Dell EMC OpenManage Enterprise バージョン 3.7 ユーザーズ ガイド

2021 年 7 月
Rev. A00

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

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

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

目次

表

1

Dell EMC OpenManage Enterprise について

OpenManage Enterprise は、仮想アプライアンスとして提供される、システムの管理およびモニタリング用 Web アプリケーションです。これにより、エンタープライズ ネットワーク上の Dell EMC サーバー、シャーシ、ストレージ、ネットワーク スイッチについての包括的なビューが提供されます。Web 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 Enterprise には、次のような機能があります。

- データ センター環境でのデバイスの検出。
- ハードウェア インベントリーの表示と、デバイスの正常性のモニター。
- アプライアンスが受信したアラートの表示と管理、およびアラート ポリシーの設定。
- ファームウェア/ドライバーのバージョンのモニター、およびファームウェア ベースラインを用いたデバイス上のファームウェア/ドライバーのアップデートの管理。
- デバイス上でのリモート タスクの管理（電源制御など）。
- 導入テンプレートを用いたデバイス間での設定管理。
- インテリジェント ID プールを用いたデバイス間での仮想 ID の設定管理。
- 設定ベースラインを用いたデバイス間での設定逸脱の検出と修復。
- デバイスの保証情報の取得とモニター。
- 静的または動的グループへのデバイスのグループ化。
- OpenManage Enterprise ユーザーの作成および管理。

メモ:

- OpenManage Enterprise のシステム管理および監視は、企業の LAN に最適であり、WAN 経由の使用には推奨されません。
- 対応するブラウザーの詳細については、サポート サイトで入手できる『*OpenManage Enterprise サポート マトリックス*』を参照してください。

OpenManage Enterprise のセキュリティ機能には、以下のようなものがあります。

- コンソール設定へのアクセス、およびデバイスのアクションを制限するロール ベースのアクセス。
- 範囲ベースのアクセス制御を使用すると、管理者はデバイス マネージャーがアクセスおよび管理できるデバイス グループを制限することができます。
- Security-Enhanced Linux（SELinux）および内部ファイアウォールを使用した強固なアプライアンス。
- 内部データベース内の機密データの暗号化。
- アプライアンス外での暗号化通信の使用（HTTPS）。
- ファームウェアおよび設定関連のポリシーの作成と実施。
- ベアメタルサーバの設定と更新に対するプロビジョニング。

OpenManage Enterprise には、ドメインタスクベースの GUI があります。このナビゲーションは管理者とデバイス マネージャーによって主に使用されるタスクのシーケンスを考慮して設計されています。環境にデバイスを追加するときに、OpenManage Enterprise は、デバイスのプロパティを自動的に検出し、関連するデバイス グループの下に配置し、デバイスを管理できます。OpenManage Enterprise ユーザーによって実行される一般的なタスクの順番：

- OpenManage Enterprise のインストール、p. 19
- テキスト ユーザー インターフェイスの使用による OpenManage Enterprise の設定、p. 26
- 監視または管理のためのデバイスの検出、p. 39
- デバイスとデバイス グループの管理、p. 52
- OpenManage Enterprise ダッシュボードを使用したデバイスの監視、p. 36
- デバイスのグループ化、p. 52
- デバイスのファームウェアおよびドライバーの管理、p. 73
- 個々のデバイスの表示と設定、p. 65
- デバイス アラートのモニターと管理、p. 113
- デバイス保証の表示と更新、p. 132
- デバイス導入テンプレートの管理、p. 82
- デバイス設定コンプライアンスの管理、p. 105
- コンプライアンス テンプレートの管理、p. 106
- 監査ログのモニター、p. 122
- OpenManage Enterprise アプライアンス設定の管理、p. 142

- インベントリジョブを今すぐ実行する 、p. 71
- デバイス保証の管理 、p. 132
- レポート 、p. 134
- MIB ファイルの管理 、p. 139
- OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15
- OpenManage Enterprise でのディレクトリサービスの統合 、p. 150

トピック：

- 本リリースの新機能
- その他の情報
- Dell EMC へのお問い合わせ
- OpenManage Enterprise Advanced ライセンス

本リリースの新機能

- CloudIQ プラグインのサポート - デバイス グループを選択して、モニタリングのために CloudIQ にデータを送信できます。

拡張機能

- [すべてのデバイス] ページから、認証に失敗したために切断されたデバイスを表示できるようになりました。
- テキスト ユーザー インターフェイス (TUI) の機能で、アプライアンスおよびプラグイン サービスのデバッグ ログの有効化/無効化を選択できるようになりました。

その他の情報

本ガイドの他にも、次のドキュメントを利用できます。OpenManage Enterprise およびその他の関連製品についての詳細情報が記載されています。

表 1. その他の情報

文書	説明	入手先
Dell EMC OpenManage Enterprise サポート マトリックス	OpenManage Enterprise 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. [Dell OpenManage Enterprise] をクリックして、必要なバージョンの OpenManage Enterprise を選択します。 3. [ドキュメント] 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 Enterprise リリース ノート	OpenManage Enterprise の既知の問題とその回避策について記載されています。	
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 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 Enterprise および OpenManage Enterprise - Modular エディション RESTful API ガイド	Representational State Transfer (REST) API を使用した OpenManage Enterprise 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 の使用例が記載されています。	
Dell EMC OpenManage Enterprise Services (旧 SupportAssist Enterprise)ユーザーズ ガイド	OpenManage Enterprise Services 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
Dell EMC OpenManage Enterprise Power Manager	OpenManage Enterprise Power Manager 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。	https://www.dell.com/support/home/en-yu/products/software_int/software_ent_systems_mgmt/ent_sys_mgmt_power_manager

表 1. その他の情報（続き）

文書	説明	入手先
Dell EMC OpenManage Enterprise Update Manager	OpenManage Enterprise Update Manager 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。	https://www.dell.com/support/home/en-yu/products/software_int/software_ent_systems_mgmt/ent_sys_mgmt_openmanage_enterprise_update_manager
Dell EMC CloudIQ	CloudIQ 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 EMC へのお問い合わせ

メモ: インターネットに接続できない環境にある場合は、ご購入時の納品書、出荷伝票、請求書、Dell EMC 製品カタログをご覧になると、連絡先をご確認いただけます。

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

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

OpenManage Enterprise Advanced ライセンス

メモ: OpenManage Enterprise をインストールして使用するには、*OpenManage Enterprise Advanced* ライセンスは必要ありません。サーバーでのデバイス設定の導入やコンプライアンス設定の検証など、サーバーの設定管理機能を使用する場合にのみ *OpenManage Enterprise Advanced* ライセンスが必要です。このライセンスは、サーバーから導入テンプレートを作成する場合には必要ありません。

OpenManage Enterprise Advanced ライセンスは、サーバーの寿命いっぱい有効な永久ライセンスで、一度に 1 台のサーバーのサービス タグにのみバインドできます。OpenManage Enterprise は、デバイスとライセンスのリストを表示するビルトインレポートを提供します。[OpenManage Enterprise] > [監視] > [レポート] > [ライセンスレポート] の順に選択し、**実行** をクリックします。「レポートの実行 、p. 135」を参照してください。

メモ: OpenManage Enterprise 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 Enterprise Advanced* ライセンスがターゲット サーバーにインストールされていれば、サーバーのサーバー設定管理機能を使用することができます。

OpenManage Enterprise Advanced ライセンス - 対応サーバー

OpenManage Enterprise Advanced ライセンスは、次の PowerEdge サーバーに導入できます。

- ファームウェアのバージョンが iDRAC8 2.50.50.50 以降の YX3X サーバー。YX3X ファームウェア バージョンは、YX2X ハードウェアと下位互換性があり、インストールすることができます。「Dell EMC PowerEdge サーバーの汎用命名規則 、p. 179」を参照してください。
- ファームウェアのバージョンが iDRAC9 3.10.10.10 以降の YX4X サーバー。参照： Dell EMC PowerEdge サーバーの汎用命名規則 、p. 179

OpenManage Enterprise Advanced ライセンスの購入

OpenManage Enterprise Advanced ライセンスは、サーバーの購入時、または営業担当者にお問い合わせの上購入してください。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。

ライセンス情報の確認

OpenManage Enterprise にはビルトインレポートが備わっており、OpenManage Enterprise の監視対象デバイスのリスト、およびそのランセンスが表示されます。[OpenManage Enterprise] > [監視] > [レポート] > [ライセンスレポート] の順にクリックします。**実行** をクリックします。「レポートの実行 、p. 135」を参照してください。

OpenManage Enterprise Advanced 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、次の方法で確認できます。

- OpenManage Enterprise のすべてのページで、右上にある **i** シンボルをクリックして **ライセンス** をクリックします。
- **ライセンス** ダイアログボックスで、メッセージを読み、適切なリンクをクリックして、OpenManage Enterprise 関連のオープンソースのファイル、または他のオープンソースのライセンスを確認しダウンロードします。

OpenManage Enterprise でのライセンスベースの機能

OpenManage Enterprise の次の機能を使用するには、*OpenManage Enterprise Advanced* ライセンスが必要です。

- サーバー設定の導入。
- サーバー設定コンプライアンスのベースラインの作成および修正。
- ISO からの起動。
- Power Manager などの使用可能なプラグインを有効にして、アプライアンスの機能を拡張します。

メモ: iDRAC に依存する仮想コンソール サポート関数などの OpenManage Enterprise の機能にアクセスするには、iDRAC Enterprise ライセンスが必要です。詳細については、サポートサイトにある iDRAC のマニュアルを参照してください。

2

OpenManage Enterprise 内のセキュリティ機能

OpenManage Enterprise のセキュリティ機能には、以下のようなものがあります。

- ロール ベースのアクセス制御を使用すると、異なるユーザーの役割（管理者、デバイス マネージャー、ビューアー）に対して異なるデバイス管理機能を許可できます。
- 範囲ベースのアクセス制御を使用すると、管理者は、デバイス マネージャーによって管理されるデバイス グループを特定することができます。
- Security-Enhanced Linux（SELinux）および内部ファイアウォールを使用した強固なアプライアンス。
- 内部データベース内の機密データの暗号化。
- アプライアンス外での暗号化通信の使用（HTTPS）。
- 256 ビット暗号化に対応したブラウザーのみがサポートされています。詳細については、次を参照： OpenManage Enterprise の導入のための最小システム要件 、p. 19

警告: 権限のないユーザーは、Dell EMC のセキュリティ制限をスキップする OpenManage Enterprise アプライアンスへの OS レベルのアクセスを取得できます。たとえば、VMDK をセカンダリドライブとして別の Linux VM に装着してから、OS レベルのログイン資格情報を変更できるかもしれない OS パーティションアクセスを取得します。Dell EMC ではお客様に、ドライブ（画像ファイル）を暗号化して不正アクセスの難度を上げることをお勧めしています。お客様は、使用する暗号化メカニズムでファイルの復号化ができることを確認する必要もあります。適切に行わないと、デバイスが起動できなくなります。

メモ:

- ユーザー役割の変更は直ちに有効になり、影響を受けるユーザーはアクティブなセッションからログアウトされます。
- AD および LDAP ディレクトリー ユーザーをインポートし、OpenManage Enterprise の役割（管理者、デバイス マネージャー、閲覧者）のいずれかを割り当てることができます。
- デバイス管理操作を実行するには、デバイス上での適切な権限を持つアカウントが必要です。

トピック：

OpenManage Enterprise ユーザーの役割タイプ

メモ:

- AD および LDAP ディレクトリー ユーザーをインポートし、OpenManage Enterprise の役割（管理者、デバイス マネージャー、閲覧者）のいずれかを割り当てることができます。
- デバイス上で操作を実行する場合、そのデバイスの特権アカウントを必要とします。

表 2. OpenManage Enterprise ユーザーの役割タイプ

この役割を持つユーザー ...	次のユーザー権限がある
システム管理者	コンソール上で実行できるタスクのすべてに対するフルアクセス権があります。 • フルアクセス権（GUI および REST を使用）による、OpenManage Enterprise の監視対象のデバイスとグループに関連する情報の読み取り、表示、作成、編集、削除、エクスポート。 • ローカル、Microsoft Active Directory（AD）、LDAP ユーザーの作成、適切な役割の割り当て • ユーザーの有効化および無効化 • 既存のユーザーの役割の変更 • ユーザーの削除

表 2. OpenManage Enterprise ユーザーの役割タイプ（続き）

この役割を持つユーザー ...	次のユーザー権限がある
	• ユーザーパスワードの変更
デバイス マネージャー（DM）	• 管理者によって割り当てられたデバイス（範囲）上のタスク、ポリシー、その他のアクションを実行します。
閲覧者	• OpenManage Enterprise に表示された情報の確認と、レポートの実行のみが可能です。 • デフォルトでは、コンソールおよびすべてのグループへの読み取り専用アクセス権があります。 • タスクを実行、またはポリシーを作成および管理することはできません。

メモ:
- 閲覧者または DM が管理者に変更されると、完全な管理者権限を持ちます。閲覧者が DM に変更されると、閲覧者は DM と同じ権限を持ちます。
- ユーザー役割の変更は直ちに有効になり、影響を受けるユーザーはアクティブなセッションからログアウトされます。
- 監査ログは、次のときに記録されます。
  - グループが割り当てられた、またはアクセス許可が変更された。
  - ユーザーの役割が変更された。

関連情報

OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15

OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御

OpenManage Enterprise には、3 つの組み込みの役割（管理者、デバイス マネージャー、ビューアー）のユーザー権限を明確に定義するロール ベースのアクセス制御（RBAC）があります。さらに、範囲ベースのアクセス制御（SBAC）を使用すると、管理者はデバイス マネージャーがアクセスできるデバイス グループを制限することができます。次のトピックでは、RBAC 機能と SBAC 機能について説明します。

OpenManage Enterprise のロール ベースのアクセス制御（RBAC）権限

アプライアンス設定およびデバイス管理機能へのアクセスレベルを指定する役割をユーザーに割り当てます。この機能は、ロールベースのアクセス制御（RBAC）と呼ばれています。コンソールは、アクションを許可する前に、特定のアクションに必要な権限を適用します。OpenManage Enterprise でのユーザー管理の詳細については、OpenManage Enterprise ユーザーの管理 、p. 143 を参照してください。

この表は、役割ごとに有効なさまざまな権限のリストです。

表 3. OpenManage Enterprise でのロール ベースのユーザー権限

OpenManage Enterprise の機能	権限の説明	OpenManage Enterprise にアクセスするためのユーザーレベル		
		管理者	デバイス マネージャー	閲覧者
アプライアンスのセットアップ	アプライアンスの設定を含むグローバル アプライアンスの設定。	Y	無	無
セキュリティ設定	アプライアンスのセキュリティ設定	Y	無	無
アラート管理	アラート アクション/管理	Y	無	無

表 3. OpenManage Enterprise でのロール ベースのユーザー権限（続き）

OpenManage Enterprise の機能	権限の説明	OpenManage Enterprise にアクセスするためのユーザーレベル		
		管理者	デバイス マネージャー	閲覧者
ファブリック管理	ファブリック アクション/管理	Y	無	無
ネットワーク管理	ネットワーク アクション/管理	Y	無	無
グループ管理	静的および動的グループの作成、読み取り、アップデート、削除（CRUD）	Y	無	無
検出管理	検出タスクのための CRUD、検出タスクの実行	Y	無	無
インベントリー管理	インベントリー タスクのための CRUD、インベントリー タスクの実行	Y	無	無
トラップ管理	MIB のインポート、トラップの編集	Y	無	無
自動導入管理	自動導入設定操作の管理	Y	無	無
セットアップのモニタリング	アラート ポリシー、転送、SupportAssist など	Y	Y	無
電源ボタン	デバイス電源の再起動/サイクル	Y	Y	無
デバイス設定	デバイスの設定、テンプレートの適用、IO ID の管理/移行、ストレージ マッピング（ストレージ デバイス用）など	Y	Y	無
オペレーティングシステムの導入	オペレーティング システムの導入、LUN へのマッピングなど	Y	Y	無
デバイスのアップデート	デバイス ファームウェアのアップデート、アップデートされたベースラインのアプリケーションなど	Y	Y	無
テンプレートの管理	テンプレートの作成/管理	Y	Y	無
ベースラインの管理	ファームウェア/設定ベースライン ポリシーの作成/管理	Y	Y	無
電源管理	電力予算の設定	Y	Y	無
ジョブ管理	ジョブの実行/管理	Y	Y	無
レポート管理	レポートでの CRUD 操作	Y	Y	無
レポート実行	レポートの実行	Y	Y	Y
表示	すべてのデータの表示、レポートの実行/管理など	Y	Y	Y

OpenManage Enterprise の範囲ベースのアクセス制御（SBAC）

ロール ベースのアクセス制御（RBAC）機能を使用すると、管理者はユーザーの作成時に役割を割り当てることができます。役割は、アプライアンス設定およびデバイス管理機能へのアクセス レベルを決定します。範囲ベースのアクセス制御（SBAC）は、管理者がデバイス マネージャーの役割を範囲と呼ばれるデバイス グループのサブセットに制限できるようにする RBAC 機能の拡張です。

デバイス マネージャー（DM）ユーザーを作成またはアップデートする際に、管理者は、1 つまたは複数のシステム グループ、カスタム グループ、プラグイン グループに DM の操作アクセスを制限するための範囲を割り当てることができます。

管理者とビューアーの役割の範囲には制限はありません。つまり、すべてのデバイスおよびグループ エンティティへの RBAC 権限によって指定された操作アクセスが可能であることを意味します。

範囲は次のように実装できます。

1. ユーザーの作成または編集
2. DM 役割の割り当て
3. 操作アクセスを制限するための範囲の割り当て

ユーザーの管理の詳細については、OpenManage Enterprise ユーザーの管理 、p. 143 を参照してください。

割り当てられた範囲を持つデバイス マネージャー (DM) ユーザーがログインしている場合、DM はスコープされたデバイスのみを表示および管理できます。また、DM は、ジョブ、ファームウェアまたは設定テンプレートやベースライン、アラート ポリシー、プロファイルなど、対象デバイスに関連づけられたエンティティを表示および管理できます (DM はそのエンティティを作成しているか、そのエンティティの所有権が割り当てられています)。DM が作成できるエンティティの詳細については、「*OpenManage Enteprise のロール ベースのアクセス制御 (RBAC) 権限*」を参照してください。

たとえば、[設定] > [テンプレート] の順にクリックすると、DM ユーザーは、デフォルト テンプレートおよび自分が所有するカスタム テンプレートを表示できます。また、DM ユーザーは、所有するテンプレートに対する RBAC 権限によってその他のタスクを実行できます。

[設定] > [ID プール] をクリックすると、DM ユーザーは、管理者または DM ユーザーによって作成されたすべての ID を確認できます。DM は RBAC 権限によって指定されたユーザーに対してアクションを実行することもできます。ただし、DM は、DM の範囲にあるデバイスに関連づけられている ID の使用のみを表示できます。

同様に、[設定] > [VLAN プール] の順にクリックすると、管理者によって作成されたすべての VLAN が表示され、エクスポートすることができます。DM はその他の操作を実行することはできません。DM がテンプレートを所有している場合は、テンプレートを編集して VLAN ネットワークを使用できますが、VLAN ネットワークを編集することはできません。

OpenManage Enterprise では、ローカル ユーザーの作成時または AD/LDAP ユーザーのインポート時に、範囲を割り当てることができます。OIDC ユーザーの範囲の割り当ては、Open ID Connect (OIDC) プロバイダーでのみ実行できます。

ローカル ユーザー向け SBAC :

DM の役割を持つローカル ユーザーを作成または編集する際に、管理者は DM の範囲を定義する 1 つまたは複数のデバイス グループを選択できます。

たとえば、(管理者として) 「dm1」という名前の DM ユーザーを作成し、カスタム グループの下に存在するグループ *g1* を割り当てます。その後、dm1 は、*g1* 内のすべてのデバイスに対してのみ操作アクセス権を持ちます。ユーザー dm1 は、他のデバイスに関連する他のグループやエンティティにアクセスすることはできません。

さらに、SBAC を使用すると、dm1 は、同じグループ *g1* で他の DM (例 : dm2) によって作成されたエンティティを表示することもできません。つまり、DM ユーザーは、自分が所有するエンティティのみを表示できます。

