システムレポート、保証とライセンス** 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. **管理 > 設定 > デバイス設定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

デバイス導入テンプレートの導入 - ベアメタル導入
デバイス設定テンプレートの導入 - ステートレス導入
デバイス設定自動導入のセットアップ - ベアメタル導入
デバイス設定自動導入のセットアップ - ステートレス導入
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：
  - 最新バージョンの iDRAC7 または 8 を装備し、Lifecycle Controller ファームウェアがインストールされている PowerEdge サーバ。
  - *OpenManage Essentials* - サーバ設定管理ライセンスが iDRAC にインストールされている。このライセンスは、iDRAC のライセンスとは異なります。
  - iDRAC Enterprise または iDRAC Express ライセンス。このライセンスは *OpenManage Essentials* - サーバ設定管理ライセンスとは異なります。iDRAC Enterprise ライセンスがターゲットサーバにインストールされていない場合、iDRAC の特定の機能が利用できません。
- シャーシの場合:
  - 対応ファームウェアバージョン：
    - シャーシファームウェアバージョン 5.10 以降がインストールされた PowerEdge M1000e。
    - シャーシファームウェアバージョン 2.1 以降がインストールされた PowerEdge VRTX。
    - シャーシファームウェアバージョン 1.3 以降がインストールされた PowerEdge FX2 または FX2s。
  - PowerEdge FX2、FX2s、および VRTX シャーシには、Enterprise ライセンスが必要です。
- IOA 用：
  - IOA を、次の動作モードのいずれかに設定する必要があります。
    - スタンドアロン
    - Virtual Link Trunk（VLT）
    - プログラム可能 MUX（PMUX）

    メモ: コンプライアンスタスクは、シャーシテンプレートの IOA および IOA 属性ではサポートされません。
  - OpenManage Essentials バージョン 2.3 では、IO アグリゲータにファームウェアバージョン 9.10.0.0、9.10.0.1P10、9.11.0.0 がインストールされている必要があります。

関連リンク

デバイス設定ファイルからのデバイス導入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導入テンプレートの作成
デバイス導入テンプレートの導入 - ベアメタル導入
デバイス設定テンプレートの導入 - ステートレス導入
ネットワーク ISO イメージの導入
デバイス設定自動導入のセットアップ - ベアメタル導入
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
デバイス設定インベントリの表示

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

ベアメタル導入の概要
ステートレスな導入の概要
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

ベアメタル導入の概要

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
デバイス導入テンプレートの作成
デバイス導入テンプレートの編集
デバイス導入テンプレートの導入 - ベアメタル導入

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。

   - **設定** → **導入設定** をクリックします。
   - **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、**ファイル共有ステータス** 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

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

デバイス導入テンプレートの導入 - ベアメタル導入
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

デバイス導入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、シャーシ、または IOA の属性を含むデバイス導入テンプレートを作成します。デバイス導入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、シャーシ、または IOA での設定の導入。
- シャーシインフラストラクチャ設定テンプレートの作成。
- サーバまたはシャーシの設定ベースラインへのコンプライアンスを確認。

  メモ: コンプライアンスタスクは IOA テンプレートではサポートされていません。

以下からデバイス導入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導入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導入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導入テンプレートの作成

デバイス導入テンプレートを既存のサーバ設定ファイルまたはシャーシ設定ファイル（.xml）または IOA 設定ファイル（.txt）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導入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。
- IOA テンプレートのみ – インポートしたい IOA のテンプレートが作成された後に編集されていないことを確認します。IOA テンプレートを編集すると、テンプレートの整合性が損なわれます。したがって、編集された IOA テンプレートの導入は失敗します。

デバイス設定ファイルからデバイス導入テンプレートを作成するには、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. 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**、**シャーシテンプレート**、または **IOA 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** をクリックするか、**コンプライアンスを開始する前に** → **テンプレートの作成** の順にクリックします。

   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. `Ｆｉｎｉｓｈ`（終了）をクリックします。

作成された導入テンプレートが **テンプレート** ペインに表示されます。

メモ: IOA テンプレートは作成と導入のみ可能です。作成した IOA テンプレートは 導入ポータル にのみ表示されます。

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導入テンプレートの作成

検出済みのサーバ、シャーシ、または IOA からデバイス導入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導入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設定テンプレートを作成している。

リファレンスデバイスから、デバイス導入テンプレートを作成するには、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. 次のいずれかを実行します。
   - **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**、**シャーシテンプレート**、または **IOA 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。

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. テンプレートの **名前** を入力します。
4. デバイスタイプ（**サーバ**、**シャーシ**、または **IOA**）を選択し、次のいずれかを実行します。
   - **適用可能なすべてのデバイス** ツリーからデバイスを選択します。
   - **デバイスを検索** ボックスを使用してデバイスを検索します。

メモ: テンプレートの作成ウィザード で、すべての該当デバイス ツリーには、検出およびインベントリ作成が行われたすべてのデバイスが表示されます。Enterprise ライセンスがないデバイスおよびサポートされないファームウェアのデバイスは、無効になり、選択できません。

5. **実行の資格情報** で管理者特権を持つデバイス資格情報を入力し、**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** で導入テンプレートのステータスを表示できます。**タスク実行履歴** 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。作成されたテンプレートが **テンプレート** ペインに表示されます。

メモ: IOA テンプレートは作成と導入のみ可能です。作成した IOA テンプレートは 導入ポータル にのみ表示されます。

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

デバイス導入テンプレートの管理

デバイス導入テンプレートには、サーバ、シャーシ、または IOA のさまざまな属性が含まれます。導入用のテンプレートを使用する前に、次のことができます。

- デバイス導入テンプレートの属性の表示
- デバイス導入テンプレートのクローン化
- デバイス導入テンプレートの編集
- デバイス導入テンプレートのエクスポート
- デバイス導入テンプレートのプロパティの表示

関連リンク

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

デバイス導入テンプレート属性の表示

デバイス導入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。

メモ: デバイス導入テンプレートのデバイス固有の属性と仮想 I/O の識別情報の属性は、テンプレートウィザードの導入 の 属性の編集 タブでのみ表示することができます。

1. **導入** → **導入ポータル** 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。

メモ: IOA テンプレートは作成と導入のみ可能です。作成した IOA テンプレートは 導入ポータル にのみ表示されます。

メモ: デバイスの導入テンプレートがブレードサーバから作成された場合は、右ペインにも IOA VLAN 属性 タブが表示されます。このタブには、ブレードサーバの導入中に導入できる VLAN 属性が表示されます。

関連リンク

デバイス導入テンプレートの管理
デバイス設定テンプレートの詳細

デバイス導入テンプレートのクローン化

デバイス導入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。
デバイス導入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. **導入** → **導入ポータル** 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

デバイス導入テンプレートの管理

デバイス導入テンプレートの編集

テンプレートを導入する前に、デバイス導入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。

メモ: IOA テンプレートの編集はサポートされていません。

デバイス導入テンプレートを編集するには、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. **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。
3. 起動設定およびネットワークインタフェース設定は右ペインの **起動およびネットワーク設定** タブに表示されます。**最初の起動設定**で、起動モードと起動タイプを選択します。

   メモ: デフォルトの起動タイプは、キャプチャされたテンプレートで指定された起動タイプに基づいて選択されます。

   FC が起動タイプとして選択されている場合は、次のフィールドに詳細を入力します。

   a. **最初のターゲット WWPN** に WWPN のアドレスを入力します。
   b. **最初のターゲット LUN ID** に最初のターゲットの LUN ID を入力します。
   c. **2 番目のターゲット WWPN** に WWPN アドレスを入力します。
   d. **2 番目のターゲット LUN ID** に 2 番目のターゲットの LUN ID を入力します。

   FCoE が起動タイプとして選択されている場合は、次のフィールドに詳細を入力します。

   a. **最初のターゲット WWPN** に WWPN のアドレスを入力します。
   b. **最初のターゲット LUN ID** に最初のターゲットの LUN ID を入力します。

   詳細設定 をクリックして **起動シーケンス** と **ハードドライブのシーケンス** を変更します。
4. **ネットワークインタフェース設定** に選択したテンプレートで使用できるネットワークインタフェース設定が表示されます。
   a. パーティションがサポートされている場合は、パーティションを有効にし、**最小帯域幅（%）** および **最大帯域幅（%）** を入力します。
   b. モジュラーサーバからキャプチャされたテンプレートの場合は、**内蔵 NIC** の IOA ポートの **タグ付き VLAN** 値および **タグなし VLAN** 値を入力します。
5. **保存** をクリックします。
   タグ付き VLAN フィールドおよび **タグなし VLAN** フィールドで指定した値は、**IOA VLAN 属性** タブに表示されます。

6. 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。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。
7. 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。
8. 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。
9. 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。
10. **保存** をクリックします。

関連リンク

デバイス導入テンプレートの管理

デバイス導入テンプレートのエクスポート

デバイス導入テンプレートは、.xml（サーバ設定テンプレート）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。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、導入用に使用することができます。

デバイス導入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め、テンプレートの全属性がエクスポートされます。

1. **導入** → **導入ポータル** 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

デバイス導入テンプレートの管理

デバイス導入テンプレートの導入 - ベアメタル導入

テンプレートの導入 タスクにより、特定のデバイスに対する設定属性セットを含む設定テンプレートを導入できます。デバイスにデバイス設定テンプレートを導入すると、デバイスの設定を確実に統一できます。ベアメタルサーバおよびシャーシは、運用のためのプロビジョニングがまだ行われていない基本 iDRAC 通信設定のみを含むデバイスです。

デバイス導入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** グループまたはコンピュートプールに追加されている。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。
- デバイス導入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* - サーバ設定管理ライセンスがすべてのターゲットサーバにインストールされます。詳細については、「OpenManage Essentials - サーバ設定管理ライセンス」を参照してください
- IOA VLAN 設定の展開には、ブレードサーバからテンプレートを作成する必要があります。

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ベアメタル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. 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、**テンプレートの導入** をクリックします。
   - **コンピュートプール** ペインで、ターゲットデバイスを含むコンピュートプールを右クリックしてから **導入** をクリックします。

   テンプレートウィザードの導入 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。
   b. **ターゲットの導入** で、**ベアメタル** を選択します。
   c. **導入オプションの選択** で、**テンプレートの導入** を選択します。

      メモ: か設定テンプレートを導入し、ネットワーク ISO イメージからデバイスを起動する場合は、テンプレートの導入 と ネットワーク ISO からの起動 の両方を選択します。操作ごとに別個のタスクが作成されます。

   d. **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、**サーバテンプレート** または **シャーシテンプレート** 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. **仮想 I/O プールの選択** ページで **次へ** をクリックします。
6. **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: コンピュートプールに割り当てられた 再利用デバイス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選択できます。

7. **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、すべてのパスワード属性を導入前に設定テンプレート内で編集する必要があります。パスワードを変更する場合は、必ず別のユーザーとして導入タスクを実行します。導入中デバイスのパスワードを変更している場合は、必ず別のユーザーアカウントを使用して導入タスクを実行します。

   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. **保存** をクリックします。
   f. **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。

   g. 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。
   h. 導入に新しい静的 IPv4 アドレスを割り当てるには、**IPv4Static 1 IPv4 アドレス** 属性の **値** コラムに静的 IPv4 アドレスを入力します。

      メモ: 変更された静的 IPv4 アドレスを使用してテンプレートを導入すると、デバイスの新しい検出タスクが開始されます。タスクの詳細については、「タスク状態」を参照してください。新規の静的 IPv4 アドレスは、管理 → 検出とインベントリ → 検出範囲 → すべての範囲 の検出範囲に追加されます。

      メモ: 静的 IPv4 アドレスが、シャーシテンプレートの導入で使用されている場合は、シャーシ内のすべてのコンポーネントは、導入タスクが完了した後に再び検出されます。

      メモ: 静的 IPv4 アドレスが提供されていて、DHCP 属性が有効になっている場合は、DHCP 設定は提供された静的 IPv4 アドレスよりも優先されます。同様に、静的 IPv4 アドレスが提供されていて、DHCP 属性が無効になっている場合は、静的 IPv4 アドレスは、テンプレートの導入に使用されます。

i. 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。
j. 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。
k. **保存** をクリックします。
l. （IOA に VLAN 設定を展開する場合のみ）**IOA の VLAN 属性** タブをクリックして、選択したテンプレートの IOA の VLAN 属性を編集します。
m. 導入する属性の **導入** チェックボックスを選択します。
n. タグ付き VLAN とタグなし VLAN の値を入力します。
o. **保存** をクリックします。
p. **次へ** をクリックします。

8. **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。
      - サーバー設定の導入 - ターゲットサーバーの iDRAC での管理者特権を持つ資格情報を入力します。
      - シャーシ設定の導入 - ターゲットシャーシの CMC の管理者特権を持つ資格情報を入力します。
   c. （IOA に VLAN 設定を導入する場合のみ）**IOA 資格情報** の下に、IOA の管理者権限のある資格情報を入力します。
   d. **次へ** をクリックします。
9. **プレビュー** ページで、次の手順を実行します。
   a. **プレビュー** をクリックして、デバイス設定テンプレートの属性がターゲットデバイスに無事に導入されたか確認します。
   b. **次へ** をクリックします。
10. 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。
11. 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実行されます。**タスク実行履歴** 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

テンプレートウィザードの導入
デバイス構成セットアップウィザード
OpenManage Essentials — サーバ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

シャーシからのシャーシ導入テンプレートの作成

IOA とともに検出したシャーシからシャーシ導入テンプレートを作成できます。
シャーシからシャーシ導入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。
- シャーシテンプレートの作成元のデバイスが、「導入およびコンプライアンスタスクのデバイス要件」で指定した要件を満たしている。
- シャーシおよび IOA は、WS-MAN および SNMP プロトコルを使用して検出される必要がある。

メモ: デバイスが SNMP プロトコルのみを使用して検出された場合、シャーシテンプレートは作成できません。

シャーシからシャーシ導入テンプレートを作成するには

1. **導入** → **導入ポータル** の順にクリックします。
2. 次のいずれかを実行します。
   - **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、**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。

   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. テンプレートの **名前** を入力します。
4. デバイスタイプ（**シャーシ**）を選択し、次のいずれかを実行します。
   - **適用可能なすべてのデバイス** ツリーからシャーシデバイスを選択します。

     メモ: Enterprise ライセンスと対応ファームウェアバージョンを備えるシャーシのみを選択できます。
   - **デバイスを検索** ボックスを使用してシャーシデバイスを検索します。
5. **実行資格情報** で、シャーシ資格情報と **IOA 資格情報（オプション）** を入力し、**完了** をクリックします。

   IOA 資格情報 が入力されていない場合、OpenManage Essentials によって、シャーシテンプレートのみが作成されます。IOA 属性はテンプレートにキャプチャされません。

   メモ: 資格情報が一致しない場合、テンプレート作成タスクで、タスクの実行履歴 タブに 警告 状態が表示され、IOA 属性がキャプチャされません。
6. タスク送信のメッセージで、**OK** をクリックします。

右側のペインの **タスク** タブで、シャーシテンプレートのインポートタスクが作成されます。次のいずれかの方法で、シャーシ導入テンプレートの状態を確認できます。

- 右側のペインの **タスクの実行履歴** ビューで確認します。
- **タスクの実行履歴** でタスクをダブルクリックすると、タスク実行の詳細が表示されます。

テンプレート タブの **シャーシテンプレート** に、シャーシテンプレートが表示されます。シャーシテンプレートをクリックして、シャーシと IOA 属性を表示します。

IOA は A1、A2、B1、B2、C1、C2 として表示され、導入に対してデフォルトで選択されます。各 IOA をクリックすると、その属性が表示されます。

シャーシ導入テンプレートの管理

シャーシ導入テンプレートには、シャーシまたは IOA（オプション）のさまざまな属性が含まれます。導入用のシャーシテンプレートを使用する前に、次のことができます。

- シャーシ導入テンプレートの属性の表示
- シャーシ導入テンプレートの導入
- シャーシ導入テンプレートのクローン化
- シャーシ導入テンプレートの名前の変更
- シャーシ導入テンプレートの削除
- シャーシ導入テンプレートのエクスポート

メモ: コンプライアンス関連タスクは IOA 属性ではサポートされていません。

シャーシ導入テンプレート属性の表示

シャーシ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. **導入** → **導入ポータル** → **テンプレート** ペインをクリックします。
2. シャーシテンプレートで、サンプルテンプレートまたは作成済みのシャーシテンプレートのいずれかをクリックします。
   右側のペインに表示されるシャーシまたは IOA テンプレートを選択し、属性を表示します。

シャーシ導入テンプレートのエクスポート

エクスポート オプションでは、シャーシインフラストラクチャを zip ファイルにエクスポートできます。.zip ファイルには、.xml 形式のシャーシテンプレートと、.txt 形式の IOA テンプレートが含まれます。

シャーシ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: シャーシ導入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シャーシテンプレートの全属性がエクスポートされます。

1. **導入** → **導入ポータル** 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。
   テンプレートのエクスポート ダイアログボックスが表示されます。
3. **Ok** をクリックします。
4. 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。
   .zip ファイルには、シャーシテンプレートが xml 形式、IOA テンプレートが txt 形式で保存されます。

シャーシ導入テンプレートのクローン化

シャーシ導入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。
シャーシ導入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. **導入** → **導入ポータル** の順にクリックします。
2. **テンプレート** ペインでシャーシ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。

クローン化されたテンプレートは、シャーシ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。

シャーシインフラストラクチャテンプレートの導入

テンプレートの導入 タスクでは、ターゲットデバイス（シャーシまたは IOA）のシャーシおよび IOA の属性を含むシャーシインフラストラクチャテンプレートを導入できます。
シャーシインフラストラクチャ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。

  メモ: 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 グループへ追加するシャーシのみを選択します。IOA の選択は必須ではありません。テンプレートに IOA 属性が含まれ、ターゲットシャーシがベアメタルグループに属する場合、IOA でも導入が実行されます。
- シャーシインフラストラクチャテンプレートはすでに作成しました。
- 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* - サーバ設定管理ライセンスがすべてのターゲットサーバにインストールされます。詳細については、「OpenManage Essentials - サーバ設定管理ライセンス」を参照してください

注意: シャーシインフラストラクチャ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。

シャーシインフラストラクチャテンプレートを導入するには、次の手順を実行します。

1. **導入** をクリックします。
   導入ポータル が表示されます。
2. 次のいずれかを実行します。
   - **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** → **シャーシテンプレート** ペインで、シャーシインフラストラクチャテンプレート を右クリックし、**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。
   b. **ターゲットの導入** で、**ベアメタル** を選択します。
   c. **導入オプションの選択** で、**テンプレートの導入** を選択します。
   d. **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. **シャーシテンプレート** をクリックします。
   b. 導入したいシャーシインフラストラクチャ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、**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、**次へ** をクリックします。

   メモ: シャーシインフラストラクチャテンプレートを作成した同じシャーシモデルのデバイスのみが選択可能です。
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、すべてのパスワード属性を導入前に設定テンプレート内で編集する必要があります。パスワードを変更する場合は、必ず別のユーザーとして導入タスクを実行します。導入中デバイスのパスワードを変更している場合は、必ず別のユーザーアカウントを使用して導入タスクを実行します。

   a. **テンプレート属性** タブをクリックして、グループ内の属性のリストで属性グループを表示します。

      メモ: シャーシインフラストラクチャテンプレートの導入用に選択された IOA ファブリックが表示されます。
   b. **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。
   c. 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。
   d. 導入に新しい静的 IPv4 アドレスを割り当てるには、**IPv4Static 1 IPv4 アドレス** 属性の **値** コラムに静的 IPv4 アドレスを入力します。

      メモ: 変更された静的 IPv4 アドレスを使用してテンプレートを導入すると、デバイスの新しい検出タスクが開始されます。タスクの詳細については、「タスク状態」を参照してください。新規の静的 IPv4 アドレスは、管理 → 検出とインベントリ → 検出範囲 → すべての範囲 の検出範囲に追加されます。

      メモ: 静的 IPv4 アドレスが、シャーシテンプレートの導入で使用されている場合は、シャーシ内のすべてのコンポーネントは、導入タスクが完了した後に再び検出されます。
   e. IOA のホスト名を編集するには、**IOA ホスト名** 属性の **値** コラムに新しいホスト名を入力します。

      メモ: 検出タスクが成功した後で、IOA のホスト名が、新しいホスト名に変更されます。タスクの詳細については、「タスク状態」を参照してください。新しいホスト名を持つ IOA は、管理 → デバイス → すべてのデバイス 下に表示されます。
   f. 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。
   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. **保存** をクリックします。
   i. **次へ** をクリックします。
7. **オプション** ページで次の手順を実行します。
   a. テンプレートに互換性がないか、または警告メッセージが表示される場合でも、**警告時に続行** を選択して、導入タスクを続行します。
   b. **次へ** をクリックします。
8. **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、シャーシ資格情報を入力します。
   c. **IOA 資格情報** に、IOA の管理者権限のある資格情報を入力します。

      メモ: すべてのターゲット IOA で、資格情報が同じであることを確認します。資格情報がいずれの IOA にも一致しない場合、特定の IOA について導入タスクは失敗します。
   d. **次へ** をクリックします。

9. 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。
10. 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実行されます。**タスク実行履歴** 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。

IOA 設定テンプレートの導入

テンプレートの導入 タスクでは、IOA 設定テンプレートをターゲットデバイスに導入することができます。
IOA 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は、**再利用デバイスとベアメタルデバイス** のグループまたはコンピュートプールに追加されます。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。
- IOA からデバイス構成テンプレートを作成しました。
- 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。

メモ: インポートする IOA テンプレートが作成後に編集されていないことを確認します。IOA テンプレートを編集すると、テンプレートの整合性が損なわれます。したがって、編集された IOA テンプレートの導入は失敗します。

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。

IOA 設定テンプレートを導入するには、次の手順を実行します。

1. **導入** をクリックします。
   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、**テンプレートの導入** をクリックします。
   - **テンプレート** ペインで、導入する IOA テンプレートを右クリックし、**導入** をクリックします。
   - **コンピュートプール** ペインで、ターゲットデバイスがあるコンピュートプールを右クリックし、**導入** をクリックします。

   テンプレートウィザードの導入 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。
   b. **ターゲットの導入** で、**ベアメタル** を選択します。
   c. **導入オプションの選択** で、**テンプレートの導入** を選択します。
   d. **Next**（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. 導入する IOA 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。
   b. **Next**（次へ） をクリックします。
5. 必要に応じて、**仮想 I/O プールの選択** ページで **次へ** をクリックします。
6. **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、**次へ** をクリックします。

   メモ: 再利用およびベアメタルデバイス グループに追加されたデバイスのみを選択できます。
7. **属性の編集** ページで次の手順を実行します。
   a. **デバイスの選択** リストからデバイスを選択します。
   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. 導入する属性を選択します。
   d. お好みに合わせて **値** の行に値を入力します。
   e. **Save**（保存） をクリックします。

f. **Next**（次へ） をクリックします。

8. **オプション** ページで次の手順を実行します。
   - デバイス設定テンプレートが正常に導入されるかどうかのみを確認する場合、**事前チェックのみを実行** を選択します。

     メモ: 事前チェックのみを実行 オプションが選択されている場合、デフォルトで 警告時に続行 オプションが無効になっています。
   - テンプレートがターゲットデバイスで使用できない時に導入を停止したくない場合は、**警告時に続行**を選択します。

     メモ: このオプションが選択されたときは、警告が無視され（ある場合 ）、デバイス設定テンプレートに互換性がない場合でも導入タスクは実行を続けます。
9. **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** の下で、IOA の管理者権限のある資格情報を入力します。
   c. **Next**（次へ） をクリックします。
10. 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。
11. 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。

IOA の動作モードと展開タスクのステータス

次の表は、IOA 動作モードと IOA 展開タスクの結果のリストです。

表 59. IOA の動作モードと展開タスクのステータス

テンプレートの作成元またはインポート元である IOA の動作モード	テンプレートが展開されている IOA の動作モード	展開タスクのステータス
スタック	任意のモード	Failed（失敗）
任意のモード	スタック	Failed（失敗）
スタンドアロン	プログラム可能 MUX（PMUX）	警告
スタンドアロン	スタンドアロン	Complete（完了）
PMUX	PMUX	警告
PMUX	スタンドアロン	警告
Virtual Link Trunk（VLT）	VLT	Complete（完了）
VLT	VLT 以外	Failed（失敗）
VLT 以外	VLT	Failed（失敗）

ネットワーク ISO イメージの導入

テンプレートの導入タスクでは、ネットワーク ISO イメージからサーバーを起動し、その後でサーバーに ISO イメージを導入することができます。

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。
   b. **導入オプションの選択** で **テンプレートの導入** をクリアして、**ネットワーク ISO からの起動** を選択します。

      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。

   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** の下に、ターゲットサーバーの iDRAC の管理者特権を持つ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 からの起動 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 イメージからターゲットサーバーを起動した後、iDRAC 仮想コンソールを起動して、ISO イメージ導入のオプションを選択する必要があります。

関連リンク

テンプレートウィザードの導入
デバイス構成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

デバイス設定の導入、ネットワーク ISO イメージの導入、または自動導入タスクの完了後に、**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。

メモ: OpenManage Essentials バージョン 2.0、2.0.1、または 2.1 で自動展開タスクを作成した後、バージョン 2.2 またはバージョン 2.3 にアップグレードする場合、自動展開タスクを正常に実行できません。このシナリオでは、バージョン 2.2 またはバージョン 2.3 へアップグレードした後、自動展開タスクを再作成することをお勧めします。

メモ: 自動導入機能は、IOA テンプレートでは使用できません。

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 - ベアメタル導入
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. **設定** → **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 - ベアメタル導入

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と、デバイスの設定を確実に統一できます。

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 ファイルに含まれています。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「ServiceTag」、「Service Tag」、または「Node ID」に示されます。

メモ: （PowerEdge FM120x4 などの）複数のコンピュートノードを持つデバイスでは、すべてのコンピュートノードは同じサービスタグを持ちます。したがって、使用する特定のコンピュートノードを識別するにはノード ID を使用する必要があります。.csv ファイルでは、自動導入する特定のコンピュートノードのノード 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* - サーバ設定管理ライセンスがすべてのターゲットサーバにインストールされます。詳細については、「OpenManage Essentials - サーバ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. **導入オプションの選択** ページで、次の手順を実行します。
   a. **ターゲットの導入** で **ベアメタル** をクリックします。
   b. 設定テンプレートを自動導入し、オペレーティングシステムの ISO のイメージからデバイスを起動する場合は、**テンプレートの導入** と **ネットワーク ISO からの起動** オプションの両方を選択します。操作ごとに別個のタスクが作成されます。
   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、**サーバテンプレート** または **シャーシテンプレート** 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。
      インポートサマリ 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、すべてのパスワード属性を導入前に設定テンプレート内で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. **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. 導入に新しい静的 IPv4 アドレスを割り当てるには、**IPv4Static 1 IPv4 アドレス** 属性の **値** コラムに静的 IPv4 アドレスを入力します。

メモ: 変更された静的 IPv4 アドレスを使用してテンプレートを導入すると、デバイスの新しい検出タスクが開始されます。タスクの詳細については、「タスク状態」を参照してください。新規の静的 IPv4 アドレスは、管理 → 検出とインベントリ → 検出範囲 → すべての範囲 の検出範囲に追加されます。

メモ: 静的 IPv4 アドレスが、シャーシテンプレートの導入で使用されている場合は、シャーシ内のすべてのコンポーネントは、導入タスクが完了した後に再び検出されます。

h. 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。
i. 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。

メモ: デバイス固有属性 は、特定のデバイス、またはすべてのデバイス用に .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。

j. （IOA に VLAN 設定を展開する場合のみ）**IOA の VLAN 属性** タブをクリックして、選択したテンプレートの IOA の VLAN 属性を編集します。
k. 導入する属性の **導入** チェックボックスを選択します。
l. タグ付き VLAN とタグなし VLAN の値を入力します。
m. **保存** をクリックします。
n. **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. （IOA に VLAN 設定を導入する場合のみ）**IOA 資格情報** の下に、IOA の管理者権限のある資格情報を入力します。
   g. **次へ** をクリックします。
8. **概要** ページで入力した情報を確認してから、**終了** 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。

OpenManage Essentials でデバイスの検出とインベントリの作成が行われるまで、サービスタグまたはノード ID が **自動導入** タブに表示されます。**未検出デバイスへの設定の導入** タスクを定期的に実行し、OpenManage Essentials でデバイスが検出され、インベントリが作成されているかどうかを検証します

メモ: 未検出デバイスへの設定の導入 は、設定 → 導入の設定 で設定された頻度に基づいて実行されます。

デバイスの検出およびインベントリ作成が完了し、導入タスクが作成された後、デバイスは **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。**タスク実行履歴** 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。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: 自動導入タスクが失敗した場合でも、自動導入 タブのデバイスは、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場合は、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作成 の手順 2～5 の指示に従って、検出範囲を作成します。
   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。

表 60. ファイルのインポート要件

フィールド	説明
Device Name (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。
Service Tag	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。

フィールド	説明
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。**
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

サーバの仮想入出力（I/O）ID の管理 - ステートレス導入

NIC または HBA など、サーバの I/O インタフェースには、インタフェースのメーカーによって割り当てられた固有 ID 属性があります。これらの固有 ID 属性は総合的に、サーバの I/O ID と呼ばれています。I/O ID によってネットワーク上の個々のサーバを識別でき、固有のプロトコルを使用してサーバがネットワークリソースと通信する方法も判断できます。OpenManage Essentials を使用すると、サーバの I/O インタフェースに対し、仮想の ID 属性を自動的に生成および割り当てることができます。

仮想 I/O ID を含むデバイス設定テンプレートを使用して導入されたサーバは、ステートレスとなることが知られています。ステートレスな導入によって、動的で柔軟性の高いサーバ環境を作成することができます。たとえば、SAN からの起動環境で仮想 I/O ID を使用してサーバを導入すると、次の操作を迅速に実行できるようになります。

- 故障が予測される、またはすでに故障したサーバーは、I/O ID を別の予備のサーバーに移動することで交換できます。
- ワークロードの高いときに追加のサーバーを導入して、コンピューティング能力を向上させることができます。

導入 ポータルでは、サーバーの仮想 I/O ID の管理に必要な次のタスクを実行できます。

- 仮想 I/O プールの作成
- コンピュートプールの作成
- サーバーの導入
- サーバーの仮想 I/O ID の回収
- サーバーの交換

ステートレスな導入の概要

ターゲットデバイスに仮想 I/O 属性を持つデバイス設定テンプレートを導入するために実行する必要がある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. **仮想 I/O プールの作成** - **一般タスク** ペインの **仮想 I/O プールの作成** タスクを使用して、1 つ、または複数の仮想 I/O ID タイプのプールを作成します。仮想 I/O ID プールは、仮想 I/O ID をターゲットデバイスに割り当てるために使用します。
4. **コンピュートプールの作成** - **一般タスク** ペインの **コンピュートプールの作成** タスクを使用して、特定の目的に使用するサーバーのグループを作成します。デバイス設定テンプレートと仮想 I/O プールはコンピュートプールに関連付けることができます。
5. **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** - **一般タスク** ペインの **テンプレートの導入** タスクを使用して、デバイス設定テンプレートと仮想 I/O ID をターゲットデバイスに導入します。

関連リンク

デバイス設定導入を開始する前に
デバイス導入テンプレートの作成
デバイス導入テンプレートの編集
仮想入出力（I/O）プールの作成
コンピュートプールの作成
デバイス設定テンプレートの導入 - ステートレス導入

仮想入出力（I/O）プール

仮想 I/O プールは、ネットワーク通信に必要な 1 つ、または複数のタイプの仮想 I/O ID の集合です。仮想 I/O プールには、次の仮想 I/O ID タイプの組み合わせを含めることができます。