たとえば、(管理者として) 別の DM ユーザー (dm2) を作成し、カスタム グループの下に存在する同じグループ *g1* を割り当てます。dm2 が *g1* でデバイスの設定テンプレート、設定ベースライン、またはプロファイルを作成した場合、dm1 はそれらのエンティティにアクセスできません。その逆も同様です。

すべてのデバイスへの範囲を持つ DM は、DM が所有するすべてのデバイスおよびグループ エンティティに対して RBAC 権限によって指定された操作アクセス権を持ちます。

AD/LDAP ユーザー向け SBAC :

管理者は、AD/LDAP グループをインポートまたは編集するときに、DM の役割を持つユーザー グループに範囲を割り当てることができます。ユーザーが DM の役割を持つ複数の AD グループのメンバーであり、各 AD グループに個別の範囲が割り当てられている場合、そのユーザーの範囲はこれらの AD グループの範囲の結合になります。

例 :

- ユーザー dm1 は、2 つの AD グループ (*RR5-Floor1-labadmins* および *RR5-Floor3-labadmins*) のメンバーです。両方の AD グループには DM の役割が割り当てられていて、AD グループの範囲の割り当ては次のようになります。*RR5-Floor1-LabAdmins* は *ptlab-servers* を取得し、*RR5-Floor3-LabAdmins* は *smdlab-servers* を取得します。DM dm1 の範囲は、*ptlab-servers* と *smdlab-servers* の結合になります。
- ユーザー dm1 は、2 つの AD グループ (*adg1* と *adg2*) のメンバーです。両方の AD グループには DM の役割が割り当てられていて、範囲の割り当ては次のようになります。*adg1* には *g1* へのアクセス権が与えられており、*adg2* には *g2* へのアクセス権が与えられています。*g1* が *g2* の上位集合である場合、dm1 の範囲は、より大きな範囲 (*g1*、すべての子グループ、およびすべてのリーフ デバイス) になります。

ユーザーが、異なる役割を持つ複数の AD グループのメンバーである場合は、より高い機能の役割が優先されます (管理者、DM、ビューアーの順)。

制限のない範囲を持つ DM は、すべてのデバイスおよびグループ エンティティに対する RBAC 権限によって指定された操作アクセス権を持ちます。

メモ: OpenManage Enterprise をバージョン 3.5 またはそれ以前のバージョンからアップグレードした後、AD/LDAP および OIDC（PingFederate または KeyCloak）デバイス マネージャーは、以前のバージョンのエンティティをすべて再作成する必要があります。これは、それらのエンティティがアップグレード後は管理者のみが使用できる状態であるためです。詳細については、https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs にあるリリース ノートを参照してください。

OIDC ユーザー向け SBAC：

OIDC ユーザーの範囲の割り当ては、OME コンソール内では発生しません。ユーザーの設定中に OIDC プロバイダーの OIDC ユーザーの範囲を割り当てることができます。ユーザーが OIDC プロバイダーの認証情報を使用してログインすると、役割と範囲の割り当てが OME に使用可能になります。ユーザーの役割と範囲の設定の詳細については OpenManage Enterprise へのロール ベースのアクセスのための PingFederate での OpenID Connect プロバイダー ポリシーの設定 、p. 155 を参照してください。

メモ: PingFederate が OIDC プロバイダーとして使用されている場合は、管理者ロールのみを使用できます。詳細については、OpenManage Enterprise へのロール ベースのアクセスのための PingFederate での OpenID Connect プロバイダー ポリシーの設定 、p. 155、および https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs にあるリリース ノートを参照してください。

所有権の移行：管理者は、所有するリソースをデバイス マネージャー（ソース）から別のデバイス マネージャーに移行することができます。たとえば、管理者は、ソース dm1 からのすべてのリソースを dm2 に移行することができます。ファームウェアおよび/または設定ベースライン、設定テンプレート、アラート ポリシー、プロファイルなどのエンティティを所有するデバイス マネージャーは、適格なソース ユーザーと見なされます。所有権の移行は、デバイス マネージャーによって所有されている、デバイス グループ（範囲）ではなく、エンティティのみを別のデバイス マネージャーに移行します。詳細については、デバイス マネージャー エンティティの所有権の移行 、p. 150 を参照してください。

関連参照文献

OpenManage Enterprise ユーザーの役割タイプ 、p. 14

3

OpenManage Enterprise のインストール

Dell EMC OpenManage Enterprise は、ハイパーバイザーにインストールしてダウンタイムを最小化するリソース管理用アプライアンスとして提供されます。初期ネットワークがテキスト ユーザー インターフェイス（TUI）でプロビジョニングされると、アプリケーション Web コンソールから仮想アプライアンスを設定することができます。コンソールバージョンを表示し、アップデートする手順については、「OpenManage Enterprise のバージョンと使用可能なプラグインの確認とアップデート 、p. 163」を参照してください。この章では、インストールの前提条件と最小要件について説明します。

メモ: 対応するブラウザーの詳細については、サポート サイトで入手できる『*OpenManage Enterprise サポート マトリックス*』を参照してください。

トピック：

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、サポート サイトおよび Dell TechCenter にある『*Dell EMC OpenManage Enterprise サポート マトリックス*』を参照してください。

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

最小推奨ハードウェア

次の表は、OpenManage Enterprise の最小推奨ハードウェアについて説明しています。

表 4. 最小推奨ハードウェア

最小推奨ハードウェア	大規模導入	小規模導入
アプライアンスで管理できるデバイスの数	最大 8000	1000
RAM	32 GB	16 GB
プロセッサ	合計 8 コア	合計 4 コア
ハードドライブ	400 GB	400 GB

OpenManage Enterprise の導入のための最小システム要件

表 5. 最小要件

項目	最小要件
対応ハイパーバイザー	• VMware vSphere バージョン： ○ vSphere ESXi 5.5 以降

表 5. 最小要件（続き）

項目	最小要件
	• 以下でサポートされている Microsoft Hyper-V： ○ Windows Server 2012 R2 以降 • 以下でサポートされている KVM： ○ Red Hat Enterprise Linux 6.5 以降
ネットワーク	OpenManage Enterprise で管理されている全デバイスの管理ネットワークにアクセスできる有効な仮想 NIC。
対応ブラウザ	• Internet Explorer（64 ビット）11 以降 • Mozilla Firefox 52 以降 • Google Chrome 58 以降 • Microsoft Edge バージョン 41.16299 以降
ユーザーインタフェース	HTML 5、JS ベース

メモ: OpenManage Enterprise の最小要件についての最新アップデート情報については、サポート サイトにある『*Dell EMC OpenManage Enterprise サポート マトリックス*』を参照してください。

VMware vSphere での OpenManage Enterprise の導入

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。「OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15」を参照してください。

メモ: 始めてアプライアンスの電源を入れる前にセカンダリー アダプターを追加すると、そのアダプターは IPv4 も IPv6 も無効と設定されます。TUI へのログイン時に EULA に同意して管理者パスワードを変更すると、アダプターは [**無効**] と表示されるため、手動で設定を行う必要があります。

1. サポート サイトから `openmanage_enterprise_ovf_format.zip` ファイルをダウンロードして、VMware vSphere クライアントがアクセスできる場所に解凍します。ローカルドライブまたは CD/DVD の使用をお勧めします。ネットワークの場所からインストールすると、最大 30 分かかることがあるからです。
2. vSphere Client で、[ファイル] > [OVF テンプレートの展開] の順に選択します。
   [OVF テンプレートの導入ウィザード] が表示されます。
3. [ソース] ページで、[参照] をクリックし、OVF パッケージを選択します。[[次へ]] をクリックします。
4. [OVF テンプレートの詳細] ページで、表示される情報を確認します。[[次へ]] をクリックします。
5. [エンドユーザーライセンス契約] ページで、ライセンス契約内容を読み、[同意します] をクリックします。続行するには、[次へ] をクリックします。
6. [名前と場所] ページで、80 文字以内で名前を入力し、テンプレートを保存するためのインベントリの場所を選択します。[[次へ]] をクリックします。
7. vCenter の設定に応じて、次のいずれかのオプションが表示されます。
   - [リソースプールが設定されている場合] — [リソースプール] ページで、アプライアンス仮想マシンを展開する仮想サーバのプールを選択します。
   - [リソースプールが設定されていない場合] — [ホスト/クラスタ] ページで、アプライアンス仮想マシンの展開先となるホストまたはクラスタを選択します。
8. ホスト上に使用可能なデータストアが複数ある場合、[データストア] ページにそれらのデータストアが表示されます。仮想マシン（VM）ファイルを格納する場所を選択し、[次へ] をクリックします。
9. [[ディスクの形式]] ページで [[シック プロビジョン]] をクリックして、ドライブの作成時に仮想マシンへ物理ストレージスペースを事前に割り当てます。
10. [完了の準備] ページで、前のページで選択したオプションを確認し、[終了] をクリックして展開ジョブを実行します。
    完了ステータスウィンドウが表示され、ジョブの進捗状況を追跡できます。

Hyper-V 2012 R2 以前のホストへの OpenManage Enterprise の導入

メモ:
- OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。参照先 OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15
- 始めてアプライアンスの電源を入れる前にセカンダリー アダプターを追加すると、そのアダプターは IPv4 も IPv6 も無効と設定されます。TUI へのログイン時に EULA に同意して管理者パスワードを変更すると、アダプターは [**無効**] と表示されるため、手動で設定を行う必要があります。
- Hyper-V でアプライアンスをインストールまたはアップグレードした後は、アプライアンスの電源を切り、標準ネットワーク アダプターを外してレガシー ネットワーク アダプターを追加してから、アプライアンスの電源を入れます。

1. サポート サイトから、**openmanage_enterprise_vhd_format.zip** ファイルをダウンロードします。ファイルを解凍し、OpenManage Enterprise 仮想ドライブを格納するシステムの適切な場所に、解凍した VHD ファイルを移動またはコピーします。
2. Windows Server 2012 R2 以前のバージョンで、**Hyper-V Manager** を起動します。Windows Hyper-V が Hyper-V マネージャーの下に表示されます。表示されない場合は、**Hyper-V マネージャ** を右クリックし、**サーバに接続** を選択します。
3. [操作] > [新規] > [仮想マシン] の順にクリックして、**新規仮想マシン ウィザード**を開始します。
4. [**作業を開始する前に**] ページで、[次へ] をクリックします。
5. [**名前と場所の指定**] ページで、
   - [仮想マシン名] を入力します。
   - (オプション)[別の場所に仮想マシンを格納する] チェック ボックスにチェックを入れて [場所] フィールドを表示し、VM の保存先フォルダーの場所を参照/移動して指定します。

   メモ: チェック ボックスにチェックを入れないと、VM はデフォルト フォルダーに格納されます。
6. [次へ] をクリックします。
7. [**世代を指定**] タブで、[**第 1 世代**] を選択して [次へ] をクリックします。

   メモ: OpenManage Enterprise は 第 2 世代 をサポートしていません。
8. [**メモリーを割り当てる**] ページで [スタートアップ メモリー] フィールドにスタートアップ メモリーを入力して、[次へ] をクリックします。

   メモ: 16,000 MB (16 GB) 以上割り当てるようにします。
9. [**ネットワーク設定**] ページの [接続] ドロップダウン リストで、ネットワーク アダプターを選択します。**仮想スイッチ**がネットワークに接続されていることを確認してください。[次へ] をクリックします。

   メモ: [**接続されていません**] に設定されていると、最初の再起動時に OME が正しく機能しません。この状況が再発する場合は、再導入する必要があります。
10. [**仮想ハードディスクの接続**] ページで [**既存の仮想ディスクドライブを使用**] を選択し、**ステップ 1** の手順でコピーした VHD ファイルがある場所に移動します。[次へ] をクリックします。
11. 画面の指示に従います。

    メモ: ストレージ サイズは 20 GB 以上あるようにしてください。
12. 新たに作成した VM の [設定] を開いて、VM の電源をオンにします。
13. TUI 画面で、EULA に同意すると、アプライアンスのパスワード変更と、アプライアンスの IP へのネットワーク パラメーターの設定を求められるので、変更および設定を行います。

Hyper-V 2016 ホストへの OpenManage Enterprise の導入

メモ:
- OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。参照 : OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15

- 始めてアプライアンスの電源を入れる前にセカンダリー アダプターを追加すると、そのアダプターは IPv4 も IPv6 も無効と設定されます。TUI へのログイン時に EULA に同意して管理者パスワードを変更すると、アダプターは [**無効**] と表示されるため、手動で設定を行う必要があります。
- Hyper-V でアプライアンスをインストールまたはアップグレードした後は、アプライアンスの電源を切り、標準ネットワーク アダプターを外してレガシー ネットワーク アダプターを追加してから、アプライアンスの電源を入れます。

1. サポート サイトから **openmanage_enterprise_vhd_format.zip** ファイルをダウンロードします。ファイルを解凍し、OpenManage Enterprise 仮想ドライブを格納するシステムの適切な場所に、解凍した VHD ファイルを移動またはコピーします。
2. Windows Server 2016 で、**Hyper-V Manager を開始します。** Windows Hyper-V が Hyper-V マネージャーの下に表示されます。表示されない場合は、**Hyper-V マネージャ** を右クリックし、**サーバに接続** を選択します。
3. [操作] > [新規] > [仮想マシン] の順にクリックして、**新規仮想マシン ウィザード**を開始します。
4. [**作業を開始する前に**] ページで、 [次へ] をクリックします。
5. [**名前と場所] ページで、**
   - [仮想マシン名] を入力します。
   - (オプション) [別の場所に仮想マシンを格納する] チェック ボックスにチェックを入れて [場所] フィールドを表示し、VM の保存先フォルダーの場所を参照/移動して指定します。

   メモ: チェック ボックスにチェックを入れないと、VM はデフォルト フォルダーに格納されます。
6. [次へ] をクリックします。
7. [**世代を指定**] タブで、[**第 1 世代**] を選択して [次へ] をクリックします。

   メモ: OpenManage Enterprise は 第 2 世代 をサポートしていません。
8. [**メモリーを割り当てる**] ページで [スタートアップ メモリー] フィールドにスタートアップ メモリーを入力して、 [次へ] をクリックします。

   メモ: 16,000 MB (16 GB) 以上割り当てるようにします。
9. [**ネットワーク設定**] ページの [接続] ドロップダウン リストで、ネットワーク アダプターを選択します。**仮想スイッチ**がネットワークに接続されていることを確認してください。[次へ] をクリックします。

   メモ: [**接続されていません**] に設定されていると、最初の再起動時に OME が正しく機能しません。この状況が再発する場合は、再導入する必要があります。
10. [**仮想ハードディスクの接続**] ページで [**既存の仮想ディスクドライブを使用**] を選択し、**ステップ 1** の手順でコピーした VHD ファイルがある場所に移動します。[次へ] をクリックします。
11. 画面の指示に従います。

    メモ: ストレージ サイズは 20 GB 以上あるようにしてください。
12. 新たに作成した VM の [設定] を開いて、VM の電源をオンにします。
13. TUI 画面で、EULA に同意すると、アプライアンスのパスワード変更と、アプライアンスの IP へのネットワーク パラメーターの設定を求められるので、変更および設定を行います。

Hyper-V 2019 ホストへの OpenManage Enterprise の導入

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。参照 : OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15
- 始めてアプライアンスの電源を入れる前にセカンダリー アダプターを追加すると、そのアダプターは IPv4 も IPv6 も無効と設定されます。TUI へのログイン時に EULA に同意して管理者パスワードを変更すると、アダプターは [**無効**] と表示されるため、手動で設定を行う必要があります。
- Hyper-V でアプライアンスをインストールまたはアップグレードした後は、アプライアンスの電源を切り、標準ネットワーク アダプターを外してレガシー ネットワーク アダプターを追加してから、アプライアンスの電源を入れます。

1. サポート サイトから、**openmanage_enterprise_vhd_format.zip** ファイルをダウンロードします。ファイルを解凍し、OpenManage Enterprise 仮想ドライブを格納するシステムの適切な場所に、解凍した VHD ファイルを移動またはコピーします。
2. Windows Server 2019 で、**Hyper-V Manager を開始します。** Windows Hyper-V が Hyper-V マネージャーの下に表示されます。表示されない場合は、**Hyper-V マネージャ** を右クリックし、**サーバに接続** を選択します。
3. [操作] > [新規] > [仮想マシン] の順にクリックして、**新規仮想マシン ウィザード**を開始します。

4. [**作業を開始する前に**] ページで、 [次へ] をクリックします。
5. [**名前と場所] ページで、**
   - [仮想マシン名] を入力します。
   - （オプション ）[別の場所に仮想マシンを格納する] チェック ボックスにチェックを入れて [場所] フィールドを表示し、VM の保存先フォルダーの場所を参照/移動して指定します。

   メモ: チェック ボックスにチェックを入れないと、VM はデフォルト フォルダーに格納されます。
6. [次へ] をクリックします。
7. [**世代を指定**] タブで、[**第 1 世代**] を選択して [次へ] をクリックします。

   メモ: OpenManage Enterprise は 第 2 世代 をサポートしていません。
8. [**メモリーを割り当てる**] ページで [スタートアップ メモリー] フィールドにスタートアップ メモリーを入力して、 [次へ] をクリックします。

   メモ: 16,000 MB (16 GB) 以上割り当てるようにします。
9. [**ネットワーク設定**] ページの [接続] ドロップダウン リストで、ネットワーク アダプターを選択します。**仮想スイッチ**がネットワークに接続されていることを確認してください。[次へ] をクリックします。

   メモ: [**接続されていません**] に設定されていると、最初の再起動時に OME が正しく機能しません。この状況が再発する場合は、再導入する必要があります。
10. [**仮想ハードディスクの接続**] ページで [**既存の仮想ディスクドライブを使用**] を選択し、**ステップ 1** の手順でコピーした VHD ファイルがある場所に移動します。[次へ] をクリックします。
11. 画面の指示に従います。

    メモ: ストレージ サイズは 20 GB 以上あるようにしてください。
12. 新たに作成した VM の [設定] を開いて、VM の電源をオンにします。
13. TUI 画面で、EULA に同意すると、アプライアンスのパスワード変更と、アプライアンスの IP へのネットワーク パラメーターの設定を求められるので、変更および設定を行います。

カーネルベースの仮想マシンを使用した OpenManage Enterprise の導入

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。参照先 : OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15
- 始めてアプライアンスの電源を入れる前にセカンダリー アダプターを追加すると、そのアダプターは IPv4 も IPv6 も無効と設定されます。TUI へのログイン時に EULA に同意して管理者パスワードを変更すると、アダプターは [**無効**] と表示されるため、手動で設定を行う必要があります。

1. オペレーティングシステムのインストール中に、必要な仮想化パッケージをインストールします。
2. サポート サイトから `openmanage_enterprise_kvm_format.zip` ファイルをダウンロードします。お使いのシステムの OpenManage Enterprise 仮想ドライブを格納する場所に、ファイルを解凍します。
3. 仮想マシンを起動し、[ファイル] > [プロパティ] の順に選択します。
4. [ネットワークインタフェース] ページで、[追加] をクリックします。
5. インタフェースタイプとして **ブリッジ** を選択し、[進む] をクリックします。
6. 開始モードを **オンブート** に設定し [今すぐアクティブ化する] チェックボックスをオンにします。
7. リストからブリッジ設定するインタフェースを選択し、プロパティがホストデバイスと一致していることを確認して、[終了] をクリックします。
   仮想インタフェースが作成され、端末を使用してファイアウォールの設定を行うことができます。
8. Virtual Machine Manager で、[ファイル] > [新規] の順にクリックします。
9. VM の名前を入力し [既存のディスクイメージをインポート] オプションを選択して、[進む] をクリックします。
10. ファイルシステムを検索し、手順 1 でダウンロードした QCOW2 ファイルを選択して、[進む] をクリックします。
11. メモリに 16 GB を割り当て、プロセッサコアを 2 つ選択して、[進む] をクリックします。
12. VM に必要なディスク容量を割り当て、[進む] をクリックします。
13. [詳細オプション] で、ブリッジ接続されたホストデバイスネットワークが選択され、KVM が仮想化タイプとして選択されていることを確認します。

14. [終了] をクリックします。
OpenManage Enterprise アプライアンスが KVM を使用して導入されるようになりました。OpenManage Enterprise を開始するには「OpenManage Enterprise へのログイン 、p. 26」を参照してください。

OpenManage Enterprise のプログラムからの導入

OpenManage Enterprise は、VMware ESXi バージョン 6.5 以降、プログラムから導入 (スクリプトを使用) することができます。

メモ: プログラム/スクリプトによる導入は、プライマリー インターフェイスを使用している場合にのみサポートされます。

メモ: 始めてアプライアンスの電源を入れる前にセカンダリー アダプターを追加すると、そのアダプターは IPv4 も IPv6 も無効と設定されます。TUI へのログイン時に EULA に同意して管理者パスワードを変更すると、アダプターは [**無効**] と表示されるため、手動で設定を行う必要があります。

メモ: プログラムからの導入を行うには、OVF ツールの最新バージョンと Python 3.0 以降が必要です。

プログラムから OpenManage Enterprise を導入するには、次の手順を実行します。

1. `openmanage_enterprise_ovf_format.zip` ファイルをダウンロードして解凍するか、あるいはサポート サイトから次の OVF ファイルを個別にダウンロードします。
   - `openmanage_enterprise.x86_64-0.0.1-disk1.vmdk`
   - `openmanage_enterprise.x86_64-0.0.1.mf`
   - `openmanage_enterprise.x86_64-0.0.1.ovf`
   - `openmanage_enterprise.x86_64-0.0.1.vmx`
   - `ovf_properties.config`
   - `update_ovf_property.py`
2. `ovf_properties.config` ファイルを開いて、次のパラメーターを設定します。

表 6. `ovf_properties.config` で使用されるパラメーター

パラメータ	許容値	説明
bEULATxt	true または false	この値を true に設定すると、エンドユーザー ライセンス契約 (EULA) の条件に同意したことになります。EULA は、ovf_properties.config ファイルの末尾にあります。
adminPassword	大文字、小文字、数字、特殊記号が少なくとも 1 文字ずつ含まれている必要があります。例 : Dell123$	OpenManage Enterprise 用の新しい管理者パスワードを入力します。
bEnableDHCP	true または false	アプライアンスで IPv4 DHCP を有効にして、静的 IPv4 を無視するようにする場合は true に設定します。
bEnableIpv6AutoConfig	true または false	アプライアンスで IPv6 自動設定を有効にして、静的 IPv6 を無視する場合は true に設定します。
staticIP	CIDR フォーマットの静的 IP	IPv4 または IPv6 を指定します。(IPv4 と IPv6 の 2 つのタイプを同時に設定することはできません。)
gateway	IPv4 または IPv6	静的ゲートウェイを、IPv4 と IPv6 の両方に同時に設定することはできません。

3. `update_ovf_property.py` スクリプトを実行します。
このスクリプトは、ovf_properties.config ファイルに設定された値に基づいて導入を行うために、`openmanage_enterprise.x86_64-0.0.1.ovf` ファイルを変更します。スクリプトの実行が終了すると、ovftool コマンドのサンプルが表示されます。そこには`<DATASTORE>`, `<user>`, `<password>`, `<IP address>`などのタグが含まれており、導入環境に合わせて置き換える必要があります。この設定により、ターゲット ESXi システム上で使用するリソースと、ターゲット システムの認証情報および IP アドレスが定義されます。

メモ: <および>記号で囲まれたタグはすべて置き換えるようにしてください。

4. 前のステップで変更した ovftool コマンドを実行します。

   メモ: プログラムから導入する場合は、ovftool コマンドに「--X:injectOvfEnv」および「--powerOn」フラグを付けて実行する必要があります。

   ovftool コマンドの実行後、マニフェストが検証されて、導入が開始されます。

4

OpenManage Enterprise をお使いになる前に

トピック：

OpenManage Enterprise へのログイン

テキスト ユーザー インターフェイス（TUI）を介して最初にシステムを起動するときは、EULA に同意し、管理者パスワードを変更するように要求されます。はじめて OpenManage Enterprise にログインする場合、TUI を介してユーザー資格情報を設定する必要があります。テキスト ユーザー インターフェイスの使用による OpenManage Enterprise の設定 、p. 26 を参照してください。

注意: 管理者パスワードを忘れた場合は、OpenManage Enterprise アプライアンスからリカバリすることはできません。

1. サポートされているブラウザーを起動します。
2. [アドレス] ボックスに OpenManage Enterprise アプライアンスの IP アドレスを入力します。

   ログイン ページには、OpenManage Enterprise のロゴと、「PC にアクセスすることで、このようなアクセスが組織のセキュリティ ポリシーに準拠していることを確認します」というセキュリティ通知が表示されます。このセキュリティ通知は、API を使用して管理者がカスタマイズできます。詳細については、『OpenManage Enterprise API ガイド』を参照してください。
3. ログイン認証情報を入力し、[ログイン] をクリックします。

   メモ: デフォルトのユーザー名は `admin` です。

OpenManage Enterprise に初めてログインする場合、[OpenManage Enterprise へようこそ] ページが表示されます。[初期設定] をクリックして、基本設定のセットアップを完了します。OpenManage Enterprise の設定 、p. 30 を参照してください。デバイスを検出するには、[デバイスの検出] をクリックしてください。

メモ: デフォルトでは、ログイン試行に 3 回失敗した後に、OpenManage Enterprise アカウントがロックされ、アカウントのロックアウト期間が経過するまでログインすることはできません。アカウントのロックアウト期間は、デフォルトでは 900 秒です。この期間を変更するには、「ログインセキュリティのプロパティの設定 、p. 160」を参照してください。

テキスト ユーザー インターフェイスの使用による OpenManage Enterprise の設定

テキスト ユーザー インターフェイス（TUI）ツールを用いることで、管理者パスワードの変更、アプライアンスのステータスとネットワーク設定の表示、ネットワーク パラメーターの設定、フィールド サービス デバッグ要求の有効化、プライマリー ネットワークの選択、ネットワーク内のサーバーの自動検出に関するアプライアンスの構成が、テキスト インターフェイス形式で行えます。

TUI から初めてシステムを起動すると、エンド ユーザー ライセンス契約（EULA）に同意するよう求められます。次に、管理者パスワードを変更し、アプライアンスのネットワーク パラメーターを構成してから、対応ブラウザーに Web コンソールを読み込んで開始します。OpenManage Enterprise の構成は、OpenManage の Administrator 権限を持つユーザーのみが行えます。

TUI インターフェイスで、TUI 上の次のオプションに移動するには矢印キーを使用するか [Tab] を押し、前のオプションに戻るには [Shift + Tab] を押します。[Enter] を押してオプションを選択します。[スペース] バーでチェック ボックスのステータスを切り替えます。

メモ:

- IPv6 を設定する場合は、vCenter サーバで設定済みであることを確認してください。

- デフォルトでは、デバイスの最後に検出された IP は、すべての操作を実行するために OpenManage Enterprise によって使用されます。IP の変更を有効にするには、デバイスを再検出する必要があります。

これで OpenManage Enterprise を TUI で設定できるようになります。TUI 画面には次のオプションが表示されます。

表 7. テキスト ユーザー インターフェイス オプション

オプション	説明
[管理者パスワードの変更]	[管理者パスワードの変更] 画面では、新しいパスワードの入力と、パスワードの確認ができます。 初回は、TUI 画面を使用してパスワードを変更する必要があります。
[現在のアプライアンスステータスを表示する]	[現在のアプライアンス ステータスの表示] を選択すると、アプライアンスの URL とステータスが表示されます。タスク実行、イベント処理、Tomcat、データベース、モニタリング サービスのステータスを表示させることもできます。
[現在のネットワーク設定を表示する]	[現在のネットワーク設定を表示] を選択すると、IP 設定の詳細情報を確認できます。 [**ネットワーク アダプターを選択**] メニューには、使用可能なネットワーク アダプターのすべてが一覧表示されます。いずれかのネットワーク アダプターをクリックすると、現在の設定が表示されます。
[アプライアンス ホスト名の設定]	[アプライアンス ホスト名の設定] を選択して、DNS のアプライアンス ホスト名を設定します。このフィールドは、ホスト名として有効な次の文字をサポートしています：英数字（a ~ z、A ~ Z、0 ~ 9）、ピリオド（.）、ダッシュ（-）。 **メモ:** ピリオドの使用は、ドメイン名情報を指定します。ドメインの詳細を DHCP から取得するのではなく、静的にアプライアンスの DNS 情報を設定する場合は、ドメインの検索情報が入力されるように、完全修飾ドメイン名（FQDN）を用いてホスト名を設定する必要があります。
[ネットワークパラメータを設定する]	[ネットワーク パラメーターの設定] を選択すると、ネットワーク アダプターを再構成できます。 [**ネットワーク アダプターの選択**] メニューに、使用可能なすべてのネットワーク アダプターが一覧表示されます。ネットワーク アダプターを選択し、そのネットワーク パラメーターを再設定して [**適用**] を選択すると、変更が適切なインターフェイスに保存されます。 デフォルトでは、プライマリー ネットワーク インターフェイスでは IPv4 のみが有効になっており、アプライアンスではプライベートの静的 IP が使用されます。ただし、新しいネットワーク インターフェイスが追加されていると、IPv4 と IPv6 の両方がマルチホーミング用に有効になります。 OpenManage Enterprise アプライアンスが IPv6 アドレスの取得に失敗した場合は、ルータ広告に対してマネージドビット（M）がオンになるように環境が設定されているかどうかを確認します。現在の Linux ディストリビューションからのネットワーク マネージャでは、このビットがオンになっていても、DHCPv6 が利用できない場合にリンク障害が発生します。DHCPv6 がネットワーク上で有効になっていること、またはルータ広告に対して管理フラグが無効になっていることを確認します。 **メモ:** • DNS 設定を利用できるのは、プライマリー ネットワーク インターフェイスだけです。このインターフェイスで DNS 解決が必要な場合は、プライマリー インターフ

表 7. テキスト ユーザー インターフェイス オプション（続き）

オプション	説明
	ェイスで設定された DNS サーバーによってすべてのホスト名が解決できる必要があります。
[プライマリー ネットワーク インターフェイスを選択]	[プライマリー ネットワーク インターフェイスを選択] では、プライマリー ネットワークを指定できます。 プライマリー インターフェイスを選択すると、ルーティングで選択されたインターフェイスが優先され、デフォルト ルートとして使用されます。あいまいな場合、このインターフェイスはルーティングを優先します。プライマリー インターフェイスは「パブリック フェーシング」インターフェイスとして企業ネットワーク/インターネット接続に使用されることも想定されています。プライマリー インターフェイスにはさまざまなファイアウォール ルールが適用されるため、IP 範囲によるアクセス制限など厳格なアクセス制御の実施が可能です。 **メモ:** マルチホーミングが有効になっている場合、2 つのネットワークからアプライアンスにアクセスできます。この場合、プライマリー インターフェイスは、すべての外部通信に対して、またプロキシ設定が使用される場合に、アプライアンスによって使用されます。OpenManage でのマルチホーミングの詳細については、サポート サイトの *Dell EMC OpenManage Enterprise* テクニカル ホワイト ペーパーを参照してください。
[固定ルートを設定]	[固定ルートを設定] は、IPv4 および IPv6 ネットワークで特定のサブネットにアクセスするためにネットワークに固定ルートを設定する必要がある場合に選択します。 **メモ:** インターフェイスごとに最大 20 の固定ルートがサポートされます。
[サーバーから開始される検出の構成]	[サーバーから開始される検出の構成] を選択すると、構成されている DNS サーバーに対して必要なレコードをアプライアンスが自動的に登録できるようになります。 **メモ:** • アプライアンスについて、DNS に登録されていることおよび、レコードの動的アップデートができることを確認します。 • ターゲット システムの構成については、登録の詳細を DNS から要求できる必要があります。 • DNS ドメイン名を変更する場合は、DNS サーバでダイナミック DNS 登録が有効になっていることを確認します。また、アプライアンスを DNS サーバに登録する場合は、ダイナミックアップデートで [非セキュアおよびセキュア] オプションを選択します。
[アプライアンスのディスク サイズの設定]	[アプライアンスのディスク サイズの設定] を選択してディスク容量または新しいディスクの可用性をスキャンし、必要に応じて、アプライアンスに追加のディスク容量またはディスクを割り当てます。 **メモ:** • ディスク構成の変更を適用する前に、コンソールの仮想マシン スナップショットをバックアップとして作成することを強くお勧めします。 • ディスク領域の追加後、拡張されたディスク領域の削除または縮小はサポートされていません。新たに追加されたディスクを削除したり、既存のディスクのサイズの

表 7. テキスト ユーザー インターフェイス オプション（続き）

オプション	説明
	増加を元に戻したりするには、前の VM スナップショットに戻す必要があります。 • 初期スキャンで未割り当て容量が検出されない場合は、ハイパーバイザーのコンソールに追加のディスク容量またはディスクを割り当て、再スキャンします。 • ディスク容量のスキャンと割り当ては、最大 4 台のディスクに制限されています。
[フィールドサービスデバッグ（FSD）モードを有効にする]	[フィールド サービス デバッグ（FSD）モードの有効化] は、コンソール デバッグを行う場合に選択します。詳細については、フィールドサービスデバッグのワークフロー 、p. 176 を参照してください。
[サービスの再起動]	[サービスの再起動] は、次のオプションを用いて、サービスおよびネットワークを再起動させる場合に選択します。 • **すべてのサービスの再起動** • **ネットワークの再起動**

[デバッグ ログのセットアップ]	[デバッグ ログのセットアップ] を選択する場合は、次のオプションを使用します。
	• [すべてのデバッグ ログの有効化]
	  ○ アプリケーション モニタリング タスク、イベント、タスク実行履歴、インストール済みプラグインすべてのデバッグ ログを収集します。
	• [すべてのデバッグ ログの無効化]
	  ○ すべてのデバッグ ログを無効にします。
	• [デバッグ ログの設定]
	  ○ アプライアンスとプラグイン サービスのデバッグ ログを選択して有効にします。
	  ○ 変更を行う前に、[オプション] メニューを使用してすべてのサービスを選択するか、すべての選択をクリアするか、状態を復元します。
	• [SCP 保持を有効化] — テンプレート.XML ファイルの収集をします。
	• [SCP 保持を無効化] - SCP 保持を無効にします。
	OpenManage Enterprise で、[監視] > [監査ログ] > [エクスポート] > [コンソール ログをエクスポート] の順にクリックして、デバッグ ログをダウンロードできます。

[キーボード レイアウトの変更]	[キーボード レイアウトの変更] は、キーボードのレイアウト変更が必要な場合に選択します。
[アプライアンスの再起動]	[アプライアンスの再起動] を選択すると、アプライアンスが再起動されます。 **メモ:** コマンドを実行してサービスを再起動すると、TUI が次のメッセージを表示する場合があります。`NMI watchdog: BUG: soft lockup - CPU#0 stuck for 36s! [java:14439].` ハイパーバイザーが過負荷になっているため、ソフト ロックアップの問題が発生する可能性があります。このような場合には、OpenManage Enterprise アプライアンスで、最低 16 GB の RAM と 8000 MHz の CPU を用意することをお勧めします。また、このメッセージが表示されたときに OpenManage Enterprise アプライアンスを再起動することをお勧めします。

OpenManage Enterprise の設定

最初に OpenManage Enterprise にログインすると、[OpenManage Enterprise にようこそ] ページが表示されます。時刻 (手動または NTP 時刻同期を使用) とプロキシの設定を行うことができます。

1. 時刻を手動で設定するには、[**時刻の設定**] セクションで次の手順を実行する必要があります。
   - [タイムゾーン] ドロップダウン メニューで、適切なタイムゾーンを選択します。
   - [日付] ボックスでは日付を入力するか選択します。
   - [時刻] ボックスには時刻を入力します。
   - 設定を保存するには、[適用] をクリックします。
2. 時刻の同期に NTP サーバーを使用する場合は、[**時刻の設定**] セクションで次の手順を実行します。

   メモ: NTP サーバの設定がアップデートされると、現在ログインしているユーザーは、OpenManage Enterprise セッションから自動的にログアウトされます。

   - [NTP の使用] チェック ボックスにチェックを入れます。
   - 時刻を同期させるには、[プライマリ NTP サーバーのアドレス] と [セカンダリ NTP サーバーのアドレス](オプション) に、IP アドレスまたはホスト名を入力します。
3. 外部通信用のプロキシサーバを設定する場合は、[プロキシ設定] セクションで次の手順を実行します。
   - [HTTP プロキシ設定を有効にする] チェック ボックスにチェックを入れます。
   - [プロキシ アドレス] を入力します。
   - プロキシ サーバーの [ポート番号] を入力します。
   - プロキシ サーバーがログインするための資格情報を要求する場合は、[プロキシ認証を有効にする] チェック ボックスにチェックを入れて、ユーザー名とパスワードを入力します。
   - 構成されたプロキシが SSL トラフィックを傍受し、信頼できるサードパーティー証明書を使用しない場合は、[証明書の検証を無視] チェック ボックスを選択します。このオプションを使用すると、保証およびカタログ同期に使用される組み込み型証明書の確認は無視されます。
4. 設定を保存するには、[適用] をクリックします。

メモ: 対応するブラウザの詳細については、サポート サイトで入手できる『*OpenManage Enterprise サポート マトリックス*』を参照してください。

OpenManage Enterprise の最適な使用のために推奨されるスケーラビリティおよびパフォーマンスの設定

次の表は、OpenManage Enterprise でサポートされている機能のパフォーマンスパラメーターの表です。OpenManage Enterprise の最適なパフォーマンスを確保するために、Dell EMC は、タスクごとに推奨されるデバイスの最大数で指定された頻度でタスクを実行することをお勧めします。

表 8. OpenManage Enterprise のスケーラビリティとパフォーマンスに関する考慮事項

タスク	タスク実行の推奨頻度	タスクが事前に準備されているかどうか	タスクごとの推奨最大デバイス数
検出	ネットワークの変更が頻繁な環境では 1 日に 1 回。	いいえ	10,000/タスク
インベントリ	OpenManage Enterprise には、インベントリを 1 日に 1 回自動的に更新する事前準備されたタスクが用意されています。	はい。この機能を無効にすることができます。	OpenManage Enterprise によって監視されているデバイス。
保証	OpenManage Enterprise には、保証を 1 日に 1 回自動的に更新する事前準備されたタスクが用意されています。	はい。この機能を無効にすることができます。	OpenManage Enterprise によって監視されているデバイス。
正常性ポーリング	1 時間 に 1 回	はい。頻度を変更することができます。	適用なし

表 8. OpenManage Enterprise のスケーラビリティとパフォーマンスに関する考慮事項（続き）

タスク	タスク実行の推奨頻度	タスクが事前に準備されているかどうか	タスクごとの推奨最大デバイス数
ファームウェア/ドライバーのアップデート	必要に応じて		150/タスク
設定インベントリ	必要に応じて		1500/ベースライン

OpenManage Enterprise でサポートされるプロトコルおよびポート

管理ステーションでサポートされるプロトコルおよびポート

表 9. OpenManage Enterprise でサポートされる管理ステーション上の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	ソース	方向	送信先	使用状況
22	SSH	TCP	256 ビット	管理ステーション	入力	OpenManage Enterprise アプライアンス	• FSD が使用されている場合にのみ受信に必要です。OpenManage Enterprise 管理者は、Dell EMC サポートスタッフと対話する場合にのみ有効にする必要があります。
25	SMTP	TCP	なし	OpenManage Enterprise アプライアンス	出力	管理ステーション	• OpenManage Enterprise から電子メールアラートを受信するため。
53	DNS	UDP/TCP	なし	OpenManage Enterprise アプライアンス	出力	管理ステーション	• DNS クエリ用。
68/546（IPv6）	DHCP	UDP/TCP	なし	OpenManage Enterprise アプライアンス	出力	管理ステーション	• ネットワークの設定。
80*	HTTP	TCP	なし	管理ステーション	入力	OpenManage Enterprise アプライアンス	• Web GUI ランディング ページ。これにより、ユーザーは HTTPS（ポート 443）にリダイレクトされます。
123	NTP	TCP	なし	OpenManage Enterprise アプライアンス	出力	NTP サーバー	• 時間の同期化（有効になっている場合）。
137、138、139、445	CIFS	UDP/TCP	なし	iDRAC/CMC	入力	OpenManage Enterprise アプライアンス	• 導入テンプレートをアップロードまたはダウンロードするため。 • TSR と診断ログをアップロードするため。