- メディアアクセスコントロール（MAC）アドレスによって定義されるイーサネット ID。MAC address は Ethernet（LAN）通信に必要です。
- ワールドワイドノード名（WWNN）と ワールドワイドポート名（WWPN）によって定義されるファイバチャネル（FC）ID。WWNN ID は、FC ファブリックのノード（デバイス）に割り当てられ、デバイスの一部またはすべてのポートで共有されることがあります。WWPN ID は FC ファブリックでの各ポートに割り当てられ、各ポートで固有です。WWNN ID と WWPN ID は、SAN からの起動のサポートや、FC および Fibre Channel over Ethernet（FCoE）プロトコルを使用したデータアクセスに必要です。
- iSCSI 修飾名（IQN）によって定義される iSCSI ID。IQN ID は iSCSI プロトコルを使用した SAN からの起動をサポートするために必要です。

OpenManage Essentials では仮想 I/O プールを利用して、サーバー導入に使用したデバイス設定テンプレートに仮想 I/O 識別情報を自動的に割り当てます。

メモ: 仮想 I/O プールは、1 つまたは複数のコンピュートプールと関連付けることができます。

関連リンク

仮想入出力（I/O）プールの作成
仮想入出力（I/O）プールの編集
仮想入出力（I/O）プールの定義の表示
仮想入出力（I/O）プールの名前の変更
仮想入出力（I/O）プールの削除

仮想入出力（I/O）プールの作成

1 つまたは複数の仮想 I/O ID のタイプが含まれている仮想 I/O プールを作成することができます。
仮想 I/O ID の タイプのプールを作成するには、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。
   - 左ペインの **共通のタスク** で、**仮想 I/O プールの作成** をクリックします。
   - 左ペインの **仮想 I/O プール** で、**仮想 I/O プール** → **仮想 I/O プールの作成** を右クリックします。

   仮想 I/O プールの作成 ウィザードが表示されます。
3. **名前と説明** ページで仮想 I/O プールの一意の名前と適切な説明を入力し、**次へ** をクリックします。
4. **Ethernet 識別情報** ページで、次のいずれかを実行します。

   メモ: MAC アドレスを仮想 I/O プールに含めない場合は、このプールに MAC アドレスを含める オプションのチェックを外し、次へ をクリックします。

   a. 開始アドレスと識別情報の数を指定するには、次を実行します。

      1. **開始アドレスの指定** ボックスで、生成する MAC アドレスで事前定義する開始アドレスを入力します。

         メモ: 仮想 I/O プールを作成または編集するときには、入力アドレスレンジ（開始アドレス + 識別情報の数）が既存のアドレスレンジに対して検証され、重複がないかどうかが確認されます。要求されたアドレスレンジが既存の仮想 I/O プールのアドレスレンジと重複している場合、要求された識別情報の数は保証されません。

      2. **識別情報の数** ボックスで、定義する識別情報の値を入力し、**次へ** をクリックします。

         メモ: 統合型ネットワークアダプタ（CNA）カードでは、WWNN と WWPN の識別情報は仮想 FIP MAC アドレスから派生します。この場合、識別情報が Ethernet の識別情報プールから生成されていないときでも、派生した識別情報が Ethernet の識別情報プールに対してカウントされます。仮想プールを使用して CNA カードが搭載されたサーバに導入する場合、Ethernet の識別情報プールサイズを定義する一方で、必要なバッファが追加されていることを確認します。

   b. .csv ファイルから MAC アドレスをインポートする場合、**ファイルからインポートする** をクリックし、次を実行します。

      メモ: .csv ファイルを使用して、最大 1000 の識別情報をインポートできます。.csv ファイルには、`Name` または `Value` と言う名前のコラムが必要です。

      1. **インポート** をクリックします。
      2. **インポートウィザード** で、**インポート** をクリックします。
      3. .csv ファイルを参照して選択し、**開く** をクリックします。**インポートの結果** ウィンドウが表示されます。
      4. **インポートの結果** ウィンドウを閉じ、**インポートウィザード** を閉じてから、**次へ** をクリックします。

	A
1	Value
2	F4-23-A5-32-70-E2
3	2B-40-04-6B-88-E6
4	01-CC-FE-0B-BC-0A
5	C9-81-33-D5-D3-65
6	B7-BC-3C-CF-27-91
7	27-1B-B5-CC-4D-26

図 23. MAC アドレスのあるサンプル .csv ファイル

5. **FCoE ノード名の識別情報** ページで、次のいずれかを実行します。

メモ: FC 属性は、仮想 FIP MAC アドレスに基づいて OpenManage Essentials によって自動的に生成されるため、統合型ネットワークアダプタ（CNA）カードでの展開には、FC 属性のある仮想 I/O プールは必要ありません。

メモ: ファイバチャネル WWNN の識別情報を仮想 I/O プールに含めない場合は、ファイバチャネル WWNN の識別情報をプールに含める オプションをオフにして、次へ をクリックします。

a. WWNN の識別情報の開始アドレスと生成する識別情報の数を指定するには、次を実行します。

1. **開始アドレスの指定** ボックスで、生成する WWNN の識別情報で事前定義する開始アドレスを入力します。

メモ: 仮想 I/O プールを作成または編集するときには、入力アドレスレンジ（開始アドレス + 識別情報の数）が既存のアドレスレンジに対して検証され、重複がないかどうかが確認されます。要求されたアドレスレンジが既存の仮想 I/O プールのアドレスレンジと重複している場合、要求された識別情報の数は保証されません。

2. **識別情報の数** ボックスで、定義する識別情報の値を入力し、**次へ** をクリックします。

b. .csv ファイルから WWNN の識別情報をインポートする場合、**ファイルからインポートする** をクリックし、次を実行します。

メモ: .csv ファイルを使用して、最大 1000 の識別情報をインポートできます。.csv ファイルには、`Name` または `Value` と言う名前のコラムが必要です。

1. **インポート** をクリックします。
2. **インポートウィザード** で、**インポート** をクリックします。
3. .csv ファイルを参照して選択し、**開く** をクリックします。**インポートの結果** ウィンドウが表示されます。
4. **インポートの結果** ウィンドウを閉じ、**インポートウィザード** を閉じてから、**次へ** をクリックします。

	A
1	Value
2	50:06:0e:80:10:13:93:20
3	50:06:0e:80:10:13:93:21
4	50:06:0e:80:10:13:93:22
5	50:06:0e:80:10:13:93:23
6	50:06:0e:80:10:13:93:24

図 24. WWNN ID のあるサンプル .csv ファイル

6. **FCoE ポート名の識別情報** ページで、次のいずれかを実行します。

メモ: ファイバチャネル WWPN の識別情報を仮想 I/O プールに含めない場合は、ファイバチャネル WWPN の識別情報をプールに含める オプションをオフにして、次へ をクリックします。

a. WWPN の識別情報の開始アドレスと生成する識別情報の数を指定するには、次を実行します。

1. **開始アドレスの指定** ボックスで、生成する WWPN の識別情報で事前定義する開始アドレスを入力します。

メモ: 仮想 I/O プールを作成または編集するときには、入力アドレスレンジ（開始アドレス + 識別情報の数）が既存のアドレスレンジに対して検証され、重複がないかどうかが確認されます。要求されたアドレスレンジが既存の仮想 I/O プールのアドレスレンジと重複している場合、要求された識別情報の数は保証されません。

2. **識別情報の数** ボックスで、定義する識別情報の値を入力し、**次へ** をクリックします。

b. .csv ファイルから WWPN の識別情報をインポートする場合、**ファイルからインポートする** をクリックし、次を実行します。

メモ: .csv ファイルを使用して、最大 1000 の識別情報をインポートできます。.csv ファイルには、`Name` または `Value` と言う名前のコラムが必要です。

1. **インポート** をクリックします。
2. **インポートウィザード** で、**インポート** をクリックします。
3. .csv ファイルを参照して選択し、**開く** をクリックします。**インポートの結果** ウィンドウが表示されます。
4. **インポートの結果** ウィンドウを閉じ、**インポートウィザード** を閉じてから、**次へ** をクリックします。

	A
1	Value
2	20:06:0e:AE:22:BE:99:20
3	20:06:0e:AE:22:BE:99:21
4	20:06:0e:AE:22:BE:99:22
5	20:06:0e:AE:22:BE:99:23
6	20:06:0e:AE:22:BE:99:24

図 25. WWPN ID のあるサンプル .csv ファイル

7. **iSCSI IQN の識別情報** ページで、次のいずれかを実行します。

メモ: iSCSI IQN 識別情報を仮想 I/O プールに含めない場合は、IQN の識別情報をプールに含める オプションをオフにして、次へ をクリックします。

a. 生成する iSCSI IQN の識別情報の接頭辞を入力する場合は、**割り当てる接頭辞の指定** をクリックし、適切なフィールドに IQN を入力します。

メモ: 一般的な iSCSI IQN フォーマットは *iqn.date.domainname-in-reverse:storage-identifier* です（例：iqn. 2001-04.com.example:storage.disk2.sys1.xyz ）。

メモ: iSCSI IQN 識別子文字列には、ハイフン、コンマ、コロン、ピリオドなどの特殊文字を含めることができます。

b. .csv ファイルから iSCSI IQN ID をインポートする場合、**ファイルからインポート** をクリックし、以下を実行します。

メモ: .csv ファイルを使用して、最大 1000 の識別情報をインポートできます。.csv ファイルには、`Name` または `Value` と言う名前のコラムが必要です。

1. **インポート** をクリックします。
2. **インポートウィザード** で、**インポート** をクリックします。
3. .csv ファイルを参照して選択し、**開く** をクリックします。**インポートの結果** ウィンドウが表示されます。
4. **インポートの結果** ウィンドウを閉じ、**インポートウィザード** を閉じてから、**次へ** をクリックします。

	A
1	Value
2	iqn.1993-01.com.example:storage.tape1.sys1.01
3	iqn.1994-01.com.example:storage.tape1.sys1.01
4	iqn.1995-01.com.example:storage.tape1.sys1.01
5	iqn.1992-01.com.example:storage.tape1.sys1.01
6	iqn.1992-01.com.example:storage.tape1.sys1.02

図 26. iSCSI IQN ID のあるサンプル .csv ファイル

8. **サマリ** ページで、I/O ID タイプに対して入力した定義と ID の数を確認し、**終了** をクリックします。

作成した仮想 I/O プールが左ペインの **仮想 I/O プール** の下に表示されます。

関連リンク

[仮想入出力（I/O）プール]
[仮想入出力（I/O）プールの作成ウィザード]

仮想入出力（I/O）プールの編集

以前に指定したことのない範囲を追加したり、新しい I/O ID タイプを追加したり、どのコンピュートプールにも割り当てられていない ID タイプの範囲を削除したりするために仮想 I/O プールを編集できます。
仮想 I/O プールの定義を編集するには、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. 左ペインの **仮想 I/O プール** で仮想 I/O プールを右クリックし、**編集** をクリックします。
   仮想 I/O プールの作成ウィザード が表示されます。
3. 必要に応じて、ウィザードの適切なページの定義を変更します。
4. **概要** ページで、**終了** をクリックします。

仮想 I/O プールに行った変更が保存されます。
関連リンク
仮想入出力（I/O）プール
仮想入出力（I/O）プールの作成ウィザード

仮想入出力（I/O）プールの定義の表示

仮想 I/O プールの定義を表示するには、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. 左ペインの **仮想 I/O プール** で仮想 I/O プールを右クリックし、**表示** をクリックします。
   仮想 I/O プールの作成ウィザード が表示されます。
3. **次へ** をクリックして、仮想 I/O プールのさまざまな I/O ID 定義を表示します。

関連リンク
仮想入出力（I/O）プール
仮想入出力（I/O）プールの作成ウィザード

仮想入出力（I/O）プールの名前の変更

仮想 I/O プールの名前を変更するには、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. 左ペインの **仮想 I/O プール** で、名前を変更する仮想 I/O プールを右クリックしてから **名前の変更** をクリックします。
   仮想 I/O プールの名前の変更 ウィンドウが表示されます。
3. 新しい名前を入力し、**OK** をクリックします。

仮想 I/O プールの名前が変更されます。
関連リンク
仮想入出力（I/O）プール

仮想入出力（I/O）プールの削除

仮想 I/O プールは、ロックされていない場合に削除することができます。
仮想 I/O プールを削除するには、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. 左ペインの **仮想 I/O プール** で、削除する仮想 I/O プールを右クリックしてから **削除** をクリックします。
3. **削除の確認** プロンプトで、**はい** をクリックします。

仮想 I/O プールが削除されます。

関連リンク

[仮想入出力（I/O）プール](#)

デバイスに割り当てまたは導入された仮想入出力（I/O）ID の表示

導入された I/O ID はターゲットデバイスに導入された仮想 I/O プールからの ID です。割り当てられた I/O ID は、デバイスに導入する前にターゲットデバイスに割り当てられた仮想 I/O プールからの ID です。**導入テンプレートウィザード** の **属性の編集** → **ID 属性** タブを使用して、仮想 I/O ID をターゲットデバイスに割り当てることができます。

デバイスに割り当てられた、または導入された仮想 I/O ID を表示するには：

メモ: 仮想 I/O ID が割り当てられた、または導入されたすべてのデバイスを表示するには、レポート → サーバー設定 → 割り当てられた ID の属性 をクリックします。

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. 左側のペインの **仮想 I/O プール** で、仮想 I/O プールを選択します。

   右側のペインに、**仮想 I/O プールサマリ** ページが表示されます。
3. **仮想 I/O プールサマリ** ページで、**ID を持つデバイス** タブをクリックします。

   割り当て済みまたは導入済みの仮想 I/O ID を持つデバイスが、グリッドに表示されます。
4. 次のいずれかを実行します。

   - グリッド上のデバイスを右クリックしてから、**ID の表示** をクリックします。
   - グリッド上のデバイスをダブルクリックします。

   ID の割り当て ウィンドウに、デバイスに割り当てられた、または導入された仮想 I/O ID が表示されます。

コンピュートプール

コンピュートプールは特定の目的のために使用するサーバーグループです。通常、コンピュートプール内のサーバーは同じハードウェア構成と属性を備えています。必要に応じて、次をはじめとするさまざまな目的でコンピュートプールを作成することができます。

- ワークロードの管理
- ビジネスユニットのサーバーの管理
- 地域内のサーバーの管理

コンピュートプールを作成すると、本番環境で新しいサーバーの導入や既存のサーバーの交換を迅速に行うことができます。

メモ: コンピュートプールは 1 つの仮想 I/O プールと 1 つのデバイス設定テンプレートだけに関連付けることができます。

関連リンク

[コンピュートプールの作成](#)
[デバイス設定テンプレートの導入 - ステートレス導入](#)
[コンピュートプールのロック解除](#)
[コンピュートプールの定義の編集](#)
[コンピュートプールの定義の表示](#)
[コンピュートプールからのサーバーの削除](#)
[コンピュートプールの名前変更](#)
[コンピュートプールの削除](#)

コンピュートプールの作成

コンピュートプールを作成して、特定の目的に使用するサーバーをグループ化できます。
コンピュートプールを作成するには、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。

   - 左ペインの **共通タスク** で、**コンピュートプールの作成** をクリックします。
   - 左ペインの **コンピュートプール** で、**再利用およびベアメタル → コンピュートプールの作成** を順に選択します（右クリックしてから選択）。

   コンピュートプールの作成ウィザード が表示されます。
3. **名前と説明** ページでコンピュートプールの一意の名前と適切な説明を入力し、**次へ** をクリックします。
4. **テンプレートの選択** ページで、次を実行します。

   メモ: テンプレートの選択はオプションです。テンプレートは、コンピュートプールの編集時、またはサーバの導入時にも選択できます。テンプレートを選択しない場合は、コンピュートプールのテンプレートの選択 オプションの選択を解除してから 次へ をクリックします。

   メモ: 選択できるのは、以前にサーバーから作成したテンプレート、またはクローンしたテンプレートのみです。

   メモ: コンピュートスプールとすでに関連付けられているテンプレートは選択できません。

   メモ: 選択したテンプレートは、最新の iDRAC ファームウェアがインストールされている PowerEdge サーバからインポートする必要があります。テンプレートには、導入された仮想 I/O ID を再起動のたびに保持することを可能にする永続性ポリシー属性が含まれている必要があります。

   a. **コンピュートプールのテンプレートの選択** オプションを選択します。
   b. リストからテンプレートを選択し、**次へ** をクリックします。
5. **ISO の保存場所の選択** ページで次を実行します。

   メモ: ISO の場所詳細を提供しない場合は、ネットワーク ISO からコンピュートプールを起動する オプションが選択されていないことを確認してから 次へ をクリックします。

   a. **ネットワーク ISO からのコンピュートプールの起動** オプションを選択します。
   b. ISO ファイル名を入力して、IP アドレスとネットワーク共有の名前を適切なフィールドに入力し、**次へ** をクリックします。
6. **仮想 I/O プールの選択** ページで、次のいずれかを実行します。

   - テンプレートを導入している間に仮想 I/O ID の属性を指定する場合は、**ユーザー定義の I/O 割り当て** をクリックしてから **次へ** をクリックします。
   - OpenManage Essentials でコンピュートプールのサーバーに自動的に仮想 I/O ID を割り当てるには、**I/O の自動割り当て** をクリックして、リストから仮想 I/O プールを選択してから **次へ** をクリックします。
7. **デバイスの選択** ページで、コンピュートプールに含めるターゲットデバイスを**適用可能なすべてのデバイス** ツリーから選択し、**次へ** をクリックします。

   メモ: 他のコンピュートプールのメンバーでない再利用およびベアメタル グループ内のデバイスのみを選択できます。

   メモ: コンピュートプールにすでに含まれているデバイスを、別のコンピュートプールに含めることはできません。

   メモ: コンピュートプールに含めるよう選択するデバイスだけが、ステートレス導入で使用可能です。
8. （ステップ 4 のテンプレートを選択した場合のみ）**属性の編集** ページでは、必要に応じて属性を選択および更新し、**次へ** をクリックします。
9. **概要** ページで選択内容を確認し、**終了** をクリックします。

作成したコンピュートプールが 左ペインの **コンピュートプール** の下に表示されます。

関連リンク

コンピュートプール
コンピュートプールの作成ウィザード

デバイス設定テンプレートの導入 - ステートレス導入

テンプレートの導入 タスクにより、特定のデバイスに対する設定属性セットを含む設定テンプレートを導入できます。デバイスにデバイス設定テンプレートを導入すると、デバイスの設定を確実に統一できます。

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は、コンピュートプールに追加されます。詳細については、コンピュートプールの作成 および コンピュートプールの編集 を参照してください。
- デバイス設定テンプレートを作成またはクローンした。
- 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* - サーバ設定管理ライセンスがすべてのターゲットサーバにインストールされます。詳細については、「OpenManage Essentials - サーバ設定管理ライセンス」を参照してください
- Mellanox HBA アダプタを装備したサーバー上で、インストールされているアダプタファームウェアのバージョンが 02.34.50.10 X08 またはそれ以降であることを確認します。
- IOA 設定の展開には、ブレードサーバからテンプレートを作成する必要があります。

メモ: ステートレスな導入をサポートする HBA カードタイプのリストについては、Dell.com/idracmanuals.にある『iDRAC User's Guide』(iDRAC ユーザーズガイド) の「Supported cards for I/O Identity Optimization」(I/O アイデンティティ最適化の対応カード) 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. 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、**テンプレートの導入** をクリックします。
   - **コンピュートプール** ペインで、導入するデバイスを含むコンピュートプールを右クリックし、**導入** をクリックします。

   テンプレートウィザードの導入 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。
   b. **ターゲットの導入** で **コンピュートプール**を選択します。
   c. **コンピュートプールの選択** リストから、コンピュートプールを選択します。
   d. **導入オプションの選択** で、**テンプレートの導入** を選択します。
   e. **次へ** をクリックします。
4. **テンプレートの選択** ページで、デバイス設定テンプレートを選択し、**次へ** をクリックします。

   メモ: 作成済みまたはクローン化が完了しているデバイス設定テンプレートのみを選択することができます。コンピュートプールにすでに割り当てられているテンプレートは選択できません。
5. **仮想 I/O プールの選択** ページで次のいずれかを実行して、**次へ**をクリックします。
   - デバイスの仮想 I/O ID を手動で提供する場合は、**ユーザー定義の I/O 割り当て** を選択します。
   - **I/O の自動割り当て** を選択して仮想 I/O プールをリストから選択すると、OpenManage Essentials で仮想 I/O ID を自動的にデバイスに割り当てることができます。
6. **デバイスの選択** ページのコンピュートプールのツリーから 1 つまたは複数のターゲットデバイスを選択してから、**次へ** をクリックします。
7. **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、すべてのパスワード属性を導入前に設定テンプレート内で編集する必要があります。

メモ: 手順 5 で ユーザー定義の I/O 割り当て を選択した場合は、テンプレートの I/O 属性を編集し、デバイスの編集 → デバイス固有の属性 タブで適切な値を入力する必要があります。

メモ: デバイス設定テンプレートの BIOS 属性リストには、属性 EnableBootDevices および DisableBootDevices を備える BIOS.Virtual インスタンスが含まれます。起動元にしたいデバイスは、EnableBootDevices リストに含める必要があります。

a. デバイス設定テンプレートの属性を編集するには、**テンプレートの属性** 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に、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** 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 **グループ化基準** バーに表示されます。
e. **保存** をクリックします。
f. **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。

g. **デバイスの選択** でデバイスを選択します。
h. 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。
i. 導入に新しい静的 IPv4 アドレスを割り当てるには、**IPv4Static 1 IPv4 アドレス** 属性の **値** コラムに静的 IPv4 アドレスを入力します。

メモ: 変更された静的 IPv4 アドレスを使用してテンプレートを導入すると、デバイスの新しい検出タスクが開始されます。タスクの詳細については、「タスク状態」を参照してください。新規の静的 IPv4 アドレスは、管理 → 検出とインベントリ → 検出範囲 → すべての範囲 の検出範囲に追加されます。

j. 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。
k. 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。
l. **保存** をクリックします。
m. （自動仮想 I/O の割り当てのみ） **識別情報の属性** タブをクリックして、仮想 I/O ID を割り当てます。

メモ: FCoE WWPN 、 WWNN 、および仮想 FIP の属性で、属性の選択を解除する場合、他のすべての関連属性は自動的に選択解除されます。

メモ: Intel ネットワークアダプタでは、単一の iSCSI イニシエータ名が生成され、すべてのポートに展開されます。IQN ID を単一のポートに展開することはできません。デフォルトでは、IQN ID はすべてのポートに展開されます。

メモ: ステータス 列は、選択された仮想 I / O プールが、仮想 I / O 属性を含むか、十分な仮想 I/O を持っていない場合にエラー ステータスが表示されます。

1. **ID の割り当て** をクリックして、仮想 I/O の ID を仮想 I/O プールから割り当てます。
2. **結果** プロンプトで、**OK** をクリックします。**識別情報の割り当て** タブが表示されます。

n. （IOA に VLAN 設定を展開する場合のみ） **IOA の VLAN 属性** タブをクリックして、選択したテンプレートの IOA の VLAN 属性を編集します。
o. 導入する属性の **導入** チェックボックスを選択します。
p. タグ付き VLAN とタグなし VLAN の値を入力します。
q. **保存** をクリックします。
r. **次へ** をクリックします。

8. **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** 下に、管理者特権がある iDRAC の資格情報を入力します。
c. （IOA に VLAN 設定を導入する場合のみ） **IOA 資格情報** の下に、IOA の管理者権限のある資格情報を入力します。
d. **次へ** をクリックします。

9. **プレビュー** ページで、次の手順を実行します。
a. **プレビュー** をクリックして、デバイス設定テンプレートの属性がターゲットデバイスに無事に導入されたか確認します。

b. **次へ** をクリックします。

10. **概要** ページで入力した情報を確認してから、**終了** 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。
11. 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** 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。導入が正常に完了すると、テンプレート導入済みアイコン  およびテキスト **導入済み** がコンピュートプール内のデバイス名に表示されます。

メモ: FCoE プロトコルのステートレス導入では、WWNN の最初のオクテットが 20:00、WWPN の最初のオクテットが 20:01 になります。残りのオクテットは、仮想 FIP MAC アドレスと同じになります。

関連リンク

OpenManage Essentials — サーバ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
コンピュートプール
コンピュートプールの自動ロック機能

コンピュートプールの自動ロック機能

コンピュートプール内にある任意のサーバーの最初の正常な導入後、コンピュートプールは自動的にロックされます。コンピュートプールがロックされると、関連するデバイス設定テンプレートおよび仮想 I/O プールもロックされます。ロックアイコン  がユーザーインタフェースに表示され、リソースがロックされていることを示します。コンピュートプールをロックすることにより、プール内のすべてのサーバーが同じデバイス設定テンプレートと仮想 I/O プールを使用することを確実にすることができます。次の操作は、ロックされたコンピュートプールのみで実行することができます。

- コンピュートプールの定義の表示
- コンピュートプールへのサーバの追加または削除
- コンピュートプールのメンバーであるサーバーの導入

メモ: 他の目的でロックされているデバイス設定テンプレートを使用する場合、そのデバイス設定テンプレートのクローンを作成し、使用することができます。

コンピュートプールのロック解除

コンピュートプールを導入およびロックした後で更新する場合、コンピュートプールのロックを解除できます。たとえば、コンピュートプールのロック解除後、デバイス設定テンプレートを編集し、その後コンピュートプール内のサーバーを再導入できます。
コンピュートプールのロックを解除するには、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. 左側のペインの **コンピュートプール** で、ロックを解除するコンピュートプールを右クリックし、その後 **ロック解除** をクリックします。
3. 確認のプロンプトで **はい** をクリックします。

コンピュートプールはロック解除されますが、コンピュートプール内にあるすでに導入されたサーバーは導入された状態のままになります。コンピュートプールをロック解除すると、関連するデバイス設定テンプレートおよび仮想 I/O プールもロック解除されます。

関連リンク

コンピュートプール
コンピュートプールの自動ロック機能

コンピュートプールの定義の編集

編集可能なコンピュートプールの定義は、コンピュートプールがロックされているかロック解除されているかによります。サーバーをコンピュートプールに導入すると、コンピュートプールは自動的にロックされます。ロックされたコンピュートプールでは、サーバーの導入および追加のみが可能です。

コンピュートプールの定義を編集するには、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. 左ペインの **コンピュートプール** でコンピュートプールを右クリックしてから **編集** をクリックします。
   コンピュートプールの作成ウィザード が表示されます。
3. 必要に応じて、ウィザードの適切なページの定義を変更します。
4. **サマリ** ページで情報を確認し、**終了** をクリックします。

コンピュートプールに行った変更が保存されます。

関連リンク

コンピュートプール
コンピュートプールの作成ウィザード

コンピュートプールの定義の表示

コンピュートプールの定義を表示するには、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. 左ペインの **コンピュートプール** でコンピュートプールを右クリックしてから、**表示** をクリックします。
   コンピュートプールの作成ウィザード が表示されます。
3. **次へ** をクリックすると、コンピュートプールのさまざまな定義が表示されます。

関連リンク

コンピュートプール
コンピュートプールの作成ウィザード

コンピュートプールからのサーバーの削除

要件に基づいてコンピュートプールからサーバーを削除することができます。たとえば、サーバーを別のコンピュートプールに移動する、または仮想 I/O ID なしでサーバーを導入するために、コンピュートプールからサーバーを削除することができます。
コンピュートプールからサーバーを削除するには、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. 左側のペインの **コンピュートプール** の下で、コンピュートプールから削除するサーバーを右クリックし、**プールから削除** をクリックします。
3. 確認のプロンプトで **はい** をクリックします。

サーバーがコンピュートプールから削除され、**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。

関連リンク

コンピュートプール

コンピュートプールの名前変更

コンピュートプールの名前を変更するには、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. 左ペインの**コンピュートプール**で、名前を変更するコンピュートプールを右クリックしてから **名前の変更** をクリックします。
   コンピュートプールの名前変更 ウィンドウが表示されます。
3. 新しい名前を入力して、**OK** をクリックします。

コンピュートプールの名前が変更されます。

関連リンク

コンピュートプール

コンピュートプールの削除

コンピュートプールを削除するには、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. 左ペインの **コンピュートプール**で、削除するコンピュートプールを右クリックしてから **削除** をクリックします。
3. **削除の確認** プロンプトで、**はい** をクリックします。

コンピュートプールは削除され、プールからすべてのサーバーが **再利用およびベアメタル** グループに戻されます。コンピュートプールに関連付けられている仮想 I/O のプールとデバイス設定テンプレートがロック解除されます。ただし、割り当てまたは導入された仮想 I/O ID はサーバーで保持されます。

メモ: コンピュートプールが削除されても、コンピュートプールに含まれていたサーバは導入された状態のままになります。

関連リンク

コンピュートプール

サーバーの交換

サーバーの交換タスクでは、本番サーバーを同じコンピュートプール内の別のサーバーにすばやく交換することができます。たとえば、故障しそうなサーバー、または故障したサーバーを別のスペアサーバーに素早く交換するためにサーバーの交換タスクを使用することができます。サーバーの交換タスクを実行すると、デバイス設定テンプレートの属性とソースサーバーの仮想 I/O ID がターゲットサーバーに移行されます。
サーバーの交換タスクを開始する前に、次を確認してください。

- コンピュートプールにサーバーが少なくとも 2 台含まれている（そのうちの一方、または両方が導入済み状態）。
- ソースサーバーが、同じコンピュートプールに導入されている。
- ターゲットサーバーがソースサーバーと同じコンピュートプール内にある。

サーバーを交換するには、次の手順を実行します。

注意: サーバーの交換タスクは、パフォーマンス、接続性、デバイスの起動機能、およびデータロスを含むデバイス設定に対して、破壊的な変更をもたらす可能性があります。

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、**サーバーの交換** をクリックします。
   - **コンピュートプール** ペインで、交換するサーバーを含むコンピュートプールを右クリックしてから、**サーバーの交換** をクリックします。

   サーバーの交換ウィザード ウィザードが表示されます。
3. **名前** ページで、タスクの適切な名前を入力し、**次へ** をクリックします。
4. **ソースとターゲット** ページで次の操作を実行します。

   メモ: ターゲットサーバーが表示されるのは、ソースサーバー選択後のみです。ターゲットの選択 セクションに表示されたサーバーには、すでに導入済み状態のサーバーも含まれます。

   a. **ソースの選択** で、ソースサーバーを選択します。
   b. **ターゲットの選択** で、ターゲットサーバーを選択します。
   c. **次へ** をクリックします。
5. **ソース属性の確認** ページで、テンプレートの属性、IOA VLAN 属性（該当する場合）、デバイス固有の属性、および仮想 I/O ID の割り当てを確認し、**次へ** をクリックします。
6. **オプション** ページでプリファランスに基づいて次のオプションのいずれかを選択します。
   - **コンピュートプールからソースを削除する** - サーバーを交換した後に、ソースサーバーをコンピュートプールから **再利用およびベアメタルデバイス** グループに移動する場合に選択します。

- **ソースから仮想 ID を回収できない場合でもターゲットに導入する** - ソースサーバーが到達不能の場合でも、ソースサーバーの仮想 I/O ID を回収する場合に選択します。

7. **次へ** をクリックします。
8. **資格情報** ページでは、ソースサーバーおよびターゲットサーバーの iDRAC ユーザー名とパスワードを適切なフィールドに入力してから、**次へ** をクリックします。
9. **サマリ** ページで選択した情報を確認してから、**終了** をクリックします。

   サーバーの交換 警告が表示されます。
10. 交換を続行するには、**はい** をクリックします。

サーバーの交換タスクが作成され、タスクがただちに実行されます。**タスク実行履歴** で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。導入が正常に完了した後、テンプレート導入済みアイコン と **導入済み** というテキストが、デバイス名と共にコンピュートプール内に表示されます。