表 9. OpenManage Enterprise でサポートされる管理ステーション上のプロトコルおよびポート（続き）

ポート番号	プロトコル	ポートタイプ	最大暗号化レベル	ソース	方向	送信先	使用状況
							• ファームウェア/ドライバー DUP、および FSD プロセスをダウンロードするため。 • ネットワーク ISO を起動します。
				OpenManage Enterprise アプライアンス	出力	CIFS 共有	• ファームウェア/ドライバー カタログを CIFS 共有からインポートするため。
111、2049（デフォルト）	NFS	UDP/TCP	なし	OpenManage Enterprise アプライアンス	出力	外部 NFS 共有	• ファームウェア アップデートのために NFS 共有からカタログと DUP をダウンロードするため。 • ネットワーク共有から手動でコンソールをアップグレードするため。
162*	SNMP	UDP	なし	管理ステーション	入力 / 出力	OpenManage Enterprise アプライアンス	• SNMP を使用したイベントの受信。トラップ転送ポリシーを使用している場合は、方向は「送信」のみです。
443（デフォルト）	HTTPS	TCP	128 ビット SSL	管理ステーション	入力 / 出力	OpenManage Enterprise アプライアンス	• Web GUI。 • Dell.com からアップデートおよび保証情報をダウンロードするため。Web GUI の HTTPS を使用して OpenManage Enterprise と通信する際は、256 ビットの暗号化が許可されます。 • サーバーから開始される検出。
514	Syslog	TCP	なし	OpenManage Enterprise アプライアンス	出力	Syslog サーバー	• アラートと監査ログ情報を Syslog サーバーに送信するため。
3269	LDAPS	TCP	なし	OpenManage Enterprise アプライアンス	出力	管理ステーション	• グローバル カタログの AD/LDAP ログイン。
636	LDAPS	TCP	なし	OpenManage Enterprise アプライアンス	出力	管理ステーション	• ドメイン コントローラーの AD/LDAP ログイン。

*ポートは、割り当て済みポート番号を除いて最大 499 まで設定できます。

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 10. OpenManage Enterprise の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	ソース	方向	送信先	使用状況
22	SSH	TCP	256 ビット	OpenManage Enterprise アプライアンス	出力	管理対象ノード	• Linux OS、Windows、Hyper-V の検出用。
161	SNMP	UDP	なし	OpenManage Enterprise アプライアンス	出力	管理対象ノード	• SNMP クエリ用。
162*	SNMP	UDP	なし	OpenManage Enterprise アプライアンス	入力/出力	管理対象ノード	• SNMP トラップの送受信。
443	専用 /WS-Man/ Redfish	TCP	256 ビット	OpenManage Enterprise アプライアンス	出力	管理対象ノード	• iDRAC7 以降のバージョンの検出とインベントリー。 • CMC 管理用。
623	IPMI/ RMCP	UDP	なし	OpenManage Enterprise アプライアンス	出力	管理対象ノード	• LAN を使用した IPMI アクセス。
69	TFTP	UDP	なし	CMC	入力	管理ステーション	• CMC ファームウェアのアップデート用。

* ポートは、すでに割り当てられているポート番号を除いて最大 499 まで設定できます。

メモ: IPv6 環境では、すべての機能が必ず想定どおりに動作するように、OpenManage Enterprise アプライアンスで IPv6 を有効にし、IPv4 を無効にする必要があります。

OpenManage Enterprise でサポートされているプロトコルとポートの使用例リンク

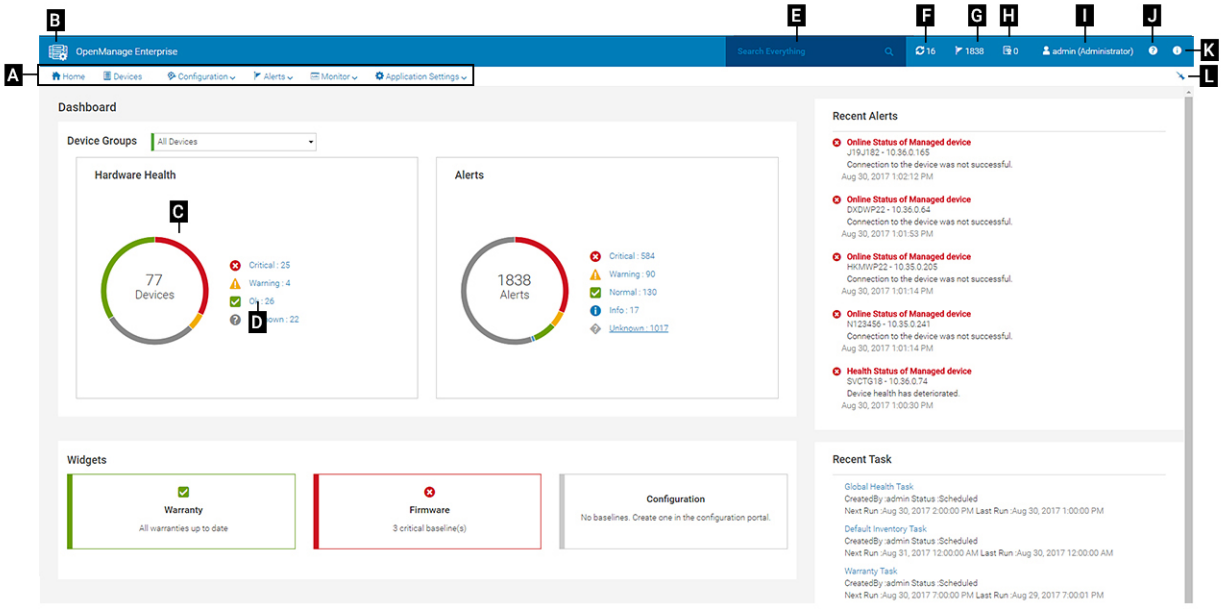
表 11. OpenManage Enterprise でサポートされているプロトコルとポートの使用例リンク

使用例	URL
OpenManage Enterprise アプライアンスのアップグレード	https://downloads.dell.com/openmanage_enterprise/
デバイス保証へのアクセス	https://apigtwb2c.us.dell.com/PROD/sbil/eapi/v5/asset-entitlements
カタログのアップデート	https://downloads.dell.com/catalog/
OpenManage Mobile アプリケーションを使用して、新しいアラート通知をプッシュします	https://openmanagecloud.dell.com

5

OpenManage Enterprise グラフィカル ユーザー インターフェイスの概要

OpenManage Enterprise グラフィカルユーザーインタフェース (GUI) では、メニューアイテム、リンク、ボタン、ペイン、ダイアログボックス、リスト、タブ、フィルタボックス、およびページを使用して、ページ間を移動してデバイス管理タスクを完了できます。デバイス リスト、ドーナツ グラフ、監査ログ、OpenManage Enterprise の設定、システム アラート、およびファームウェア/ドライバーのアップデートなどの機能は、複数の場所に表示されます。OpenManage Enterprise を簡単かつ効率的に使用してデータセンターのデバイスを管理するためには、GUI 要素についてしっかり理解しておくことをお勧めします。



- A - OpenManage Enterprise のすべてのページに表示される [OpenManage Enterprise] メニューは、管理者がダッシュボードの表示 (**ホーム**)、デバイスの管理 ([デバイス])、ファームウェア/ドライバーのベースライン、テンプレート、および設定コンプライアンスのベースライン ([設定]) の管理、アラートの作成および保存 ([アラート]) を行い、ジョブの実行、検出、インベントリー データの収集、レポートの生成 ([監視]) を行えるようにする機能へのリンクを提供します。OpenManage Enterprise の異なるプロパティをカスタマイズすることもできます (**アプリケーションの設定**)。右上の角にあるピンのシンボルをクリックして、メニューアイテムがすべての OpenManage Enterprise のページに表示されるようにピン留めします。ピン留めを外すには、再度ピンの記号をクリックします。
- B - ダッシュボードの記号。これをクリックして、OpenManage Enterprise の任意のページからダッシュボードページを開きます。または、**ホーム** をクリックします。「ダッシュボード」を参照してください。
- C - ドーナツグラフには、OpenManage Enterprise が監視するすべてのデバイスの正常性状態のスナップショットが提供されます。重要な状態にあるデバイスで、すばやく処置を実行することができます。グラフ内の各色は、特定の正常性状態を持つデバイスのグループを表します。対応する色の範囲をクリックすると、デバイスリストにそれぞれのデバイスが表示されます。デバイスの名前または IP アドレスをクリックすると、デバイスプロパティのページが表示されます。個々のデバイスの表示と設定 、p. 65 を参照してください。
- D - デバイスの正常性状態を示すのに使用される記号。デバイスの正常性状態 、p. 38 を参照してください。
- E - **すべてを検索**ボックスに、範囲ベースのアクセス制御 (SBAC) によって定義されている範囲内のすべてのデバイスのデバイス IP、ジョブ名、グループ名、ファームウェア/ドライバー ベースライン、保証データなどの結果を表示するために、OpenManage Enterprise によって監視および表示される内容について入力します。すべてを検索 機能を使用して取得されたデータを並べ替えまたはエクスポートできません。個別のページまたはダイアログボックスで、**詳細フィルタ** セクションに入力またはそこから選択して検索結果を絞り込みます。
  - **このとき、+、- の演算子、および " はサポートされません。**
- F - 現在、キューに入っている OpenManage Enterprise のジョブ数。検出、インベントリー、保証、ファームウェア/ドライバーの更新などに関連するジョブ。クリックすると、ジョブの詳細 ページの正常性、インベントリ、レポートカテゴリで実行され

たジョブのステータスが表示されます。すべてのイベントを表示するには、**すべてのジョブ** をクリックします。デバイスコントロール用ジョブの使い方 、p. 124 を参照してください。クリックして更新します。

- G - アラートログに生成されたイベントの数。また、このセクションのアラート数は、未確認アラートを表示するかしないかの設定によっても異なります。デフォルトでは、未確認アラートのみが表示されます。確認したアラートの表示/非表示については、「アラート表示のカスタマイズ 、p. 160」を参照してください。アラートを削除すると数が減ります。重大なステータスを示すのに使用した記号については、「デバイスの正常性状態 、p. 38」を参照してください。重大度の記号をクリックすると、アラート ページの重大カテゴリのすべてのイベントを表示します。すべてのイベントを表示するには、**すべてのイベント** をクリックします。「デバイスのアラートの管理」を参照してください。
- H - ステータスがクリティカル (期限切れ) または警告 (もうすぐ期限切れ) のデバイス保証の合計数。「デバイス保証の管理」を参照してください。
- I - 現在ログインしているユーザーのユーザー名。ユーザーに割り当てられている役割を表示するには、ユーザー名上でポインタを停止します。ロール ベースのユーザーの詳細については、OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。クリックしてログアウトし、別のユーザーとしてログインします。
- J - 現在、コンテスト依存ヘルプ ファイルは、現在のページに対してのみ表示され、ホーム ポータル ページには表示されません。これをクリックすると、OpenManage Enterprise でリンク、ボタン、ダイアログボックス、ウィザード、ページを効果的に使用するためのタスクベースの手順が表示されます。
- K - クリックして、システムにインストールされている OpenManage Enterprise の現在のバージョンを表示します。**ライセンス** をクリックし、メッセージをよく読みます。該当するリンクをクリックして、OpenManage Enterprise 関連のオープンソースファイル、または他のオープンソースライセンスを表示およびダウンロードします。
- L - ピンをクリックして、メニュー項目をピン留めするか、ピン留めを外します。ピン留めを外した後にメニュー項目をピン留めするには、**OpenManage Enterprise** メニューを展開させて、ピンの記号をクリックします。

表にリストされるアイテムについてのデータは、包括的に表示され、全体で、または選択したアイテムに基づいてエクスポートできます。すべてまたは選択したデータのエクスポート 、p. 64 を参照してください。青色のテキストで表示される場合、表内のアイテムについて詳細情報は、同じウィンドウまたは個別のページで開いて、表示および更新できます。表形式データは、**詳細フィルタ** 機能を使用してフィルタリングできます。フィルタリング内容は、表示されているコンテンツによって異なります。フィールドからデータを選択するか入力します。テキストまたは数値が不完全な場合は、予想する出力が表示されません。フィルター基準に一致するデータがリストに表示されます。フィルタリング結果を削除するには、**すべてのフィルタのクリア** をクリックします。

表のデータを並べ替えるには、列のタイトルをクリックします。すべてを検索 機能を使用して取得されたデータを並べ替えまたはエクスポートできません。

シンボルは、主要メイン アイテム、ダッシュボード、デバイスの正常性のステータス、アラート カテゴリ、ファームウェア/ドライバーのコンプライアンス状態、接続状態、電源状態、その他を識別するために使用します。ブラウザの 次へ または 前へ ボタンをクリックして、OpenManage Enterprise 上のページ間を移動します。サポートされているブラウザの詳細については、サポートサイトにある『*Dell EMC OpenManage Enterprise サポート マトリックス*』を参照してください。

該当する場合は、ページが左、作業、および右ペインに分割されて、デバイス管理のタスクを簡略化します。必要に応じて、ポインタを GUI 要素上で停止させると、オンラインヘルプとツールヒントが表示されます。

デバイス、ジョブ、インベントリー、ファームウェア/ドライバーのベースライン、管理アプリケーション、仮想コンソールなどについてのプレビューが右ペインに表示されます。作業ペインでアイテムを選択し、右ペインで **詳細の表示** をクリックして、そのアイテムについての詳細情報を表示します。

ログインしている場合、すべてのページが自動的に更新されます。アプライアンスの導入後、以後のログイン時に、OpenManage Enterprise のアップデート バージョンがある場合は、[**アップデート**] をクリックしてただちにバージョンをアップデートするよう警告されます。すべての OpenManage Enterprise 権限 (管理者、デバイスマネージャ、ビューア) を持つユーザーはメッセージ表示を行うことができますが、バージョンをアップデートできるのは管理者のみです。管理者は、後で通知するか、メッセージを閉じるかを選択できます。OpenManage Enterprise のバージョンをアップデートする方法の詳細については、「OpenManage Enterprise のバージョンと使用可能なプラグインの確認とアップデート 、p. 163」を参照してください。

OpenManage Enterprise によるすべてのジョブベースのアクションについては、ジョブが作成または実行が開始された場合、画面の右下隅に適切なメッセージが表示されます。ジョブに関する詳細は、[ジョブの詳細] ページで確認できます。ジョブ リストの表示 、p. 124 を参照してください。

6

OpenManage Enterprise ホームポータル

[OpenManage Enterprise] > [ホーム] をクリックして、OpenManage Enterprise のホームページを表示します。ホームページでは、次の項目を実行できます。

- ダッシュボードを表示して、デバイスの正常性状態についてのライブスナップショットを取得し、必要に応じてアクションを行います。「ダッシュボード」を参照してください。
- 重要および警告カテゴリのアラートを表示し、それらを解決します。「デバイスのアラートの管理」を参照してください。
- [ウィジェット] セクションには、すべてのデバイスのロールアップ保証、ファームウェア/ドライバーのコンプライアンス、設定コンプライアンス ステータスがリストされます。ウィジェットで利用可能な機能についての詳細は、「OpenManage Enterprise ダッシュボードを使用したデバイスの監視 、p. 36」を参照してください。右ペインには、OpenManage Enterprise が最近生成したアラートおよびタスクがリストされます。そのアラートまたはタスクに関する詳細を表示する場合は、アラートまたはタスクのタイトルをクリックします。デバイス アラートのモニターと管理 、p. 113 およびデバイスコントロール用ジョブの使い方 、p. 124 を参照してください。
- OpenManage Enterprise のアップデートバージョンが利用可能になると、すぐに通知されます。アップデートするには [アップデート] をクリックします。OpenManage Enterprise のバージョンをアップデートする方法の詳細については、「OpenManage Enterprise のバージョンと使用可能なプラグインの確認とアップデート 、p. 163」を参照してください。
- **最近のアラート** セクションには、OpenManage Enterprise により監視されるデバイスによって生成されたアラートがリストされます。アラートのタイトルをクリックして、アラートに関するより詳細な情報を表示します。「デバイスのアラートの管理」を参照してください。
- **最近のタスク** セクションには、作成された最新のタスク (ジョブ) をリストします。タスクのタイトルをクリックして、ジョブに関するより詳細な情報を表示します。ジョブ リストの表示 、p. 124 を参照してください。

メモ: デバイス マネージャーとしてログインしている場合、ホーム ポータルには、DM が所有するデバイス/デバイス グループに関連する情報が表示されます。また、[デバイス グループ] ドロップダウンには、デバイス マネージャーが操作アクセスできるデバイス グループのみがリストされます。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

トピック：

- OpenManage Enterprise ダッシュボードを使用したデバイスの監視
- ドーナツグラフ
- デバイスの正常性状態

OpenManage Enterprise ダッシュボードを使用したデバイスの監視

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

初回ログインを別にすれば、それ以降、OpenManage Enterprise にログインした後に毎回表示される最初のページがダッシュボードです。

OpenManage Enterprise の任意のページからダッシュボードのページを開くには、左上隅にあるダッシュボード記号をクリックします。または、**ホーム** をクリックします。

ダッシュボードには、リアルタイムのモニタリング データを使用して、データ センター環境にあるデバイスおよびデバイス グループの、デバイスの正常性、ファームウェア/ドライバーのコンプライアンス、保証、アラート、その他の項目が表示されます。

使用可能なコンソールのアップデートもダッシュボードに表示されます。OpenManage Enterprise のバージョンをすぐにアップグレードするか、後で通知するように OpenManage Enterprise を設定できます。

デフォルトでは、アプリケーションを初めて起動する際、ダッシュボード ページは空白です。OpenManage Enterprise へデバイスを追加すると、ダッシュボード上でそれらのデバイスが監視され表示されるようになります。デバイスを追加するには、監視または管理のためのデバイスの検出 、p. 39 およびデバイスのグループ化 、p. 52 を参照してください。

- デバイスのファームウェアおよびドライバーの管理 、p. 73
- デバイスアラートの管理
- デバイスの検出
- レポートの作成
- OpenManage Enterprise アプライアンス設定の管理 、p. 142

メモ: [デバイス グループ] ドロップダウンでデバイス グループを選択すると、ダッシュボードに表示されるすべてのデータは、選択したデバイス グループに対してのみ使用されます。

ハードウェアの正常性 セクションは、デフォルトで、OpenManage Enterprise によって監視されているすべてのデバイスの現在の正常性を示すドーナツグラフを表示します。ドーナツグラフのセクションをクリックすると、デバイスのそれぞれの正常性状態についての情報が表示されます。

アラート セクションのドーナツグラフは、選択したデバイスグループのデバイスが受信したアラートをリストします。デバイスアラートのモニターと管理 、p. 113 を参照してください。ドーナツ グラフのアラート総数は、未確認アラートを表示するかどうかの設定によって異なります。デフォルトでは、未確認アラートのみが表示されます。アラート表示のカスタマイズ 、p. 160 を参照してください。各項目の下のアラートを表示するには、それぞれの色の帯をクリックします。[アラート] ダイアログボックスで、重要 セクションは、重要状態にあるデバイスをリストします。生成されたすべてのアラートを表示するには、[すべて] をクリックします。[ソース名] 列は、アラートを生成したデバイスを示します。名前をクリックしてデバイスのプロパティを表示し、設定します。個々のデバイスの表示と設定 、p. 65 を参照してください。

ドーナツ グラフの詳細については、ドーナツグラフ 、p. 37 およびデバイスの正常性状態 、p. 38 を参照してください。
OpenManage Enterprise が監視するさまざまなデバイスグループ内のデバイスの概要を表示するには、**デバイスグループ** ドロップダウンメニューから選択します。ある正常性状態に属する デバイスリスト を表示するには、正常性カテゴリに関連付けられている色の帯をクリックするか、ドーナツグラフの横にあるそれぞれの正常性状態の記号をクリックします。

メモ: デバイス リストで、デバイス名または IP アドレスをクリックしてデバイスの設定データを表示し、次に編集します。個々のデバイスの表示と設定 、p. 65 を参照してください。

ウィジェット セクションには、OpenManage Enterprise の主要な機能の一部についての概要が表示されます。各項目の下の概要を表示するには、ウィジェットのタイトルをクリックします。