メモ: サーバーが交換されると、デバイス設定テンプレート（作業負荷移動のデバイス固有の ID 属性を含む）の選択されているすべての属性が、ターゲットサーバーに導入されます。サーバーを交換した後、デバイス設定テンプレートを再導入しようとすると、デバイス固有の属性は、テンプレートの導入 ウィザードに自動的に入力されません。したがって、必要に応じて、テンプレートの導入 ウィザードの テンプレートの編集 ページでデバイス固有の属性を手入力する必要があります。

メモ: 交換サーバータスクが実行されると、デバイスコンプライアンス ポータルの円グラフに、ソースサーバーが 2 つのデバイスとして表示されます（1 つは、非準拠 または準拠、もう 1 つは 非インベントリ）。サーバー交換タスクが完了した後、円グラフに、ソースサーバーの正しいコンプライアンスステータスが表示されます。

サーバの導入済み仮想入出力（I/O）ID の回収

ID の回収タスクでは、導入済みのすべての仮想 I/O ID をサーバーから回収することができます。
ID の回収タスクを開始する前に、次を確認してください。

- サーバーがコンピュートプールから導入されている。
- OpenManage Essentials を使用して、サーバーに仮想 I/O ID が割り当てられている。

サーバーの導入済み仮想 I/O ID を回収するには、次の手順を実行します。

注意: ID の回収タスクは、サーバーの 1 つ、または複数のネットワーク設定に影響する可能性があり、サーバーとの接続が失われる場合があります。

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. 次のいずれかを実行します。

   - **一般タスク** ペインで、**ID の回収** をクリックします。
   - **コンピュートプール** ペインで、交換するサーバーを含むコンピュートプールを右クリックし、**ID の回収** をクリックします。
   - **仮想 I/O プール** ペインで、仮想 I/O プールをクリックします。右側のペインで、**ID を持つデバイス** タブをクリックします。デバイスを右クリックしてから、**導入済み仮想 ID の回収** をクリックします。

   ID の回収ウィザード ウィザードが表示されます。
3. **名前** ページで、タスクの適切な名前を入力し、**次へ** をクリックします。
4. **デバイスの選択** ページで **次へ** をクリックします。
5. **ID の割り当て** ページで仮想 I/O ID 属性を確認してから、**次へ** をクリックします。
6. **オプション** ページでプリファランスに基づいて次のオプションのいずれかを選択します。

   - **コンピュートプールからソースを削除する** - 仮想 I/O ID の回収後に、サーバーをコンピュートプールから **再利用およびベアメタルデバイス** グループに移動する場合に選択します。
   - **ターゲットに接続できない場合でも回収処置を強制する** - ソースサーバーが到達不能の場合でもサーバーの仮想 I/O ID を回収する場合に選択します。
7. **次へ** をクリックします。
8. **資格情報** ページで、該当するフィールドに iDRAC のユーザー名とパスワードを入力し、**次へ** をクリックします。

9. **サマリ** ページで選択した情報を確認してから、**終了** をクリックします。
   ID の回収 警告メッセージが表示されます。
10. サーバーの仮想 I/O ID の回収を続行する場合は、**はい** をクリックします。

ID の回収タスクが作成され、ただちに実行されます。**タスク実行履歴** 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。

割り当て済み仮想入出力（I/O）ID の回収

プリファランスに基づいて、デバイスから割り当てられた仮想 I/O ID を回収することもできます。
割り当て済み仮想 I/O ID を回収するには、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. 左側のペインの **仮想 I/O プール** で、仮想 I/O プールを選択します。
   右側のペインに、**仮想 I/O プールサマリ** ページが表示されます。
3. **仮想 I/O プールサマリ** ページで、**ID を持つデバイス** タブをクリックします。
   割り当て済みまたは導入済みの仮想 I/O ID を持つデバイスが、グリッドに表示されます。
4. グリッド上のデバイスを右クリックしてから、**割り当て済み ID の回収** をクリックします。
   割り当て済み ID の回収 警告メッセージが表示されます。
5. デバイスの割り当てられている仮想 I/O ID の回収を続行する場合は、**はい** をクリックします。

回収された仮想 I/O ID が仮想 I/O プールに戻されます。

デバイス設定自動導入のセットアップ - ステートレス導入

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と、デバイスの設定を確実に統一できます。
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 ファイルに含まれています。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「ServiceTag」、「Service Tag」、または「Node ID」に示されます。

  メモ: （PowerEdge FM120x4 などの）複数のコンピュートノードを持つデバイスでは、すべてのコンピュートノードは同じサービスタグを持ちます。したがって、使用する特定のコンピュートノードを識別するにはノード ID を使用する必要があります。.csv ファイルでは、自動導入する特定のコンピュートノードのノード 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。
- コンピュートプールはすでに作成しています。詳細については、「コンピュートプールの作成」を参照してください。
- 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* - サーバ設定管理ライセンスがすべてのターゲットサーバにインストールされます。詳細については、「OpenManage Essentials - サーバ設定管理ライセンス」を参照してください
- Mellanox HBA アダプタを装備したサーバー上で、インストールされているアダプタファームウェアのバージョンが 02.34.50.10 X08 またはそれ以降であることを確認します。
- IOA 設定の展開には、ブレードサーバからテンプレートを作成する必要があります。

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. **導入オプションの選択** ページで、次の手順を実行します。
   a. **ターゲットの導入** の下にある **コンピュートプールの選択** リストから、コンピュートプールを選択します。
   b. **導入オプションの選択** で、**テンプレートの導入** 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、設定テンプレートを選択し、**次へ** をクリックします。

   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。
5. **仮想 I/O プールの選択** ページで次のいずれかを実行して、**次へ**をクリックします。

   - デバイスに I/O の識別情報を提供するためにテンプレートの属性を編集する場合は、**ユーザー定義の I/O 割り当て** を選択します。
   - **I/O の自動割り当て** を選択して仮想 I/O プールをリストから選択すると、OpenManage Essentials で仮想 I/O ID を自動的にデバイスに割り当てることができます。
6. **仮想 I/O プールの選択** ページで、次を実行します。
7. **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。

      インポートサマリ 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。
8. **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、すべてのパスワード属性を導入前に設定テンプレート内で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. 変更を加えた場合は、**保存** をクリックします。
   f. **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。
   g. 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。
   h. 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。
   i. 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。

      メモ: デバイス固有属性 は、特定のデバイス、またはすべてのデバイス用に .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。
   j. **ID 属性** タブをクリックして、仮想 I/O 属性を確認します。
   k. 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。
   l. 変更を加えた場合は、**保存** をクリックします。
   m. (IOA に VLAN 設定を導入する場合のみ) **IOA の VLAN 属性** タブをクリックして、ターゲットデバイスに対して固有である IOA の VLAN 属性を編集します。

n. 導入する属性の **導入** チェックボックスを選択します。
o. タグ付き VLAN とタグなし VLAN の値を入力します。
p. **保存** をクリックします。
q. **次へ** をクリックします。

9. **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。

      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. （IOA に VLAN 設定を導入する場合のみ）**IOA 資格情報** の下に、IOA の管理者権限のある資格情報を入力します。
   g. **次へ** をクリックします。
10. **概要** ページで入力した情報を確認してから、**終了** 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。
11. **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。

OpenManage Essentials でデバイスの検出とインベントリの作成が行われるまで、サービスタグまたはノード ID が **自動導入** タブに表示されます。**未検出デバイスへの設定の導入** タスクを定期的に実行し、OpenManage Essentials でデバイスが検出され、インベントリが作成されているかどうかを検証します

メモ: 未検出デバイスへの設定の導入 は、設定 → 導入の設定 で設定された頻度に基づいて実行されます。

デバイスの検出およびインベントリ作成が完了し、導入タスクが作成された後、デバイスは適切なコンピュートプールに移動されます。**タスク実行履歴** 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。導入が正常に完了すると、テンプレート導入済みアイコン  およびテキスト **導入済み** がコンピュートプール内のデバイス名に表示されます。

関連リンク

OpenManage Essentials — サーバ設定管理ライセンス

プロファイルの表示 - 最後に導入された属性

デバイスのプロファイルには、デバイス固有の属性や仮想 I/O ID 属性を含む、デバイス設定テンプレートの最後に導入された属性のリストが含まれています。
最後に導入された属性を表示するには、次の手順を実行します。

次のいずれかを実行します。

- **デバイス** ポータルで、デバイスツリーから導入済みのデバイスを選択します。右ペインで、**設定** → **プロファイル** の順にクリックします。
- **導入** ポータルで、**コンピュートプール** セクションから導入済みデバイスを選択します。右ペインで、**プロファイル** をクリックします。

最後に導入された属性が、**テンプレート属性**、**デバイス固有属性**、および **仮想 ID** タブ内に表示されます。

メモ: プロファイル タブには、導入のためのデバイス設定テンプレートで選択した属性のみが表示されます。

ステートレスな導入の既知の制限事項

以下は、ターゲットサーバーへの仮想 I/O の導入に関する制限事項です。

- Broadcom ネットワークアダプタでは、OpenManage Essentials は、仮想 I/O ID と共に SAN へオペレーティングシステムをインストールするために、ISO からブートをサポートしません。ただし、オペレーティングシステムが、すでに SAN 上にインストールされている場合は、仮想 I/O ID の導入後、サーバーは SAN から起動することができます。
- PowerEdge FC430、FC630 および FC830 スレッドの場合、PowerEdge FX2s シャーシの共有 PCIe スロット内の PCIe カード（FC および iSCSI）では、ステートレスな導入がサポートされます。ただし、PCIe カードがマッピングされている場合は、別のシャーシ内で同じ PCIe のマッピングを持つ同じスロット内の完全に同種のスレッドとのみ交換できます。PCIe カードがマッピングされていない場合は、同種のどのスレッドとも交換できます。

- ブレードサーバー上でステートレスな導入を実行する場合、ホストシャーシが I/O ID 属性を割り当てないよう、ブレードサーバー上の FlexAddress モードを無効にする必要があります。FlexAddress モードが有効になっている場合でも、OpenManage Essentials が FlexAddress モードよりも優先されます。
- QLogic 統合型ネットワークアダプタで、サーバー上にステートレスな導入を実行する間、OpenManage Essentials は、仮想 MAC（vMAC）と仮想 FIP（vfip）MAC 属性の異なる複数の属性値を生成します。ただし、vMAC 属性の値のみが vMAC および vFIP MAC 属性の両方に導入されます。展開する前に SAN 起動のゾーンを作成する場合、ゾーンが 仮想 WWPN（ vWWPN）および仮想 WWNN（vWWNN）を生成しながら、vMAC アドレスに基づいてを生成することを確認して ください 。たとえば、20:00:vWWNN の vMAC と 20:01:vWWPN の vMAC です。
- Intel NIC カードは、各ポートに固有の iSCSI イニシエータ名をサポートしません。OpenManage Essentials は、Intel NIC カード内のすべてのポートに同じ IQN 値を導入します。

補足情報

delltechcenter.com で取得できる次の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

ベアメタルおよびステートレス導入に関する詳細な情報を、**delltechcenter.com/OME** で取得できるサーバ導入のテクニカルホワイトペーパーの OpenManage Essentials を使用して検索することもできます。

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。
- 共通タスク — 導入セットアップタスク、および作成可能なタスクが表示されます。
  - テンプレートの作成
  - 仮想 I/O プールの作成
  - コンピュートプールの作成
  - 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
  - サーバーの交換
  - ID の回収
- 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 - FX2 シャーシ
    - 例 - VRTX シャーシ
    - 例 - M1000e シャーシ
  - IOA テンプレート
- コンピュートプール — **再利用およびベアメタル** グループと作成したコンピュートプールに追加したデバイスが表示されます。
- 仮想 I/O プール — 作成した仮想 I/O プールが表示されます。
- 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
    - IOA 設定の事前チェック — IOA 用に作成したデバイス設定事前チェックタスクを表示します。
    - IOA 設定展開 — IOA 用に作成したデバイス設定展開タスクを表示します。
    - IOA 設定インポート — IOA 用に作成した **テンプレートの作成** タスクを表示します。
    - サーバーの交換 - 交換されたサーバーの履歴を表示します。
    - ID の回収 - 回収された仮想 I/O ID の履歴を表示します。
    - デバイス設定プレビュー — デバイス設定導入履歴のプレビューが表示されます。
    - 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。

アイコンと説明

表 61. アイコンと説明

アイコン	説明
	読み取り専用デバイス設定テンプレートです。読み取り専用テンプレートは、導入または設定コンプライアンスタスク用に使用する前にクローンする必要があります。
	作成、インポート、またはクローンされたデバイスの設定テンプレートです。
	デバイス設定テンプレートのターゲットデバイスへの導入が正常に行われました。
	仮想 I/O プールです。
	コンピュートプールです。
	ロックされているリソースです。

アイコン	説明
	読み取り専用ですが、導入可能なデバイス設定テンプレートです。

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
- IOA VLAN 属性
- デバイス構成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
- テンプレートウィザードの導入
- 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** グループとユーザーが作成したコンピュートプールに追加されたデバイスが表示されます。また、このタブには、最後の導入の結果とデバイスに購入した最後のテンプレートも表示されます。

メモ: 再利用およびベアメタルデバイス タブには、コンピュートプールに含まれないデバイスのみが表示されます。

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。

表 62. 再利用およびベアメタルデバイス

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。
Device Name (デバイス名)	デバイス名を表示します。
Service Tag	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。

表 63. 自動導入

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。
コンピュートプール	デバイスが属しているコンピュートプールの名前が表示されます。
仮想 IO プール	デバイスが属している仮想 IO プールの名前が表示されます。
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。
IOA への VLAN の設定	IOA に VLAN を設定することを選択した場合に表示されます。
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。
Created By（作成者）	タスクを作成したユーザーの名前を表示します。
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 - ベアメタル導入

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。

表 64. タスク

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。
タイプ	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。
更新日	タスクが更新された日付と時刻が表示されます。
Updated By（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。
Created By（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。

表 65. タスクの実行履歴

フィールド	説明
ステータス	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。 • Running（実行中） • Complete（完了） • Stopped（停止） • Failed（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。

表 66. デバイス設定テンプレートの詳細

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。
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を表示します。
属性名	属性の名前を表示します。

フィールド	説明
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

デバイス導入テンプレート属性の表示

IOA VLAN 属性

導入ポータル の **IOA VLAN 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。

表 67. IOA VLAN 属性

フィールド	説明
元に戻す	IOA テンプレートに加えられた変更を元に戻す場合にクリックします。
保存	IOA テンプレートに加えられた変更を保存する場合にクリックします。
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値が導入されず、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	変更された属性がある場合に表示されます。
NIC	NIC の完全修飾デバイス記述子（FQDD）を表示します。
ファブリック	シャーシの特定のスロットに関連付けられたファブリックが表示されます。ファブリックは、グループ名（A、B、または C）およびスロット番号（1 または 2）の組み合わせで識別されます。
Tagged VLAN(s)（タグ付き VLAN）	タグ付き VLAN の値を入力するフィールド。
Untagged VLAN（タグなし VLAN）	タグなし VLAN の値を入力するフィールド。

デバイス構成セットアップウィザード

デバイス構成セットアップウィザード の指示に従って、構成導入とコンプライアンスタスクを開始できます。

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。

表 68. ファイル共有の設定

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。
Password（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: 再利用とベアメタルデバイスグループ へのデバイスの追加は、デバイス構成導入タスクにのみ該当します。

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。

表 69. テンプレートの作成ウィザード

フィールド	説明
Name（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。
Device Type（デバイスタイプ）	設定テンプレートを作成する元のデバイスに基づいて、**サーバー**、**シャーシ** または **IOA** 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	
User Name（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。
Password（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導入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導入テンプレートの作成

仮想入出力（I/O）プールの作成ウィザード

仮想 I/O プールの作成ウィザード は、1 つ、または複数の仮想 I/O ID タイプのプールを作成するためのガイドを提供します。OpenManage Essentials は、サーバのネットワークインタフェースに対し、固有の ID を割り当てるためにプールから仮想 IO ID を利用します。ウィザードのさまざまなページに表示されるフィールドについては、次のセクションで説明します。

メモ: 仮想 I/O プールの作成は、サーバのネットワークインタフェースの仮想 ID を自動的に割り当てて管理するための前提条件です。

関連リンク

名前と説明
Ethernet の識別情報
FCoE ノード名の識別情報
FCoE ポート名の識別情報
iSCSI IQN の識別情報
Summary（サマリ）

名前と説明

名前と説明 ページでは、タスクの名前と説明を指定します。

仮想 I/O プールの作成ウィザード の **名前と説明** ページに表示されるフィールドを、次の表で説明します。

表 70. 名前と説明

フィールド	説明
Name（名前）	仮想 I/O プール の名前を入力します。
説明（オプション）	仮想 I/O プール の説明を入力します。

関連リンク

仮想入出力（I/O）プールの作成ウィザード

Ethernet の識別情報

Ethernet ID ページでは、メディアアクセスコントロール（MAC）アドレスを仮想 I/O プールに生成またはインポートできます。MAC address は Ethernet（LAN）通信に必要です。

仮想 I/O プールの作成ウィザード の **Ethernet 識別情報** ページに表示されるフィールドを、次の表で説明します。

表 71. Ethernet の識別情報

フィールド	説明
MAC アドレスをこのプールに含める	MAC アドレスを仮想 I/O プールに含める場合に選択します。
開始アドレスを指定します	生成する MAC アドレスの開始アドレスを選択します。
ID の数	生成する MAC アドレスで事前定義する ID の数を設定します。
ファイルからインポートする	.csv ファイルから MAC アドレスをインポートする場合に選択します。
インポート	クリックすると、.csv ファイルから MAC アドレスをインポートするのに使用するウィザードが開きます。 **メモ: .csv の 1 行には、1 つのアドレスまたは識別情報のみを含めることができます。**
表示	クリックすると、仮想 I/O プールに MAC アドレスが表示されます。 **メモ: .csv ファイルからインポートした MAC アドレスのみを表示できます。**

関連リンク

仮想入出力（I/O）プールの作成ウィザード

FCoE ノード名の識別情報

FCoE ノード名 ID ページでは、ワールドワイドノード名（WWNN）ID の生成、または WWNN ID の仮想 I/O プールへのインポートが可能です。WWNN ID は Fibre Channel（FC）および Fibre Channel over Ethernet（FCoE）通信に必要です。

仮想 I/O プールの作成ウィザード の **FCoE ノード名の識別情報** ページに表示されるフィールドを、次の表で説明します。

表 72. FCoE ノード名の識別情報

フィールド	説明
ファイバチャネル WWNN の識別情報をプールに含める	WWNN の識別情報を仮想 I/O プールに含める場合に選択します。
開始アドレスを指定します	生成する WWNN の識別情報の開始アドレスを選択します。
ID の数	生成する WWNN の識別情報で事前定義する ID の数を設定します。
ファイルからインポートする	.csv ファイルから WWNN の識別情報をインポートする場合に選択します。
インポート	クリックすると、.csv ファイルから WWNN の識別情報をインポートするのに使用するウィザードが開きます。 **メモ: .csv の 1 行には、1 つのアドレスまたは識別情報のみを含めることができます。**
表示	クリックすると、仮想 I/O プールに WWNN の識別情報が表示されます。 **メモ: .csv ファイルからインポートした WWNN の識別情報のみを表示できます。**

関連リンク

仮想入出力（I/O）プールの作成ウィザード

FCoE ポート名の識別情報

FCoE ポート名 ID ページでは、ワールドワイドポート名（WWPN）ID の生成、または WWPN ID の仮想 I/O プールへのインポートが可能です。WWPN ID は Fibre Channel（FC）および Fibre Channel over Ethernet（FCoE）通信に必要です。

仮想 I/O プールの作成ウィザード の **FCoE ポート名の識別情報** ページに表示されるフィールドを、次の表で説明します。

表 73. FCoE ポート名の識別情報

フィールド	説明
ファイバチャネル WWPN の識別情報をプールに含める	WWPN の識別情報を仮想 I/O プールに含める場合に選択します。
開始アドレスを指定します	生成する WWPN の識別情報の開始アドレスを選択します。
ID の数	生成する WWPN の識別情報で事前定義する ID の数を設定します。
ファイルからインポートする	.csv ファイルから WWPN の識別情報をインポートする場合に選択します。
インポート	クリックすると、.csv ファイルから WWPN の識別情報をインポートするのに使用するウィザードが開きます。 **メモ: .csv の 1 行には、1 つのアドレスまたは識別情報のみを含めることができます。**
表示	クリックすると、仮想 I/O プールに WWPN の識別情報が表示されます。 **メモ: .csv ファイルからインポートした WWPN の識別情報のみを表示できます。**

関連リンク

仮想入出力（I/O）プールの作成ウィザード

iSCSI IQN の識別情報

iSCSI IQN の識別情報 ページでは、iSCSI 修飾名（IQN）を仮想 I/O プールに生成またはインポートできます。IQN の識別情報は iSCSI プロトコルを使用して SAN からの起動をサポートするのに必要です。

仮想 I/O プールの作成ウィザード の **iSCSI IQN の識別情報** ページに表示されるフィールドを、次の表で説明します。

表 74. iSCSI IQN の識別情報

フィールド	説明
IQN の識別情報をプールに含める	IQN の識別情報を仮想 I/O プールに含める場合に選択します。
割り当てる接頭辞を指定する	生成する IQN の識別情報の接頭辞を選択します。 **メモ: 一般的な iSCSI IQN フォーマットは *iqn.date.domainname-in-reverse:storage-identifier* です（例：iqn.2001-04.com.example:storage.disk2.sys1.xyz）。**
ファイルからインポートする	.csv ファイルから IQN の識別情報をインポートする場合に選択します。
インポート	クリックすると、.csv ファイルから IQN の識別情報をインポートするのに使用するウィザードが開きます。 **メモ: .csv の 1 行には、1 つのアドレスまたは識別情報のみを含めることができます。**
表示	クリックすると、仮想 I/O プールに IQN の識別情報が表示されます。 **メモ: .csv ファイルからインポートした IQN の識別情報のみを表示できます。**

関連リンク

仮想入出力（I/O）プールの作成ウィザード

Summary（サマリ）

サマリ ページには、仮想 I/O プール作成タスクのために入力した定義が表示されます。

サマリ ページに表示されるフィールドを、次の表で説明します。

表 75. 概要

フィールド	説明
Name（名前）	タスク名を表示します。
Ethernet の定義	MAC address の定義が表示されます。
Ethernet ID の数	Ethernet ID の仮想 I/O プールサイズを表示します。
FCoE WWNN の定義	WWNN ID の定義が表示されます。
FCOE WWNN ID の数	WWNN ID の仮想 I/O プールサイズを表示します。
FCoE の WWPN の定義	WWPN ID の定義が表示されます。
FCOE WWPN ID の数	WWPN ID の仮想 I/O プールサイズを表示します。
QoS の定義	iSCSI イニシエータの IQN の定義が表示されます。

フィールド	説明
iSCSI IQN ID の数	iSCSI IQN ID の仮想 I/O プールサイズを表示します。 **メモ: iSCSI IQN ID の数 は、iSCSI IQN ID が .csv ファイルからインポートされたときにのみ表示されます。**

関連リンク

仮想入出力（I/O）プールの作成ウィザード

仮想入出力（I/O）プール

仮想 I/O プール ページには、作成したすべての仮想 I/O プールの詳細が表示されます。

仮想 I/O プール ページに表示されるフィールドを、次の表で説明します。

表 76. 仮想 I/O プール

フィールド	説明
グループ化基準	仮想 I/O プールの詳細表示に選択したグループが表示されます。
ロックがかかった状態	仮想 I/O プールがロックされているかどうかが表示されます。
Name（名前）	仮想 I/O プールの名前が表示されます。
ID の数	仮想 I/O プールの ID の合計数を表示します。
使用中の識別情報の合計	ターゲットデバイスに割り当てられたか導入された仮想 I/O ID の合計数が表示されます。

仮想入出力（I/O）プールの概要

仮想 I/O プールの概要 ページには、選択した仮想 I/O プールの詳細が表示されます。

仮想 I/O プールの概要 ページに表示されるフィールドを、次の表で説明します。

概要

表 77. Summary（サマリ）

フィールド	説明
グループ化基準	仮想 I/O プールの詳細表示に選択したグループが表示されます。
識別情報タイプ	仮想 I/O プールに含まれている仮想 ID タイプが表示されます。
範囲情報	仮想 ID タイプに対して入力した定義が表示されます。
ID の数	仮想 I/O プールの ID の合計数を表示します。
使用中の識別情報の合計	ターゲットデバイスに割り当てられたか導入された仮想 I/O ID の合計数が表示されます。

ID を持つデバイス

表 78. ID を持つデバイス

フィールド	説明
グループ化基準	デバイスの詳細の表示用に選択したグループが表示されます。
Device Name（デバイス名）	デバイスの名前を表示します。
サービスタグまたはノード ID	デバイスに割り当てられた固有の識別子が表示されます。
割り当てた識別情報の合計	デバイスに割り当てられた仮想 I/O ID の合計数が表示されます。
導入された識別情報の合計	デバイスに導入された仮想 I/O ID の合計数が表示されます。
使用中の識別情報の合計	デバイスに割り当てられた、または導入された仮想 I/O ID の合計数が表示されます。
デバイスは削除されていますか	デバイスが仮想 I/O ID と共に導入された後で OpenManage Essentials から削除されたかどうかを表示します。
テンプレート名	デバイスに割り当てられたテンプレートの名前が表示されます。
コンピュートプール	デバイスが属しているコンピュートプールの名前が表示されます。
前回の導入時刻	デバイスでの最後の導入のタイムスタンプが表示されます。
モデル	デバイスのモデル名を表示します（該当する場合）。例えば、PowerEdge R710 となります。

コンピュートプールの作成ウィザード

コンピュートプールの作成ウィザード に従って、特定の目的で使用するサーバのプールを作成します。ウィザードの様々なページに表示されるフィールドは、次のセクションで説明しています。

関連リンク

- 名前と説明
- テンプレートの選択
- ISO の場所の選択
- 仮想入出力（I/O）プールの選択
- デバイスの選択
- 属性の編集
- Summary（サマリ）

名前と説明

名前と説明 ページでは、タスクの名前と説明を指定します。

コンピュートプール作成ウィザード の **名前と説明** ページに表示されるフィールドを、次の表で説明します。

表 79. 名前と説明

フィールド	説明
Name（名前）	コンピュートプールの名前を入力します。
説明（オプション）	コンピュートプールの説明を入力します。

関連リンク

- コンピュートプールの作成ウィザード

テンプレートの選択

テンプレートの選択 ページでは、コンピュートプールに割り当て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はオプションです。テンプレートは、コンピュートプールの編集時、またはサーバーの導入時にも選択できます。

コンピュートプールの作成ウィザード の **テンプレートの選択** ページに表示されるフィールドを、次の表で説明します。

表 80. テンプレートの選択

フィールド	説明
コンピュートプールのテンプレートを選択	コンピュートプールにテンプレートを割り当てる場合に選択します。
サーバーテンプレート	コンピュートプールに割り当てることのできるテンプレートのリストが表示されます。テンプレート名をクリックしてテンプレートを選択します。 **メモ: コンピュートプールに割り当てられていないテンプレートだけが表示されます。**

関連リンク

コンピュートプールの作成ウィザード

ISO の場所の選択

ISO の場所の選択 ページでは、起動可能なオペレーティングシステムの ISO ファイルの詳細を入力できます。

メモ: ISO ファイルの詳細は、仮想 I/O ID のないターゲットサーバーについてのみ入力できます。通常、仮想 I/O ID のあるサーバーは SAN から起動する必要があります。

コンピュートプールの作成ウィザード の **ISO の場所の選択** ページに表示されるフィールドを、次の表で説明します。

表 81. ISO の場所の選択

フィールド	説明
ネットワーク ISO からのコンピュートプールの起動	オペレーティングシステムの ISO ファイルから、コンピュートプールに含まれたデバイスで起動するために選択します。
ISO ファイル名	ISO ファイルの名前を指定します。
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。

関連リンク

コンピュートプールの作成ウィザード

仮想入出力（I/O）プールの選択

仮想 I/O プールの選択 ページでは、ターゲットサーバーでの仮想 I/O ID の割り当ての方法を選択することができます。

次の表で、**仮想 I/O プールの選択** ページに表示されるフィールドについて説明します。

表 82. 仮想 I/O プールの選択

フィールド	説明
ユーザー定義の I/O 割り当て	これを選択して、仮想 I/O ID を手動で割り当てます。
自動 I/O 割り当て	選択すると、OpenManage Essentials で、ターゲットサーバに自動的に仮想 I/O ID を割り当てることができます。仮想 I/O ID は、選択した仮想 I/O プールから割り当てられます。 **メモ: 仮想 I/O プールは仮想 I/O プールをすでに作成している場合のみ選択できます。**

関連リンク

コンピュートプールの作成ウィザード

デバイスの選択

デバイスの選択 ページでは、コンピュートプールに含めるサーバーを選択できます。

メモ: 再利用およびベアメタル グループに追加したサーバーのみを選択できます。

デバイスの選択 ページには、コンピュートプールに含めることのできるサーバーがツリー表示されます。コンピュートプールに含めるサーバーは 1 つ、または複数選択できます。

関連リンク

コンピュートプールの作成ウィザード

属性の編集

属性の編集 ページでは、選択したデバイス設定テンプレートの属性、デバイス固有の属性、および IOA の VLAN 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、コンピュートプールに対してテンプレートが選択または割り当てられている場合にのみ表示されます。

メモ: テンプレートの属性の編集はオプションです。テンプレートの属性は、コンピュートプールの編集時、またはサーバー導入時に編集することもできます。

テンプレート属性

テンプレート属性 タブに表示されるフィールドを、次の表で説明します。

表 83. テンプレート属性

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

フィールド	説明
	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を表示します。
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。
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。

IOA VLAN 属性

IOA の VLAN 属性 タブに表示されるフィールドを、次の表で説明します。

表 84. IOA VLAN 属性

フィールド	説明
テンプレート用 IOA の VLAN 属性	選択したテンプレートの名前を表示します。
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値が導入されず、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	変更された属性がある場合に表示されます。
NIC	NIC の完全修飾デバイス記述子（FQDD）を表示します。
ファブリック	シャーシの特定のスロットに関連付けられたファブリックが表示されます。ファブリックは、グループ名（A、B、または C）およびスロット番号（1 または 2）の組み合わせで識別されます。
Tagged VLAN(s)（タグ付き VLAN）	選択したファブリックのタグ付き VLAN のリストを表示します。
Untagged VLAN（タグなし VLAN）	選択したファブリックのタグなし VLAN が表示されます。
元に戻す	選択したテンプレートの IOA VLAN 属性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	選択したテンプレートの IOA VLAN 属性に加えられた変更を保存する場合はクリックします。

デバイス固有属性

デバイス固有属性 タブに表示されるフィールドを、次の表で説明します。

表 85. テンプレート属性

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を表示します。
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。
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。

デバイス固有属性のインポート/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 ウィンドウに表示されるフィールドを、次の表で説明します。

表 86. デバイス固有属性のインポート/エクスポート

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、選択したすべて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。

フィールド	説明
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。

識別情報の属性

識別情報の属性 タブに表示されるフィールドを、次の表で説明します。

表 87. 識別情報の属性

フィールド	説明
テンプレートの属性	選択したデバイス設定テンプレートが表示されます。
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。デフォルトでは、属性は **セクション** ごとにグループ化されます。
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値が導入されず、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。
識別情報の影響	識別情報の属性が自動生成されるかどうかが表示されます。
ステータス	D 属性の生成のステータスが表示されます。選択された仮想 I/O プールが仮想 I/O 属性を含んでいない、または十分な属性がない場合、**エラー** ステータスが表示されます。
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を表示します。
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	属性が属する論理グループが表示されます。
識別情報を割り当てる	ターゲットデバイスに仮想 I/O ID を自動的に割り当てる場合にクリックします。
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。
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。