- **保証** : 保証期限の終了が近づいているデバイスの数が表示されます。これは [保証設定] に基づいています。期限切れの保証を通知するようにすると、保証期限が切れたデバイスの数が表示されます。それ以外の場合は、期限切れが近いデバイスと、保証が有効なデバイスの数が表示されます。クリックすると、**保証** ダイアログボックスの詳細が表示されます。デバイスの保証の管理については、デバイス保証の管理 、p. 132 を参照してください。**保証** セクション上でポインタを停止して、セクションで使用されているシンボルの定義を確認します。
- **ファームウェア/ドライバー** : OpenManage Enterprise に作成されたデバイス ベースライン ファームウェア/ドライバーのコンプライアンス ステータスを表示します。使用可能な場合は、「重要」および「警告」ファームウェア/ドライバーのベースラインがこのセクションにリストされます。
  - ロールアップ正常性状態の詳細については、Dell TechCenter のテクニカル ホワイト ペーパー『*Dell EMC 第 14 世代以降の PowerEdge サーバーで iDRAC を使用してロールアップ正常性状態を管理する*』を参照してください。
  - クリックすると、[**ファームウェア/ドライバーのコンプライアンス**] ページに詳細が表示されます。
  - ファームウェアのアップデート、ファームウェア カタログの作成、ファームウェア ベースラインの作成、およびベースライン コンプライアンス レポートの生成に関する詳細については、デバイスのファームウェアおよびドライバーの管理 、p. 73 を参照してください。
- **設定** : OpenManage Enterprise で作成された設定コンプライアンスベースラインのロールアップステータスが表示されます。使用可能な場合は、重要 および 警告 設定ベースラインが一覧表示されます。コンプライアンス テンプレートの管理 、p. 106 を参照してください。
- **リソースの使用率** : アプライアンスの CPU とメモリーの使用率が表示されます。以下の色分けされたチェックを使用して、使用率のさまざまな段階が示されます。
  - 緑色 - リソースの使用率が 80%未満である
  - 黄色 - リソースの使用率が 80%を超えるが 95%未満である
  - 赤色 - リソースの使用率が 95%を超える

  メモ: ウィジェットの左側にある色分けされた垂直バーとして表示されている全体のリソース使用率は、すべてのリソースの最悪の場合のロールアップです。

ドーナツグラフ

OpenManage Enterprise の異なるセクションに、ドーナツグラフを表示できます。ドーナツグラフで表示される出力は、表内で選択するアイテムに基づいています。ドーナツグラフは、OpenManage Enterprise 内の複数の状態を示します。

- デバイスの正常性状態 : ダッシュボード ページに表示されます。ドーナツグラフの色は、OpenManage Enterprise によって監視されるデバイスの正常性を示すように相対的に分割されます。すべてのデバイスステータスは、色の付いた記号で示されます。

「デバイスの正常性状態 、p. 38」を参照してください。ドーナツグラフはグループの 279 デバイスの正常性状態を示し、そのうち 131 = 重要、50 =警告、95 = OK で、これらの数字を相対的に表す色の範囲で円が形成されます。

メモ: 単一デバイスのドーナツグラフは、そのデバイスのステータスを示す 1 色だけを使用して、厚みのある円で形成されます。たとえば、警告 状態のデバイスの場合は、黄色の円で表示されます。

- デバイスのアラートのステータスは、OpenManage Enterprise が監視するデバイスに対して生成された合計アラートを示します。「デバイス アラートのモニターと管理 、p. 113」を参照してください。

  メモ: ドーナツ グラフのアラート総数は、未確認アラートを表示するかどうかの設定によって異なります。デフォルトでは、未確認アラートのみが表示されます。「アラート表示のカスタマイズ 、p. 160」を参照してください。
- カタログのバージョンに対するデバイスのファームウェアバージョンコンプライアンスレベルは、「デバイスのファームウェアおよびドライバーの管理 、p. 73」を参照してください。
- デバイスおよびデバイスグループの設定コンプライアンスベースラインについては、「デバイス設定コンプライアンスの管理 、p. 105」を参照してください。

メモ: ドーナツグラフで示される選択したデバイスのコンプライアンスレベル。複数のデバイスが 1 つのベースラインに関連付けられているときは、そのベースラインに対するコンプライアンスレベルの一番低いデバイスのステータスが、そのベースラインのコンプライアンスレベルとして示されます。たとえば、多くのデバイスがファームウェアベースラインに関連付けられており、少数のデバイスのコンプライアンスレベルが 正常 またはダウングレード になっていても、グループ内の 1 台のデバイスのコンプライアンスがアップグレード になっている場合は、ファームウェア ベースラインのコンプライアンスレベルはアップグレードと示されます。ロールアップ状態は、重大度の高いデバイスのステータスと同じです。ロールアップ正常性状態の詳細については、Dell TechCenter のテクニカルホワイトペーパー『*MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS*』(Dell EMC 第 14 世代以降の PowerEdge サーバの iDRAC を使用してロールアップ正常性状態を管理する) を参照してください。

メモ: 単一デバイスのドーナツグラフは、そのデバイスのファームウェアコンプライアンスレベルを示す 1 色だけを使用して、厚みのある円で形成されます。たとえば、重要 状態のデバイスは赤色の円で表示され、デバイスのファームウェアをアップデートする必要があることが示されます。

デバイスの正常性状態

表 12. OpenManage Enterprise におけるデバイスの正常性状態

正常性状態	定義
重要	デバイスまたは環境の重要な側面において不具合が発生したことを示します。
警告	デバイスは故障しそうです。デバイスまたは環境の一部の局面が正常でないことを示します。ただちに対処する必要があります。
OK	デバイスは完全に機能しています。
不明	デバイスのステータスが不明です。

メモ: ダッシュボードに表示されるデータは、OpenManage Enterprise 使用時のユーザー権限によって決まります。ユーザーの詳細については、「ユーザーの管理」を参照してください。

7

監視または管理のためのデバイスの検出

[OpenManage Enterprise] > [監視] > [検出] をクリックすると、データセンター環境にあるデバイスを検出して管理し、操作性を向上させ、ビジネスの重要な処理に対するリソースの可用性を改善できます。[検出] ページに、タスクで検出されたデバイスの数およびそのデバイスに対する検出ジョブのステータスに関する情報が表示されます。ジョブのステータスは 待機、完了、停止 のいずれかです。右ペインには、可能なデバイスの合計、デバイスタイプ で検出されたデバイスとそれぞれの数、次の実行時刻 (スケジュールされている場合)、検出された最後の時刻など、タスクに関する情報が表示されます。右ペインの [詳細の表示] は、個々の検出ジョブの詳細を表示します。

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- OpenManage Enterprise (バージョン 3.2 以降) では、ドメイン認証情報による検出をサポートするため、旧バージョンで使用されていた WSMAN プロトコルではなく、OpenSSH プロトコルが使用されます。そのため、アプライアンスのアップデート前に検出済みの Windows デバイスおよび Hyper-V デバイスはいったん削除し、OpenSSH 認証情報を使用して再検出する必要があります。Windows および Hyper-V で OpenSSH を有効にする方法については、Microsoft のマニュアルを参照してください。
- [検出とインベントリのスケジュール] ページに、スケジュール済みジョブのステータスは [待機] と [ステータス] 列に示されます。ただし、[ジョブ] ページでは、[スケジュール済み] として同じステータスが示されます。
- デフォルトでは、デバイスの最後に検出された IP は、すべての操作を実行するために OpenManage Enterprise によって使用されます。IP の変更を有効にするには、デバイスを再検出する必要があります。
- サード パーティー製のデバイスでは、複数のプロトコルを使用して検出されたエントリーが重複して表示されることがあります。IPMI プロトコルのみを使用して、エントリーを削除し、デバイスを再検出することで、この重複を修正することができます。

検出機能を使用すると、次の操作を実行できます。

- グローバル除外リストでデバイスを表示、追加、および削除します。グローバル除外範囲 、p. 46 を参照してください。
- デバイス検出ジョブを作成、実行、編集、削除、および停止します。

関連タスク

デバイス検出ジョブの削除 、p. 51
デバイス検出ジョブの詳細の表示 、p. 45
デバイス検出ジョブの停止 、p. 46
デバイス検出ジョブの実行 、p. 45
サーバ検出ジョブを作成するための検出モードの指定 、p. 47
サーバー用にカスタマイズされたデバイス検出ジョブ プロトコルの作成 - 検出プロトコルの追加設定 、p. 47
Dell ストレージ検出ジョブを作成するための検出モードの指定 、p. 50
SNMP デバイス用のカスタマイズしたデバイス検出ジョブプロトコルの作成 、p. 51
複数のプロトコル検出ジョブを作成する検出モードの指定 、p. 51
デバイス検出ジョブの編集 、p. 45

トピック :

- .csv ファイルからデータをインポートして複数のデバイスを指定
- グローバル除外範囲
- サーバ検出ジョブを作成するための検出モードの指定
- サーバー用にカスタマイズされたデバイス検出ジョブ プロトコルの作成 - 検出プロトコルの追加設定
- シャーシ検出ジョブを作成する検出モードの指定
- シャーシ用にカスタマイズされたデバイス検出ジョブ プロトコルの作成 - 検出プロトコルの追加設定
- Dell ストレージ検出ジョブを作成するための検出モードの指定
- ネットワーク スイッチ検出ジョブを作成するための検出モードの指定
- HTTPS ストレージ デバイス用にカスタマイズされたデバイス検出ジョブ プロトコルの作成 - 検出プロトコルの詳細設定
- SNMP デバイス用のカスタマイズしたデバイス検出ジョブプロトコルの作成
- 複数のプロトコル検出ジョブを作成する検出モードの指定
- デバイス検出ジョブの削除

サーバーから開始される検出機能を用いたサーバーの自動検出

OpenManage Enterprise では、iDRAC ファームウェアがバージョン 4.00.00.00 以降であるサーバーの自動検出が行えます。アプライアンスの構成において、DNS のクエリーによって自動的にコンソールを見つけて、検出を開始できるように、アプライアンスを設定可能です。

サーバーから開始される検出を利用するには、次の前提条件を満たしている必要があります。

- この機能の適用は、iDRAC ファームウェアがバージョン 4.00.00.00 以降のサーバーの場合のみ可能です。
- サーバーは OpenManage Enterprise と同じドメインまたはサブドメインに存在する必要があります。
- TUI を用いて DNS に構成情報を追加するには、OpenManage Enterprise が DNS に登録されている必要があります。DNS が OpenManage Enterprise からの自動アップデートを許可することが推奨されます。
- サーバーからの複数のアナウンスを回避するために、DNS 上のアプライアンス コンソールの古いレコードをクリーンアップする必要があります (存在する場合)。

メモ: 範囲ベースのアクセス制御 (SBAC) は、[監視] > [サーバーから開始される検出] ページのデバイス リストには影響しません。デバイス マネージャーには、このページのスコープ外のデバイスが表示されます。

OpenManage Enterprise でサーバーの自動検出を行うには、次の手順に従います。

1. 次のいずれかの方法を用いて、OpenManage Enterprise の構成情報を DNS に追加します。
   - TUI - TUI インターフェイスを用いて [サーバーから開始される検出の構成] オプションを有効にします。詳細については、テキスト ユーザー インターフェイスの使用による OpenManage Enterprise の設定 、p. 26 を参照してください。
   - 手動 - アプライアンス上でインターフェイスが構成されているネットワーク上の DNS サーバーに、次の 4 つのレコードを追加します。すべての`<domain>`または`<subdomain.domain>`のインスタンスを適切な DNS ドメインとシステム ホスト名に置き換えます。
     - `<OME hostname>.<domain> 3600 A <OME IP address>`
     - `_dcimprovsrv._tcp.<domain> 3600 PTR ptr.dcimprovsrv._tcp.<domain>`
     - `ptr.dcimprovsrv._tcp.<domain> 3600 TXT URI=/api/DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence`
     - `ptr.dcimprovsrv._tcp.<domain> 3600 SRV 0 0 443 <hostname>.<domain>`

     Linux で `nsupdate` を使用してレコードを作成するには、次のコマンドを使用します。
     - ホスト名レコードを作成する

       ```
       >update add omehost.example.com 3600 A XX.XX.XX.XX
       ```

     - サーバーから開始される検出のレコードを追加する

       ```
       >update add _dcimprovsrv._tcp.example.com 3600 PTR ptr.dcimprovsrv._
       tcp.example.com.

       >update add ptr.dcimprovsrv._tcp.example.com 3600 TXT URI=/api/DiscoveryConfigService/
       Actions/DiscoveryConfigService.SignalNodePresence

       >update add ptr.dcimprovsrv._tcp.example.com 3600 SRV 0 0 443 omehost.example.com.
       ```

     Windows DNS サーバーで `dnscmd` を使用してレコードを作成するには、次のコマンドを使用します。

- ホスト名レコードを作成する

```
>dnscmd <DnsServer> /RecordAdd example.com omehost A XX.XX.XX.XX
```

- サーバーから開始される検出のレコードを追加する

```
>dnscmd <DnsServer> /RecordAdd example.com _dcimprovsrv._tcp PTR
ptr.dcimprovsrv._tcp.example.com

>dnscmd <DnsServer> /RecordAdd example.com ptr.dcimprovsrv._tcp TXT URI=/api/
DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence

>dnscmd <DnsServer> /RecordAdd example.com ptr.dcimprovsrv._tcp SRV 0 0 443
omehost.example.com
```

2. デフォルトでは、アプライアンスの検出と承認ポリシーは自動に設定されており、コンソールとの接続を確立するサーバーは自動的に検出されます。設定の変更については「コンソールプリファレンスの管理 、p. 158」を参照してください。
3. アプライアンスの構成をここまでの手順で説明したように行うと、DNS へのクエリーによってサーバーは OpenManage Enterprise との接続を開始することができます。アプライアンスによるサーバーの検証が、サーバーのクライアント証明書が Dell CA によって署名されていることが確認された後に行われます。

   メモ: サーバーの IP アドレスや SSL 証明書が変更されていた場合、サーバーは再度 OpenManage Enterprise との接続を開始します。
4. [監視] > [サーバーから開始される検出] ページには、コンソールとの接続が確立されたサーバーが一覧表示されます。また、コンソールには認証情報が追加されているが、まだ接続が開始されていないサーバーも表示されます。サーバーに関する次のステータスが、前述した条件に基づいて表示されます。
   - アナウンス済み — サーバーはすでにコンソールとの接続を開始しているが、サーバーの認証情報はコンソールに追加されていません。
   - 認証情報追加済み — サーバーの認証情報はすでにコンソールに追加されているが、サーバーはコンソールとの接続を開始していません。
   - 検出準備完了 — サーバーの認証情報は追加されており、サーバーは接続を開始しています。

     メモ: アプライアンスは、「検出準備完了」ステータスとされた全サーバーを検出するために、10 分ごとに検出ジョブをトリガーします。ただし、アプライアンスの検出と承認ポリシーが「手動」に設定されている場合は、ユーザーが各サーバーに対する検出ジョブを手動でトリガーする必要があります。詳細については、次を参照 : コンソールプリファレンスの管理 、p. 158
   - 検出用ジョブが送信済み — このステータスは、サーバーに対して自動または手動のいずれかで検出ジョブが開始されたことを示します。
   - 検出済み — サーバーが検出され、[すべてのデバイス] ページにリストされています。

[監視] > [サーバーから開始される検出] ページでは、次のタスクを実行できます。

1. [インポート] — サーバー認証情報をインポートするには、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. ファイルからインポート ウィザードで、[サービス タグ ファイルのアップロード] をクリックして、.csv ファイルのある場所に移動して選択します。

      サーバー認証情報のサンプル CSV ファイルを確認するには、[サンプル CSV ファイルのダウンロード] をクリックします。
   c. [終了] をクリックします。
2. [検出] — 「検出準備完了」ステータスのサーバーを手動で検出するには、次の手順を実行します。
   a. [サーバーから開始される検出] ページに一覧表示されているサーバーで、「検出準備完了」ステータスのものを選択します。
   b. [検出] をクリックします。

   検出ジョブがトリガーされてサーバーの検出が行われ、検出後にこれらのサーバーは [すべてのデバイス] ページに一覧されます。
3. [削除] — [サーバーから開始される検出] ページに一覧されたサーバーを削除するには、次の手順を実行します。
   a. すでに検出済みで [すべてのデバイス] ページに一覧された、[サーバーから開始される検出] ページにあるサーバーを選択します。
   b. [削除] をクリックします。

   サーバーが、[サーバーから開始される検出] ページから削除されます。

   メモ: 検出されたサーバーに対応するエントリーは、30 日後に自動的にパージされます。

4. [エクスポート] — サーバーの認証情報を、HTML、CSV、または PDF フォーマットでエクスポートするには、次の手順を実行します。
   a. [サーバーから開始される検出] ページで、1 つまたは複数のサーバーを選択します。
   b. [エクスポート] をクリックします。
   c. すべてをエクスポート ウィザードで、HTML、CSV、PDF のいずれかのファイル フォーマットを選択します。
   d. [終了] をクリックします。ジョブが作成され、選択した場所にデータがエクスポートされます。

デバイス検出ジョブの作成

次の手順では、OpenManage Enterprise でデバイス検出ジョブを開始して、[検出ジョブの作成] ウィザードを使用して、データ センター内のデバイスを検出する方法について説明します。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

1. 検出ジョブの作成を開始するには、次のいずれかの手順を実行します。
   - [監視] > [検出] > [作成] の順にクリックします。
   - または、[すべてのデバイス] ページ ([OpenManage Enterprise] > [デバイス]) から [検出] ドロップダウン メニューをクリックして、[デバイスの検出] をクリックします。
2. **検出ジョブの作成** ダイアログボックスには、デフォルトジョブ名が入力されます。変更するには、検出ジョブ名を入力します。デフォルトでは、一度に同様のデバイスのプロパティを定義できます。
   - 現在の検出ジョブにさらにデバイスまたは範囲を含めるには、[追加] をクリックします。デバイスプロパティを指定可能な場所に、次の一連のフィールドがもう 1 つ表示されます：タイプ、IP/ ホスト名 / 範囲、設定。

     警告: OpenManage Enterprise は、最大で 8000 のデバイスを管理できます。従って、OpenManage Enterprise でサポートされるデバイス最大数よりもデバイス数が多い大規模ネットワークは指定しないでください。指定すると、システムが応答を突然停止する可能性があります。

     メモ: 多数のデバイスを検出する場合は、個々の IP アドレスを使用して複数の検出ジョブを作成するかわりに、デバイスの IP 範囲を使用してください。
   - .csv ファイルから範囲をインポートすることによりデバイスを検出するには、次の手順を実行します。.csv ファイルからデータをインポートして複数のデバイスを指定 、p. 46 を参照してください。
   - 特定のデバイスを除外するには除外されたものからデバイスを削除します。または検出から除外されたデバイスのリストを表示するには、「検出結果からデバイスをグローバルに除外する」を参照してください。
3. [デバイスタイプ] ドロップダウンメニューから、以下を検出します。
   - サーバ、[サーバ] を選択します。「サーバ検出ジョブを作成するための検出モード指定」を参照してください。
   - シャーシ、[シャーシ] を選択します。「シャーシ検出ジョブを作成する検出モードの指定」を参照してください。
   - Dell EMC ストレージデバイス、またはネットワーク スイッチ、[Dell ストレージ] または [ネットワーキング スイッチ] を選択します。「ストレージ、Dell ストレージ、およびネットワーク スイッチ検出ジョブを作成するための検出モードの指定」を参照してください。
   - 複数のプロトコルを使用してデバイスを検出するには、[複数] を選択します。複数のプロトコル検出ジョブを作成する検出モードの指定 、p. 51 を参照してください。
4. **IP/ ホスト名 / 範囲** ボックスには、検出される、または含まれる IP アドレス、ホスト名、または IP アドレスの範囲を入力します。このフィールドに入力可能なデータの詳細については、**i** シンボルをクリックしてください。

   メモ:
   - 範囲のサイズは 16,385 (0x4001) に制限されています。
   - IPv6 と IPv6 CIDR の形式もサポートされています。
5. **設定** セクションで、範囲を検出するために使用されるプロトコルのユーザー名とパスワードを入力します。
6. [追加の設定] をクリックして、別のプロトコルを選択し、設定を変更します。
7. [検出ジョブのスケジュール] セクションでは、ジョブをすぐに実行したり、後の時点で実行するようにスケジュールします。スケジュールジョブフィールドの定義 、p. 174 を参照してください。
8. [検出された iDRAC サーバおよび MX7000 シャーシからのトラップ受信の有効化] を選択し、OpenManage Enterprise が検出されたサーバおよび MX7000 シャーシから着信トラップを受信するのを有効にします。