識別情報の割り当て

識別情報の割り当て タブに表示されるフィールドを、次の表で説明します。

メモ: 識別情報の割り当て タブは、識別情報の属性 タブの 識別情報を割り当てる をクリックした場合のみ表示されます。

表 88. 識別情報の割り当て

フィールド	説明
Device	選択したデバイス設定テンプレートが表示されます。
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を表示します。
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。

関連リンク

コンピュートプールの作成ウィザード

Summary (サマリ)

サマリ ページには、コンピュートプールを作成するために入力した情報が表示されます。

サマリ ページに表示されるフィールドを、次の表で説明します。

表 89. Summary (サマリ)

フィールド	説明
Name (名前)	タスク名を表示します。
選択したテンプレート	選択したテンプレートの名前が表示されます。
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。
識別情報の割り当て	選択した I/O 識別情報の割り当てのタイプが表示されます。
関連するデバイス	コンピュートプールに含める対象として選択したデバイスが表示されます。
デバイス固有属性	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。
IOA への VLAN の設定	IOA に VLAN を設定することを選択した場合に表示されます。

関連リンク

コンピュートプールの作成ウィザード

コンピュートプールの概要

コンピュートプールの概要 ページに表示されるフィールドを、次の表で説明します。

表 90. コンピュートプールの概要

フィールド	説明
グループ化基準	コンピュートプールの詳細表示に選択したグループが表示されます。
ロックがかかった状態	コンピュートプールがロックされているか表示されます。

フィールド	説明
プール名	コンピュートプールの名前が表示されます。
サーバーテンプレート	コンピュートプールに割り当てられたテンプレートの名前が表示されます。
仮想 I/O プール	コンピュートプールに割り当てられた仮想 I/O プールの名前が表示されます。
サーバーの合計	コンピュートプールのサーバー数の合計が表示されます。
導入されたサーバー	コンピュートプールに導入されたサーバー数が表示されます。

コンピュートプール詳細

コンピュートプールの詳細 ページに表示されるフィールドを、次の表で説明します。

表 91. コンピュートプール詳細

フィールド	説明
テンプレート	コンピュートプールに割り当てられたテンプレート名が表示されます。テンプレートの属性を表示するには、テンプレート名をクリックします。
仮想 I/O プール	コンピュートプールに割り当てられた仮想 I/O プールの名前が表示されます。
ネットワーク ISO イメージ	コンピュートプールに割り当てられたネットワーク ISO ファイルの名前が表示されます。
デバイス数	コンピュートプールのサーバー数の合計が表示されます。
導入数	コンピュートプールに導入されたサーバー数が表示されます。
グループ化基準	コンピュートプールの詳細表示に選択したグループが表示されます。
Device	サーバーの名前を表示します。
展開済み	サーバーを導入しているかどうかが表示されます。
前回の導入時刻	サーバーで最後に導入されたときのタイムスタンプが表示されます。

サーバー詳細

次の表で、サーバーの **詳細** ページに表示されるフィールドについて説明します。

表 92. サーバー詳細

フィールド	説明
サーバーテンプレート	サーバーに割り当てられたテンプレートの名前を表示します。
仮想 I/O プール	サーバーに割り当てられた仮想 I/O プールの名前を表示します。
インベントリ	サーバーの設定属性のインベントリを表示します。
プロファイル	サーバーに最後に導入されたテンプレートの属性、デバイス固有の属性、および仮想 I/O ID 属性を表示します。

テンプレートウィザードの導入

テンプレートウィザードの導入 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
- オプション
- スケジュールの設定
- プレビュー
- Summary（サマリ）

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。

表 93. 名前および導入オプション

フィールド	説明
タスク名	タスクの名前を入力します。
ターゲットの導入	
コンピュートプール	コンピュートプール内の 1 台または複数のデバイスにデバイス設定テンプレートを導入する場合に選択します。
コンピュートプール を選択します。	デバイス設定テンプレートを導入するコンピュートプールを選択します。
ベアメタル	これを選択して、**再利用およびベアメタル** グループ内の 1 台、または複数のデバイスにデバイス設定テンプレートを導入します。
導入オプションの選択	
テンプレートの導入	これを選択して、1 台、または複数のデバイスに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	これを選択して、指定されたネットワーク ISO イメージから各ターゲットデバイスを起動します。 **メモ: テンプレートの導入 オプションも選択されている場合、boot-to-ISO 操作は導入完了後に開始されます。**

関連リンク

- テンプレートウィザードの導入

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 導入オプションの選択 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。

表 94. テンプレートの選択

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 導入オプションの選択 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。
IOA テンプレート **メモ: 名前と導入のオプションページでコンピュートプールを選択した場合、IOA テンプレートオプションは表示されません。** **メモ: 名前と導入の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 で起動の両方を選択した場合は、IOA テンプレートオプションは無効になっています。**	作成またはクローンした IOA 設定テンプレートを表示します。

関連リンク

テンプレートウィザードの導入

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

テンプレートウィザードの導入

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 導入オプションの選択 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。

表 95. ISO の場所の選択

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。

フィールド	説明
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

テンプレートウィザードの導入

仮想入出力（I/O）プールの選択

仮想 I/O プールの選択 ページでは、ターゲットサーバーでの仮想 I/O ID の割り当ての方法を選択することができます。

次の表で、**仮想 I/O プールの選択** ページに表示されるフィールドについて説明します。

表 96. 仮想 I/O プールの選択

フィールド	説明
ユーザー定義の I/O 割り当て	これを選択して、仮想 I/O ID を手動で割り当てます。
自動 I/O 割り当て	選択すると、OpenManage Essentials で、ターゲットサーバに自動的に仮想 I/O ID を割り当てることができます。仮想 I/O ID は、選択した仮想 I/O プールから割り当てられます。 **メモ: 仮想 I/O プールは仮想 I/O プールをすでに作成している場合のみ選択できます。**

関連リンク

コンピュートプールの作成ウィザード

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、デバイス固有の属性、および IOA の VLAN 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

メモ: 導入の際に IOA テンプレートを選択した場合は、テンプレート属性タブは表示されません。

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。

表 97. テンプレート属性

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

フィールド	説明
	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を表示します。
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。
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。

IOA VLAN 属性

IOA の VLAN 属性 タブに表示されるフィールドを、次の表で説明します。

表 98. IOA VLAN 属性

フィールド	説明
テンプレート用 IOA の VLAN 属性	選択したテンプレートの名前を表示します。
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値が導入されず、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	変更された属性がある場合に表示されます。
NIC	NIC の完全修飾デバイス記述子（FQDD）を表示します。
ファブリック	シャーシの特定のスロットに関連付けられたファブリックが表示されます。ファブリックは、グループ名（A、B、または C）およびスロット番号（1 または 2）の組み合わせで識別されます。
Tagged VLAN(s)（タグ付き VLAN）	選択したファブリックのタグ付き VLAN のリストを表示します。
Untagged VLAN（タグなし VLAN）	選択したファブリックのタグなし VLAN が表示されます。
元に戻す	選択したテンプレートの IOA VLAN 属性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	選択したテンプレートの IOA VLAN 属性に加えられた変更を保存する場合はクリックします。

デバイス固有属性

デバイス固有属性 タブに表示されるフィールドを、次の表で説明します。

表 99. デバイス固有属性

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が表示されます。
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値が導入されず、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を表示します。
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。
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。
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。

デバイス固有属性のインポート/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 ウィンドウに表示されるフィールドを、次の表で説明します。

表 100. デバイス固有属性のインポート/エクスポート

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、選択したすべて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。

フィールド	説明
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。

識別情報の属性

識別情報の属性 タブに表示されるフィールドを、次の表で説明します。

表 101. 識別情報の属性

フィールド	説明
テンプレートの属性	選択したデバイス設定テンプレートが表示されます。
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。デフォルトでは、属性は **セクション** ごとにグループ化されます。
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値が導入されず、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。
識別情報の影響	識別情報の属性が自動生成されるかどうかが表示されます。
ステータス	D 属性の生成のステータスが表示されます。選択された仮想 I/O プールが仮想 I/O 属性を含んでいない、または十分な属性がない場合、**エラー** ステータスが表示されます。
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を表示します。
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	属性が属する論理グループが表示されます。
識別情報を割り当てる	ターゲットデバイスに仮想 I/O ID を自動的に割り当てる場合にクリックします。
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。
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。

識別情報の割り当て

識別情報の割り当て タブに表示されるフィールドを、次の表で説明します。

メモ: 識別情報の割り当て タブは、識別情報の属性 タブの 識別情報を割り当てる をクリックした場合のみ表示されます。

表 102. 識別情報の割り当て

フィールド	説明
Device	選択したデバイス設定テンプレートが表示されます。
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を表示します。
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。

関連リンク

テンプレートウィザードの導入
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

オプション

オプション ページでは、IOA テンプレートがターゲットデバイスと互換性があるかどうかを確認するために使用できるオプションを選択できます。

メモ: オプションページは、テンプレートの選択ページで IOA テンプレートを選択した場合にのみ表示されます。

テンプレートウィザードの導入 の **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。

表 103. オプション

フィールド	説明
事前チェックのみを実行	**事前チェックのみ実行**を選択し、デバイス設定テンプレートが正常に導入される状態であることの確認だけを行います（導入はしません）。 **メモ: 事前チェックのみを実行 オプションが選択されている場合、デフォルトで 警告時に続行 オプションが無効になっています。**
警告時に続行	テンプレートがターゲットデバイスで使用できない場合もテンプレートの導入を続行するには、**警告時に続行** を選択します。 **メモ: このオプションが選択されたときは、警告が出た場合はその警告は無視され、デバイス設定テンプレートに互換性がない場合でも展開タスクが続行されます。**

関連リンク

テンプレートウィザードの導入

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。

表 104. スケジュールの設定

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	
User Name（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。
Password（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。
IOA 資格情報	**メモ: IOA 資格情報 フィールドは、次のようなシナリオでのみ表示されます。** • 選択したデバイス設定テンプレートはブレードサーバから作成されました。 • IOA に VLAN 属性の導入を選択しています。
User Name（ユーザー名）	VLAN 属性を導入するために必要な IOA の管理者ユーザ名を指定します。
Password（パスワード）	VLAN 属性を導入するために必要な IOA の管理者パスワードを指定します。

関連リンク

テンプレートウィザードの導入

プレビュー

メモ: プレビューアクティビティはオプションです。

プレビュー ページを指定すると、ターゲットデバイスで正常に適用されていない選択された設定の属性を表示することができます。プレビューアクティビティは、各ターゲットデバイスに保留中の設定を送信しますが、あくまで検証専用です（設定は変更されません）。各デバイスは、設定内の設定の妥当性を検証し、問題を識別します。検証は、属性値そのものの問題、または属性間の依存関係に基づいた問題を識別することができます。たとえば、PowerEdge R 720 サーバーからデバイス設定テンプレートを作成し、PowerEdge R 620 サーバー上にテンプレートを導入すると、エラーになります。プレビューの実行によって、正常に導入されない属性を識別することができます。それらの属性（必要な場合）を識別した後、テンプレートからこれらの属性をオフにしてテンプレートを導入することができます。

メモ: プレビューアクティビティでは多くの問題が識別されますが、問題には実際に導入するまで判別することができないものもあります。

プレビュー ボタンをクリックして、選択したデバイスでのデバイス設定テンプレートの属性を検証します。

関連リンク

テンプレートウィザードの導入

Summary（サマリ）

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。

表 105. Summary（サマリ）

フィールド	説明
タスク名	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 からの起動	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。

フィールド	説明
ターゲットの導入	選択したターゲットデバイスが表示されます。
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。
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入力されたユーザー名を表示します。
識別情報の割り当て	選択した I/O 識別情報の割り当てのタイプが表示されます。
仮想 IO プール	デバイスが属している仮想 IO プールの名前が表示されます。
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。
IOA への VLAN の設定	IOA に VLAN 属性を導入することを選択した場合に表示されます。
事前チェックのみを実行	**事前チェックのみを実行** オプションを選択した場合に表示されます。
警告時に続行	**警告時に続行** オプションを選択した場合に表示されます。
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

テンプレートウィザードの導入

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

導入オプションの選択
テンプレートの選択
ISO の場所の選択
サービスタグまたはノード ID のインポート
属性の編集
実行の資格情報
Summary（サマリ）

導入オプションの選択

導入オプションの選択 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 **導入オプションの選択** ページに表示されるフィールドを次の表で説明します。

表 106. 導入オプションの選択

フィールド	説明
ターゲットの導入	
コンピュートプール	コンピュートプール内のサーバーを自動導入する場合に選択します。

フィールド	説明
コンピュートプール を選択します。	仮想 I/O ID を持つデバイス設定テンプレートを自動導入するコンピュートプールを選択します。
ベアメタル	ベアメタルサーバーにデバイス設定テンプレートを自動導入する場合に選択します。
導入オプションの選択	
テンプレートの導入	ターゲットサーバーにデバイス設定テンプレートを自動導入する場合に選択します。
ネットワーク ISO からの起動	ネットワーク ISO イメージからターゲットサーバーを起動する場合に選択します。

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 導入オプションの選択 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。

表 107. テンプレートの選択

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 導入オプションの選択 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。

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 導入オプションの選択 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。

表 108. ISO の場所の選択

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

テンプレートウィザードの導入

仮想入出力（I/O）プールの選択

仮想 I/O プールの選択 ページでは、ターゲットサーバーでの仮想 I/O ID の割り当ての方法を選択することができます。

次の表で、**仮想 I/O プールの選択** ページに表示されるフィールドについて説明します。

表 109. 仮想 I/O プールの選択

フィールド	説明
ユーザー定義の I/O 割り当て	これを選択して、仮想 I/O ID を手動で割り当てます。
自動 I/O 割り当て	選択すると、OpenManage Essentials で、ターゲットサーバに自動的に仮想 I/O ID を割り当てることができます。仮想 I/O ID は、選択した仮想 I/O プールから割り当てられます。 **メモ: 仮想 I/O プールは仮想 I/O プールをすでに作成している場合のみ選択できます。**

関連リンク

コンピュートプールの作成ウィザード

サービスタグまたはノード 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、後で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:（PowerEdge FM120x4 などの）複数のコンピュートノードを持つデバイスでは、すべてのコンピュートノードは同じサービスタグを持ちます。したがって、使用する特定のコンピュートノードを識別するにはノード ID を使用する必要があります。.csv ファイルでは、自動導入する特定のコンピュートノードのノード 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 27. 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、デバイス固有の属性、および IOA の VLAN 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

メモ: 導入の際に IOA テンプレートを選択した場合は、テンプレート属性タブは表示されません。

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。

表 110. テンプレート属性

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を表示します。
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。

フィールド	説明
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。
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。

IOA VLAN 属性

IOA の VLAN 属性 タブに表示されるフィールドを、次の表で説明します。

表 111. IOA VLAN 属性

フィールド	説明
テンプレート用 IOA の VLAN 属性	選択したテンプレートの名前を表示します。
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値が導入されず、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	変更された属性がある場合に表示されます。
NIC	NIC の完全修飾デバイス記述子（FQDD）を表示します。
ファブリック	シャーシの特定のスロットに関連付けられたファブリックが表示されます。ファブリックは、グループ名（A、B、または C）およびスロット番号（1 または 2）の組み合わせで識別されます。
Tagged VLAN(s)（タグ付き VLAN）	選択したファブリックのタグ付き VLAN のリストを表示します。
Untagged VLAN（タグなし VLAN）	選択したファブリックのタグなし VLAN が表示されます。
元に戻す	選択したテンプレートの IOA VLAN 属性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	選択したテンプレートの IOA VLAN 属性に加えられた変更を保存する場合はクリックします。

デバイス固有属性

デバイス固有属性 タブに表示されるフィールドを、次の表で説明します。

表 112. デバイス固有属性

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が表示されます。
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。

フィールド	説明
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値が導入されず、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を表示します。
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。
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。
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。

デバイス固有属性のインポート/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 ウィンドウに表示されるフィールドを、次の表で説明します。

表 113. デバイス固有属性のインポート/エクスポート

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、選択したすべて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。

識別情報の属性

識別情報の属性 タブに表示されるフィールドを、次の表で説明します。

表 114. 識別情報の属性

フィールド	説明
テンプレートの属性	選択したデバイス設定テンプレートが表示されます。
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。デフォルトでは、属性は **セクション** ごとにグループ化されます。
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値が導入されず、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。
識別情報の影響	識別情報の属性が自動生成されるかどうかが表示されます。
ステータス	D 属性の生成のステータスが表示されます。選択された仮想 I/O プールが仮想 I/O 属性を含んでいない、または十分な属性がない場合、**エラー** ステータスが表示されます。
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を表示します。
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	属性が属する論理グループが表示されます。
識別情報を割り当てる	ターゲットデバイスに仮想 I/O ID を自動的に割り当てる場合にクリックします。
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。
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。

識別情報の割り当て

識別情報の割り当て タブに表示されるフィールドを、次の表で説明します。

メモ: 識別情報の割り当て タブは、識別情報の属性 タブの 識別情報を割り当てる をクリックした場合のみ表示されます。

表 115. 識別情報の割り当て

フィールド	説明
Device	選択したデバイス設定テンプレートが表示されます。
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を表示します。
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。

関連リンク

テンプレートウィザードの導入
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。

表 116. 資格情報

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。
Username（ユーザー名）	ユーザー名を表示します。
Password（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。

表 117. デバイス

フィールド	説明
Device Name（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。

IOA 資格情報

メモ: IOA 資格情報 フィールドは、次のようなシナリオでのみ表示されます。

- 選択したデバイス設定テンプレートがモジュラーサーバから作成されています。
- IOA に VLAN 属性の導入を選択しています。

表 118. IOA 資格情報

フィールド	説明
User Name（ユーザー名）	VLAN 属性を導入するために必要な IOA の管理者ユーザ名を指定します。
Password（パスワード）	VLAN 属性を導入するために必要な IOA の管理者パスワードを指定します。

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。

表 119. 資格情報の追加

フィールド	説明
説明	資格情報の説明を入力します。
Username（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。
Password（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。
Default（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。

Summary（サマリ）

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。

表 120. Summary（サマリ）

フィールド	説明
Name（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 からの起動	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。
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。

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入力されたユーザー名を表示します。
関連付けられているサービスタグ / ノード ID	ターゲットデバイスのサービスタグまたはノード ID を表示します。
デバイス固有属性	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。
IOA への VLAN の設定	IOA に VLAN 属性を導入することを選択した場合に表示されます。

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。

表 121. 資格情報

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。
Username（ユーザー名）	ユーザー名を表示します。
Password（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。

表 122. デバイス

フィールド	説明
Device Name（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、デバイスで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

サーバーの交換ウィザード

サーバーウィザードの交換 では、本番サーバーを同じコンピュートプールの別のサーバーと交換する手順を示します。ウィザードのさまざまなページに表示されるフィールドについては、次のセクションで説明します。

関連リンク

- サーバーの交換
- 名前
- ソースとターゲット
- ソース属性の確認
- オプション
- 資格情報
- Summary（サマリ）

名前

名前 ページでは、タスクの名前を指定できます。

関連リンク

- サーバーの交換ウィザード

ソースとターゲット

ソースとターゲット ページでは、交換するソースサーバーとターゲットサーバーを選択できます。

次の表で、**サーバーの交換ウィザード** の **ソースとターゲット** ページに表示されるフィールドについて説明します。

表 123. ソースとターゲット

フィールド	説明
ソースの選択	すでに導入されているコンピュートプール内のサーバーのツリービューを表示します。
ターゲットの選択	同じコンピュートプール内の他のサーバーをすべて表示します。 **メモ: ターゲットサーバーが表示されるのは、ソースサーバーを選択した後のみです。**

関連リンク

- サーバーの交換ウィザード

ソース属性の確認

ソース属性の確認 ページでは、I/O ID の属性を含む、デバイス設定テンプレートを表示し、編集することができます。

テンプレート属性

テンプレート属性 タブに表示されるフィールドを、次の表で説明します。

表 124. テンプレート属性

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。
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。

フィールド	説明
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を表示します。
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。
元に戻す	デバイス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	デバイス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。

IOA VLAN 属性

IOA の VLAN 属性 タブに表示されるフィールドを、次の表で説明します。

表 125. IOA VLAN 属性

フィールド	説明
テンプレート用 IOA の VLAN 属性	選択したテンプレートの名前を表示します。
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値が導入されず、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	変更された属性がある場合に表示されます。
NIC	NIC の完全修飾デバイス記述子（FQDD）を表示します。
ファブリック	シャーシの特定のスロットに関連付けられたファブリックが表示されます。ファブリックは、グループ名（A、B、または C）およびスロット番号（1 または 2）の組み合わせで識別されます。
Tagged VLAN(s)（タグ付き VLAN）	選択したファブリックのタグ付き VLAN のリストを表示します。
Untagged VLAN（タグなし VLAN）	選択したファブリックのタグなし VLAN が表示されます。
元に戻す	選択したテンプレートの IOA VLAN 属性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	選択したテンプレートの IOA VLAN 属性に加えられた変更を保存する場合はクリックします。

デバイス固有属性

デバイス固有属性 タブに表示されるフィールドを、次の表で説明します。

表 126. テンプレート属性

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を表示します。
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。
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。

識別情報の割り当て

識別情報の割り当て タブに表示されるフィールドを、次の表で説明します。

表 127. 識別情報の割り当て

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。
セクション	属性が属するコンポーネントを表示します。たとえば、NIC 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を表示します。
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。

関連リンク

サーバーの交換ウィザード

オプション

オプション ページでは、サーバーの交換タスクのオプションを選択できます。

次の表で、**サーバーの交換ウィザード** の **オプション** ページに表示されるフィールドについて説明します。

表 128. オプション

フィールド	説明
コンピュートプールからソースを削除する	サーバー交換後、ソースサーバーをコンピュートプールから **再利用およびベアメタルデバイス** グループに移動する場合に選択します。 **メモ: このオプションが選択されていない場合、サーバー交換後もソースサーバーがコンピュートプール内に保持されます。**
仮想 ID をソースから回収できない場合でもターゲットに展開する	サーバーが到達不能の場合でもソースサーバーの仮想 I/O ID を回収する場合に選択します。 **メモ: ソースサーバーに到達できず、このオプションが選択されていない、または選択されている場合の状態は次のとおりです。** • 選択されていない - サーバーの交換タスクは不成功です。 • 選択されている - ソースサーバーがネットワークに戻された場合、ネットワーク上に重複する I/O ID を持つサーバーが存在する可能性があります。

関連リンク

サーバーの交換ウィザード

資格情報

資格情報 ページでは、ソースサーバとターゲットサーバの資格情報を入力することができます。

次の表で、**サーバーの交換ウィザード** の **資格情報** ページに表示されるフィールドについて説明します。

表 129. 資格情報

セクション	フィールド	説明
ソース資格情報	**User Name (ユーザー名)**	ソースサーバーの iDRAC のユーザー名を入力します。
	Password (パスワード)	ソースサーバーの iDRAC のパスワードを入力します。
ターゲット資格情報	**User Name (ユーザー名)**	ターゲットサーバーの iDRAC のユーザー名を入力します。
	Password (パスワード)	ターゲットサーバーの iDRAC のパスワードを入力します。

関連リンク

サーバーの交換ウィザード

Summary (サマリ)

サマリ ページには、サーバーの交換タスク用に選択したオプションが表示されます。

次の表で、**サーバーの交換ウィザード** の **サマリ** ページに表示されるフィールドについて説明します。

表 130. Summary（サマリ）

フィールド	説明
Name（名前）	タスクに指定されている名前を表示します。
コンピュートプール	選択されているコンピュートプールの名前を表示します。
ソース	選択されているソースサーバーの名前を表示します。
ターゲット	選択されているターゲットサーバーの名前を表示します。
IOA への VLAN の設定	IOA に VLAN を設定することを選択した場合に表示されます。
プールから削除する	コンピュートプールからソースサーバーを削除することが選択されているかどうかを表示します。
ID の回収を強制する	ソースサーバーが到達不能の場合でもソースサーバーの仮想 I/O ID を回収することを選択したかどうかを表示します。
スケジュール	事前定義されたタスクスケジュールを表示します。

関連リンク

サーバーの交換ウィザード

ID の回収ウィザード

ID の回収ウィザード を使用すると、サーバーからすべての管理下仮想 I/O ID を回収できます。ウィザードのさまざまなページに表示されるフィールドについては、次のセクションで説明します。

関連リンク

名前
デバイスの選択
識別情報の割り当て
オプション
資格情報
Summary（サマリ）
サーバの導入済み仮想入出力（I/O）ID の回収

名前

名前 ページでは、タスクの名前を指定できます。

関連リンク

ID の回収ウィザード

デバイスの選択

デバイスの選択 ページから、管理下仮想 I/O ID を回収することが可能なデバイスを選択することができます。

次の表で、**ID の回収ウィザード** の **デバイスの選択** ページに表示されるフィールドについて説明します。

表 131. デバイスの選択

フィールド	説明
Device Name（デバイス名）	デバイスの名前を表示します。
サービスタグまたはノード ID	デバイスに割り当てられた固有の識別子が表示されます。
使用中の ID の合計	デバイスに導入されている ID の合計数を表示します。
デバイスは削除されていますか	デバイスが仮想 I/O ID と共に導入された後で OpenManage Essentials から削除されたかどうかを表示します。

フィールド	説明
テンプレート名	デバイスに割り当てられたデバイス設定テンプレートの名前を表示します。
コンピュートプール	デバイスが属するコンピュートプールの名前を表示します。
前回の導入時刻	最後にデバイスを導入したときのタイムスタンプを表示します。
モデル	PowerEdge R710 など、デバイスのモデル名が表示されます（モデル名がある場合）。

関連リンク

ID の回収ウィザード

識別情報の割り当て

識別情報の割り当て ページでは、選択したサーバに割り当てられている仮想 I/O ID を表示することができます。

次の表で、**ID の回収ウィザード** の **識別情報の割り当て** ページに表示されるフィールドについて説明します。

表 132. 識別情報の割り当て

フィールド	説明
Device	デバイスの名前を表示します。
デバイスは削除されていますか	デバイスが仮想 I/O ID と共に導入された後で OpenManage Essentials から削除されたかどうかを表示します。
セクション	属性が属するコンポーネントを表示します。たとえば、NIC 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を表示します。
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。

関連リンク

ID の回収ウィザード

オプション

オプション ページでは、ID の回収タスクのオプションを選択することができます。

次の表で、**ID の回収ウィザード** の **オプション** ページに表示されるフィールドについて説明します。

表 133. オプション

フィールド	説明
コンピュートプールからソースを削除する	サーバーの ID の回収後に、サーバーをコンピュートプールから **再利用およびベアメタルデバイス** グループに移動する場合に選択します。 **メモ: このオプションが選択されていない場合、サーバーは、サーバーの ID 回収後もコンピュートプール内に保持されます。**
ターゲットにアクセスできない場合でも回収処置を強制する	サーバーが到達不能の場合でも選択されたサーバーの仮想 I/O ID を回収する場合に選択します。

フィールド	説明
	メモ: ソースサーバーに到達できず、このオプションが選択されていない、または選択されている場合の状態は次のとおりです。 • 選択されていない - ID の回収タスクは不成功です。 • 選択されている — 仮想 I/O ID が回収され、使用可能です。ただし、サーバーがネットワークに再度追加された場合は、ネットワーク上に I/O ID が重複するデバイスが見つかる可能性があります。

関連リンク

ID の回収ウィザード

資格情報

資格情報 ページでは、選択したサーバーの資格情報を入力することができます。

次の表で、**ID の回収ウィザード** の **資格情報** ページに表示されるフィールドについて説明します。

表 134. 資格情報

フィールド	説明
User Name（ユーザー名）	サーバーの iDRAC のユーザー名を入力します。
Password（パスワード）	サーバーの iDRAC のパスワードを入力します。

関連リンク

ID の回収ウィザード

Summary（サマリ）

サマリ ページには、ID の回収タスクに対して選択したオプションが表示されます。

次の表で、**ID の回収ウィザード** の **サマリ** ページに表示されるフィールドについて説明します。

表 135. Summary（サマリ）

フィールド	説明
Name（名前）	タスクに指定されている名前を表示します。
関連するデバイス	仮想 I/O ID を回収するために選択されているデバイスの名前を表示します。
プールから削除する	仮想 I/O ID を回収した後でコンピュートプールからサーバーを削除することを選択したかどうかを表示します。
ID の回収を強制する	ソースサーバーが到達不能の場合でもサーバーの仮想 I/O ID を回収することを選択したかどうかを表示します。
スケジュール	事前定義されたタスクスケジュールを表示します。

関連リンク

ID の回収ウィザード

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またはシャーシ設定は、サーバ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ベースラインに対する複数のサーバ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、現在の設定とそれに対応する設定ベースライン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、ベースラインを作成し、複数の実稼働サーバに希望のベースラインを割り当てて、コンプライアンスを確立することができます。

メモ: デバイスに関連するベースライン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ベースライン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。関連するベースラインが変更された場合は、そのベースラインを関連するデバイスに再導入する必要があります。

メモ: コンプライアンスタスクは IOA テンプレートではサポートされていません。

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。

- サーバまたはシャーシからの設定ベースラインの作成
- サーバまたはシャーシへの設定ベースラインの関連付け
- 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、iDRAC を搭載した対応 PowerEdge サーバに対してライセンス付与（有料）されています。PowerEdge VRTX または PowerEdge FX2/FX2s デバイスでこの機能を使用するには、Enterprise ライセンスが必要です。ただし、PowerEdge M1000e デバイスで使用する場合、ライセンスは不要です。サーバからのデバイス設定ベースライン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
デバイス導入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
ベースライン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
補足情報

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

デバイス設定ベースライン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ベースラインに順守させるのに必要な手順は次の通りです。

1. **ベースラインの作成** — **共通タスク** ペインの **ベースラインの作成** タスクを使用してデバイス設定ベースラインを作成します。設定ファイルまたはリファレンスデバイスから選んでベースラインを作成することができます。
2. **ベースラインへのデバイスの関連付け** — ベースラインを選択し、該当するデバイスにそのベースラインを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、ベースライン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付けられたベースラインのコンプライアンス状態を表示するには、**ベースライン** ペインでベースラインを選択します。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。

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、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定期的に収集できます。インベントリ情報は、特定のデバイス設定ベースラインに対するデバイスのコンプライアンス状態の確認に使用されます。
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* - サーバ設定管理ライセンスがすべてのターゲットサーバにインストールされます。詳細については、「OpenManage Essentials - サーバ設定管理ライセンス」を参照してください

メモ: 設定インベントリのコレクションまたはアップデートのスケジュールは、IOA では使用できません。

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: 管理者特権を持つ iDRAC 資格情報を提供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. **Ｆｉｎｉｓｈ**（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** 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

デバイス設定インベントリの表示

デバイスの設定インベントリは、**デバイス** ポータルを使用して表示することができます。
開始する前に、設定インベントリを表示する対象のデバイスが「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していることを確認します。
設定インベントリを表示するには、次の手順を実行します。

1. **管理** → **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. デバイスツリーで設定インベントリの詳細を表示するデバイスを右クリックし、**デバイス設定** → **デバイス設定インベントリの更新** をクリックします。
3. 右側のペインで、**設定** → **インベントリ** をクリックします。
   インベントリ設定の詳細が表示されます。デバイスにインベントリ設定タスクが実行されていない場合は、**インベントリ設定の実行** ボタンが表示されます。**インベントリ設定の実行** ボタンをクリックすると、**インベントリ設定スケジュール** でデバイスの資格情報を設定していることを条件として、設定の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