   メモ: この設定を有効にすると、iDRAC のアラートが有効になり (無効になっている場合)、OpenManage Enterprise サーバーの IP アドレスのアラート送信先が設定されます。特定のアラートを有効にする必要がある場合は、適切なアラート ファ

イラーと SNMP トラップを有効にして、iDRAC でこれらを設定する必要があります。詳細については、『iDRAC ユーザーズガイド』を参照してください。

9. [トラップの宛先のコミュニティー文字列をアプリケーションの設定から設定] を選択します。このオプションは、検出された iDRAC サーバーおよび MX7000 シャーシでのみ使用できます。
10. [完了時にメール送信] チェック ボックスを選択して、検出ジョブステータスの通知を受信する電子メールアドレスを入力します。電子メールが設定されていない場合、[SMTP 設定に進む] リンクが表示されます。このリンクをクリックして SMTP の設定を行います。SMTP、SNMP、Syslog アラートの設定 、p. 118 を参照してください。このチェック ボックスを選択した場合、SMTP の設定をしなければ **終了** ボタンが表示されず、タスクを続行できません。
11. **終了** をクリックします。終了 ボタンは、フィールドが誤って入力された場合や不完全に入力された場合は表示されません。検出ジョブが作成され、実行されます。ステータスは、**ジョブの詳細** ページに表示されます。

デバイスの検出中に、検出範囲に指定されたユーザー アカウントが、リモートデバイス上で有効にされているすべての使用可能な権限に基づいて検証されます。ユーザー認証が成功すると、デバイスは自動的にオンボードされるか、デバイスを別のユーザー資格情報で後でオンボードすることができます。デバイスのオンボーディング 、p. 43 を参照してください。

メモ: CMC の検出中に、CMC 上にあるサーバ、IOM およびストレージモジュール (IP および SNMP をコミュニティー文字列として「パブリック」に設定) も検出されオンボードされます。CMC の検出中にトラップ受信を有効にした場合は、シャーシではなくすべてのサーバーで、OpenManage Enterprise がトラップの宛先として設定されます。

メモ: CMC の検出中に、Programmable MUX (PMUX) モードでの FN I/O アグリゲータは検出されません。

デバイスのオンボーディング

オンボーディングでは、監視するだけではなく、サーバの管理を可能にします。

- 管理者レベルの資格情報が検出中に提供されている場合は、サーバがオンボードされます (すべてのデバイス ビューでデバイスのステータスが「管理対象」として表示されます)。
- より低い資格情報が検出中に提供されている場合は、サーバがオンボードされません (すべてのデバイス ビューでステータスが「監視対象」として表示されます)。
- コンソールが、サーバ上でトラップレシーバーとして設定された場合も、オンボーディングのステータスは「アラートの管理対象」として示されます。
- **エラー** : デバイスのオンボーディングの際に発生した問題を示しています。
- **プロキシ使用** : MX7000 シャーシでのみ使用可能です。デバイスが MX7000 シャーシから検出され、直接検出されないことを示しています。

検出で指定されたアカウント以外のユーザー アカウントでデバイスをオンボードする場合、または検出でオンボードに失敗したためオンボードを再実行する場合は、次を実行します。

メモ:

- このウィザードでオンボードされたデバイスはすべてこのユーザー アカウントでオンボードされたままとなり、そのデバイスに対して将来検出される検出ユーザーアカウントによって置換されません。
- すでに検出されたデバイスの場合、SNMP トラップの宛先が iDRAC で OpenManage Enterprise として「手動」で設定されている場合、アラートはそのアプライアンスによって受信され、処理されます。ただし、[すべてのデバイス] ページに表示されているデバイスの [管理状態] は、最初に検出されたときの「監視対象」、「管理対象」、または「アラートによる管理対象」状態のままとなります。
- [すべてのデバイス] ページには、オンボーディング時に使用されたシャーシのユーザー役割の資格情報に関係なく、オンボードされたすべてのシャーシの**管理状態**が「管理対象」として表示されます。シャーシが「読み取り専用」ユーザーの資格情報を使用してオンボードされた場合、シャーシでのアップデート アクティビティの実行中に障害が発生する可能性があります。そのため、すべてのアクティビティを実行するには、シャーシ管理者の資格情報を使用してシャーシをオンボードすることをお勧めします。
- OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

1. [OpenManage Enterprise] メニューの [デバイス] の下で、[すべてのデバイス] をクリックします。
ドーナツグラフには、作業中のペインの全デバイスのステータスが示されます。「ドーナツグラフ」を参照してください。表には、選択したデバイスのプロパティをそのオンボーディングステータスとともに一覧表示しています。
   - [**エラー**] : デバイスをオンボードできません。推奨される権限を使用してログインしてください。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
   - [**管理対象**] : デバイスが正常にオンボードされ、OpenManage Enterprise コンソールによって管理できます。
   - [**監視対象**] : デバイスに管理オプション (SNMP を使用して検出されたオプションなど) がありません。

- [**アラートによる管理対象**]: デバイスは正常にオンボードされ、OpenManage Enterprise コンソールは検出中にそのデバイスの IP アドレスをトラップの宛先として正常に登録しました。

2. 作業中のペインで、デバイスに対応するチェック ボックスを選択し、[追加アクション] > [オンボーディング] の順にクリックします。

   このとき、すべてのデバイス ページからオンボードをサポートしているデバイスタイプのみが選択されていることを確認してください。表内の適切なデバイスを検索するには、[詳細フィルタ] をクリックしてから、フィルタボックスのオンボードステータスデータを選択するか入力します。

   メモ: 検出されたすべてのデバイスがオンボーディングでサポートされるわけではありません。iDRAC と CMC のみがサポートされます。サポートされるデバイスタイプに対してオンボードオプションを選択していることを確認してください。

3. [オンボード] ダイアログボックスに、WS-Man 資格情報 (ユーザー名とパスワード) を入力します。
4. [共通設定] セクションで次の手順を実行します。
   a. [再試行] ボックスに、サーバを検出するために繰り返す必要がある試行回数を入力します。
   b. [タイムアウト] ボックスに、以降のジョブの実行を停止する必要がある時刻を入力します。

      メモ: 入力されたタイムアウト値が現在のセッションの有効期限を超えている場合は、OpenManage Enterprise から自動的にログアウトされます。ただし、この値が現在のセッション有効期限のタイムアウト時間枠内の場合、セッションは継続され、ログアウトされません。

   c. [ポート] ボックスに、ジョブで検出に使用する必要があるポート番号を入力します。
   d. オプションのフィールドです。[コモンネーム (CN) チェックの有効化] を選択します。
   e. オプションのフィールドです。[認証局 (CA) チェックの有効化] を選択して、証明書ファイルを参照します。
5. [終了] をクリックします。

   メモ: [検出からのトラップ受信の有効化] チェック ボックスは、iDRAC インタフェースを使用して検出されたサーバに対してのみ、有効になります。他のサーバ (OS 検出を使用して検出されたサーバなど) に対する選択は無効になります。

デバイス検出のためのプロトコル 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。

メモ: iDRAC6 搭載の PowerEdge YX1X サーバーを検出、モニター、管理するサポート対象のプロトコルの機能には制限があります。詳細については、「Dell EMC PowerEdge サーバーの汎用命名規則 、p. 179」を参照してください。

表 13. 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						
	Web Services-Management (WS-Man)	**Redfish**	**簡易ネットワーク管理プロトコル (SNMP)**	**セキュアシェル (SSH)**	**Intelligent Platform Management Interface (IPMI)**	**ESXi (VMware)**	**HTTPS**
iDRAC6 以降	**対応**	**対応** iDRAC9 バージョン 4.40.10.00 以降のみ **非対応**	非対応	非対応	非対応	非対応	非対応
PowerEdge C*	**対応**	非対応	非対応	非対応	非対応	非対応	非対応
PowerEdge シャーシ (CMC)	**対応**	非対応	非対応	非対応	非対応	非対応	非対応
PowerEdge MX7000 シャーシ	非対応	**対応**	非対応	非対応	非対応	非対応	非対応
ストレージデバイス	非対応	非対応	**対応**	非対応	非対応	非対応	非対応

表 13. 検出用のプロトコル サポート マトリックス（続き）

デバイス / オペレーティング システム	プロトコル						
	Web Services-Management (WS-Man)	Redfish	簡易ネットワーク管理プロトコル (SNMP)	セキュアシェル (SSH)	Intelligent Platform Management Interface (IPMI)	ESXi (VMware)	HTTPS
イーサネットスイッチ	非対応	非対応	**対応**	非対応	非対応	非対応	非対応
ESXi	非対応	非対応	非対応	非対応	非対応	**対応**	非対応
Linux	非対応	非対応	非対応	**対応**	非対応	非対応	非対応
Windows	非対応	非対応	非対応	**対応**	非対応	非対応	非対応
Hyper-V	非対応	非対応	非対応	**対応**	非対応	非対応	非対応
Dell 製以外のサーバー	非対応	非対応	非対応	非対応	**対応**	非対応	非対応
PowerVault ME	非対応	非対応	非対応	非対応	**対応**	非対応	**対応**

デバイス検出ジョブの詳細の表示

1. [監視] > [検出] の順にクリックします。
2. 検出ジョブ名に対応する列を選択し、右ペインで [詳細の表示] をクリックします。
   [ジョブの詳細] ページに、各検出ジョブ情報が表示されます。
3. ジョブの管理の詳細については、「デバイスコントロール用ジョブの使い方 、p. 124」を参照してください。

関連情報

監視または管理のためのデバイスの検出 、p. 39

デバイス検出ジョブの編集

デバイス検出ジョブは一度に 1 つずつしか編集できません。

1. 編集したい検出ジョブに対応するチェックボックスを選択して、[編集] をクリックします。
2. [検出ジョブの作成] ダイアログボックスで、プロパティを編集します。
   このダイアログボックスで実行するタスクの詳細については、「デバイス検出ジョブの作成」を参照してください。

関連情報

監視または管理のためのデバイスの検出 、p. 39

デバイス検出ジョブの実行

メモ: すでに実行中のジョブを再実行できません。

デバイス検出ジョブを実行するには、次の手順を実行します。

1. 既存のデバイス検出ジョブのリストで、今すぐ実行したいジョブに対応するチェックボックスを選択します。
2. [実行] をクリックします。
   ジョブがただちに開始され、メッセージが右下隅に表示されます。

関連情報

監視または管理のためのデバイスの検出 、p. 39

デバイス検出ジョブの停止

ジョブを実行中にのみ停止できます。完了した検出ジョブや失敗した検出ジョブは停止できません。ジョブを停止するには次の手順を実行します。

1. 既存の検出ジョブのリストで、停止したいジョブに対応するチェックボックスを選択します。

   メモ: 複数のジョブは一度に停止できません。

2. [停止] をクリックします。
   ジョブが停止され、メッセージが右下隅に表示されます。

関連情報

監視または管理のためのデバイスの検出 、p. 39

.csv ファイルからデータをインポートして複数のデバイスを指定

1. デフォルトでは、[検出ジョブの作成] ダイアログボックスの [検出ジョブ名] には、検出ジョブ名が入力されています。変更するには、検出ジョブ名を入力します。
2. [インポート] をクリックします。

   メモ: 必要に応じて、CSV ファイルのサンプルをダウンロードします。

3. [インポート] ダイアログボックスで [インポート] をクリックし、有効な範囲のリストが含まれている .CSV ファイルを参照して [OK] をクリックします。

   メモ: .CSV ファイルに無効な範囲がある場合はエラーメッセージが表示され、重複する範囲はインポート操作中に除外されます。

グローバル除外範囲

[グローバル除外範囲]ウィザードを使用して OpenManage Enterprise の監視および管理アクティビティから除外する必要のあるデバイスのアドレスまたは範囲を入力することができます。次の手順では、デバイスの範囲を除外する方法について説明します。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

メモ: 現在、デバイスのホスト名を使用してデバイスを除外することはできず、IP アドレスまたは FQDN を使用してのみ除外できます。

1. [グローバル除外範囲] ウィザードを有効にするには、次のいずれかを実行できます。
   - [すべてのデバイス] ページ ([OpenManage Enterprise] > [デバイス])、[検出] ドロップダウン メニューで、[除外範囲の編集] をクリックします。
   - [監視] > [検出] で、右上隅の [グローバル除外リスト] をクリックします。
2. [グローバル除外範囲] ダイアログボックスで次の手順を実行します。
   a. [除外範囲の説明] ボックスに、除外されている範囲に関する情報を入力します。
   b. [除外範囲の入力] ボックスに、除外するデバイスのアドレス (複数可) または範囲を入力します。ボックスには一度に 1,000 件のアドレスエントリが入りますが、改行で区切る必要があります。つまり、すべての除外範囲をボックス内に別の行で入力する必要があります。
   除外することができる範囲は、デバイス検出中に該当するサポートの範囲と同じです。デバイス検出ジョブの作成 、p. 42 を参照してください。

   メモ:
   - 範囲のサイズは 16,385 (0x4001) に制限されています。

- IPv6 と IPv6 CIDR 形式もサポートされています。

3. [追加] をクリックします。
4. プロンプトが表示されたら、[はい] をクリックします。
   IP アドレスまたは範囲はグローバルに除外され、除外された範囲のリストに表示されます。このようなデバイスはグローバルに除外されており、それらが OpenManage Enterprise によって実行されるアクティビティに参加しないことを意味します。

   メモ: グローバルに除外されるデバイスは、**ジョブの詳細** ページで グローバルに除外 と明記されます。

   グローバル除外リストからデバイスを削除するには :
   a. チェックボックスを選択して、**除外から削除** をクリックします。
   b. プロンプトが表示されたら、**はい** をクリックします。デバイスが、グローバル除外リストから削除されます。ただし、グローバル除外リストから削除されたデバイスは自動的には OpenManage Enterprise によって監視されていません。OpenManage Enterprise が監視を開始するように、デバイスを検出する必要があります。

メモ:

- コンソールにとって既知の (つまり、コンソールによってすでに検出されている) デバイスを グローバル除外リスト に追加すると、そのデバイスが OpenManage Enterprise から削除されます。
- グローバル除外リストに新たに追加されたデバイスは、次の検出サイクルまでは [すべてのデバイス] グリッドに表示され続けます。そのようなデバイスでのタスク実行を回避するには、それらのデバイスを [すべてのデバイス] ページから手動で除外することを強くお勧めします。そのためには、該当するデバイスのチェック ボックスを選択してから [除外] をクリックします。
- グローバル除外リスト に示されているデバイスは、コンソール内のすべてのタスクから除外されます。デバイスの IP が グローバル除外リスト に含まれていて、検出タスクでその IP を含む検出範囲が作成された場合、そのデバイスは検出されません。ただし、検出タスクが作成されているとき、コンソールにエラーは表示されません。検出される必要のあるデバイスが検出されていないと感じた場合は、グローバル除外リスト をチェックして、そのデバイスがリストに含まれているかどうか確認する必要があります。

。

サーバ検出ジョブを作成するための検出モードの指定

1. [デバイスタイプ] ドロップダウンメニューから、[サーバ] を選択します。
2. プロンプトが表示されたら、次のように選択します。
   - [Dell iDRAC] : iDRAC を使用して検出します。
   - [ホスト OS] : VMware ESXi、Microsoft Window Hyper-V、Linux オペレーティングシステムを使用して検出します。
   - [Dell 以外のサーバー (帯域外経由)] : IPMI を使用してサード パーティーのサーバーを検出します。
3. [OK] をクリックします。
   選択に基づいて、[設定] の下にあるフィールドが変更されます。
4. [IP/ ホスト名 / 範囲] でプロトコルに関連付けられている IP アドレス、ホスト名、または IP 範囲を入力します。
5. [設定] に、検出されたサーバのユーザー名とパスワードを入力します。
6. 検出プロトコルをカスタマイズする場合は、[追加の設定] をクリックします。「サーバー用のカスタマイズしたデバイス検出ジョブ テンプレートの作成」を参照してください。
7. 検出ジョブをスケジュールします。スケジュールジョブフィールドの定義 、p. 174 を参照してください。
8. **終了**をクリックします。
   検出ジョブが検出ジョブのリストに作成され、表示されます。

関連情報

監視または管理のためのデバイスの検出 、p. 39

サーバー用にカスタマイズされたデバイス検出ジョブ プロトコルの作成 - 検出プロトコルの追加設定

[追加設定] ダイアログ ボックスで、サーバーを検出する適切なプロトコルの詳細情報を入力します。

メモ: 適切なプロトコルは、初期入力に基づいて事前に自動的に選択されます。

1. [WS-Man/Redfish を使用して検出（iDRAC、サーバー、シャーシ）] する場合
   a. 認証情報セクションで、[ユーザー名] と [パスワード] を入力します。
   b. [共通設定] セクションで次の手順を実行します。
      - [再試行] ボックスに、サーバーの検出時に繰り返す試行回数を入力します。
      - [タイムアウト] ボックスに、経過したらジョブの実行を停止する時間を入力します。
      - ポート番号を編集する場合は、[ポート] ボックスに値を入力します。デフォルトでは、デバイスに接続するために 443 が使用されます。サポートされているポート番号については、次のセクションを参照してください： OpenManage Enterprise でサポートされるプロトコルおよびポート 、p. 31
      - デバイスの共通名が OpenManage Enterprise へのアクセスに使用されるホスト名と同じ場合は、[共通名（CN）の有効化] チェック ボックスを選択します。
      - 必要に応じて、[認証局（CA）の有効化] チェック ボックスを選択します。
2. [IPMI を使用して検出（OOB 経由で Dell 以外）] する場合
   a. 認証情報セクションで、[ユーザー名] と [パスワード] を入力します。
   b. [共通設定] セクションで次の手順を実行します。
      - [再試行] ボックスに、サーバーの検出時に繰り返す試行回数を入力します。
      - [タイムアウト] ボックスに、経過したらジョブの実行を停止する時間を入力します。
      - [KgKey] ボックスに適切な値を入力します。
3. [SSH を使用して検出（Linux、Windows、Hyper-V）] する場合

   メモ: Windows と Hyper-V の OpenSSH のみがサポートされています。Cygwin SSH はサポートされていません。

   a. 認証情報セクションで、[ユーザー名] と [パスワード] を入力します。
   b. [共通設定] セクションで次の手順を実行します。
      - [再試行] ボックスに、サーバーの検出時に繰り返す試行回数を入力します。
      - [タイムアウト] ボックスに、経過したらジョブの実行を停止する時間を入力します。
      - ポート番号を編集する場合は、[ポート] ボックスに値を入力します。デフォルトでは、デバイスに接続するために 22 が使用されます。サポートされているポート番号については、次のセクションを参照してください： OpenManage Enterprise でサポートされるプロトコルおよびポート 、p. 31
      - [既知のホスト キーを確認する] チェック ボックスを選択して、既知のホスト キーに対してホストを検証します。
        メモ: 既知のホスト キーは、*/DeviceService/HostKeys REST API* サービスを介して追加されます。ホスト キーを管理する方法の詳細については、『*OpenManage Enterprise RESTful API ガイド*』を参照してください。
      - sudo アカウントを使用する場合は、[SUDO オプションを使用] チェック ボックスを選択します。
        メモ: sudo アカウントを機能させるには、サーバーの `/etc/sudoer` ファイルが NOPASSWD を使用するように設定する必要があります。
4. [ESXi を使用して検出（VMware）] する場合
   a. 認証情報セクションで、[ユーザー名] と [パスワード] を入力します。
   b. [共通設定] セクションで次の手順を実行します。
      - [再試行] ボックスに、サーバーの検出時に繰り返す試行回数を入力します。
      - [タイムアウト] ボックスに、経過したらジョブの実行を停止する時間を入力します。
      - ポート番号を編集する場合は、[ポート] ボックスに値を入力します。デフォルトでは、デバイスに接続するために 443 が使用されます。サポートされているポート番号については、次のセクションを参照してください： OpenManage Enterprise でサポートされるプロトコルおよびポート 、p. 31
      - デバイスの共通名が OpenManage Enterprise へのアクセスに使用されるホスト名と同じ場合は、[共通名（CN）の有効化] チェック ボックスを選択します。
      - 必要に応じて、[認証局（CA）の有効化] チェック ボックスを選択します。

関連情報

監視または管理のためのデバイスの検出 、p. 39

シャーシ検出ジョブを作成する検出モードの指定

1. [デバイスタイプ] ドロップダウンメニューから、[シャーシ] を選択します。
   選択に基づいて、[設定] の下にあるフィールドが変更されます。
2. [IP/ ホスト名 / 範囲] に IP アドレス、ホスト名、または IP 範囲を入力します。

3. [設定] で、検出するサーバのユーザー名とパスワードを入力します。
4. コミュニティタイプを入力します。
5. カスタマイズした検出テンプレートを [追加設定] をクリックして作成する場合は、「シャーシ用にカスタマイズされたデバイス検出ジョブ プロトコルの作成 - 検出プロトコルの追加設定 、p. 49」を参照してください。

メモ: 現在、検出された任意の M1000e シャーシで ハードウェアログ の下の タイムスタンプ 行に表示される日付は、CMC 5.1x 以前のバージョンの場合、2013 年 1 月 12 日となります。ただし、CMC VRTX および FX2 シャーシのすべてのバージョンでは、正確な日付が表示されます。

メモ: シャーシ内のサーバが個別に検出された場合、サーバに関するスロット情報は、**シャーシの情報** セクションには表示されません。ただし、シャーシで検出された場合は、スロット情報が表示されます。たとえば、MX7000 シャーシで、MX740c サーバが検出された場合などです。

シャーシ用にカスタマイズされたデバイス検出ジョブ プロトコルの作成 - 検出プロトコルの追加設定

[追加の設定] ダイアログボックスで、次の手順を実行します。

1. [WS-Man/Redfish を使用して検出 (iDRAC、サーバー、シャーシ)] チェック ボックスをオンにします。

   メモ: シャーシの場合、[WS-Man/Redfish を使用して検出] チェックボックスがデフォルトで選択されています。この 2 つのプロトコルのいずれかを使用してシャーシを検出できることを意味します。M1000e、CMC VRTX、FX2 シャーシは、WS-Man コマンドをサポートしています。MX7000 シャーシは、Redfish プロトコルをサポートしています。

2. 検出するシャーシのユーザー名とパスワードを入力します。
3. [共通設定] セクションで次の手順を実行します。
   a. [再試行] ボックスに、サーバを検出するために繰り返す必要がある試行回数を入力します。
   b. [タイムアウト] ボックスに、以降のジョブの実行を停止する必要がある時刻を入力します。
   c. ポート番号を編集する場合は、[ポート] ボックスに値を入力します。デフォルトでは、デバイスに接続するために 443 が使用されます。サポートされるポート番号については、「OpenManage Enterprise でサポートされるプロトコルおよびポート 、p. 31」を参照してください。
   d. デバイスの共通名が OpenManage Enterprise へのアクセスに使用されるホスト名と同じ場合は、[共通名 (CN) チェックの有効化] チェックボックスを選択します。
   e. [認証局 (CA) チェックの有効化] チェックボックスを選択します。
4. IO モジュールを検出するには、[シャーシで IO モジュールを検出] チェックボックスをオンにします。

   メモ: CMC VRTX、M1000e、FX2 シャーシにのみ適用されます (モデル FN2210S、FN410T、FN410S)。MX7000 シャーシの場合、IO モジュールが自動的に検出されます。

   メモ: 検出可能な IO モジュールは、スタンドアロン、PMUX (プログラム可能 MUX)、VLT (仮想リンク トランキング) モードのみです。フル スイッチおよびスタック モードは検出されません。

   a. M I/O アグリゲーターのユーザー資格情報がシャーシのものと同じ場合は、[シャーシ資格情報を使用] を選択します。
   b. M I/O アグリゲーターのユーザー資格情報がシャーシの資格情報と異なる場合は、[異なる資格情報を使用] を選択して、次の手順を実行します。
      - [ユーザー名] と [パスワード] を入力します。
      - 必要に応じて、[再試行]、[タイムアウト]、[ポート] のデフォルト値を変更します。
      - [既知のホスト キーを確認する] を選択して、既知のホスト キーに対してホストを検証します。

        メモ: 既知のホスト キーは、*/DeviceService/HostKeys REST API* サービスを介して追加されます。ホスト キーを管理する方法の詳細については、『*OpenManage Enterprise RESTful API ガイド*』を参照してください。
      - 必要に応じて [SUDO オプションを使用] を選択します。
5. [終了] をクリックします。
6. 「デバイス検出ジョブの作成 、p. 42」のタスクを完了します。

Dell ストレージ検出ジョブを作成するための検出モードの指定

1. [デバイス タイプ] ドロップダウン メニューで、[Dell ストレージ] を選択します。
2. プロンプトが表示されたら、次のように選択します。
   - PowerVault ME：PowerVault ME のような HTTPS プロトコルを使用するストレージ デバイスを検出します。
   - その他：SNMP プロトコルを使用するストレージ デバイスを検出します。

   選択に基づいて、[設定] の下にあるフィールドが変更されます。
3. [IP/ ホスト名 / 範囲] に IP アドレス、ホスト名、または IP 範囲を入力します。
4. [設定] で、最初の選択に応じて、Storage HTTPS の [ユーザー名] と [パスワード] を入力するか、[SNMP バージョン] と検出するデバイスの [コミュニティ タイプ] を入力します。
5. [詳細設定] をクリックして、各検出プロトコルをカスタマイズします。「SNMP デバイス用デバイス検出ジョブのカスタム テンプレートの作成」または「HTTPS ストレージ デバイス用にカスタマイズされたデバイス検出ジョブ プロトコルの作成 - 検出プロトコルの詳細設定 、p. 50」を参照してください。
6. 「デバイス検出ジョブの作成 、p. 42」のタスクを完了します。

関連情報

監視または管理のためのデバイスの検出 、p. 39

ネットワーク スイッチ検出ジョブを作成するための検出モードの指定

1. [デバイス タイプ] ドロップダウン メニューで、[ネットワーク スイッチ] を選択します。
2. [IP/ ホスト名 / 範囲] に IP アドレス、ホスト名、または IP 範囲を入力します。
3. [設定] で、検出するデバイスの [SNMP バージョン] と [コミュニティ タイプ] を入力します。
4. [詳細設定] をクリックして、各検出プロトコルをカスタマイズします。「SNMP デバイス用デバイス検出ジョブのカスタム テンプレートの作成」を参照してください。
5. 「デバイス検出ジョブの作成 、p. 42」のタスクを完了します。

HTTPS ストレージ デバイス用にカスタマイズされたデバイス検出ジョブ プロトコルの作成 - 検出プロトコルの詳細設定

[追加の設定] ダイアログボックスで、次の手順を実行します。

1. 検出する PowerVault ME のユーザー名とパスワードを入力します。
2. [共通設定] セクションで次の手順を実行します。
   a. [再試行] ボックスに、サーバを検出するために繰り返す必要がある試行回数を入力します。
   b. [タイムアウト] ボックスに、以降のジョブの実行を停止する必要がある時刻を入力します。
   c. 編集する [ポート] ボックスにポート番号を入力します。デフォルトでは、デバイスに接続するために 443 が使用されます。サポートされるポート番号については、「OpenManage Enterprise でサポートされるプロトコルおよびポート 、p. 31」を参照してください。
   d. デバイスの共通名が OpenManage Enterprise へのアクセスに使用されるホスト名と同じ場合は、[共通名 (CN) チェックの有効化] チェックボックスを選択します。
   e. [認証局 (CA) チェックの有効化] チェックボックスを選択します。
3. [終了] をクリックします。
4. 「デバイス検出ジョブの作成 、p. 42」のタスクを完了します。

SNMP デバイス用のカスタマイズしたデバイス検出ジョブプロトコルの作成

デフォルトでは、[SNMP を使用して検出] チェックボックスは、ストレージ、ネットワークなどの SNMP デバイスの検出を有効にするために選択されています。

メモ: 検出可能な IO モジュールは、スタンドアロン、PMUX (プログラム可能 MUX)、VLT (仮想リンク トランキング) モードのみです。フル スイッチおよびスタック モードは検出されません。

1. [資格情報] で、SNMP バージョンを選択して、コミュニティタイプを入力します。
2. [共通設定] セクションで次の手順を実行します。
   a. [再試行] ボックスに、サーバを検出するために繰り返す必要がある試行回数を入力します。
   b. [タイムアウト] ボックスに、以降のジョブの実行を停止する必要がある時刻を入力します。
   c. [ポート] ボックスに、ジョブで検出に使用する必要があるポート番号を入力します。

   メモ: 現在、[再試行] ボックスと [タイムアウト] ボックスの設定は、SNMP デバイスの検出ジョブに機能的な影響を与えません。このため、これらの設定は無視できます。
3. [終了] をクリックします。
4. 「デバイス検出ジョブの作成 、p. 42」のタスクを完了します。

関連情報

監視または管理のためのデバイスの検出 、p. 39

複数のプロトコル検出ジョブを作成する検出モードの指定

1. [タイプ] ドロップダウンメニューから、[複数] を選択し、複数のプロトコルを使用してデバイスを検出します。
2. [IP/ ホスト名 / 範囲] に IP アドレス、ホスト名、または IP 範囲を入力します。
3. カスタマイズした検出テンプレートを [追加設定] をクリックして作成する場合は、「サーバー用にカスタマイズされたデバイス検出ジョブ プロトコルの作成 - 検出プロトコルの追加設定 、p. 47」を参照してください。

関連情報

監視または管理のためのデバイスの検出 、p. 39

デバイス検出ジョブの削除

メモ: デバイスは、そこでタスクが実行中でも、削除できます。タスクの完了前にデバイスが削除された場合、そのデバイスで開始されたタスクは失敗します。

デバイス検出ジョブを削除するには、次の手順を実行します。

1. 削除したい検出ジョブに対応するチェックボックスを選択して、[削除] をクリックします。
2. 選択したジョブを削除する必要があるかどうか尋ねるプロンプトが表示されたら、[はい] をクリックします。
   検出ジョブが削除され、画面の右下隅にメッセージが表示されます。

メモ: 検出ジョブが削除されても、ジョブに関連付けられたデバイスは削除されません。コンソールから削除される検出タスクによって検出されたデバイスを削除したい場合は、[すべてのデバイス] ページから削除します。

メモ: デバイス検出ジョブを **ジョブ** ページから削除することはできません。

関連情報

監視または管理のためのデバイスの検出 、p. 39

8

デバイスとデバイス グループの管理

[OpenManage Enterprise] > [デバイス] の順にクリックして、OpenManage Enterprise で検出されたデバイス グループとデバイスを表示および管理することができます。デバイス マネージャーとしてログインしている場合は、そのスコープにあるデバイス グループとそれに関連付けられているツリーのみを表示および管理できるようになります。

左ペインには、次のようにデバイス グループが表示されます。

- すべてのデバイス - すべてのグループを含む最上位レベルのルート グループ。
- システム グループ - 出荷時に OpenManage Enterprise によって作成されるデフォルト グループ。
- カスタム グループ - 管理者やデバイス マネージャーなどのユーザーによって作成されたグループ。カスタム グループでは、「クエリ」グループまたは「静的」グループを作成できます。
- プラグイン グループ - プラグインによって作成されたグループ。

これらの親グループの下に子グループを作成できます。詳細については、「デバイス グループ」を参照してください。

作業中のペインの上に、ドーナツ グラフには、デフォルトですべてのデバイスの正常性状態とアラートが表示されます。ただし、左ペインでグループが選択されている場合、これらのドーナツ グラフには、選択されているグループの正常性状態とアラートが表示されます。さらに、プラグインがインストールされている場合は、3 番目のドーナツ グラフに、インストールされているプラグインのデータが表示されることがあります。ドーナツグラフの詳細については、「ドーナツグラフ」を参照してください。

ドーナツ グラフの後の表は、デバイスを一覧表示し、それらの正常性状態、電源状態、名前、IP アドレス、および識別子を表示します。デフォルトでは、すべてのデバイスがリストされますが、左ペインでグループが選択されている場合は、そのグループのデバイスのみが表示されます。デバイスリストの詳細については、「デバイスリスト」を参照してください。

[高度なフィルタ] を使用して、デバイスリストに表示されるデバイスを、正常性状態、電源状態、接続ステータス、名前、IP アドレス、識別子、デバイス タイプ、管理状態などに基づいてさらに絞り込むことができます。

リスト内のデバイスを選択すると、右側のペインには、選択されたデバイスについてのプレビューが表示されます。複数のデバイスが選択されると、最後に選択されているデバイスについてのプレビューが表示されます。[**クイック アクション**] の下に、それぞれのデバイスに関連付けられている管理リンクが表示されます。選択をクリアするには、[選択のクリア] をクリックします。

メモ:

- OpenManage Enterprise を最新バージョンにアップグレードした後、検出ジョブが再実行されると、デバイスリストがアップデートされます。
- ページごとに最大 25 台のデバイスを選択し、さらにデバイスを選択するためにページを移動して、タスクを実行することができます。
- [すべてのデバイス] ページで実行できるデバイス関連タスクの一部 (ファームウェアのアップデート、インベントリーの更新、ステータスの更新、サーバー制御など) は、それぞれの [**デバイスの詳細**] ページから個々のデバイスで実行することもできます。

トピック：

デバイスのグループ化

データセンターでデバイスを効率良く素早く管理するには、次の操作を行います。

- デバイスをグループ化します。たとえば、機能、OS、ユーザープロファイル、場所、ジョブの実行、実行クエリなどでデバイスをグループ化して、デバイスを管理します。
- デバイスの管理、ファームウェアのアップデート、デバイスの検出、アラートポリシーとレポートの管理を行う際に、デバイス関連のデータをフィルタ処理します。
- デバイスのプロパティをグループで管理できます。個々のデバイスの表示と設定 、p. 65 を参照してください。

OpenManage Enterprise は、OpenManage Enterprise の監視対象デバイスについての概要を取得するためのビルトインレポートを提供します。[OpenManage Enterprise] > [監視] > [レポート] > [デバイスの概要レポート] の順にクリックします。**実行** をクリックします。レポートの実行 、p. 135 を参照してください。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

選択したデバイスまたはグループに関連するダッシュボードデータを表示するには、[デバイスグループ] ドロップダウンメニューから選択します。

メモ: デバイスまたはグループの正常性状態が適切なシンボルで示されます。グループの正常性状態は、グループの中で最も重大な正常性状態を持つデバイスの正常性です。たとえば、多数のデバイスが存在するグループで特定のサーバの正常性が「警告」の場合、グループの正常性も「警告」です。ロールアップ状態は、重大度の高いデバイスのステータスと同じです。ロールアップ正常性状態の詳細については、Dell TechCenter のテクニカル ホワイト ペーパー『*Dell EMC 第 14 世代以降の PowerEdge サーバーで iDRAC を使用してロールアップ正常性状態を管理する*』を参照してください。

グループは親および子グループを持つことができます。1 つのグループは、そのグループ自体を子グループとした親グループにはなれません。デフォルトでは、OpenManage Enterprise には次の組み込みグループが含まれています。

[システムグループ]: OpenManage Enterprise で作成されたデフォルトグループ。システムグループは編集も削除もできません。ただし、ユーザー権限に基づいて表示することはできます。システムグループの例：

- **HCI アプライアンス**：ハイパーコンバージド デバイス (VxRAIL、Dell EMC XC Series デバイスなど)
- **ハイパーバイザシステム**：Hyper-V サーバ、VMware ESXi サーバ
- **モジュラーシステム**：PowerEdge シャーシ、PowerEdge FX2、PowerEdge 1000e シャーシ、PowerEdge MX7000 シャーシ、および PowerEdge VRTX シャーシ。

  メモ: MX7000 シャーシには、リード、スタンドアロン、またはメンバーシャーシがあります。MX7000 シャーシがリードシャーシで、メンバーシャーシを持つ場合、後者は、リードシャーシの IP を使用して検出されます。MX7000 シャーシは、次のいずれかの構文を使用して識別されます。

  - **MCM グループ** — 複数のシャーシを持つマルチシャーシ管理 (MCM) グループを示し、これは次の構文で識別されます：`Group_<MCM group name>_<Lead_Chassis_Svctag>`。ここで、
    - `<MCM group name>`：MCM グループの名前
    - `<Lead_Chassis_Svctag>`：リード シャーシのサービス タグ。シャーシ、スレッド、およびネットワーク IOM がこのグループを形成します。
  - **スタンドアロン シャーシ グループ** — `<Chassis_Svctag>`構文を使用して識別されます。シャーシ、スレッド、およびネットワーク IOM がこのグループを形成します。
- **ネットワーク デバイス**：Dell Force10 ネットワーキング スイッチとファイバー チャネル スイッチ
- **サーバ**：Dell iDRAC サーバ、Linux サーバ、Dell 以外のサーバ、OEM サーバ、および Windows サーバ
- **ストレージ デバイス：** Dell Compellent ストレージ アレイ、PowerVault MD ストレージ アレイ、PowerVault ME ストレージ アレイ
- **検出グループ**：検出タスクの範囲にマッピングするグループ。含める / 含めない条件が適用されている検出ジョブで制御されるグループを編集または削除することはできません。監視または管理のためのデバイスの検出 、p. 39 を参照してください。

メモ: グループ内のすべてのサブグループを展開するには、そのグループを右クリックし、[すべて展開] をクリックします。

[カスタム グループ]: 管理者が特定の要件で作成したグループ。たとえば、ホスト電子メールサービスがグループ化されているサーバ。ユーザーは、ユーザー権限およびグループタイプに基づいて表示、編集、削除ができます。

- **静的グループ**：グループに特定のデバイスを追加することで、ユーザーによって手動で作成される。これらのグループは、ユーザーが手動でグループ内またはサブグループ内のデバイスを変更した場合にのみ変更されます。グループの項目は、親グループが編集されるまで、または子デバイスが削除されるまで、静的の状態を保ちます。
- **クエリグループ**：ユーザーが定義した基準に一致することで動的に定義されるグループ。このグループのデバイスは、基準を使用して検出されたデバイスの結果に基づいて変化します。たとえば、経理部に割り当てられたサーバを検出するクエリを実行します。ただし、クエリグループは階層のないフラット構造にする必要があります。

メモ: 静的およびクエリグループ：

- 複数の親グループは持てません。つまり、親グループの下にサブグループとしてグループを追加することはできません。
- 静的グループ (デバイスの追加または削除) またはクエリ グループ (クエリの更新) に変更が加えられた場合、これらのグループに関連付けられたデバイスのファームウェア/ドライバーのコンプライアンスは自動的に更新されません。このような場合、ユーザーは新しく追加/削除されたデバイスに対してファームウェア/ドライバーのコンプライアンスを開始することをお勧めします。

メモ: デバイスグループ階層内に複数のカスタム（クエリ）グループを作成すると、OpenManage Enterprise の全体的なパフォーマンスに影響します。最適なパフォーマンスを得るため、OpenManage Enterprise は 10 秒ごとに正常性ロールアップ状態をキャプチャし、複数の動的グループがあるとこのパフォーマンスに影響します。

すべてのデバイス ページの左側のペインで、親の静的およびクエリグループの下に子グループを作成できます。静的デバイス グループの作成 、p. 54 およびクエリデバイスグループの作成 、p. 55 を参照してください。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

静的またはクエリグループの子グループを削除するには、次の手順を実行します。

1. 静的またはクエリグループを右クリックして、**削除** をクリックします。
2. プロンプトが表示されたら、**はい** をクリックします。グループが削除され、グループの下のリストがアップデートされます。

[プラグイン グループ]: Services、Power Manager プラグインがインストールされている場合、プラグイン グループが作成されます。プラグインは、インストールされている場合、独自のシステム グループを持ち、Power Manager プラグインなどの一部のプラグインで、ユーザーがカスタム グループを作成できるようにします。

関連タスク

OpenManage Enterprise からのデバイスの削除 、p. 60
単一デバイスのデバイス インベントリーの更新 、p. 69
デバイス グループのデバイス正常性の更新 、p. 62

カスタム グループの作成（静的またはクエリ）

[OpenManage Enterprise] > [デバイス]([すべてのデバイス] ページ）では、カスタム グループの作成ウィザードを使用して、静的グループまたはクエリ グループを作成することができます。

OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。参照先： OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15