サーバおよびシャーシ向けデバイスコンプライアンスベースラインの作成

検出済みのサーバまたはシャーシからデバイスコンプライアンスベースラインを作成することができます。

メモ: シャーシのベースラインには、IOA 属性は含まれません。

サーバまたはシャーシのベースラインを作成するには：

1. **管理** → **設定** をクリックします。
2. **共通タスク** ペインで、**ベースラインの作成** をクリックします。
   ベースラインの作成 ウィザードが表示されます。
3. **名前** フィールドに、ベースラインの名前を入力します。
4. 次のいずれか 1 つを選択します。
   - **ファイルから作成**：XML テンプレートをインポートしてベースラインを作成
   - **デバイスから作成**：デバイスからベースラインを作成。
5. デバイスタイプ（サーバまたはシャーシ）を選択し、次のいずれかを実行します。
   - **適用可能なすべてのデバイス** ツリーからデバイスを選択します。
   - **デバイスを検索** ボックスを使用してデバイスを検索します。
6. **実行の資格情報** で管理者特権を持つデバイス資格情報を入力し、**終了** をクリックします。
7. タスク送信のメッセージで、**OK** をクリックします。

メモ: 破壊的な情報およびパスワード属性の情報は、ベースラインの設定中に表示されません。ベースラインの非破壊的属性情報のみが表示されます。

ベースラインへのターゲットデバイスの関連付け

ベースライン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ベースライン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ベースラインは 1 つのみです。2 つ目のベースラインをデバイスに関連付けると、2 つ目のベースラインがデバイスに関連付けられた唯一の設定ベースラインになります。

ターゲットデバイスをベースラインに関連付けるには、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、**デバイスをベースラインに関連付ける** をクリックします。
   - **ベースラインによるコンプライアンス** ペインで、ベースラインを右クリックして **関連付けるデバイス** をクリックするか、またはベースラインをクリックします。**デバイスの関連付け** ポップアップウィザードが表示されたら、**デバイスの関連付け** をクリックします。
3. **ベースラインへのデバイスの関連付け** ウィザードが表示されます。
4. **ベースラインの選択** ページで、関連付けるベースラインを選択します。
   a. ターゲットデバイスタイプに基づいて、**サーバのベースライン** または **シャーシのベースライン** のいずれかをクリックします。

      メモ: 作成済みまたはクローン化が完了している設定ベースライン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ベースラインを選択します。
   c. **次へ** をクリックします。
5. **デバイスの選択** ページで、**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

ベースラインの関連付け
ベースラインへのデバイスの関連付けウィザード

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 **設定** タブで **設定インベントリの実行** をクリックします。

メモ: コンプライアンスタスクは IOA テンプレートではサポートされていません。

デバイスと関連する設定ベースライン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。

非対応デバイスの修正

関連するベースラインに対応していないデバイスは、修正してベースラインの設定に対応させることができます。

メモ: デバイスの破壊的属性およびパスワード属性は、コンプライアンスについては考慮されません。このため、これらの属性は修正タスクについて考慮されません。

メモ: ユーザー設定の属性は、同じユーザーがターゲットデバイス上に存在する場合にのみ正常に修正されます。パスワード属性は修正について考慮されないため、新規ユーザーを作成することはできません。新規ユーザーの作成の詳細については、次の項を参照： 導入と再プロビジョニング

メモ: デバイスの修正タスクが失敗します。属性がないため、またはコンプライアンスベースラインに含まれていない他の属性に一部の属性が依存しているため、デバイスが非対応デバイスになっているからです。対応するベースラインで不足している属性の 導入 チェックボックスをオフにして、デバイスを適合させます。

対応していないデバイスを修正するには：

1. **管理** → **設定** → **デバイスのコンプライアンスの確保** の順にクリックします。

   名前 ページが表示されます。
2. 修正タスクの **名前** を入力し、**次へ** をクリックします。
3. **デバイスの選択** ページに、対応する非対応属性を持った、非対応のサーバおよびシャーシのリストが表示されます。リストからすべての非対応デバイス、または必要なデバイスを選択して、**次へ** をクリックします。
4. **オプション** ページで次の手順を実行します。
   a. メンテナンス期間中に、**手動でのサーバの再起動** を選択して手動でサーバを再起動します。再起動後、スケジュールどおり（または手動で）設定インベントリが更新されると、サーバのコンプライアンスが更新されます。シャーシに関連するベースラインが導入され、すぐに構成の変更が適用されます。
   b. **サーバの自動再起動** を選択し、選択したデバイスに関連するベースラインを即時導入します。構成の変更によってサーバの再起動が必要な場合は、まず正常なシャットダウンが行われます。正常なシャットダウンに失敗すると、強制シャットダウンが実行されます。

   メモ: シャーシの設定が即時適用されます。関連するサーバは再起動されません。
5. **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** 下に、選択したデバイスの資格情報を入力します。
   c. **次へ** をクリックします。
6. **概要** ページで入力した情報を確認してから、**終了** をクリックします。

   修正タスクが作成され、選択されたスケジュールに従って実行されます。**タスク実行履歴** 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。修正タスク中に割り当てられた新しい属性値が、**詳細 1** タブに表示されます。

デバイスのコンプライアンスは修正タスクの結果に基づいて計算されます。デバイスのコンプライアンスの状態を表示するには、次の項を参照： 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

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** とクリックします。
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。

   メモ: コンプライアンスタスクは IOA テンプレートではサポートされていません。

関連リンク

タスク

バックアッププロファイルの表示

デバイス設定インベントリをスケジュールすることによって、バックアッププロファイルが作成されます。デバイスは、**再利用およびベアメタルデバイス** グループに属する必要がありますが、仮想 I/O コンピュートプールに属する必要はありません。

サーバのバックアッププロファイルは、**設定のバックアップ** → **バックアップされたデバイス** に表示されます。**デバイス** セクションでいずれかのバックアップ・プロファイルを選択すると、**属性** セクションにプロファイルの属性が表示されます。バックアッププロファイルの属性は読み取り専用で、変更できません。

バックアッププロファイルを使用してターゲットサーバを交換するには、次を参照してください。 バックアッププロファイルからのサーバの交換

バックアッププロファイルからのサーバの交換

サーバの交換タスクでは、バックアッププロファイルから実稼働サーバを交換ができます。サーバの交換タスクを実行する場合、ソースサーバの属性はターゲットサーバに移行されます。

ターゲットサーバを交換する前に、次のことを確認します。

- 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。
- 資格情報が設定され、デバイスの設定インベントリがスケジュールされている。参照先 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
- ソースデバイスと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** グループに追加されている。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。

バックアッププロファイルからターゲットサーバを交換するには、次の手順を実行します。

1. **管理** → **設定** で、**サーバの交換** をクリックします。

   サーバの交換ウィザード が表示されます。

   メモ: 個々のバックアッププロファイルを選択するには、デバイス ペインで、バックアップされた デバイス名 を右クリックし、交換 を選択します。
2. タスク名を入力して、**次へ** をクリックします。
3. **ソースとターゲット** ページで次の操作を実行します。
   a. **ソースの選択** で、ソースサーバーを選択します。
   b. **ターゲットの選択** で、ターゲットサーバーを選択します。
   c. **次へ** をクリックします。

   メモ : ターゲットサーバは、再利用およびベアメタルグループに属する必要があります。ターゲットサーバをベアメタルグループに手動で追加する方法については、「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。
4. **ソース属性の確認** で、**テンプレート属性**、**デバイス固有属性**、および **識別情報の属性** が表示されます。**次へ** をクリックします。

   メモ: ソース属性の確認 に表示される属性は、読み取り専用です。
5. **オプション** ページでプリファランスに基づいて次のオプションのいずれかを選択します。

   - **ベアメタルプールからターゲットを削除** - サーバを交換した後に、ターゲットサーバを再利用およびベアメタルデバイス グループから削除する場合に選択します。
   - **仮想 ID をソースから削除できない場合でもターゲットに展開する** を選択すると、ソースサーバが到達不能の場合でも、ソースサーバの仮想 I/O ID を回収します。
6. **資格情報** ページで、**ソース資格情報** と **ターゲット資格情報** に入力します。**Next**（次へ） をクリックします。

   Summary（サマリ）ページが表示されます。
7. **サマリ** ページには、さまざまな属性とその値が表示されます。選択した情報を確認してから、**終了** をクリックします。

   ターゲットサーバが、ソースサーバのバックアッププロファイルに置き換えられ、サーバの交換タスクが **タスク** → **設定タスク** → **バックアップからのサーバ設定の復元** に表示されます。**タスク実行履歴** のタスクを右クリックして、タスク実行の詳細を表示することができます。ソースデバイスから回収された仮想 ID は、**詳細 1** タブに表示されます。**詳細 2** タブには、ターゲットサーバに導入された属性が表示されます。

   メモ: ベアメタルプールからターゲットを削除 オプションを選択した場合、ターゲットサーバは 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。

   メモ: ターゲットサーバが再検出されると、ターゲットサーバのインベントリの詳細が更新されます。

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、および作成可能なその他のタスクを表示します。
  - ベースラインの作成
  - ベースラインへのデバイスの関連付け
  - デバイスのコンプライアンスの確保
  - 設定インベントリスケジュール
  - ファイル共有の設定
  - サーバーの交換
- ベースラインによるコンプライアンス - サンプルのデバイス設定ベースライン、および作成またはクローンしたベースラインを表示します。
  - サーバのベースライン
    - サンプル
  - シャーシのベースライン
    - サンプル
- 構成のバックアップ - ターゲットデバイスと交換可能なバックアップされたデバイスが表示されます。
  - バックアップされたデバイス
- 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
    - デバイス設定の修正 - 非準拠デバイスの修正タスクが表示されます。
    - バックアップからのサーバ設定の交換 - ターゲットデバイス用に作成した **サーバの交換** タスクが表示されます。
    - シャーシベースライン設定インポート — シャーシ用に作成した **ベースラインの作成** タスクを表示します。
    - デバイスベースライン設定インポート — サーバ用に作成した **ベースラインの作成** 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
ベースライン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
バックアップされたデバイス

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ベースラインに適合するデバイス。
- 非準拠 — 関連付けられている設定ベースラインに準拠していないデバイス。
- インベントリ未施行 — 構成インベントリが完了していないデバイス。
- 非関連 — 設定ベースライン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。

表 136. デバイスコンプライアンスの表

フィールド	説明
コンプライアンスステータス	設定ベースラインに関連するデバイスのコンプライアンスステータスを示すアイコンを表示します。
Device Name（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。
Service Tag	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。

表 137. タスク

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。
タイプ	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。
更新日	タスクが更新された日付と時刻が表示されます。
更新者	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。

フィールド	説明
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。

表 138. タスクの実行履歴

フィールド	説明
ステータス	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。 • Running（実行中） • Complete（完了） • Stopped（停止） • Failed（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。

ベースラインへのデバイスの関連付けウィザード

ベースラインへのデバイスの関連付けウィザード では、デバイスをベースラインに関連付けることができます。**ベースライン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

[ベースラインの選択]
[デバイスの選択]
[ベースラインへのターゲットデバイスの関連付け]

ベースラインの選択

ベースラインの選択 ページでは、ターゲットデバイスに関連付けるベースラインを選択できます。

次の表に **ベースラインの選択** ページの各フィールドが記載されています。

表 139. ベースラインの選択

フィールド	説明
サーバのベースライン	作成またはクローンしたサーバ設定ベースラインを表示します。
シャーシのベースライン	作成またはクローンしたシャーシ設定ベースラインを表示します。

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の設定ベースラインに関連付けることができます。

デバイスのコンプライアンスの確保

デバイスのコンプライアンスの確保ウィザード では、非対応デバイスを修正することができます。**デバイスのコンプライアンスの確保ウィザード** に表示されるフィールドは、次の項で説明されています。

Name（名前）

表 140. Name（名前）

フィールド	説明
Name（名前）	修正タスクの名前を表示します。

デバイスの選択

表 141. デバイスの選択

フィールド	説明
チェックボックス	非対応デバイスのリストからデバイスまたはすべてのデバイスを選択します。
デバイス名	デバイスの名前を表示します。
サービスタグ	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。
最後に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。
非対応結果	不足している属性の数と非対応の属性の数を表示します。
デバイス名	デバイスの名前を表示します。
コンプライアンス結果	構成ベースラインに関連するデバイスのコンプライアンス結果を表示します。
コンポーネント名	属性が属するコンポーネントの名前を表示します。
属性名	属性の名前を表示します。
テンプレート値	属性のテンプレート値を表示します。
インベントリ値	属性のインベントリ値を表示します。

オプション

表 142. オプション

フィールド	説明
手動でのサーバの再起動	メンテナンス期間中の、手動によるサーバの再起動を選択します。シャーシに関連するベースラインが導入され、すぐに構成の変更が適用されます。 **メモ: シャーシの構成が変更されても、そのシャーシに関連するサーバは再起動しません。**
サーバの自動再起動	デバイスに関連するベースラインの即時導入を選択します。構成の変更によってサーバの再起動が必要な場合は、まず正常なシャットダウンが行われます。正常なシャットダウンに失敗すると、強制シャットダウンが実行されます。 **メモ: シャーシの構成が変更されても、そのシャーシに関連するサーバは再起動しません。**

スケジュールの設定

表 143. スケジュールの設定

フィールド	説明
今すぐ実行	これを選択すると、修正タスクがすぐに実行されます。
実行時刻	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。
実行の資格情報	
ユーザー名	タスクを実行するデバイスで設定する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。

概要

表 144. 概要

フィールド	説明
Name（名前）	修正タスクの名前を表示します。
非対応デバイス	選択した非対応のデバイス名が表示されます。
再起動オプション	選択した再起動オプションが表示されます。
スケジュール	修正タスクを実行するために選択したスケジュールを表示します。

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対する資格情報の追加および関連付けを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、次の表で説明します。

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。

表 145. 資格情報

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。
Username（ユーザー名）	ユーザー名を表示します。
Password（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、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。

表 146. デバイス

フィールド	説明
Device Name（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、デバイスで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。

表 147. スケジュール

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。

フィールド	説明
	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。 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。

バックアップされたデバイス

バックアップされたデバイス ウィンドウに、バックアップされたデバイスが表示されます。次に、**バックアップされたデバイス** ウィンドウに表示される表について説明します。

デバイス表

バックアップされたデバイス ポータルの **デバイス** 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。

表 148. デバイス表

フィールド	説明
接続ステータス	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。
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**、**不明** です。
デバイス名	ネットワーク上でデバイス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	デバイスに割り当てられた固有の識別子が表示されます。
モデル	デバイスのモデル名を表示します。例えば、PowerEdge R730 となります。
最後のバックアップの結果	デバイスで最後に実行したバックアップ操作の結果を表示します。
最後のバックアップ成功時刻	デバイスの最後のバックアップ成功時刻を表示します。

属性表

バックアップされたデバイス ポータルの **属性** 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。**グループ化基準** フィルタを使用することで、選択したフィルタオプションに基づいて、表の内容を表示できます。

表 149. 属性表

フィールド	説明
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。例えば、iDRAC、BIOS、NIC 等です。
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を表示します。
属性名	属性の名前を表示します。

フィールド	説明
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示されます。依存す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。

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

表 150. 事前定義されたレポート

カテゴリ	レポート	説明
サーバーインベントリ	**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。 • 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。

カテゴリ	レポート	説明
		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。
	エージェント正常性ステータス	システム名、エージェントのグローバルステータス、エージェント名、およびエージェントの説明などのエージェントに関する情報を提供します。
	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。
	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。
	ハードドライブ情報	シリアルナンバー、リビジョン、製造元、バスタイプ、およびハードドライブの自己暗号化機能を識別します。
	iDRAC パフォーマンス最小 / 最大	プロセッサ、メモリ、およびサーバーの I/O 帯域幅の最小使用率と最大使用率を提供します。
	iDRAC パフォーマンス平均 / ピーク	プロセッサ、メモリ、およびサーバーの I/O 帯域幅の平均使用率とピーク使用率を提供します。
	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。
	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。
	プロセッサ情報	サーバー内のプロセッサに関する詳細を提供します。
	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。

カテゴリ	レポート	説明
サーバー設定	**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。
	BIOS 設定	システムの BIOS 設定情報を提供します。
	iDRAC ネットワーク設定	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。
	デバイス設定コンプライアンス	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設定テンプレートに提供します。
	テンプレートの関連付け	デバイス設定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。
	割り当てられた識別情報の属性	デバイスに割り当てられるか、導入され、OpenManage Essentials によって管理される仮想 I/O ID に関する情報を提供します。
	すべての識別情報の属性	デバイスに存在し、OpenManage Essentials によってインベントリされたすべての仮想 I/O ID に関する情報を提供します。
保証とライセンス	**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。
	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。
Virtualization	**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。
資産	**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。
	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。

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。

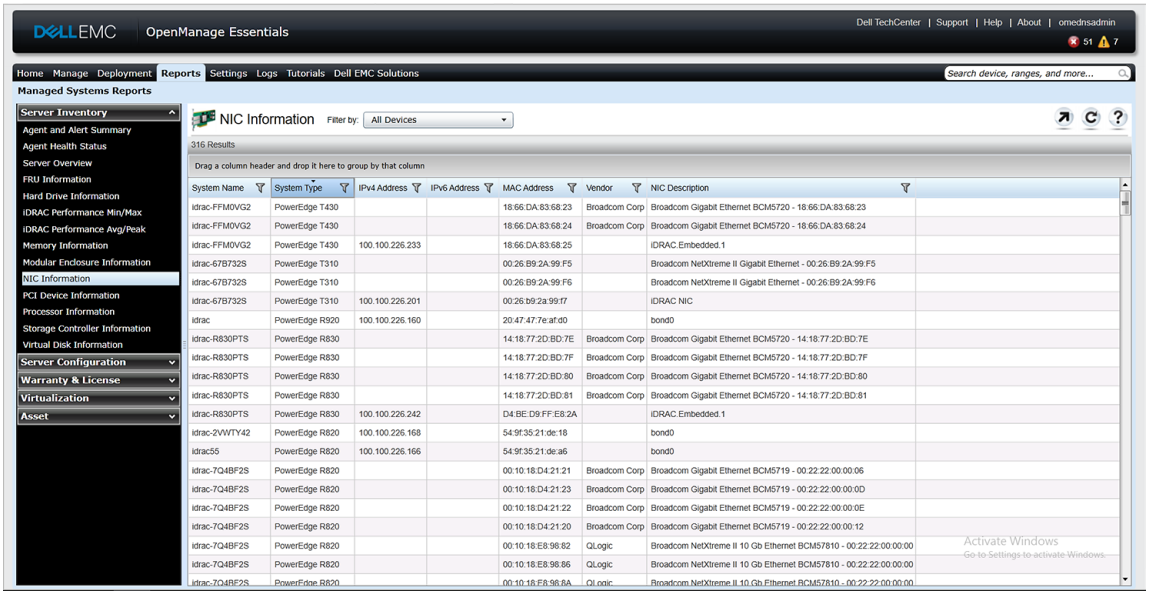

図 28. NIC 情報レポート

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 ポータルでは、次のセクションで使用可能な様々なレポートを表示できます。

- **サーバーインベントリ**
- **サーバー設定**
- **保証とライセンス**
- **仮想化**
- **資産**

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

サーバーインベントリレポート
サーバー設定レポート
保証とライセンスレポート
仮想化レポート
資産レポート

サーバーインベントリレポート

サーバーインベントリ セクションには、次のレポートが含まれています。

- **エージェントおよびアラート概要**
- **エージェント正常性ステータス**
- **サーバーの概要**
- **FRU 情報**
- **ハードドライブ情報**
- **iDRAC パフォーマンス最小 / 最大**
- **iDRAC パフォーマンス平均 / ピーク**
- **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**
- **プロセッサ情報**
- **ストレージコントローラ情報**
- **仮想ディスク情報**

関連リンク

エージェントおよびアラート概要
エージェント正常性ステータス
サーバーの概要
フィールドで交換可能なパーツ（FRU）に関する情報
ハードドライブ情報
iDRAC パフォーマンス最小または最大
iDRAC パフォーマンス平均またはピーク
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
プロセッサ情報
ストレージコントローラ情報
仮想ディスク情報

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サマリ には、次の内容が表示されます。

- **エージェントサマリ**
- **iDRAC サービスモジュールサマリ**
- **1 デバイス当たりの警告**
- **最多警告生成**

エージェントサマリ

エージェントサマリ ペインは、エージェントサマリ情報を表およびグラフで表示します。

表 151. エージェントサマリ

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サマリ

iDRAC サービスモジュールサマリ ペインには iDRAC Service Module のサマリ情報が表およびグラフで表示されます。

表 152. iDRAC サービスモジュールサマリ

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	
iDRAC サービスモジュールの詳細	検出されたサーバー上での iDRAC サービスモジュール導入の可能性を表示します。
システムの数	サーバーの数を表示します。

iDRAC サービスモジュールサマリ チャートには、次のようにサーバーが表示されます。

- 対応 Linux - サーバーが一部の iDRAC サービスモジュールの導入要件を満たしていません。たとえば、サーバーで 64 ビットのオペレーティングシステムが実行されていない、またはシステムにインストールされている iDRAC ファームウェアが 1.51.51 よりも前のバージョンである可能性があります。
- 導入可能 Linux - iDRAC サービスモジュールをサーバーに導入することができます。
- 対応 Windows - サーバーが一部の iDRAC サービスモジュールの導入要件を満たしていません。たとえば、システムで 64 ビットのオペレーティングシステムが実行されていない、またはシステムにインストールされている iDRAC ファームウェアが 1.51.51 よりも前のバージョンである可能性があります。

- 導入可能 Windows - iDRAC サービスモジュールをサーバーに導入することができます。
- 非対応 - iDRAC サービスモジュールをサーバーにインストールすることができません。たとえば、システムがデルの第 11 世代またはそれ以前の PowerEdge サーバーである可能性があります。

1 デバイス当たりの警告

表 153. 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	
Device Name（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。

エージェント正常性ステータス

表 154. エージェント正常性ステータス

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。
Service Tag	システムに割り当てられた固有の識別子を表示します。
エージェントのグローバルステータス	エージェントのグローバルな正常性ステータスを表示します。
エージェント名	エージェント名を表示します。
Agent Version（エージェントバージョン）	エージェントのバージョンを表示します。
エージェントの説明	デバイスのエージェント詳細情報を表示します。
エージェントの製造元	エージェントの製造元名を表示します。

サーバーの概要

表 155. 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。

フィールド	説明
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。
Total Memory（総メモリ量）	システムに取り付けられたメモリの合計を表示します。

フィールドで交換可能なパーツ（FRU）に関する情報

表 156. 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。
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。
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。

ハードドライブ情報

表 157. 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。
Service Tag	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。
説明	メディアの説明を表示します。
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。

フィールド	説明
バスのタイプ	使用されているバス接続のタイプを表示します。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	メディアのタイプを表示します。例えば HDD などです。
Vendor（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。
Model number（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。
定格書き込み耐性の残存率	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。
サポートされる暗号化タイプ	暗号化対応のハードドライブリストが表示されます。次が表示されます。 • **自己暗号化ドライブ（SED）**：ハードドライブが暗号化に対応しています。 • **なし**：ドライブは暗号化に対応していません。 • **該当なし（N/A）**：インベントリからデータを取得できません。 **メモ: この機能は、WS-MAN プロトコルを使用した iDRAC デバイスおよび SNMP プロトコルを使用した OMSA をデバイスでのみ使用できます。**

iDRAC パフォーマンス最小または最大

メモ: iDRAC パフォーマンス最小 / 最大 レポートは、デルの第 13 世代以降の PowerEdge サーバーの情報のみを提供します。

表 158. iDRAC パフォーマンス最小 / 最大

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。
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。
属性	報告されたパフォーマンス属性の名前を表示します。
過去 1 時間 (%)	過去 1 時間における属性の使用レベルを表示します。
過去 1 時間のタイムスタンプ	過去 1 時間に使用レベルが報告された時刻を表示します。
過去 1 日 (%)	過去 1 日における属性の使用レベルを表示します。
過去 1 日のタイムスタンプ	過去 1 日に使用レベルが報告された時刻を表示します。
過去 1 週間 (%)	過去 1 週間における属性の使用レベルを表示します。
過去 1 週間のタイムスタンプ	過去 1 週間に使用レベルが報告された時刻を表示します。

iDRAC パフォーマンス平均またはピーク

メモ: iDRAC パフォーマンス平均 / ピーク レポートは、デルの第 13 世代以降の PowerEdge サーバーの情報のみを提供します。

表 159. iDRAC パフォーマンス平均 / ピーク

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。
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。
属性	報告されたパフォーマンス属性を表示します。
過去 1 時間の平均 (%)	過去 1 時間における属性の平均使用レベルを表示します。
過去 1 日の平均 (%)	過去 1 日における属性の平均使用レベルを表示します。
過去 1 週間の平均 (%)	過去 1 週間における属性の平均使用レベルを表示します。
ピークタイムスタンプ	過去 1 週間にピーク使用レベルが報告された時刻を表示します。

メモリ情報

表 160. 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。
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。
Service Tag	システムに割り当てられた固有の識別子を表示します。
Name（名前）	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。
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。
メモリデバイスタイプ	メモリデバイスのタイプを表示します。たとえば、DDR3 です。
メモリデバイスタイプ詳細	メモリデバイスタイプについての詳細を表示します。
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

表 161. 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	エンクロージャ上のスロット番号を表示します。
サブスロット	サブスロット名を表示します。
スロット名	エンクロージャのスロット名を表示します。
スロットコンテンツ	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。
Firmware Version（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

表 162. 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。
Vendor（ベンダー）	NIC サプライヤの名前を表示します。
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

表 163. 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。
Service Tag	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。

プロセッサ情報

表 164. プロセッサ情報

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。
Service Tag	システムに割り当てられた固有の識別子を表示します。
シリーズ	プロセッサシリーズの名前を表示します。
速度（MHz）	プロセッサの速度を MH z 単位で表示します。
最大速度（MHz）	プロセッサの最大速度を MH z 単位で表示します。
コア	プロセッサ内のコアの数が表示されます。
Brand（ブランド）	プロセッサ製造元の名前を表示します。
モデル	プロセッサのモデル情報が表示されます。
ステッピング	プロセッサモデルのバージョンを表示します。
スロット	プロセッサが占有するスロットを示します。
ステータス	プロセッサの状態を表示します。

ストレージコントローラ情報

表 165. 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。
Vendor（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

表 166. 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。
Service Tag	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。
Name（名前）	仮想ディスクの名前を表示します。
Device Name（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。

サーバー設定レポート

サーバー設定 セクションには、次のレポートが含まれています。

- **サーバーコンポーネントとバージョン**

- **BIOS 設定**
- **iDRAC ネットワーク設定**
- **デバイス設定コンプライアンス**
- **テンプレートの関連付け**
- **割り当てられた識別情報の属性**
- **すべての識別情報の属性**

関連リンク

サーバーコンポーネントとバージョン
BIOS 設定
iDRAC ネットワーク設定
デバイス設定コンプライアンス
ベースラインの関連付け
割り当てられた識別情報の属性
すべての識別情報の属性

サーバーコンポーネントとバージョン

表 167. 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。
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。
Service Tag	システムに割り当てられた固有の識別子を表示します。
説明	ソフトウェアの情報を表示します。
ソフトウェアタイプ	システムで使用可能なソフトウェアタイプを表示します。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。

BIOS 設定

表 168. 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。
Service Tag	システムに割り当てられた固有の識別子を表示します。
Virtualization Technology（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のいずれになっているかを表示します。
System Profile（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。

フィールド	説明
User Accessible USB Ports（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。
Node Interleaving（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。
Logical Processor（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。
Integrated RAID Controller（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 Global Enable（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。
Execute Disable（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

表 169. 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。
Service Tag	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。

デバイス設定コンプライアンス

表 170. デバイス設定コンプライアンス

フィールド	説明
コンプライアンスステータス	構成ベースライン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。
Device Name（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。
Service Tag	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。
コンプライアンスベースライン	デバイスに関連付けられたデバイス設定ベースラインを表示します。
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。

ベースラインの関連付け

表 171. ベースラインの関連付け

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。
Service Tag	システムに割り当てられた固有の識別子を表示します。
関連するベースライン	システムに関連付けられているデバイス設定ベースラインを表示します。

関連リンク

ベースラインへのターゲットデバイスの関連付け

割り当てられた識別情報の属性

表 172. 割り当てられた識別情報の属性

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。
Service Tag	システムに割り当てられた固有の識別子を表示します。
セクション	属性が属するコンポーネントを表示します。たとえば、NIC、FC 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を表示します。

フィールド	説明
属性名	属性の名前を表示します。
値	システム上の割り当て済みまたは導入済みの仮想 I/O ID を表示します。
コンピュートプール	デバイスが属しているコンピュートプールの名前が表示されます。
仮想 I/O プール	システムに割り当てられている仮想 I/O ID の仮想 I/O プールの名前を表示します。
ステータス	システムが仮想 I/O ID を使用して導入されているかどうかを表示します。

メモ: ID 属性の展開された状態は、OpenManage Essentials によって生成された ID がネットワークに複数がある場合、冗長性がある場合があります。

すべての識別情報の属性

表 173. すべての識別情報の属性

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。
Service Tag	システムに割り当てられた固有の識別子を表示します。
セクション	属性が属するコンポーネントを表示します。たとえば、NIC、FC 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を表示します。
属性名	属性の名前を表示します。
値	システム上の割り当て済みまたは導入済みの仮想 I/O ID を表示します。

保証とライセンスレポート

保証とライセンス セクションには、次のレポートが含まれています。

- **保証情報**
- **ライセンス情報**

関連リンク

保証情報
ライセンス情報

保証情報

表 174. 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。
Device Name（デバイス名）	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。
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。
Device Type（デバイスタイプ）	デバイスタイプを表示します。例えば、サーバー、Remote Access Controller などです。
Service Tag	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。
保証タイプ	保証タイプを表示します。たとえば、初期、延長などです。
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。
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。
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。
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。
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。

ライセンス情報

表 175. 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。

仮想化レポート

仮想化 セクションには、次のレポートが含まれています。

- **ESX 情報**
- **HyperV 情報**

関連リンク

ESX 情報
HyperV 情報

ESX 情報

表 176. ESX 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、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 タイプ	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 タイプ	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

表 177. HyperV 情報

フィールド	説明
システム名	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。

資産レポート

資産 セクションには、次のレポートが含まれています。

- **資産取得情報**
- **資産メンテナンス情報**

- **資産サポート情報**
- **デバイス位置の情報**

資産 セクションのレポートは次の条件に左右されます。

- サーバは SNMP プロトコルにより帯域内で検出される必要があります。
- 資産情報は OMSA で設定される必要があります。OMSA で資産情報を設定するには、**システム** → **プロパティ** → **資産情報を** にアクセスします。

関連リンク

資産取得情報
資産メンテナンス情報
資産サポート情報
デバイス位置の情報

資産取得情報

表 178. 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。
Service Tag	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。
Vendor（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

表 179. 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。
Service Tag	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

表 180. 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。
Service Tag	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。

フィールド	説明
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。

デバイス位置の情報

表 181. 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。
Service Tag	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。
通路	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。

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、スイッチ、ストレージなど）で利用できます。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なことから、OpenManage Essentials のレポートの中でも特殊です。インターネットアクセスがない場合は、保証情報は表示されません。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ときにダウンロードされます。

メモ: 特定のサービスタグについて 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 に表示される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は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** をクリックします。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 または iOS 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 User's Guide*』(OpenManage Mobile ユーザーズガイド) を参照してください。

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
- MIB ファイルの管理
- トラップの管理

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 182. アラートの種類

アイコン	アラート	説明
 **図 29. 正常アラートアイコン**	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。
 **図 30. 警告アラートアイコン**	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。
 **図 31. 重要アラートアイコン**	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失が差し迫っていることを示す重要なイベントです。
 **図 32. 不明アラートアイコン**	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。

アイコン	アラート	説明
 **図 33. 情報アラートアイコン**	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、**設定** 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ステータス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

表 183. alertCoolingDeviceFailure アラートソースの値と説明

フィールド名	値	説明
Name（名前）	alertCoolingDeviceFailure	
タイプ	snmp	SNMP アラートベースのソースです。
Catalog	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。
フォーマット文字列	$3	
SNMP Enterprise OID	.1.3.6.1.4.1.674.10892.1	
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
      - $r = 推奨される解決策
      - $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
      - $loc = デバイスの場所
      - $mod = モデル名
   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. **重要度の関連** 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. **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。
   アラートログ設定 ウィンドウが表示されます。
2. 次のフィールドで値を入力するか、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。
   a. **アラートログの最大サイズ**
   b. **警告が発行されるアラートログの最大サイズ**
   c. **アラートログが最大容量に達した時にパージする**

   メモ: アラートログのデフォルトの最大サイズは 40,000 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。
3. **パージされたアラートの保存** を選択し、パージされたアラートのログを .csv 形式で保存します。
4. **パージされたアラートの保存場所** に入力します。
5. **終了** をクリックします。
   アラートログ設定 が設定されます。最大サイズに達すると、指定したアラートログがパージされます。アラートログのパージタスクのステータスが **ログ** → **アプリケーションログ** に表示されます。

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。

- アラートタイプおよび頻度。
- デバイスツリー内のデバイスに移動するリンクとしての各デバイスの名前。

  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. **設定** → **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. **設定** → **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

MIB ファイルの管理

OpenManage Essentials は、ほぼすべてのエンタープライズデバイスのハードウェアアラート（SNMP トラップ）をフォーマットできます。Dell 製以外のデバイスをお使いの場合、**アラート** ポータルを使用して OpenManage Essentials 用のアラートを定義することができます。アラートを定義することにより、OpenManage Essentials がより広範囲のハードウェアを監視し、これらのデバイス用に電子メールおよび転送のルールをセットアップできるようになります。

アラート ポータルで、SMIv1 または SMIv2 管理情報ベース（MIB）ファイルからトラップ定義を抽出できます。抽出されたトラップは、OpenManage Essentials にインポートする前に表示および編集できます。このユーティリティを使うと、トラップを手動で定義および管理することもできます。OpenManage Essentials は、インポートされたトラップ定義、および手動で管理されているトラップ定義を使用することによって、特定デバイスから受信されるトラップを適切に分類します。

メモ: トラップのインポート ポータルはオプションであり、デル製以外のデバイスからのアラートをフォーマットする場合にのみ必要となります。

MIB のインポート

使用事例シナリオ： 管理者として、OpenManage Essentials でサポートされていないデバイスをモニタ（受信トラップのリッスンおよび分類）することが必要です。

ソリューション：デバイスが SNMP プロトコルをサポートしているかどうかを確認します。デバイスが SNMP プロトコルをサポートしている場合、サービスが実行されており、トラップの宛先が OpenManage Essentials ベースのシステムになっていることを確認します。非対応デバイストラップについては、**アラート** ポータルを使用してトラップ定義をインポートすることにより、OpenManage Essentials でトラップを定義します。以下の表は、OpenManage Essentials データベースにインポートされる前と後のトラップに関する情報を示しています。

表 184. MIB のインポート

機能	MIB を OpenManage Essentials データベースにインポートする前	MIB を OpenManage Essentials データベースにインポートした後
デバイスから送信されるトラップを OpenManage Essentials アラートポータルで表示できますか?	はい	はい
トラップには、重要度の値が含まれていますか?	いいえ、重要度は不明です。	はい
トラップには有効な名前がありますか?	いいえ、名前は不明です。	はい、トラップ名は MIB で定義されています。

機能	MIB を OpenManage Essentials データベースにインポートする前	MIB を OpenManage Essentials データベースにインポートした後
トラップには、有効なイベントカテゴリ名がありますか?	いいえ、イベントカテゴリ名は不明です。	はい、デフォルトで新しいカテゴリが作成されます。
トラップには説明がありますか?	はい、すべての説明詳細があります。ただし、詳細はフォーマットされていません。	はい、トラップのインポート中に定義されたフォーマットの説明があります。
トラップはトラップ変数値を表示しますか?	はい	はい（デフォルト）ただし、トラップを OpenManage Essentials にインポートする前にフォーマット文字列値が削除されていない場合に限ります。
トラップは、エンタープライズオブジェクト識別子（OID）、固有 OID、および汎用 OID を表示しますか?	はい	はい
トラップは、デバッグで使用できる追加のトラップ変数を表示しますか?	はい、ただし詳細はフォーマットされていません。	はい
トラップは、デバイスのホスト名または IP アドレスを表示しますか?	はい	はい
別の管理コンソールへのトラップの転送、タスクの実行、または不要なトラップのフィルタを行うために、各種アラート処置でトラップを使用することはできますか?	はい、ただし機能は限られています。重要度、イベントカテゴリ、イベント名などに固有の規則は使用不可能です。	はい、トラップは、アラート処置がトラップ名、カテゴリ、重要度などに基づいてサポートされるように定義されています。
トラップで各種 UI 処置（承認、削除など）を行うことはできますか?	はい	はい
アラートのパージはトラップで機能しますか?	はい	いいえ

MIB ファイルのインポート

作業を開始する前に、OmeAdministrator 権限を持つアカウントでログインしていることを確認します。

1. **管理 → アラート → Manage MIBs（ MIB の管理 ）** をクリックします。
2. **Manage MIBs**（MIB の管理） で、**Import MIB**（MIB のインポート） をクリックします。
3. **Select files for upload**（アップロードするファイルの選択） で、**Browse**（参照） をクリックします。
   a. インポートする MIB ファイルを選択します。
   b. **開く** をクリックします。
4. **Select a MIB File**（MIB ファイルの選択） リストから、MIB ファイルを選択し、**Parse MIB**（MIB の解析） をクリックします。
   トラップデータがグリッド形式で表示されます。
5. **トラップのインポート** をクリックして、トラップを OpenManage Essentials データベースにインポートします。

OpenManage Essentials からの MIB ファイルの削除

OpenManage Essentials からの MIB の削除は、コンソール内の関連アラート処置および既存アラートに影響します。
作業を開始する前に、OmeAdministrator 権限を持つアカウントでログインしていることを確認します。

1. **管理 → アラート → Manage MIBs（ MIB の管理 ）** をクリックします。
2. **Manage MIBs**（MIB の管理） で、**MIB の削除** をクリックします。
3. **Imported MIB**（インポートされた MIB） で MIB を選択します。
4. **MIB の削除** をクリックします。

トラップの管理

トラップ定義のカスタマイズ

Custom Trap Definitions（カスタムトラップ定義）ビューでは、OpenManage Essentials データベースにトラップ定義を追加することができます。新規トラップ定義の追加、OpenManage Essentials で受信した不明トラップの検索、トラップ詳細の定義、およびトラップの追加を行うことができます。

メモ: 不明トラップ ボタンを使用して OpenManage Essentials で受信された不明トラップを追加すると、エンタープライズ OID、汎用 ID および 固有 ID フィールドが自動的に入力されます。

作業を開始する前に、OmeAdministrator 権限を持つアカウントでログインしていることを確認します。

トラップを追加するには、次の手順を実行します。

1. **管理** → **アラート** → **Manage Traps（ トラップの管理 ）** をクリックします。
2. **Manage Traps**（トラップの管理） で、**Custom Trap Definitions**（トラップ定義のカスタマイズ） をクリックします。
   Custom Trap Definitions（カスタムトラップ定義） ビューが表示されます。
3. 新規トラップ定義を追加する場合：
   a. **カテゴリ名** リストで、既存のカテゴリを選択、または新しいカテゴリ名を入力します。
   b. **トラップ名**、**説明**、**エンタープライズ OID**、**固有 ID**、および **フォーマット文字列** を入力します。
   c. **重要度** リストで、トラップの重大度レベルを選択します。
4. OpenManage Essentials で受信された不明トラップを追加する場合：
   a. **不明トラップの検索** をクリックします。
      OpenManage Essentials の不明トラップ ウィンドウが表示されます。
   b. 定義して追加する不明トラップを選択し、**OK** をクリックします。
      エンタープライズ OID、**汎用 ID** および **固有 ID** フィールドは、選択した不明トラップに基づいて自動的に入力されます。
   c. **カテゴリ名** リストで、既存のカテゴリを選択、または新しいカテゴリ名を入力します。
   d. **トラップ名**、**説明**、および **フォーマット文字列** を入力します。
   e. **重要度** リストで、トラップの重大度レベルを選択します。
5. **トラップの追加** をクリックします。
   入力したトラップの詳細が **User-defined Trap(s)**（ユーザー定義のトラップ） グリッドに表示されます。

トラップの削除

Custom Trap Definitions（カスタムトラップ定義） ビューでは、ユーザー定義のトラップを削除することもできます。OpenManage Essentials で事前定義されたトラップは削除できません。

作業を開始する前に、OmeAdministrator 権限を持つアカウントでログインしていることを確認します。

トラップを削除するには、次の手順を実行します。

1. **管理** → **アラート** → **Manage Traps（ トラップの管理 ）** をクリックします。
2. **Manage Traps**（トラップの管理） で、**Custom Trap Definitions**（カスタムトラップ定義） をクリックします。
3. **ユーザ定義のトラップ** グリッドで、削除するトラップを選択します。
   選択したトラップがハイライト表示されます。
4. **トラップの削除** をクリックします。
   確認ダイアログボックスが表示されます。
5. **はい** をクリックします。

ビルトインのトラップ定義のリセット

ビルトインのトラップ定義のリセット ビューでは、これまでに編集した事前定義の OpenManage Essentials トラップをリセットすることができます。

作業を開始する前に、OmeAdministrator 権限を持つアカウントでログインしていることを確認します。

トラップを元に戻すには、次の手順を実行します。

1. **管理** → **アラート** → **Manage Traps（トラップの管理）** をクリックします。
2. **Manage Traps**（トラップの管理） で、**Reset Built-in Trap Definitions**（ビルトインのトラップ定義のリセット） をクリックします。
   トラップを元に戻す ビューに、編集した事前定義のトラップ定義がすべて表示されます。
3. **Edited Traps**（編集済みトラップ） グリッドで、元に戻すトラップを選択し、**Revert Traps**（トラップを元に戻す） をクリックします。
   確認ダイアログボックスが表示されます。
4. **はい** をクリックします。

SNMP V3 トラップの設定

OpenManage Essentials の最新バージョンは、SNMP v3 トラップをサポートします。SNMP v3 トラップは、v1/v2c 通知よりもセキュリティが強化されています。SNMP v3 トラップを選択すると、Windows Trap サービスが無効になります。詳細については、「アラート設定」を参照してください。
SNMP V3 トラップを設定するには

1. **管理** → **アラート** → **一般タスク** → **SNMP V3 トラップの設定** を選択します
   SNMP V3 トラップの設定 ウィンドウが表示されます。

   メモ: SNMP v3 トラップの設定の詳細は、SNMP v3 プロトコルを使用して検出されたデバイスに自動的に入力されます。SNMP v3 トラップを受信するには、設定 → アラート設定 で SNMP v3 トラップリスナーを有効にします。
2. SNMP v1/v2c または WSMAN プロトコルを使用して検出されたデバイスの詳細を次の列に入力します。

   メモ: SNMP V3 トラップの設定 ウィンドウの詳細は、アラート設定 → SNMP リスナー設定 で V1/V2c/V3 トラップのサポートが選択されている場合のみ編集できます。V1/V2c のサポート が選択されている場合は、詳細のみ表示できます。

   a. ユーザー名
   b. 認証プロトコル
   c. 認証パスワード
   d. 暗号化プロトコル
   e. 暗号化パスワード
3. SNMP V3 トラップを手動で設定するには：
   a. **新しく追加** をクリックします。
      SNMP V3 トラップの設定 ウィンドウが表示されます。
   b. 次のフィールドで詳細を入力します。
      - エージェントの IP アドレス
      - エンジン ID
      - ユーザー名
   c. リストから **認証プロトコル** を選択します。

      メモ: SHA1 がデフォルトで選択される認証プロトコルです。
   d. **認証パスワード** に入力します。
   e. リストから、**暗号化プロトコル** を選択します。

      メモ: AES がデフォルトで選択される暗号化プロトコルです。

      メモ: 認証プロトコル が なし に設定されている場合、認証と暗号化のオプションは無効になります。
   f. **OK** をクリックします。
      設定された SNMP V3 トラップ・プロファイルが、**SNMP V3 トラップの設定** ウィンドウに表示されます。
4. または、次のようにして、資格情報を含む CSV ファイルをインポートします。
   a. サンプル .csv ファイルを生成するには、**エクスポート** をクリックします。
   b. システムにファイルを保存し、.csv ファイルのエージェントの IP アドレス、エンジン ID、ユーザー名、認証プロトコル、認証パスワード、暗号化プロトコル、および暗号化パスワードのフィールドに入力します。
   c. **インポート** をクリックして .csv ファイルをインポートします。
      インポートした資格情報が **SNMP V3 トラップの設定** ウィンドウに表示されます。

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
  - SNMP V3 トラップ設定
- 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
- MIB の管理
- トラップの管理

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。

表 185. 事前定義されたアラート表示フィルタ

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

表 186. 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
Acknowledged (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。
Device	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。
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

表 187. 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。
Acknowledged (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。
推奨される解決策	これをクリックして、アラートの原因となった問題に対して推奨される解決策を表示します。 **メモ: 推奨される解決策は、サーバーにインストールされている OMSA から、またはサーバーの iDRAC から受信されたアラートに関してのみ使用できます。OMSA で 拡張メッセージフォーマット オプションが有効になっている場合のみ、OMSA から受信されたアラートに推奨される解決策が含まれます。**
Device	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	モニタ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。

表 188. アラートログ設定

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。
パージされたアラートの保存	選択した場合、指定した数のアラートがパージされ、.csv ファイルに保存されます。
パージされたアラートの保存場所	パージされたアラートが .csv ファイルとして保存される場所を指定します。

アラート表示フィルタ

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 または iOS 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 User's Guide*』(Dell OpenManage Mobile ユーザーズガイド) を参照してください。

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。

表 189. 重大度

フィールド	説明
Name (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）。
Enabled (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

表 190. 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。

フィールド	説明
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

サマリ 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 **サマリの表示** 右クリックオプションをクリックすると表示されます。

表 191. アラート表示フィルタ

フィールド	説明
Name（名前）	アラート処置の名前です。
タイプ	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。
説明	アラート処置の説明です。
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。
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

表 192. 名前と説明

フィールド	説明
Name（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。
Enabled（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

表 193. 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。

表 194. アプリケーションの起動設定

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 = 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 • $r = 推奨される解決策 • $e = エンタープライズ OID • $sp = 特定のトラップ ID • $g = 汎用トラップ ID • $cn = アラートカテゴリ名

フィールド	説明
	• $sn = アラートソース名 • $pkn = パッケージ名 • $at = 管理タグ • $loc = デバイスの場所 • $mod = モデル名 **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 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。

表 195. 電子メール設定

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。
From（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。
Message（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ており、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では、トラップ転送を使用する必要がある場合があります。

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。

表 196. トラップ転送

フィールド	説明
Destination（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。

SNMP V3 設定

次の表は、**SNMP V3 設定** の項に表示されるフィールドについての説明です。

表 197. SNMP V3 設定

フィールド	説明
エージェントの IP アドレス	SNMP エージェントの IP アドレスを入力します。
エンジン ID	SNMP エージェントの一意のエンジン ID を入力します。
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。
認証プロトコル	デバイスの検出用の認証プロトコルを選択します。使用可能なオプションは、MD5、SHA1、およびなしです。デバイスを正常に検出するには、同じ認証プロトコルを使用してデバイスを設定する必要があります。認証プロトコルを なし にした場合、暗号化オプションも無効になります。
認証パスワード	認証パスワードを指定します。
暗号化プロトコル	デバイスの検出用の暗号化プロトコルを選択します。使用可能なオプションは、AES、DES、およびなしです。デバイスを正常に検出するには、同じ暗号化プロトコルを使用してデバイスを設定する必要があります。
暗号化パスワード	暗号化パスワードを入力します。
更新	クリックして、SNMP V3 の設定 ページをリフレッシュし、追加された SNMP V3 トラップを表示します。
新規追加	クリックして、SNMP V3 トラップを手動で設定します。
インポート	クリックして、SNMP V3 トラップ資格情報を含む .csv ファイルをインポートします。
エクスポート	クリックして、SNMP V3 トラップ資格情報を .csv ファイルにエクスポートします。
保存	資格情報を .csv ファイルからインポートした後、または資格情報を手動で入力した後にクリックして、SNMP V3 トラップを保存します。
削除	クリックして、選択した SNMP V3 トラップをリストから削除します。

SNMP V3 設定ウィザード

表 198. SNMP V3 設定ウィザード

フィールド	説明
エージェントの IP アドレス	SNMP エージェントの IP アドレスを入力します。
エンジン ID	SNMP エージェントの一意のエンジン ID を入力します。
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。
認証プロトコル	デバイスの検出用の認証プロトコルを選択します。使用可能なオプションは、MD5、SHA1、およびなしです。デバイスを正常に検出するには、同じ認証プロトコルを使用してデバイスを設定する必要があります。認証プロトコルを なし にした場合、暗号化オプションも無効になります。
認証パスワード	認証パスワードを指定します。
暗号化プロトコル	デバイスの検出用の暗号化プロトコルを選択します。使用可能なオプションは、AES、DES、およびなしです。デバイスを正常に検出するには、同じ暗号化プロトコルを使用してデバイスを設定する必要があります。
暗号化パスワード	暗号化パスワードを入力します。

カテゴリおよびソースの関連

OpenManage Essentials には、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

表 199. 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 Controller 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。
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

表 200. 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

表 201. 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 秒 ~ 24 時間）に受信した重複アラートの無視。	このオプションを選択し、重複アラートを無視する間隔を設定します。最長 24 時間アラートを無視することができます。
無	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）。

表 202. サマリ — アラート処置の詳細

フィールド	説明
Name（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。
タイプ	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。
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。
From（差出人）	電子メール発信元の電子メールアドレスです。

フィールド	説明
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。
Message（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）。
Destination（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。
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、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

表 203. 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。
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。
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。

フィールド	説明
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。
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。

トラップ定義の編集

表 204. トラップ定義の編集

フィールド	説明
トラップ名またはエンタープライズ OID	編集するトラップのトラップ名またはエンタープライズ OID を入力するフィールドです。
検索	クリックすると、OpenManage Essentials データベースから入力したトラップ名またはエンタープライズ OID を検索します。

フィールド	説明
イベントカテゴリ	これをクリックして、OpenManage Essentials データベースで定義されたイベントカテゴリを表示します。カテゴリを選択して、そのカテゴリ用に定義されたすべてのトラップを **トラップの編集** グリッドに表示することができます。また、カテゴリで特定のトラップに移動して選択することもできます。
トラップの編集	
Name（名前）	トラップ名を表示します。
カテゴリ名	トラップのカテゴリ名を表示します。
重大度	トラップの重大度を表示します。
フォーマット文字列	OpenManage Essentials アラートログに表示されたメッセージ文字列を表示します。
エンタープライズ OID	モニタするイベントソースのエンタープライズ OID（SNMP OID プレフィックス）を表示します。
説明	トラップの説明を表示します。
汎用トラップ ID	必要なイベントソースから、モニタする SNMP トラップの汎用トラップ ID を表示します。
固有トラップ ID	必要なイベントソースから、モニタする SNMP トラップの固有トラップ ID を表示します。
保存	クリックすると、OpenManage Essentials データベースへの変更を保存します。

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。

表 205. アラートソース

フィールド	説明
Name（名前）	新しいアラートソースの名前です（例：myFanAlert）。
タイプ	プロトコル情報です。
Catalog	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。
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

フィールド	説明
SNMP Enterprise OID	モニタ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。

MIB の管理

MIB の管理ペイン

MIB の管理 ペインは、次のビューで構成されています。

- **MIB のインポート** ビュー — MIB ファイルをインポートします。「MIB ファイルのインポート」を参照してください。
- **MIB の削除** ビュー — OpenManage Essentials データベースから MIB ファイルを削除します。「OpenManage Essentials からの MIB ファイルの削除」を参照してください。

トラップの管理 ペイン

トラップの管理 ペインは、次のビューで構成されています。

- **Custom Trap Definitions**（カスタムトラップ定義） ビュー — OpenManage Essentials データベースにトラップ定義を追加します。「トラップの追加」を参照してください。
- **ビルトインのトラップ定義のリセット** ビュー - 編集した事前定義トラップをリセットします。「トラップを元に戻す」を参照してください。

MIB のインポート

表 206. MIB のインポート

フィールド	説明
Select files for upload（アップロードするファイルを選択）	アップロードするために選択した MIB ファイルを表示します。
MIB ファイルの選択	解析用に選択されたファイルのパスを表示します。
参照	クリックすると、ファイルの場所に移動します。
イベント詳細	
カテゴリ名	選択すると、OpenManage Essentials で定義されたイベント項目名と、解析された MIB の項目名を表示します。
重大度	選択すると、OpenManage Essentials で定義された重大度を表示します。
選択されたイベントカテゴリをすべてのトラップに適用	選択すると、すべてのトラップの項目名を変更します。 **メモ: チェックボックスを選択しない場合、トラップを手動で選択し、ドロップダウンリストからカテゴリ名を選択する必要があります。**
選択された重要度をすべてのトラップに適用	このチェックボックスを選択して、すべてのトラップの重要度を変更します。

フィールド	説明
	メモ: チェックボックスを選択しない場合、トラップを手動で選択し、ドロップダウンリストから重大度を選択する必要があります。
インポート可能トラップ	
Name（名前）	MIB ファイルからのトラップ名を表示します。
カテゴリ名	トラップのカテゴリ名を表示します。
重大度	トラップの重大度を表示します。トラップの重大度は次のように変更することができます。 • 不明 • 情報 • 正常 • 警告 • 重要 • 「値による重要度設定」を参照してください。
フォーマット文字列	トラップの説明を表示します。
エンタープライズ OID	モニタするイベントソースを定義する 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）を表示します。
説明	トラップの説明を表示します。
汎用トラップ ID	必要なイベントソースから、モニタする SNMP トラップの汎用トラップ ID を表示します。
固有トラップ ID	必要なイベントソースから、モニタする SNMP トラップの固有トラップ ID を表示します。
すべてをリセット	クリックすると、すべてのトラップの重要度をデフォルト値に戻します。
トラップのインポート	クリックすると、トラップを OpenManage Essentials データベースにインポートします。

値による重要度設定

値による重要度設定 ウィンドウでは、トラップに関連付けられた 1 つまたは複数の変数バインディングの値に基づくアラートの重要度を指定することができます。

表 207. 値による重要度設定

フィールド	説明
トラップ変数	トラップの変数インデックスを表示します。
重大度	各オブジェクト値またはオブジェクト ID のに割り当てられた重要度を表示します。
オブジェクト ID	トラップの変数インデックスに基づいた数値を表示します。
オブジェクト値	トラップの変数インデックスに基づいた文字列値を表示します。
新規追加	クリックすると、重大度設定を追加します。
Select the Variable（変数の選択）	アップデートするトラップ変数を選択します。
OK	これをクリックして、変更を保存します。

フィールド	説明
リセット	クリックすると、トラップの重要度をデフォルト値に戻します。

MIB の削除

表 208. MIB の削除

フィールド	説明
インポートされた MIB	OpenManage Essentials データベースにインポートされた MIB のリストを表示します。
MIB の削除	クリックすると、OpenManage Essentials データベースからインポートされた MIB を削除します。

MIB インポートのトラブルシューティング

問題：MIB インポートで次のエラーメッセージが表示されます：`Dependent MIB files need to be imported. Please import: RFC1155-SMI to the Mib Repository before continuing to import this Mib`

原因：MIB ファイルが別の MIB ファイルに依存している可能性があります。ソース MIB ファイルの解析中は、ソース MIB ファイルが参照するすべてのファイルが、参照ディレクトリまたは MIB リポジトリに存在している必要があります。このエラーメッセージが表示されるのは、参照された MIB ファイルが参照ディレクトリにないことが原因です。

解決策：この問題を解決するには、次の手順を実行してください。

- OpenManage Essentials の管理者権限があることを確認してください。MIB ファイルをインポートする前に、少なくとも 1 回 OpenManage Essentials を起動する必要があります。
- 不足している MIB ファイルを取得し、そのファイルを参照ディレクトリに追加します。2 個以上のファイル上に親 MIB の依存が複数存在する場合、必要な MIB ファイルすべてをインポートしてから、親 MIB ファイルを解析します。

メモ: 上記の解決方法は、無効 MIB ファイルにも適用されます。

問題： MIB ファイルが解析できません。

解決策：ログを参照して、MIB コンパイラの問題がないか確認します。コンパイラの問題がない場合、標準 MIB コンパイラで MIB をコンパイルして、MIB が正しく定義されているかどうかを検証します。

問題： MIB ファイルの解析後、解析済みトラップの定義を OpenManage Essentials にインポートできません。

解決方法： C:\Program Files (x86)\Dell\MIBImport の *Readme* で、OpenManage Essentials にインポートできない MIB ファイルのリストを参照してください。

トラップの管理

カスタムトラップ定義

表 209. カスタムトラップ定義

フィールド	説明
トラップの追加	
カテゴリ名	OpenManage Essentials で定義されたイベントカテゴリ名を選択、または新しいカテゴリ名を入力します。
不明トラップ	これをクリックして、OpenManage Essentials で受信された不明トラップを表示します。
説明	トラップの説明を入力します。
トラップ名	トラップ名を入力または編集します。

フィールド	説明
汎用 ID	必要なイベントソースから、モニタする SNMP トラップの汎用トラップ ID を入力または編集します。
エンタープライズ OID	モニタするイベントソースのエンタープライズ OID（SNMP OID プレフィックス）を入力または編集します。
固有 ID	必要なイベントソースから、モニタする SNMP トラップの固有トラップ ID を入力します。
フォーマット文字列	OpenManage Essentials アラートログに表示されたメッセージ文字列を入力または編集します。
重大度	トラップの重大度を表示します。トラップの重大度は次のように変更することができます。 • 不明 • 情報 • 正常 • 警告 • 重要 • 「値による重大度設定」を参照してください。
トラップの追加	クリックすると、トラップ定義を **User-defined Trap(s)**（ユーザー定義のトラップ） グリッドに追加します。
ユーザー定義のトラップの削除	
Name（名前）	トラップ名を表示します。
カテゴリ名	トラップのカテゴリ名を表示します。
重大度	トラップの重大度を表示します。
エンタープライズ OID	モニタするイベントソースのエンタープライズ OID（SNMP OID プレフィックス）を表示します。
説明	トラップの説明を表示します。
フォーマット文字列	OpenManage Essentials アラートログに表示されたメッセージ文字列を表示します。
汎用トラップ ID	必要なイベントソースから、モニタする SNMP トラップの汎用トラップ ID を表示します。
固有トラップ ID	必要なイベントソースから、モニタする SNMP トラップの固有トラップ ID を表示します。
トラップの削除	クリックすると、選択したトラップを削除します。

ビルトインのトラップ定義のリセット

表 210. ビルトインのトラップ定義のリセット

フィールド	説明
編集されたトラップ	
Name（名前）	トラップ名を表示します。
カテゴリ名	トラップのカテゴリ名を表示します。

フィールド	説明
重大度	トラップの重大度を表示します。
エンタープライズ OID	モニタするイベントソースのエンタープライズ OID（SNMP OID プレフィックス）を表示します。
フォーマット文字列	OpenManage Essentials アラートログに表示されたメッセージ文字列を表示します。
説明	トラップの説明を表示します。
汎用トラップ ID	必要なイベントソースから、モニタする SNMP トラップの汎用トラップ ID を表示します。
固有トラップ ID	必要なイベントソースから、モニタする SNMP トラップの固有トラップ ID を表示します。
トラップを元に戻す	クリックすると、OpenManage Essentials データベースで選択されたトラップの状況を元の状態に戻します。

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: WAN 環境の OpenManage Essentials に必要な最小ネットワーク帯域幅の推奨値は、10 Mbps（監視の場合）および 20 Mbps（アップデートの場合）です。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 PowerEdge 11 世代、12 世代、13 世代のサーバ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"）。OpenManage 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には、スペースとピリオドを使用できます。システムアップデート（帯域内、OpenManage System Administrator 経由）でも、スペースとピリオドがサポートされています。帯域外アップデート（RAC デバイス経由）や RACADM などのコマンドでは、ユーザー名にスペースとピリオドを使用できません。

メモ: 導入タスクが BIOS システムパスワードで設定されているターゲットサーバで実行されている場合は、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ます。プロンプトが表示されない場合は、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。

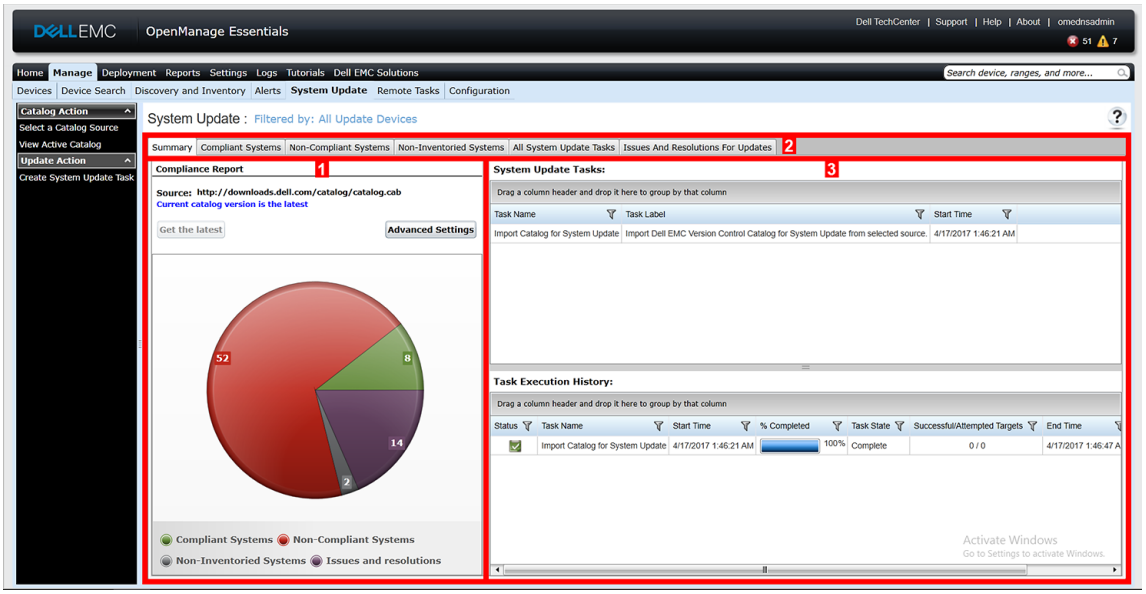

図 34. システムアップデートページ

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の理解

サーバ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** — 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ドライバおよびファームウェアを常時最新バージョンに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、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 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を管理しやすくなります。Repository Manager は独立したツールで、OpenManage Essentials インストールパッケージからインストールできます。

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。

準拠サーバーの表示

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。

非対応システムの表示

非対応サーバーを表示するには、次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。
   カタログとは異なるドライバとファームウェアバージョンを持つシステムが表示されます。

インベントリされていないシステムの表示

インベントリされていないシステムを表示するには、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、**インベントリされていないシステム** タブを選択します。
   インベントリされていないシステムが表示されます。

   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。

   メモ: インベントリされていないサーバーをインベントリするには、インベントリされていないサーバーを選択し、インベントリ をクリックします。インベントリコレクションの方法は、次の条件に基づいて異なります。

   - サーバーが SNMP を介して検出され、OMSA がインストールされていると、デフォルトの検出とインベントリが開始されます。
   - サーバーが WMI/SSH を介して検出され、OMSA がインストールされていない場合は、**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** ウィンドウが開きます。

システムの問題と解決策の表示

システムの問題と解決策を表示するには、次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、**アップデートの問題と解決策** タブを選択します。
   システムの問題と解決策が表示されます。詳細については、「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。

表 211. システムアップデート使用例シナリオ

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。

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
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。** 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	

非対応システム タブを使用した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。
- iDRAC ファームウェアのバージョンが 1.40.40 以前である場合、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:\Windows\Temp および 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 フォルダ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 を同じネットワーク上に配置することを推奨します。これらが異なるネットワークにある場合、システムアップデートタスクを正常に実行できません。iDRAC に Active Directory 認証を使用している場合は、OpenManage Essentials がインストールされているシステムと iDRAC を同じネットワークドメイン上に配置することを推奨します。

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することもできます。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の場合は、該当するすべての 64 ビットパッケージがアップデートに使用できます。コンポーネント用の 64 ビットパッケージがカタログに含まれていない場合は、対応する 32 ビットパッケージをアップデートに使用できます。
   - 帯域外アップデートの場合（iDRAC）– 選択したターゲットが第 12 世代または 13 世代 PowerEdge サーバの iDRAC で、1.40.40 より後のバージョンの iDRAC ファームウェアがインストールされている場合は、すべての該当 64 ビットパッケージがアップデートに使用できます。コンポーネント用の 64 ビットパッケージがカタログに含まれていない場合は、対応する 32 ビットパッケージをアップデートに使用できます。
   - 帯域内または帯域外のアップデートの場合 - 選択した第 12 または 13 世代 PowerEdge 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、1.40.40 より後の iDRAC のファームウェアバージョンがインストールされているときは、iDRAC のみに対して既知であり、OMSA には既知ではないパッケージがある場合を除き、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用に使用可能になります。
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. 変更内容をすぐに適用する場合は、**アップデート後は、必要であれば、ターゲットサーバを再起動** を選択します。
   帯域外の再起動タイプ オプションが表示されます。
   帯域外の再起動タイプ オプションを使用して、システムのアップデートで使用可能な再起動の方法の種類を設定できます。再起動の方法は次のとおりです。

   - **パワーサイクル**（コールド） - 電源オフにしてからシステムを再起動するには、このオプションを選択します。
   - **シャットダウンを強制しない正常再起動**（ウォーム） - ターゲットシステムの電源を強制的にオフにせずにシャットダウンしてからオペレーティングシステムを再起動するには、このオプションを選択します。
   - **シャットダウンを強制する正常再起動**（強制のあるウォーム） - ターゲットシステムの電源を強制的にオフにして、シャットダウンしてからオペレーティングシステムを再起動するには、このオプションを選択します。

   メモ: デフォルトでは、シャットダウンを強制する正常再起動 の再起動の方法が選択されます。
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. 帯域外アップデート限定 — iDRAC を使用したアップデートの実行中にエラーが発生する場合は、**Before update, reset the iDRAC**（アップデートの前に iDRAC をリセットする） を選択します。

    注意: アップデートの前に iDRAC をキャンセルする オプションが選択されている場合、アップデートが適用される前に、現在キューに入っているすべての iDRAC ジョブが削除されます。必要に応じてジョブを再度作成する必要があります。
11. ターゲットデバイスのオペレーティングシステムまたは iDRAC の管理者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に属している場合は、ドメイン管理者または管理者グループの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に属している場合でも、ターゲットシステムのローカルの、非ドメインアカウントの資格情報は入力しないでください。
- ターゲットシステムがドメインに属していない場合、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指定する場合は、そのユーザーアカウントでリモート WMI 権限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、root 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。

12. **Ｆｉｎｉｓｈ**（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。

システムアップデートタスクウィザードを使用したシステムアップデートの適用

システムアップデートタスクにより、非準拠システムとそれらの該当アップデートを表示して選択することができます。

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。
- iDRAC ファームウェアのバージョンが 1.40.40 以前である場合、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:\Windows\Temp および 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 フォルダ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 を同じネットワーク上に配置することを推奨します。これらが異なるネットワークにある場合、システムアップデートタスクを正常に実行できません。iDRAC に Active Directory 認証を使用している場合は、OpenManage Essentials がインストールされているシステムと iDRAC を同じネットワークドメイン上に配置することを推奨します。

システムアップデートタスクを作成するには、次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。
   システムアップデート ポータルが表示されます。
2. **アップデート処置** セクションで、**システムアップデートタスクの作成** をクリックします。
   システムアップデート ウィザードの **非準拠システム** ページが表示されます。
3. アップデートする非準拠システムを選択し、**次へ** をクリックします。

   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。
   - 帯域外アップデートの場合（iDRAC）- 選択したターゲットが第 12 または 13 世代 Dell PowerEdge サーバーの iDRAC で、1.40.40 より後の iDRAC のファームウェアバージョンがインストールされているときは、すべての該当 64 ビットパッケージがアップデート用に使用可能です。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用に使用できます。
   - 帯域内または帯域外のアップデートの場合 - 選択した第 12 または 13 世代 PowerEdge 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、1.40.40 より後の iDRAC のファームウェアバージョンがインストールされているときは、iDRAC のみに対して既知であり、OMSA には既知ではないパッケージがある場合を除き、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用に使用可能になります。

   該当パッケージ ページが表示されます。
4. アップデートするパッケージを選択し、**次へ** をクリックします。
   サマリと資格情報 ページが表示されます。
5. 適切なフィールドにタスクの名前を入力します。
6. **タスクスケジュールの設定** セクションで、次の手順を実行します。
   a. 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。
   b. 変更内容をすぐに適用する場合は、**アップデート後は、必要であれば、ターゲットサーバを再起動** を選択します。
   帯域外の再起動タイプ オプションが表示されます。
   帯域外の再起動タイプ オプションを使用して、システムのアップデートで使用可能な再起動の方法の種類を設定できます。再起動の方法は次のとおりです。

   - **パワーサイクル**（コールド） - 電源オフにしてからシステムを再起動するには、このオプションを選択します。
   - **シャットダウンを強制しない正常再起動**（ウォーム） - ターゲットシステムの電源を強制的にオフにせずにシャットダウンしてからオペレーティングシステムを再起動するには、このオプションを選択します。

- **シャットダウンを強制する正常再起動**（強制のあるウォーム） - ターゲットシステムの電源を強制的にオフにして、シャットダウンしてからオペレーティングシステムを再起動するには、このオプションを選択します。

メモ: デフォルトでは、シャットダウンを強制する正常再起動 の再起動の方法が選択されます。

c. 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。
d. 帯域外アップデート限定 — iDRAC を使用したアップデートの実行中にエラーが発生する場合は、**Before update, reset the iDRAC**（アップデートの前に iDRAC をリセットする） を選択します。

注意: Before update, reset the iDRAC（アップデートの前に iDRAC をキャンセルする）オプションが選択されている場合、アップデートが適用される前に、iDRAC でスケジュールされている保留中のジョブまたはアクティビティがすべてキャンセルされます。iDRAC ジョブは、必要に応じて再度作成しなければなりません。

7. **タスク実行のための資格情報入力** セクションで、iDRAC （帯域外アップデートの場合）またはオペレーティングシステム（帯域内アップデートの場合）のユーザー名とパスワードを入力します。

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。

8. **Finish**（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。

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. サーバーからのソフトウェアインベントリを収集します。「ファームウェアおよびドライバ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。「非対応システム タブを使用したシステムアップデートの適用」または「システムアップデートタスクウィザードを使用した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。
表 212. アクティブなカタログの表示

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。
表 213. 問題と解決の使用事例シナリオ

問題	解像度
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。	モジュラーサーバでサポートされている iDRAC の最小バージョンは 2.20 で、モノリシックサーバの場合は 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、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を推奨します。

ダウンロードされたファイルの自動パージの設定

ターゲットデバイスでシステムアップデートを適用する、およびリモートを実行するため、OpenManage Essentials では適切な BIOS、ファームウェア、ドライバ、およびアプリケーションファイルをダウンロードする場合があります。ダウンロードされたファイルは、デフォルトで **<install location>\Essentials\System Update** フォルダに保存されます。ダウンロードフォルダ（**<install location>\Essentials\System Update**）が定義されたサイズ制限に達した場合にダウンロードされたファイルの一部を自動的にパージするよう、OpenManage Essentials を設定することができます。

メモ: ダウンロードされたファイルのパージは、デフォルトで無効になっています。

ダウンロードされたファイルの自動パージを設定するには、次の手順を実行します。

1. **設定 → ダウンロードの設定のパージ** をクリックします。

ダウンロードの設定のパージ ページが表示されます。

2. **ダウンロード済みファイルのパージの有効化** を選択し、デフォルトの設定を使用して、ダウンロードされたファイルの自動パージを許可します。
3. 必要であれば、プリファランスに基づいて、ダウンロードフォルダーのサイズ制限を設定します。

   メモ: ダウンロードされたファイルのパージは、ダウンロードフォルダが定義されたサイズ制限に達すると開始されます。
4. 必要であれば、プリファランスに基づいて、ダウンロード済みファイルの概算サイズがパージされるよう設定します。

   メモ: ダウンロードフォルダ内のファイルは、パージされたファイルの合計サイズが定義済みの概算サイズに到達する、またはそれを超過するまでパージされます。
5. **適用** をクリックします。

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

表 214. 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。
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。

フィルタオプション	説明
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

表 215. 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、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、BIOS、ドライバ、およびアプリケーションのバージョン以降をインストールすることができます。 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。

フィールド	説明
	• 帯域内（オペレーティングシステム） – システム上のすべてのコンポーネントをアップデートすることができます。 • 帯域外（iDRAC） – BIOS、特定のファームウェア、特定のアプリケーションのみ更新することができます。 **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。** **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** を選択してアップデートした後、プリファランスを設定して、ターゲットサーバーを再起動します。このオプションが選択されている場合、**システムアップデートタスク** ウィザードに **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** が選択されています。 **メモ: システムアップデートタスク ウィザードの 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 オプションをオンまたはオフすることによって、このプリファランスを上書きすることができます。** **アップデート後は、必要に応じてターゲットサーバを再起動します** オプションが選択されている場合、**帯域外の再起動タイプ** オプションが表示されます。このオプションはデフォルトで無効に設定されています。**帯域外の再起動タイプ** オプションを使用して、システムのアップデートで使用可能な再起動の方法の種類を設定できます。再起動の方法は次のとおりです。 • **パワーサイクル**（コールド） - 電源オフにしてからシステムを再起動するには、このオプションを選択します。 • **シャットダウンを強制しない正常再起動**（ウォーム） - ターゲットシステムの電源を強制的にオフにせずにシャットダウンしてからオペレーティングシステムを再起動するには、このオプションを選択します。 • **シャットダウンを強制する正常再起動**（強制のあるウォーム） - ターゲットシステムの電源を強制的にオフにして、シャットダウンしてからオペレーティングシステムを再起動するには、このオプションを選択します。 **メモ: デフォルトでは、シャットダウンを強制する正常再起動 の再起動の方法が選択されます。**
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。
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。

フィールド	説明
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。

表 216. 準拠システム

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。
Service Tag	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。

表 217. 非準拠システム

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	システムモデル名です。例えば、PowerEdge です。
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。
Service Tag	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。

表 218. 選択したアップデートを適用

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。
タイプ	ソフトウェアアップデートの種類です。
Installed Version（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。

フィールド	説明
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

表 219. 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	システム用のソフトウェアアップデートの要件です。
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。
タイプ	ソフトウェアアップデートの種類です。
Installed Version（ 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。
再起動必須	アップデート後にシステムを再起動する必要があるかどうかを示します。
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。
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。
アップデート後は、必要であれば、ターゲットサーバーを再起動	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。
帯域外の再起動タイプ	システムアップデートで使用可能な再起動の方法の種類を表示します。 **メモ: 帯域外の再起動タイプ オプションは、アップデート後は、必要であれば、ターゲットサーバを再起動 オプションを選択した場合のみ使用できます。** 以下のオプションから、再起動の方法を選択します。 • **パワーサイクル**（コールド） - 電源オフにしてからシステムを再起動するには、このオプションを選択します。 • **シャットダウンを強制しない正常再起動**（ウォーム） - ターゲットシステムの電源を強制的にオフにせずにシャットダウンしてからオペ

フィールド	説明
	レーティングシステムを再起動するには、このオプションを選択します。 • **シャットダウンを強制する正常再起動**（強制のあるウォーム） - ターゲットシステムの電源を強制的にオフにして、シャットダウンしてからオペレーティングシステムを再起動するには、このオプションを選択します。 **メモ: デフォルトでは、シャットダウンを強制する正常再起動 の再起動の方法が選択されます。**
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。
Before update, reset the iDRAC(アップデートの前に iDRAC をリセットする)	iDRAC を使用したアップデートの実行中にエラーが発生した場合、このオプションを選択します。 **注意: このオプションを選択することによってアップデートが正常に行われる場合もありますが、iDRAC で保留されているのジョブ / アクティビティがキャンセルされる可能性もあります。**
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。

表 220. インベントリ未施行システム

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。

表 221. すべてのシステムアップデートタスク

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

表 222. 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。
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。

表 223. タスクの実行履歴

フィールド	説明
ステータス	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。 • Running（実行中） • 完了 • Stopped（停止） • Failed（失敗）

フィールド	説明
	• 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。

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。

表 224. カタログソースの選択

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 アップデートパッケージ

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、PowerEdge システム、デスクトップ、およびノートパソコン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デル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。

OpenManage Server Update Utility

OpenManage Server Update Utility（SUU）は DVD ベースのアプリケーションで、お使いのシステム用のアップデートを識別し、適用します。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 PowerEdge システム、デスクトップまたはノートパソコンに最新の 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を確実に搭載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。

表 225. アクティブなカタログの表示

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: リモートタスクを正常に実行するには最新コマンドを実行していることを確認します。

  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。
- OpenManage Server Administrator（OMSA）がインストールされていないサーバ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) でも、スペースとピリオドがサポートされています。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。

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

表 226. 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 → 8.x)	マイナーバージョンアップグレード (8.x → 8.y)
.msi	対応	対応	対応
.msp	非対応	非対応	対応
.exe **メモ: .exe パッケージを使用した OMSA の導入は、Dell Update Package (DUP) のみでサポートされます。**	非対応	対応	対応

Linux パッケージ

表 227. 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

オペレーティングシステム	パッケージ
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

表 228. 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

Upgrade (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 PowerEdge 第 12 世代以降のサーバ
- 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 フォルダ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。iDRAC サービスモジュールの導入タスクをスケジュールする日付と時間を計画することもできます。

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** を選択しタスク名を入力します。Windows ベースのサーバに iDRAC サービスモジュールを導入する場合は、**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。デバイス機能をオーバーライドしてすべての利用可能なデバイスをタスクターゲットとして選択することを許可する場合は、すべて有効にする 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. **Ｆｉｎｉｓｈ**（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

表 229. 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: .msi パッケージは、iDRAC サービスモジュールバージョン 2.0 以降の導入のみに適用できます。**	対応	対応
.exe **メモ: .exe パッケージを使用した iDRAC サービスモジュールの導入は、Dell Update Package (DUP) のみでサポートされます。**	非対応	対応

Linux パッケージ

表 230. 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	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

オペレーティングシステム	パッケージ
• SUSE Linux Enterprise Server 11 • Community Enterprise Operating System（CentOS）5.9 • CentOS 6.5	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では、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から収集します。収集されたインベントリ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識別と適用を行います。このタスクでは、次の状況下で OpenManage Essentials では利用できない、ファームウェアおよびドライバのインベントリ情報を収集できます。

- WMI または SSH プロトコルで検出されたサーバで、OpenManage Server Administrator（OMSA）がインストールされていないサーバ。
- OMSA がインストールされていない PowerEdge サーバまたは OEM サーバ。
- OMSA はインストールされているが、インベントリコレクタコンポーネントがアンインストールされている Linux 実行のサーバー。

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。

メモ: 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では、インベントリコレクタコンポーネントを使用して、ターゲットサーバからファームウェアおよびドライバのインベントリを収集します。インベントリコレクタコンポーネントは、インベントリ情報を収集するために、各ターゲットサーバに導入されます。タスクが完了すると、インベントリコレクタコンポーネントは自動的に削除されます。

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。
   - サーバが WMI / SSH プロトコルで検出され、OMSA がインストールされていない場合は、**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** をクリックします。
     1. 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。
     2. **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。

      メモ: OMSA がインストールされているターゲットデバイスは、デフォルトで タスクターゲット タブに表示されません。
   c. **OMSA ベースのターゲットの表示** を選択すると、**タスクターゲット** タブで OMSA がインストールされたターゲットデバイスも表示することができます。
   d. **OMSA ベースのターゲットを表示** を選択した場合は、**今後のソフトウェアインベントリデータの制御基準** セクションで次のいずれかを実行します。

メモ: 今後のソフトウェアインベントリデータの制御基準 オプションは、帯域内システムアップデート後に OpenManage Essentials がターゲットデバイスからファームウェアおよびドライバのインベントリ情報を収集するために使用する方法のみを指定します。ファームウェアおよびドライバタスクベースのインベントリ オプションが選択されている場合、スケジュールされた検出およびインベントリサイクルにより、OMSA ベースのインベントリ（ソフトウェアインベントリ表内の情報は除く）がターゲットデバイスから引き続き収集されます。

- **OMSA ベースのインベントリ** - これを選択して、OMSA がインストールされたターゲットデバイス上の OMSA を使用したファームウェアおよびドライバインベントリ情報の収集に戻します。

  メモ: OMSA を使用したファームウェアおよびドライバインベントリ情報の収集に戻すには、ファームウェアとドライバインベントリタスクを実行する、またはデバイスを削除して再検出する必要があります。
- **ファームウェアおよびドライバタスクベースのインベントリ** - これを選択して、デバイスに OMSA がインストールされている場合でも、インベントリコレクタコンポーネントを経由でファームウェアおよびドライバインベントリ情報を収集します。

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. **Ｆｉｎｉｓｈ**（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

インベントリコレクタコンポーネントのアップデート

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 では、インベントリコレクタコンポーネントを使用して Dell サーバからソフトウェアインベントリ情報を収集します。インベントリコレクタコンポーネントの新しいバージョンが利用可能になるときが時折あります。OpenManage Essentials のインベントリコレクタコンポーネントが最新バージョンであるかどうかは、**Dell Solutions** ポータルを介して確認できます。インベントリコレクタコンポーネントの新しいバージョンが使用可能な場合は、**アップデート** リンクが **Dell Solutions** ポータルに表示されます。

インベントリコレクタコンポーネントをアップデートするには、次の手順を実行します。

1. **Dell Solutions** をクリックします。

   Dell Solutions ポータルが表示されます。
2. **インベントリコレクタコンポーネント** 行に表示される **アップデート** リンクをクリックしてます。
3. 確認のプロンプトで **はい** をクリックします。

インベントリコレクタコンポーネントはバックグラウンドでダウンロードされます。**ホーム** ポータルの **タスクステータス** グリッドに、アップデートのステータスを表示できます。

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 XML 設定サンプル** — この使用例を有効にして、特定のサーバ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 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。
- **RACADM ロックダウンを無効にするサンプル** — この使用例を有効にして、iDRAC9 サーバのロックダウンモードを無効にします。
- **インベントリコレクタの無効化サンプル** — この使用例を有効にして、OMSA サーバのインベントリコレクタを無効にします。
- **インベントリコレクタの有効化サンプル** — この使用例を有効にして、OMSA サーバのインベントリコレクタを有効にします。

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 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とおりです。

- 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 XML 設定サンプル コマンドラインタスクでは、特定のサーバ設定を複数の管理下ノードに適用することができます。Lifecycle Controller 2 バージョン 1.2 以降を使用すると、「サーバ設定のエクスポート」操作によって、サーバの設定概要を 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 にあるホワイトペーパー『*Configuration XML Workflows*』(設定 XML ワークフロー) を参照してください。

サーバ設定概要 XML ファイルは、**サーバ 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。必須条件の詳細に関しては、DellTechCenter.com/LC にあるホワイトペーパー、『*Lifecycle Controller (LC) XML Schema Guide*』、『*Server Configuration XML File*』、および『*Configuration XML Workflows*』を参照してください。

サーバ 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 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. **Finish**（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。

表 231. 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

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 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

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	
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。

表 232. iDRAC サービスモジュールの検出要件

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。

表 233. 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

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。 **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	非対応	対応

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

表 234. 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。
Updated By (アップデート者)	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。

表 235. タスクの実行履歴

フィールド	説明
ステータス	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。 • Running（実行中） • 完了 • Stopped（停止） • Failed（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。

表 236. サーバーの電源オプション

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。 **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スタートします。** • 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
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、PowerEdge 第 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。

表 237. 導入タスク

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** • **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。

フィールド	説明
	• Linux に iDRAC サービスモジュールを導入する場合： – tar.gz、.rpm 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 サーバのみ • ADDLOCAL = SSA — Server Instrumentation のみ Linux では次のようなパラメータがあります。 • -w — Server Administrator Web サーバのみ • -d — Server Instrumentation 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。
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の導入手順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	
User Name（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。

フィールド	説明
Password (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。

表 238. コマンドラインタスク

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

表 239. 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。 • **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。

フィールド	説明
	– **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

表 240. 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 $IP です。この引数が tracert コマンドに渡されると、**タスクのターゲット** タブで選択されたサーバの IP に対して IPV4 のみの Traceroute が実行されます。実行されるコマンドは `tracert -4 10.35.0.55` になります。 詳細に関しては、「トークンについて」を参照してください。
デバイスの ping	このオプションは、デバイスにタスクを実行する前に、そのデバイスが到達可能かどうかを検証するための ping テストを実行します。このオプションは、$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。

フィールド	説明
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。 • **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** — 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。
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

表 241. 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。

フィールド	説明
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。
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** — 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	
User Name（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。
Password（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。 **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

表 242. 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。
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** — 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。

フィールド	説明
	• **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すると、OpenManage Server Administrator がインストールされていないサーバから、ファームウェアとドライバのインベントリ情報が収集されます。

表 243. 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

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。
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。
OMSA ベースのターゲットの表示	これを選択して、**タスクターゲット** タブに現在 OMSA 経由でインベントリが収集されているデバイスを表示します。
今後のソフトウェアインベントリデータの制御基準：	次のオプションから選択します。 • **OMSA ベースのインベントリ** - これを選択して、ターゲットベースからのインベントリ情報の収集に OMSA を使用します。 • **ファームウェアおよびドライバタスクベースのインベントリ** — これを選択して、ターゲットベースからのインベントリ情報の収集にインベントリコレクタコンポーネントを使用します。
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。

フィールド	説明
	• **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。
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** のアクセスおよび権限は制限付きで、OpenManage Essentials で読み取り操作を実行できます。コンソールへのログイン、検出タスクおよびインベントリタスクの実行、ビューの設定、イベントの承認ができます。Windows ユーザーグループは、このグループのメンバーです。
- **OmeAdministrators** には、OpenManage Essentials ですべての操作を実行できる権限があります。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** で、カスタムデバイスグループの作成のみ可能です。**OmeAdministrators** によりカスタムデバイスグループに割り当てられた場合に限り、カスタムデバイスグループでリモートまたはシステムアップデートタスクを作成できます。
    - 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。
  - アクセス許可があるデバイスでコンピュートプールを作成できます。
  - アクセス許可があるデバイスでベアメタルおよびステートレスな展開を実行できます。
  - アクセス許可があるコンピュートプールのみを編集、名前の変更、ロック解除、削除できます。
  - アクセス許可があるコンピュートプール内のサーバのみ交換できます。
  - アクセス許可があるコンピュートプールに含まれるデバイスからのみ ID を回収できます。

  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** と同じ権限を持っていますが、OpenManage Essentials の設定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** の順にクリックして、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. <サーバ名> を展開して、**サーバ証明書** → **サイト** の順にクリックします。
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

メモ: ポートとプロトコルの詳細については、DellTechCenter.com/OME を参照してください。

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

表 244. 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
445	SMB	TCP	なし	入力 / 出力	サーバの設定と導入
1278	HTTP	TCP	なし	入力 / 出力	ウェブ GUI：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	タスクのスケジュール
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

表 245. 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 — 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。
1311	HTTPS	TCP		入力 / 出力	コンテキスト依存アプリケーション起動 — OMSA。
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。
2463	専有	TCP	なし	OpenManage Essentials から管理ノード	PowerVault MD ストレージアレイの検出とインベントリ

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
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。
5900 - 5901	専有	TCP	なし	入力 / 出力	iDRAC 仮想メディアサービス。
5900 - 5901	専有	TCP	なし	入力 / 出力	iDRAC コンソールリダイレクト。
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、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 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 モジュラーディスクアレイ — 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、再試行、タイムアウトを使用して、リモートノードへの SNMP 接続を確認します。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。このテストを使用して、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でこの問題を解決するには、次の手順を行います。

1. 『*Systems Management Tools and Documentation DVD*』（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 PowerEdge システムの場合は、OpenManage Server Administrator がそのデバイス上にイン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ネットワークデバイス（プリンタ、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、**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する必要があります。
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. **受け入れるコミュニティ名** の下で、**パブリック**（またはカスタマイズ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、**コミュニティ名** にコミュニティ文字列を入力します。また、コミュニティ権限を **読み取り専用** または **読み取り / 書き込み**.として選択します。
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、OpenManage 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 ライセンスのある PowerEdge VRTX CMC デバイスまたは PowerEdge FX2/FX2s デバイスを WS-Man プロトコルを使用して検出した場合に限って使用できます。Enterprise ライセンスのあるデバイスが SNMP プロトコルで検出された場合は、**マップビュー** 機能は使用できません。ライセンス済みデバイス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は、WS-Man プロトコルでデバイスを再検出する必要があります。

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 ライセンスを持つ PowerEdge VRTX および PowerEdge FX2/FX2s 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 の **設定** → **一般設定** ページでプロキシを設定します。
  - 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、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に時間がかかります。

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。

- **マップの設定** に、有効なマッププロバイダキーが入力されたかどうかを確認します。
- 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 の **設定** → **一般設定** ページでプロキシを設定します。
  - 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。
- 住所の入力方法を変えてください。完全な住所も試してみてください。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す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 が管理サーバで起動されていると、マップのレンダリングが改善されます。

24

よくあるお問い合わせ（FAQ）

インストール

質問：リモート SQL データベースの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、どうすればよいですか?

回答：リモートで接続するには、名前付きインスタンスを使用する SQL Server で、**SQL Server Browser** サービスを実行する必要があります。

質問：OpenManage Essentials は、Microsoft SQL Server の評価エディションをサポートしていますか?

回答：いいえ、SQL Server の評価エディションはサポートしていません。

質問：SQL Server の最小ログインロールは何ですか?

回答：「Microsoft SQL Server の最小ログインロール」および「リレーショナルデータベース管理システムの利用規約」を参照してください。

質問：OpenManage Essentials のインストーラを起動すると、特定ライブラリのロードの失敗（例：`failed to load OMIL32.DLL`）、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。どうすればいいですか。

回答：これは、システム上のコンポーネントオブジェクトモデル（COM）のアクセス許可が十分でないことが原因です。この状況を改善するには、**support.installshield.com/kb/view.asp?articleid=Q104986** を参照してください。OpenManage Essentials のインストーラは、Systems Management Software またはその他のソフトウェア製品の以前のインストールが正常に実行されなかった場合にも失敗することがあります。Windows インストーラの一時的なレジストリ **HKLM\Software\Microsoft\Windows\CurrentVersion\Installer\InProgress** が存在する場合は、これを削除します。

質問：Microsoft ASP .NET の必須ファイルをインストールしているときに、次のエラーメッセージが表示されます。「**必須ファイルの 1 個がインストールに失敗しました。必須ファイルのワンクリックインストーラが終了します。**」どうすればいいですか。

回答：この不具合を解決するには、次の手順のいずれかを実行します。

- Windows Update を実行して、すべての更新プログラムが正常にインストールされていることを確認します。
- 必要なセキュリティ証明書をダウンロードしてインストールします。必要なセキュリティ証明書についての詳細は、**https://blogs.msdn.microsoft.com/vsnetsetup/2016/03/28/a-certificate-chain-could-not-be-built-to-a-trusted-root-authority-2/** を参照してください。

Upgrade（アップグレード）

質問：次のエラーメッセージ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?

```
Https error 503. The service is unavailable?
```

回答：この問題を解決するには、IIS のリセットを行い、OpenManage Essentials を起動します。IIS の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 サーバでホストされているウェブサイトもすべてリセットされます。

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** で『*Dell EMC OpenManage Essentials User's Guide*』（Dell EMC OpenManage Essentials ユーザーズガイド）の「**Minimum Recommended Hardware**」（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 2.1 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 2.1 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）に非対応です。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 2.1 にアップグレードする際には、次のメッセージが表示されます。

```
Dell EMC 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 2.1 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 Database re-target process*」（OpenManage Essentials データベース再ターゲットプロセス）の手順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 2.1 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 2.1 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 2.1 に移行されます。

質問：OpenManage Essentials バージョン 2.2 からバージョン 2.3 へのアップグレード後、PowerVault MD シリーズのストレージアレイの重複がデバイスツリーで確認されました。どうすればよいですか?

回答：重複したエントリを削除するには、PowerVault MD シリーズのストレージアレイを削除して再検出する作業を確実に行います。

質問：OpenManage Essentials がインストールされているサーバのオペレーティングシステムをアップグレードすることはできますか?

回答：OpenManage Essentials がインストールされているサーバのオペレーティングシステムのアップグレードは推奨されていません。アップグレードを続行すると、OpenManage Essentials が正常に動作しなくなります。オペレーティングシステムをアップグレードするには、次の手順を実行します。

1. OpenManage Essentials データベースのバックアップを作成します。
2. OpenManage Essentials をアンインストールします。詳細については、dell.com/support で OpenManage Essentials のアンインストール
3. サーバのオペレーティングシステムをアップグレードします。
4. OpenManage Essentials を再インストールし、インストール中に、先ほどバックアップしたデータベースを選択します。

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：リモートシステムから OpenManage Essentials にアクセスした場合、特定のリモートシステム上で使用できる OMSA / iDRAC サービスモジュールパッケージを使用して、リモートタスクを作成してターゲットデバイス上に OMSA/iDRAC サービスモジュールを導入することができますか?

回答：いいえ。ターゲットタスク上に OMSA / iDRAC サービスモジュールパッケージを導入するリモートタスクは、OpenManage Essentials の OpenManage Essentials をインストールまたは実行しているサーバーからアクセスして作成する必要があります。

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。

質問：「chassis power on」IPMI コマンドラインタスクに失敗しました。次のエラーが表示されます。**IPMI v2/ RMCP+ とセッションを確立することができません、シャーシ電源制御をオンに設定できません。**エラーを解決するには、何をすればよろしいですか?

回答：iDRAC では、キューに問題があるか、いくつかのタスクがある場合に、エラーが発生することがあります。iDRAC をリセットし、もう一度タスクを実行してください。

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 246. 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。 **/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** の各カスタマイズ用 CLI パラメーターを使用すると、サイレント状態で実行する際や無人で実行する際のインストール、再インストール、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。これらのカスタマイズ用パラメーターを使用すると、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すること、または別のサーバグループで、Server Administrator をインストールして Storage Management Service 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 247. ソフトウェア機能 ID

機能 ID	説明
All（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	OpenManage Server Administrator Web サーバ
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ーをコマンドラインで指定し、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、無人モード（サイレントモードではない）で 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ーをコマンドラインで指定し、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。たとえば、次のとおりです。

```
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（サイレントモードではない）で 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アンインストールされます。

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、アンインストールを行うことも選択できます。たとえば、次のとおりです。

```
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: Globally Unique Identifier (GUID) は 128 ビットの長さで、GUID の生成に使用されるアルゴリズムにより、各 GUID は固有の値になります。製品の GUID により、アプリケーションが一意に識別されます。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 248. 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 yes に設定して、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ている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、technet.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。

質問:SNMP プロトコルを使用してサーバーを検出しましたが、iDRAC の RAC 名がデバイスツリー、ポータル、およびウィザードに表示されません。

回答:RAC 名が表示されるのは、WS-Man プロトコルを使用して iDRAC を検出した場合に限られます。それ以外の場合、RAC 名ではなくシステム名が表示されます。

質問：すでに検出されているデバイスが、検出中デバイスツリーから消えるのはなぜですか？

回答:この問題は、重複する MAC アドレスが存在する場合に起こります。これは、ゼロ 16 個のみで構成される MAC アドレスを持つ仮想デバイスでよく見られます。

この問題を解決するには、次の手順を実行してください。

1. 管理者権限でシステムにログインしていることを確認します。

   メモ: 変更を加える前に、必ず dconfig.ini ファイルのバックアップコピーを作成してください。

2. SysMgt\Essentials\configuration にある dconfig.ini ファイルを開きます。
3. 次のように、PRIVATE_MAC_EXCLUDE_LIST 行を編集します。
   PRIVATE_MAC_EXCLUDE_LIST=127.0.0.1,0.0.0.0,005345000000,33506F453030,505054503030,0000FFFFFFFF,204153594EFF,000000000000,000000000000000e0,020054554e01,204153594eff,0000000000000000
4. dconfig.ini ファイルを保存し、**OpenManage Essentials** サービスを再開します。

質問：SNMP プロトコルで PowerEdge FN IO Aggregator（IOA）を検出しました。FN IOA のサービスタグがデバイスインベントリに N/A（なし）と表示されるのはなぜですか？

回答：2016 年 2 月 1 日以前に製造された FN IOA にはサービスタグがありません。そのため、サービスタグは N/A（なし）と表示されます。

質問：WS-Man プロトコルを使用してデルのデバイスを検出しようとすると、基本認証による接続が失敗したというエラーメッセージが表示されます。どうすればいいですか。

回答：この問題は、認証タイプの **基本認証** が OpenManage Essentials システムで有効になっていない場合に発生します。OpenManage Essentials システムで**基本認証**の認証タイプを有効にするには、**Microsoft.com** ナレッジベースの記事「**Authentication for Remote Connections**」（リモート接続の認証方式）を参照してください。

次に、WinRM が機能するために必要となる設定を示します。

```
>winrm get winrm/config/client

Client

NetworkDelayms = 5000

URLPrefix = wsman

AllowUnencrypted = false

Auth
```

```
Basic = true
Digest = true
Kerberos = true
Negotiate = true
Certificate = true
CredSSP = false
DefaultPorts
HTTP = 5985
HTTPS = 5986
TrustedHosts
```

質問：帯域内メソッドを使用して、PowerEdge R830 サーバを検出しました。このサーバには OMSA バージョン 8.3 もインストールされています。iDRAC および Mellanox、QLogic、Intel などのネットワークカードのソフトウェアインベントリ情報を表示できないのはなぜですか？

回答：ネットワークカードのソフトウェアインベントリ情報を取得するには、帯域外メソッドを使用して PowerEdge R830 サーバを検出するか、またはサーバに対してファームウェアおよびドライバインベントリタスクを実行する必要があります。

質問：OpenManage Essentials が、WS-Man プロトコルを使用する iDRAC または CMC の検出、インベントリ、またはステータスポーリングタスクを実行できないのはなぜですか？

回答：

1. トラブルシューティングツールを開いて、ターゲットデバイスの WS-Man テストを実行します。
2. テストの結果、デバイスで TLS 1.1 または 1.2 が有効になっていることが示された場合、OpenManage Essentials がインストールされているシステムで次の手順を実行します。
    a. Microsoft.com の KB3140245 で使用可能なアップデートをインストールして WinRM で TLS プロトコルを有効にします。
    b. 次の場所の DWORD レジストリエントリ `DefaultSecureProtocols` で、デフォルトのプロトコルを TLS 1.2 に設定します。
        - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp`
        - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp`
        - 値を **0x00000A00** に設定して TLS 1.0、TLS 1.1 および TLS 1.2 を有効にします。
    c. システムを再起動し、OpenManage Essentials でタスクを再試行します。

質問：CMC で テンプレートの作成 タスクまたは テンプレートの適用 タスクが失敗するのはなぜですか?

回答：

1. トラブルシューティングツールを開いて、ターゲットデバイスの WS-Man テストを実行します。
2. テストの結果、デバイスで TLS 1.1 または 1.2 が有効になっていることが示された場合、OpenManage Essentials がインストールされているシステムで次の手順を実行します。
    a. ウェブブラウザで TLS を有効にするには、次の手順を実行します。
        1. **スタート → ファイル名を指定して実行**の順にクリックして、`inetcpl.cpl` と入力し、Enter を押します。
        2. **詳細設定** タブをクリックします。
        3. **セキュリティ** の項で、**TLS 1.0 を使用**、**TLS 1.1 を使用**、および **TLS 1.2 を使用** を選択します。
    b. すべてのユーザーアカウントの TLS を有効にするには、次の手順を実行します。
        1. DWORD レジストリエントリ `SecureProtocols` を `[HKLM]\Software\Microsoft\Windows\CurrentVersion\Internet Settings` に作成します。
        2. 値を **0xA80** に設定して TLS 1.0、TLS 1.1 および TLS 1.2 に対するサポートを有効にします。
    c. システムを再起動し、OpenManage Essentials でタスクを再試行します。

質問：iDRAC または CMC で RACADM コマンドライン タスクが失敗するのはなぜですか?

回答：

1. トラブルシューティングツールを開いて、ターゲットデバイスの WS-Man テストを実行します。
2. テストの結果、デバイスで TLS 1.1 または 1.2 が有効になっていることが示された場合、OpenManage Essentials がインストールされているシステムで次の手順を実行します。
    a. ウェブブラウザで TLS を有効にするには、次の手順を実行します。
        1. **スタート → ファイル名を指定して実行**の順にクリックして、`inetcpl.cpl` と入力し、Enter を押します。
        2. **詳細設定** タブをクリックします。
        3. **セキュリティ** の項で、**TLS 1.0 を使用**、**TLS 1.1 を使用**、および **TLS 1.2 を使用** を選択します。
    b. すべてのユーザーアカウントの TLS を有効にするには、次の手順を実行します。
        1. DWORD レジストリエントリ `SecureProtocols` を `[HKLM]\Software\Microsoft\Windows\CurrentVersion\Internet Settings` に作成します。
        2. 値を **0xA80** に設定して TLS 1.0、TLS 1.1 および TLS 1.2 に対するサポートを有効にします。
    c. システムを再起動し、OpenManage Essentials でタスクを再試行します。

質問：デバイス名が同じでサービスタグがなしに設定されている Fibre Channel スイッチが 2 台検出されましたが、デバイスツリーにスイッチは 1 台しか表示されません。デバイスツリーに両方のデバイスが表示されるようにするにはどうすればよいですか？

回答：両方のスイッチに一意の名前を割り当ててから、再度検出します。

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。

質問：WS-Man プロトコルを使用してファームウェアバージョン 1.1 搭載の PowerEdge FX または FX2s シャーシを検出しましたが、デバイスが **システム → 非対応システム** タブに表示されず、ソフトウェアインベントリ表も表示されません。どうすればよいですか?

回答：手動（OpenManage Essentials の外部）で、PowerEdge FX または FX2s ファームウェアをバージョン 1.2 以降にアップグレードします。

質問：ESXi サーバーが **システムアップデート → インベントリされていないシステム** タブの下に表示されません。**インベントリされていないシステム** タブからインベントリタスクを実行しましたが、デバイスが引き続き **インベントリされていないシステム** タブの下に表示されます。

回答：ESXi サーバーのインベントリ情報は、サーバーのホスト名を IP アドレスに解決できない場合は取得できません。この問題を解決するには、次の手順を実行します。

1. サーバーのホスト名の ping を実行して、結果の IP アドレスを確認します。
2. IP アドレスが ESXi サーバーの IP アドレスと同じでない場合は、DNS サーバーで ESXi サーバーの IP アドレスを正しく設定します。
3. インベントリをもう一度実行します。

質問：デフォルトの WS-Man タイムアウト値および再試行値が設定された WS-Man プロトコルを使用して検出した iDRAC6 搭載のモジュラーサーバーが **RAC** デバイスグループの下に分類されます。ただし、インベントリ情報は表示されません。どうすればよいですか?

回答：検出に使用する WS-Man タイムアウトの設定を確認し、タイムアウト値が 4～99 の範囲内であるようにします。

質問：SNMP プロトコルを使用して、シャーシ内でホストされるブレードサーバーを何台か検出し、その後で **ガイド付きウィザード** の **シャーシ（CMC）検出 – すべてのコンポーネント** フィルタを使用して Dell シャーシとそのコンポーネントを検出しました。以前検出したブレードサーバーの検出範囲グループが、シャーシの検出範囲グループ内に移動されていることに気付きましたが、以前検出したブレードサーバーは今も SNMP プロトコルを使用してインベントリされています。どうすればよいですか?

回答：各ブレードサーバーを個別に検出する、またはシャーシとそのコンポーネントを **ガイド付きウィザード** の **シャーシ（CMC）検出 – すべてのコンポーネント** フィルタを使用して検出することをお勧めします。**ガイド付きウィザード** の **シャーシ（CMC）検出 – すべてのコンポーネント** フィルタを使用してシャーシを検出する前にブレードサーバーを何台か検出した場合は、次の操作を実行してください。

1. シャーシ検出範囲グループを編集します。
2. **シャーシ（CMC）検出 - すべてのコンポーネント** フィルタを選択します。
3. シャーシおよびブレードサーバー（iDRAC）の資格情報を入力します。

   メモ: iDRAC 資格情報は、iDRAC 資格情報がシャーシ資格情報と異なる場合にのみ入力します。
4. 変更を保存します。
5. シャーシ範囲グループを右クリックし、**検出とインベントリを今すぐ実行** をクリックします。

ブレードサーバーは、次回のインベントリサイクルで WS-Man 資格情報を使用するようになります。

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 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 サービスを再開し、IIS を再開してください。

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、またはリモート Dell サーバに 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：アクセス不能または劣化しているハードドライブ上でファームウェアアップデートを適用するシステムアップデートタスクを実行すると、エラーが発生します。どうすることができますか?

回答：Dell Knowledge Base 記事「How to troubleshoot hard drive and RAID controller errors on Dell PowerEdge 12G servers」（Dell PowerEdge 12G サーバーでのハードドライブおよび RAID コントローラのエラーをトラブルシューティングする方法）の「Physical Disk Failures and Rebuilds」（物理ディスクの故障と再構築）セクションにあるトラブルシューティング手順に従ってください。

質問：32 ビット Linux オペレーティングシステムを実行するシステムに該当する Dell Update Package（DUP）を適用したら、**このパッケージは 32 ビットオペレーティングシステムでの実行をサポートしません** というメッセージが表示されました。どのような理由が考えられますか?

回答：Linux 向けの DUP には、64 ビットおよび 32 ビットオペレーティングシステムの両方に適用できるパッケージが含まれている場合があります。OpenManage Essentials は、ターゲットデバイスのオペレーティングシステムに関わらず、64 ビットおよび 32 ビット両方のパッケージを該当パッケージとして表示します。このため、32 ビット Linux オペレーティングシステムを実行するデバイスで 64 ビット Linux アップデートパッケージを適用していると、このメッセージが表示される場合があります。

質問：Dell カタログをソフトウェアアップデートのためにロードするにはどうすればよいですか? 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何をすればよいですか?

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。

質問：デバイスインベントリの **データソース** テーブルに、同じエージェントの正常性が **不明** の状態の情報が追加または重複して表示されるのはなぜですか?

回答：この問題は次のような状況の場合に発生します。

- OpenManage Essentials との接続中にエージェントのデータソース情報が使用されなくなった。
- エージェントがデバイスの正常性および接続状態を判断できない。
- エージェントが到達不能か応答しない。

この問題を解決するには、デバイスを削除してから、再度そのデバイスを検出します。

デバイスグループ権限

デバイスグループ権限ポータル

質問：**OmeSiteAdministrators** 役割にユーザーグループを追加できますか?

回答 : できます。**OmeSiteAdministrators** ロールにユーザーグループを追加することができます。

質問：**OmeSiteAdministrators** 役割に OmeAdministrator を追加できますか?

回答：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処置を実行できます。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。

展開と設定コンプライアンス

質問： OmeSiteAdministrator は、**導入** および **デバイスコンプライアンス** ポータルでデバイス設定テンプレートに使用できる右クリック処置を実行できますか?

回答：はい、OmeSiteAdministrator は、**導入** および **デバイスコンプライアンス** ポータルでデバイス設定テンプレートに使用できるすべての右クリック処置を実行できます。

展開と設定コンプライアンス

質問： FQDD とは何ですか?

回答： 完全修飾デバイス記述子（FQDD）は、システム内の特定のコンポーネントを識別するために使用されます。通常、デバイス設定テンプレートには、システムの各種コンポーネントの FQDD とそれらに対応する設定値が含まれています。たとえば、iDRAC の FQDD は、iDRAC.embedded.1 として表される場合があります。複数のポートまたはパーティションを持つネットワークカード（NIC）などのコンポーネントの FQDD は、次のように表すことがあります。

- NIC.Integrated.1-2-2 は、システム基板上に統合された NIC のポート 2 のパーティション 2 を示します。
- NIC.Slot-3.1.2 は、システム基板上のスロット 3 に挿入されている NIC アダプタで使用できる、ポート 1 のパーティション 2 を示します。

質問： 導入タスクの完了後、**実行の詳細** タスクウィンドウの結果セクションに NIC のすべてのパーティションが同じ FQQD で表示されます。正しい値が導入されているかどうかは、どのように確認できますか?

回答： 属性値が複数のパーティションに導入されると、結果タブに誤った FQDD 値が表示される場合があります（具体的には、同じ FQDD が異なるパーティションに繰り返される場合があります）。ただし、正しい値はデータベースに保存されます。デバイス設定インベントリを表示して、実際の値を確認できます。

質問：サーバー（ソース）と別のサーバー（ターゲット）をコンピュートプールから交換しました。既存の警告とタスクは、ターゲットサーバーに関連付けられていますか?

回答：以下は、サーバーを交換した後の予期される動作です（ここで、ソースとは、ソースオペレーティングシステムのことを言います）。

- サーバーの交換前に作成された警告とタスクは、ソースサーバーでのみ関連付けられています。
- サーバーの交換後に作成された警告とタスクは、ターゲットサーバーでのみ関連付けられています。

質問：OpenManage Essentials が、QLogic CNA カード内で導入したとき、仮想 WWPN との WWNN の 2 つ目のオクテット値が 01 と 00 ではなく 08 と 07 に設定されました。この問題を解決する方法はありますか?

回答：以下の手順を行います。

1. すべての NIC パーティションをクリアにします。
2. サーバーを再起動します。
3. NIC のパーティションをもう一度行います。
4. 仮想 I/O 属性を使用してサーバーをもう一度導入します。

質問：サーバで設定テンプレートを導入しました。同じ設定テンプレートの一部の属性を編集して別のサーバに展開するには、何をする必要がありますか?

回答：設定テンプレートのクローンを作成し、属性を編集して、クローンされたテンプレートを別のサーバに導入することをお勧めします。

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。

表 249. ログレベル

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。 **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。

バックアップと復元

質問：OpenManage Essentials データベースのバックアップと復元後、サンプルタスクと作成したタスクのどちらも使用できません。なぜでしょうか?

回答：タスク設定データは暗号化されたフォーマットで OpenManage Essentials データベースに保存されます。バックアップと復元が実行されると、暗号化されたデータが使用不能になるため、作成したタスクのすべてを作成しなおす必要が生じます。サンプルタスクはその後も使用不能のままとなります。

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

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. **設定** → **許可** をクリックします。
   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、**OmeSiteAdministrators 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、**OmeSiteAdministrators** を右クリックし、**OmeSiteAdministrators のメンバーの編集** をクリックします。

OmeSiteAdministrators 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

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. **設定** → **許可**をクリックします。

デバイスグループの**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

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. **設定** → **許可** をクリックします。

デバイスグループの **許可** ポータルページが表示されます。

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、**OmeSiteAdministrators 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、**OmeASitedministrators** を右クリックし、**OmeSiteAdministrators のメンバーの編集** をクリックします。

   OmeSiteAdministrators 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

許可

26

OpenManage Mobile 設定

OpenManage Mobile は、お使いの Android を使用して、1 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 User's Guide』(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ステータスの表示
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。**設定** → **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、「一般設定」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、**設定** → **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、**設定** → **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、**設定** → **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ステータスの表示

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、**通知サービスステータス** 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ステータスを表示するには、**設定** → **Mobile 設定** をクリックします。

関連リンク

OpenManage Mobile 設定
通知サービスステータス

通知サービスステータス

次の表では、**設定** → **モバイル設定** ページに表示される **通知サービスステータス** についての情報を説明しています。

表 250. 通知サービスステータス

ステータスアイコン	Status Description（ステータスの説明）
	サービスが稼働しており、正常に動作しています。 **メモ: このサービスステータスは、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 **設定** → **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、**設定** → **Mobile 設定** ページに表示される **Mobile サブスクライバー** の表についての情報が説明されています。

表 251. Mobile サブスクライバー情報

フィールド	説明
Enabled（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。
ステータス	OpenManage Essentials コンソールが 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ステータスを表示します。
状態メッセージ	モバイルデバイスのステータスを表示します。
Username（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。

フィールド	説明
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	OpenManage Essentials から 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	クリックして Mobile サブスクライバーリストからサブスクライバーを削除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 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。

表 252. OpenManage Mobile のトラブルシューティング

問題	理由	解像度
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、「一般設定」の「プロキシ設定」を参照してください。
	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。
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 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 User's Guide』（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。

問題	理由	解像度
		デバイスが OpenManage Essentials に接続されていない場合は、サブスクライバーを削除します。
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

設定 - 参照

設定 ページでは、OpenManage Essentials コンソールを設定することができます。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の調整、データベースメンテナンススケジュール、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、夏時間の実施、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: 一般設定の変更後には、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

アラート設定
カスタム URL 設定
導入設定
デバイスツリーの設定
検出設定
電子メール設定
一般設定
OpenManage Mobile 設定
タスク設定
保証通知の設定
ダウンロードの設定のパージ
許可

アラート設定

表 253. 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ステータスが変化するときに、OpenManage Essentials が内部アラートを生成します。
内部接続ステータスアラートの有効化	チェックボックスを選択して内部接続ステータス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ステータスが変化するときに、OpenManage Essentials が内部アラートを生成します。
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	このチェックボックスを選択して、アラートを受け取った時のポップアップ通知の表示を有効化します。
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。
SNMP リスナ設定	
V1/V2c トラップをサポート	トラップを受信するには、Windows SNMP Trap サービスの使用オプションを選択します。
V1/V2c/V3 トラップをサポート	トラップを受信するには、専用の .NET SNMP トラップ受信ポートの使用オプションを選択します。

フィールド	説明
トラップリスニング専用ポート	SNMP トラップ受信ポートを入力します。デフォルトでは、トラップ受信専用ポートは 162 です。

カスタム URL 設定

表 254. カスタム URL 設定

フィールド	説明
Name（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。
Date Updated（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

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。

表 255. 導入設定

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。
Password（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。

デバイスツリーの設定

表 256. デバイスツリーの設定

フィールド	説明
常に RAC デバイス名を RAC グループ配下に表示	チェックボックスを選択して、デバイスツリー、ポータル、およびウィザードで iDRAC の RAC 名（RAC の DNS 名または計装名）を表示します。

フィールド	説明
	メモ: RAC 名は WS-Man プロトコルを使用して iDRAC を検出した場合にのみ表示されます。そうではない場合、RAC 名ではなくシステム名が表示されます。
デバイスツリーで接続が切断されたデバイスを確認する	チェックボックスを選択して、到達不能なデバイスに対して アイコンをデバイスツリーとポータルに表示します。

検出設定

検出設定 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することができます。**検出設定** ページに表示されるフィールドについては次の表で説明されています。

表 257. 検出設定

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。**
検出時に ICMP ping をスキップ	選択した場合、**デバイスの検出** ウィザードからは **ICMP 設定** の設定は無効になります。このオプションを選択すると、デバイスの検出とインベントリ作成、システムのアップデート、設定、および導入タスク時に ICMP ping がスキップされます。
選択されたデバイスタイプのみ検出	OpenManage Essentials 2.3 では、このオプションはデフォルトで有効に設定されています。選択した場合、ガイド付きウィザードで、このオプションによりデバイスタイプの検出が可能になります。 **メモ: 以前のバージョンの OME で検出されたデバイス範囲には、WS-MAN プロトコルを使用してシャーシと iDRAC の両方が検出されている場合があります。OpenManage Essentials 2.3 では、検出設定で 選択されたデバイスタイプのみ検出 オプションが有効である場合、ガイド付きウィザードで選択した特定のデバイスのみが検出され、その他のデバイスは不明なデバイスとして分類されます。例えば、WS-MAN プロトコルと iDRAC デバイスタイプを選択すると、WS-MAN プロトコルを使用して iDRAC デバイスのみが検出されます。**

電子メール設定

表 258. 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。

フィールド	説明
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。
Password (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。

一般設定

表 259. 一般設定

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、ステータスポーリングなど) 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。 **メモ: OpenManage Essentials サービスを再開する前に、検出、インベントリ、状態ポーリングといった他のタスクを完了することをお勧めします。**
セキュリテイ設定 (ActiveX)	
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	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。

フィールド	説明
OME サーバーの夏時間ステータス	サーバ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。
Password（パスワード）	ユーザーのプロキシパスワードです。
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。

タスク設定

表 260. タスク設定

フィールド	説明
タスクの実行履歴の設定	
保持するタスクの実行履歴レコード	タスクの実行履歴でロードするレコードの数を選択します。 **メモ: この制限を超えると、古いタスクの実行履歴レコードがパージされます。ただし、検出、インベントリ、状態ポーリング、システムアップデート用のカタログのインポート、デバイス構成インベントリ、OME 内部コンポーネントのアップデート、未検出デバイスへの設定の導入の各タスクの実行履歴レコードはパージされません。**
タスクポップアップ通知設定	
タスクポップアップ通知の有効化	このチェックボックスを選択して、タスクが完了した時のポップアップ通知の表示を有効化します。
ポップアップ通知間の時間（秒）	各タスクポップアップ通知の間の時間間隔を選択します。

保証通知の設定

次の表に、**設定** → **保証通知設定** ページに表示されるフィールドについての情報を示します。

表 261. 保証通知の設定

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なければなりません。電子メールアドレスを複数入力する場合は、アドレスをセミコロンで区切ります。
From（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。指定できる電子メールアドレスは 1 つだけです。電子メールアドレスは、有効な電子メールアドレスでなければなりません。
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めるかを決めます。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。
期限切れの保証を含む	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。
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。このフィールドのアップデートが有効になるのは、次回の保証電子メール通知が送信された後です。
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できます。電子メール通知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 ヘッダーバナーへの保証通知アイコンの表示を有効または無効にします。保証通知アイコンが表示されるのは、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**で指定されている日数以下の場合です。
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めるかを決めます。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。
期限切れの保証を含む	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が表示されるのは、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です。
保証アップデート設定	
保証アップデートを有効にする	サポートサイトで検出されたデバイスの保証情報のチェックを有効または無効にします。

フィールド	説明
保証アップデートの頻度：*x* 日	保証アップデートを継続的にチェックする間隔です。
次回の保証アップデート日：	保証アップデートが次回チェックされる日時です。このフィールドで、保証アップデートの次回のチェックを設定できます。保証情報が正常に送信された後、このフィールドは**保証アップデートの頻度：*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。

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

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。

表 262. デバイスグループ許可の管理

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。
Name（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

ダウンロードの設定のパージ

ダウンロードの設定のパージ ページでは、ダウンロードした BIOS、ファームウェア、ドライバ、およびアプリケーションのファイルの自動パージを設定できます。

次の表では、**設定** → **ダウンロードの設定のパージ** ページに表示されるフィールドの情報が説明されています。

表 263. ダウンロードの設定のパージ

フィールド	説明
ダウンロードしたファイルのパージを有効にする	OpenManage Essentials によってダウンロードされた BIOS、ファームウェア、ドライバ、またはアプリケーションのファイルのパージを許可する場合に選択します。
ダウンロードフォルダのサイズ制限（GB）	OpenManage Essentials でシステムアップデートまたはリモートタスクを適用するために必要なファイルをダウンロードする先のフォルダのサイズ制限を選択します。デフォルトでは、ダウンロードされたファイルは、<install location>\Essentials\System Update フォルダに保存されます。フォルダサイズが定義されたサイズ制限に達すると、ファイルはダウンロードフォルダ（<install location>\Essentials\System Update）から自動的にパージされます（範囲：5 GB ～ 20 GB、デフォルトでは 20 GB）。
パージされるダウンロード済みファイルの概算サイズ	パージするダウンロード済みファイルの概算サイズを選択します。ファイルは、パージされたファイルの合計サイズが定義済みの概算サイズに到達する、またはそれを超過するまでパージされます（範囲：1 GB ～ 4 GB、デフォルトでは 4 GB）。

関連リンク

ダウンロードされたファイルの自動パージの設定

28

ログ — 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

図 35. ツールバー — エクスポート

検出ログのファイルシステムへのエクスポート — 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

表 264. ユーザーインタフェースログ

フィールド	説明
Enabled（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。
Clear（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。
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

表 265. 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。
Message（メッセージ）	動作に関する情報です。

29

Dell Solutions

Dell Solutions ポータルには、OpenManage Essentials に関連付けられているその他ツールへのリンクのリストが表示されます。このページにはツールに関する情報が提供され、ツールがインストールされているかどうかを検知し、インストールされている場合にはツールを起動することができます。

メモ: 一部の拡張子は、検出に ActiveX が必要となる場合があります。ActiveX を有効にする方法については、設定 ページの「一般設定」を参照してください。

表 266. Dell Solutions

フィールド	説明
Name（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。
Action	ツールがインストール済みで ActiveX が有効されている場合、リンクが表示されます。このリンクをクリックしてツールを起動することができます。 **メモ: インベントリコレクタコンポーネントの アクション 列には、次が表示される場合があります。** • **最新** - OpenManage Essentials のインベントリコレクタコンポーネントが最新版であることを示します。 • **アップデート** - より新しいバージョンのインベントリコレクタコンポーネントが使用可能なことであることを示します。クリックして Windows と Linux の両方のインベントリコレクタコンポーネントをバックグラウンドでダウンロードします。
バージョン	ツールのファームウェアバージョンを表示します。 **メモ: インベントリコレクタコンポーネントの バージョン 列には、次が表示される場合があります。** • 最新 アイコン - OpenManage Essentials のインベントリコレクタが最新バージョンであることを示します。 • 警告アイコン - OpenManage Essentials のインベントリコレクタが最新バージョンではないことを示します。
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。

関連リンク

インベントリコレクタコンポーネントのアップデート

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

表 267. スケジュールビュー

Action	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。

表 268. アクション アイテム

処置	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。
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

表 269. デバイス状態

Action	説明
IP アドレスまたはデバイス名	デバイスの IP アドレスまたは名前を表示します。
アプリケーションの起動	これを選択して、関連するアプリケーションを起動します。
デバイス構成	• **デバイス設定インベントリの更新** - デバイスの設定インベントリを更新します。 • **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** - 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します。 • **テンプレートへの関連付け** - デバイスをデバイス設定テンプレートに関連付けます。 • **テンプレートの作成** - デバイス設定テンプレートをデバイスから作成します。 • **テンプレートの導入** - デバイスにデバイス設定テンプレートを導入します。 • **識別情報の再利用** - デバイスから導入された仮想 I/O 識別情報属性を再利用します。 • **サーバの交換** — バックアッププロファイルから本番サーバを交換します。
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 Troubleshooting Tool を起動します。Troubleshooting Tool はデフォルトで無効になっています。Troubleshooting Tool を有効にするには、「設定 - 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。

表 270. 包括範囲の管理

Action	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。**

Action	説明
<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。
Disable（ 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。
エクスポート範囲	これを選択して、エクスポート範囲を .csv ファイルとしてエクスポートします。

表示フィルタ

表 271. 表示フィルタ

Action	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

表 272. アラート

Action	説明
詳細	これを選択して、アラートの詳細を表示します。
デバイス詳細	これを選択して、デバイスの詳細を表示します。
デバイスアプリケーションの起動	これを選択して、デバイスに関連付けられたコンソールを起動します。
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

表 273. リモートタスク

Action	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

表 274. カスタム URL

Action	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

表 275. システムのアップデートタスク

Action	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

表 276. 属性タブ

Action	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。

。

テンプレート

表 277. テンプレート

Action	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。

。

コンピュートプール

再利用およびベアメタル

表 278. 再利用およびベアメタル

Action	説明
コンピュートプールの作成	コンピュートプールを作成します。

コンピュートプール

表 279. コンピュートプール

Action	説明
導入	デバイス設定テンプレートを導入します。
編集	コンピュートプールを編集します。
ロック解除	コンピュートプールのロックを解除します。
表示	コンピュートプールウィザードを表示します。
名前の変更	コンピュートプールの名前を変更します。
削除	コンピュートプールを削除します。
サーバーの交換	サーバーを同じコンピュートプール内の別のサーバーと交換します。

デバイス

表 280. デバイス

Action	説明
デバイス設定インベントリの更新	デバイスの設定インベントリを更新します。
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	現在、再利用およびベアメタルデバイスグループにあるデバイスを削除します。
テンプレートの作成	サーバーからデバイス設定テンプレートを作成します。

Action	説明
ID の回収	サーバーの仮想 I/O ID を回収します。
プールから削除する	コンピュートプールからサーバーを削除します。
サーバーの交換	サーバーを同じコンピュートプール内の別のサーバーと交換します。

仮想入出力（I/O）プール

仮想 I/O プール

表 281. 仮想 I/O プール

アクション	説明
仮想 I/O プールの作成	仮想 I/O プールを作成します。
編集	仮想 I/O プールを編集します。
表示	仮想 I / O プールウィザードを表示します。
名前の変更	仮想 I/O プールの名前を変更します。
削除	仮想 I/O プールを削除します。

ID を持つデバイス

表 282. ID を持つデバイス

アクション	説明
ID の表示	導入され、デバイスに割り当てられた仮想 I/O ID を表示します。
割り当てられた識別情報の回収	デバイスに割り当てられた仮想 I/O ID を回収します。
導入された ID の回収	デバイスの導入された仮想 I/O ID を回収します。
エクスポート	詳細を HTML、CSV、テキスト、または XML 形式でエクスポートします。

テンプレートによるコンプライアンス

表 283. テンプレートによるコンプライアンス

Action	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。

。

デバイスコンプライアンス

表 284. デバイスコンプライアンス

Action	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 セキュリティ設定
- 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 2.3 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。**DiscoveryProfile.xml** ファイルは、**C:\Program Files\Dell\SysMgt\Essentials\Tools\CLI** に配置されています。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 コマンドを使用すると、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できます。

- `-wmiPassword<secure password>`
- `-ipmiPassword<secure password>`
- `-wsmanPassword<secure password>`
- `-emcPassword<secure password>`
- `-sshPassword<secure password>`
- `-SNMPv3AuthenticationPassword<secure password>`
- `-SNMPv3EncryptionPassword<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。

<セキュアなパスワード > 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な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。このセキュアなパスワードは、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。たとえば、次のとおりです。

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">
        <SNMPV1V2CConfig Enable="True">
        <GetCommunity>public</GetCommunity>
        <SetCommunity></SetCommunity>
        </SNMPV1V2CConfig>
        <SNMPV3Config Enable="True">
        <SNMPV3Username>user1</SNMPV3Username>
        <SNMPV3AuthenticationProtocol>SHA1</SNMPV3AuthenticationProtocol>
        <SNMPV3EncryptionProtocol>AES</SNMPV3EncryptionProtocol>
        </SNMPV3Config>
        <Timeout>4</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 を検出した場合、および証書ファイルがローカルシステムにある必要があるセキュアモードを使用している場合、証書ファイルへの完全なパスを指定してください。例：c:\192.168.1.5.cer。

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、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\Dell\SysMgt\Essentials\Tools\CLI\Samples の samples 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。

表 285. RangeList.csv の例

Name（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\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\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
```