1. [カスタム グループの作成] ウィザードを有効にするには、次の手順を実行します。
   - [OpenManage Enterprise] > [デバイス] の左ペインのカスタム グループで、3 つの点の垂直メニューを右クリックまたはクリックして、[カスタム グループの作成] をクリックします。
   - [すべてのデバイス] ページの [グループ アクション] ドロップダウン メニューで、[カスタム グループの作成] をクリックします。
2. [カスタム グループの作成] ウィザードで、次のいずれかのカスタム グループを選択します。
   a. [静的グループ]。
   b. [クエリ グループ]
3. [作成] をクリックします。
   選択に応じて（静的またはクエリ）、静的グループの作成ウィザードまたはクエリ グループの作成ウィザードのいずれかが有効になります。

グループ（静的またはクエリ）が作成されると、そのグループはカスタム グループ、静的グループ、またはクエリ グループの下に一覧表示されます。

静的デバイス グループの作成

[すべてのデバイス] ページ（[OpenManage Enterprise] > [デバイス]）では、静的グループ作成ウィザードを使用して静的グループを作成することができます。静的グループのデバイスは、グループ内のデバイスが追加または削除されるまで静的のままです。

OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

1. 静的グループ作成ウィザードを有効にするには、次のいずれかを実行します。
   - カスタム グループの下で、[**静的グループ**] を右クリックまたは 3 つの縦方向のドット メニューをクリックして、[**新規静的グループの作成**] をクリックします。
   - [グループアクション] > [カスタム グループの作成] > [静的グループ] の順にクリックします。

2. [**静的グループ作成ウィザード**] ダイアログ ボックスで、グループの名前と説明 (オプション) を入力し、新しい静的グループを作成する親グループを選択します。

   メモ: OpenManage Enterprise の静的または動的グループ名とサーバ構成に関連する名前は、一意である必要があります(大文字と小文字を区別しません)。たとえば *name1* と *Name1* を同時に使用することはできません。

3. **次へ**をクリックします。
4. [グループ メンバーの選択] ダイアログ ボックスで、静的グループに含める必要があるデバイスを選択します。
5. [終了] をクリックします。

静的グループが作成され、左側ペインの親グループの下にリストされます。子グループは親グループからインデント付きで表示されます。

クエリデバイスグループの作成

クエリ グループは、いくつかのユーザー指定の条件に一致することによってデバイスが定義されている、動的なグループです。グループのデバイスは、クエリ基準を使用して検出されたデバイスの結果に基づいて変化します。[すべてのデバイス] ページ ([OpenManage Enteprise] > [デバイス]) で、[クエリ グループの作成] ウィザードを使用してクエリ グループを作成することができます。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

1. [クエリ グループの作成] ウィザードを有効にするには、次のいずれかを実行します。
   - [カスタム グループ] の下で、[クエリ グループ] を右クリックするまたはクエリ グループの横にある 3 つの縦方向のドットのメニューをクリックして、[新規クエリ グループの作成] をクリックします。
   - [グループ アクション] > [カスタム グループの作成] > [クエリ グループ] をクリックします。
2. [**クエリ グループの作成ウィザード**] ダイアログ ボックスで、グループの [名前] と [説明](オプション) を入力します。
3. **次へ**をクリックします。
4. **クエリ条件の選択** ダイアログボックスの **コピーする既存のクエリを選択** ドロップダウンメニューで、クエリを選択し、次に他のフィルタ条件を選択します。クエリ条件の選択 、p. 55 を参照してください。
5. **終了** をクリックします。
   クエリ グループが作成され、左側ペインのクエリ グループ セクションの下にリストされます。

クエリ条件の選択

クエリ条件を作成中に以下のためのフィルタを定義します。

- カスタマイズしたレポートの生成。「レポートの作成 、p. 137」を参照してください。
- カスタムグループ の下のクエリベースのデバイスグループの作成。「クエリデバイスグループの作成 、p. 55」を参照してください。

次の 2 つのオプションを使用してクエリ条件を定義します。

- **コピーする既存のクエリを選択** : デフォルトで OpenManage Enterprise では、自身のクエリ条件をコピーおよび構築可能な組み込みクエリテンプレートのリストを提供しています。クエリの定義中に最大 6 件の条件 (フィルター) を使用できます。フィルタを追加するには、**タイプの選択** ドロップダウンメニューから選択する必要があります。
- **タイプの選択** : このドロップダウンメニューに一覧表示されている属性を使用して、一からクエリ条件を構築します。メニュー内の項目は、OpenManage Enterprise によって監視されているデバイスによって異なります。クエリタイプを選択するときには、=、>、<、null などの適切な演算子のみがクエリタイプに基づいて表示されます。このメソッドは、カスタマイズされたレポートの構築において、クエリ条件を定義するために推奨されます。

  メモ: 複数の条件でクエリを評価する場合、評価順序は SQL と同じです。条件の評価に特定の順序を指定するには、クエリを定義するときに括弧を追加または削除します。

メモ: 選択すると、既存のクエリ条件のフィルタは、新しいクエリ条件を構築するためにのみ仮想的にコピーされます。既存のクエリに関連付けられたデフォルトのフィルタは変更されません。組み込みクエリ条件の定義 (フィルタ) は、カスタマイズされたクエリ条件を構築するための開始点として使用されます。たとえば、次のとおりです。

1. *Query1* は、次の事前定義されたフィルターを持つ組み込みクエリ条件です : `Task Enabled=Yes`
2. *Query1* のフィルター プロパティをコピーし、*Query2* を作成してから、別のフィルターを追加してクエリ条件をカスタマイズします : `Task Enabled=Yes` および `(Task Type=Discovery)`
3. その後、*Query1* を開きます。そのフィルター条件は、`Task Enabled=Yes` のままです。

1. **クエリ条件の選択** ダイアログボックスで、クエリグループ用か、またはレポート生成用にクエリ条件を作成したいかどうかに基づいて、ドロップダウンメニューから選択します。
2. プラス記号またはゴミ箱記号をそれぞれクリックしてフィルタを追加または削除します。
3. [**終了**] をクリックします。
   クエリ条件が生成され、既存のクエリのリストに保存されます。監査ログエントリが作成され、監査ログのリストに表示されます。「監査ログのモニター 、p. 122」を参照してください。

関連情報

デバイス設定コンプライアンスの管理 、p. 105
設定コンプライアンスベースラインの編集 、p. 109
設定コンプライアンスベースラインの削除 、p. 111

静的グループの編集

[すべてのデバイス] ページ ([OpenManage Enterprise] > [デバイス]) では、既存の静的グループの名前を変更したり、位置を変更したり、静的グループのデバイスを [静的グループの編集] ウィザードを使用して追加または削除したりすることができます。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

1. 静的グループを右クリックするまたは静的グループの横にある 3 つの縦方向のドットのメニューをクリックしてから、[編集] をクリックして [静的グループの編集] ウィザードをアクティブにします。
2. [静的グループの編集] ウィザードで、[名前]、[説明]、[親グループ] を編集することができます。
3. [次へ] をクリックします。
4. [グループ メンバーの選択] 画面で、デバイスのチェックをオンまたはオフにして、デバイスを静的グループに含めるか除外することができます。
5. [終了] をクリックします。

静的グループに加えられた変更が実装されます。

クエリ グループの編集

[すべてのデバイス] ページ ([OpenManage Enterprise] > [すべてのデバイス]) では、既存のクエリ グループの名前を変更し、再配置することができます。また、デバイスがクエリ グループに含まれる基準となるクエリ条件は、[クエリ グループの編集] ウィザードを使用して編集できます。

OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

1. [カスタム グループ] の下で、クエリ グループを右クリックするまたはクエリ グループの横にある 3 つの縦方向のドットのメニューをクリックして、[編集] をクリックします。
2. [クエリ グループの編集] ウィザードで、必要に応じて [名前] と [説明] を変更します。
3. [次へ] をクリックします。
4. [クエリ条件の選択] ダイアログ ボックスの [コピーする既存のクエリを選択] ドロップダウン メニューで、クエリを選択し、次に他のフィルター条件を選択します。
5. [終了] をクリックします。

クエリ グループに加えられた変更が実装されます。

静的またはクエリ グループの名前変更

[すべてのデバイス] ページ ([OpenManage Enterprise] > [デバイス]) で静的グループまたはクエリ グループの名前を変更するには、次の手順を実行します。

1. [カスタム グループ] で、静的グループまたはクエリ グループを右クリックするか、名前を変更するグループの横にある 3 つの点をクリックして、[名前の変更] をクリックします。または、グループを選択し、[グループ アクション] > [グループの名前変更] をクリックします。
2. **グループの名前変更**ダイアログ ボックスで、新しいグループ名を入力します。
3. [終了] をクリックします。
   更新された名前が左側ペインに表示されます。

静的またはクエリ デバイス グループの削除

[すべてのデバイス] ページ ([OpenManage Enterprise] > [デバイス]) では、既存の静的グループまたはクエリ グループを次のように削除できます。

OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。「OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15」を参照してください。

メモ: この手順は、静的グループまたはクエリ グループを削除する場合にのみ適用されます。ただし、グループ内のデバイスは、[すべてのデバイス] ページから削除されません。OpenManage Enterprise からデバイスを削除するには、OpenManage Enterprise からのデバイスの削除 、p. 60 を参照してください。

1. **カスタム グループ**の下で、静的グループまたはクエリ グループを右クリックするまたはグループの横にある 3 つの縦方向のドットのメニューをクリックして、[削除] をクリックします。または、削除するグループを選択し、[グループ アクション] ドロップダウン メニューから [グループの削除] をクリックします。
2. 確認のメッセージが表示されたら、[はい] をクリックします。

グループが [カスタム グループ] から削除されます。

静的グループまたはクエリ グループのクローン作成

既存の静的グループまたはクエリ グループのクローンを作成し、[カスタム グループ] に追加することができます。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。参照先： OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15

1. 静的グループまたはクエリ グループを右クリックするまたは静的グループまたはクエリ グループの横にある 3 つの縦方向のドットのメニューをクリックしてから、**クローン**をクリックします。
2. **グループのクローン作成**ダイアログ ボックスで、グループの名前と説明を入力します。さらに静的グループの場合、クローン作成された「静的」グループを作成する必要がある親グループを選択します。
3. **終了** をクリックします。
   クローン化されたグループが作成され、左側ペインの親グループの下にリストされます。

新しいグループへのデバイスの追加

新しいグループを作成し、[すべてのデバイス] ページで使用可能なデバイス リスト テーブルからデバイスを追加することができます。

OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

1. [OpenManage Enterprise] メニューで、[デバイス] をクリックします。
   [すべてのデバイス] ページが表示されます。
2. デバイス リストで、デバイスに対応するチェックボックスを選択し、[グループアクション] > [新規グループに追加] をクリックします。
   a. [新しいグループへのデバイスの追加ウィザード] ダイアログ ボックスで、[名前] と [説明] (オプション) を入力し、新しい子グループを作成する [親グループ] を選択します。グループの詳細については、「デバイスグループ」を参照してください。
   b. グループに複数のデバイスを追加する場合は、[次へ] をクリックします。それ以外の場合は、手順 3 に進みます。
3. [グループメンバーの選択] ダイアログボックスで、**デバイスの追加** リストから複数のデバイスを選択します。

[すべてのデバイス] タブでデバイスを選択した後は、選択したデバイスが **選択されたすべてのデバイス** に一覧表示されます。

4. **終了** をクリックします。
   新しいグループが作成され、デバイスは選択したグループに追加されます。
   メモ: グループの作成またはグループにデバイスを追加するには、グループの親子関係に従う必要があります。「デバイス グループ」を参照してください。

既存グループへのデバイスの追加

[すべてのデバイス] ページで使用可能なデバイス リストの表から既存のグループにデバイスを追加することができます。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

1. [OpenManage Enterprise] メニューで、[デバイス] をクリックします。
   [すべてのデバイス] ページが表示されます。
2. デバイス リストで、デバイスに対応するチェック ボックスを選択し、[グループ アクション] > [既存グループに追加] の順にクリックします。
3. [選択したデバイスを既存グループに追加] ダイアログ ボックスで、データを入力または選択します。グループの詳細については、「デバイスグループ」を参照してください。
4. **終了** をクリックします。
   デバイスが選択した既存のグループに追加されます。
   メモ: グループの作成またはグループにデバイスを追加するには、グループの親子関係に従う必要があります。「デバイス グループ」を参照してください。

グループでの正常性の更新

次の手順では、選択したグループの正常性およびオンライン ステータスを更新する方法について説明します。

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- ESXi および Linux オペレーティング システムを使用して検出されたインバンド デバイスの場合、正常性状態 ( ) は不明 ( ) として表示されます。

1. [OpenManage Enterprise] > [デバイス] の順にクリックして、[すべてのデバイス] ページに移動します。
2. 左ペインで、正常性を更新するグループを選択します。
   グループを選択すると、デバイスのリストに選択したグループのデバイスがリストされます。
3. [正常性の更新] ドロップダウン メニューをクリックしてから、[グループでの正常性の更新] をクリックします。[正常性] ウィザードが表示されます。
4. [正常性] ウィザードの [ジョブ名] には、アプライアンスによって生成された正常性更新タスクのジョブ名が表示されます。必要に応じて、ジョブ名を変更することができます。
5. [グループの選択] ドロップダウンに、選択したグループが表示されます。
6. [スケジュール] ドロップダウンから、次のいずれかのオプションを選択できます。
   a. [今すぐ実行] - 選択したグループの正常性の更新をただちに実行します。
   b. [後で実行] - [後で実行] を選択すると、グループの正常性更新ジョブが実行される日付と時刻を選択できます。
   c. [スケジュールに従って実行] - このオプションを選択してから [毎日] または [毎週] を選択して、毎日または毎週の特定の時刻にグループの正常性を更新できます。

グループの正常性およびオンライン ステータスを更新するジョブが作成されます。ジョブの詳細を表示するには、[ジョブ] ページ ([OpenManage Enterprise] > [監視] > [ジョブ]) を使用します。

デバイスリスト

デバイスリストには、IP アドレスやサービスタグなど、デバイスのプロパティが表示されます。ページごとに最大 25 台のデバイスを選択し、さらにデバイスを選択するためにページを移動して、タスクを実行することができます。すべてのデバイス ページで実行できるタスクの詳細については、「[すべてのデバイス] ページ - デバイス リスト アクション 、p. 59」を参照してください。

メモ: デフォルトで、デバイスリストには、ドーナツグラフの形成中に考慮されるすべてのデバイスが表示されます。特定の正常性状態に属するデバイスリストを表示するには、ドーナツグラフで対応する色の範囲をクリックするか、正常性状態の記号をクリックします。選択したカテゴリのみに属しているデバイスが一覧表示されます。

- **正常性状態** は、デバイスの動作状態を示します。正常性状態 (正常、重要、警告) は、色記号によって識別されます。参照先 : デバイスの正常性状態 、p. 38
- **電源状態**は、デバイスのオンまたはオフを示します
- **接続状態**は、検出されたデバイスと OpenManage Enterprise との接続状態を、[接続]、[切断]、または [切断 (認証エラー)] で示します
- **名前** はデバイス名を示します。
- **IP アドレス**は、デバイスにインストールされている iDRAC の IP アドレスを示します
- **識別子**は、デバイスのサービス タグを示します
- **モデル**は、モデル番号を示します
- **タイプ**は、デバイスのタイプ (サーバー、シャーシ、Dell ストレージ、ネットワーキング スイッチ) を示します
- **シャーシ名**は、シャーシ名を示します
- **スロット名**は、シャーシ デバイスのスロット名を示します
- **管理状態**列は、デバイスが監視されている、管理されている、またはプロキシされているかどうかを示します。監視または管理のためのデバイスの検出 、p. 39 を参照してください。

表のデータをフィルターするには、[高度なフィルター] またはフィルター アイコンをクリックします。HTML、CSV、または PDF ファイルフォーマットのデータをエクスポートするには、右上隅にあるエクスポートアイコンをクリックします。

メモ: デバイス リストで、デバイス名または IP アドレスをクリックしてデバイスの設定データを表示し、次に編集します。個々のデバイスの表示と設定 、p. 65 を参照してください。

メモ: 作業中ペインには、選択したデバイスグループのドーナツグラフが表示されます。このドーナツグラフを使用すると、そのグループで異なる正常性状態にあるデバイスリストを表示することができます。異なる正常性状態のデバイスを表示するには、ドーナツグラフの対応する色をクリックします。表内のデータが変更されます。ドーナツグラフの使用方法については、「ドーナツグラフ」を参照してください。

[すべてのデバイス] ページ - デバイス リスト アクション

[すべてのデバイス] ページ ([OpenManage Enterprise] > [デバイス]) デバイス リストでは、様々なデバイス アクションを実行することができます。

アクション ボタンは、左側のツリーとグリッドで選択したデバイスに対して、グループの選択の両方に対して、状況に応じて異なります。このため、アクションがグループに関連づけられている場合は、「グループでのインベントリーの実行」ループや「グループでの正常性の更新」などのグループ アクションは、デフォルトで選択されたグループになります。デバイスのすべてのアクションは、選択したデバイスに対してデフォルトで実行されます。ただし、検出などのいくつかのアクションは、選択なしで常に適用されます。また、デバイスごとに使用可能なアクションのタイプは、選択したデバイスのタイプによって異なります。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

- [グループ アクション] ドロップダウンでは、次の操作を実行できます。
  - カスタム デバイス グループを作成します。カスタム グループの作成 (静的またはクエリ) 、p. 54 を参照してください。
  - 静的グループを作成します。静的デバイス グループの作成 、p. 54 を参照してください。
  - クエリ グループを作成します。参照先 : クエリデバイスグループの作成 、p. 55
  - 静的またはクエリ グループを編集します。静的グループの編集 、p. 56 およびクエリ グループの編集 、p. 56 を参照してください。
  - グループのクローンを作成します。静的グループまたはクエリ グループのクローン作成 、p. 57 を参照してください。
  - グループの名前を変更します。静的またはクエリ グループの名前変更 、p. 56 を参照してください。
  - グループを削除します。静的またはクエリ デバイス グループの削除 、p. 57 を参照してください。
  - 新しいグループにデバイスを追加します。新しいグループへのデバイスの追加 、p. 57 を参照してください。

- 既存のグループにデバイスを追加します。既存グループへのデバイスの追加 、p. 58 を参照してください。
- [検出] ドロップダウンでは、次の操作を実行できます。
  - デバイスを検出してオンボードします。監視または管理のためのデバイスの検出 、p. 39 およびデバイスのオンボーディング 、p. 43 を参照してください。
  - デバイスを除外します。OpenManage Enterprise からのデバイスの除外 、p. 61 を参照してください。
  - 除外範囲を編集します。グローバル除外範囲 、p. 46 を参照してください。
- [インベントリー] ドロップダウンでは、次の操作を実行できます。
  - デバイス グループでインベントリーを実行します。「インベントリー ジョブの作成と実行」を参照してください。
  - デバイスでインベントリーを実行します。デバイスでのインベントリーの実行 、p. 61 を参照してください。
- [正常性の更新] ドロップダウン メニューでは、次の操作を実行できます。
  - グループの正常性状態を更新します。グループでの正常性の更新 、p. 58 を参照してください。
  - デバイスの正常性状態を更新します。デバイスでの正常性の更新 、p. 62 を参照してください。
- [その他のアクション] ドロップダウン メニューでは、次の操作を実行できます。
  - LED をオンにします。デバイスの LED を点灯させるジョブの作成 、p. 128 を参照してください。
  - LED をオフにします。デバイスの LED を点灯させるジョブの作成 、p. 128 を参照してください。
  - デバイスの電源をオンにします。電源デバイス管理のためのジョブの作成 、p. 129 を参照してください。
  - デバイスの電源をオフにします。電源デバイス管理のためのジョブの作成 、p. 129 を参照してください。
  - デバイスを正常にシャットダウンします。電源デバイス管理のためのジョブの作成 、p. 129 を参照してください。
  - システムの電源を入れ直します (コールド ブート)。電源デバイス管理のためのジョブの作成 、p. 129 を参照してください。
  - システムをリセットします (ウォーム ブート)。電源デバイス管理のためのジョブの作成 、p. 129 を参照してください。
  - デバイスで IPMI CLI リモートコマンドを実行します。個々のデバイスでのリモート RACADM および IPMI コマンドの実行 、p. 68 を参照してください。
  - デバイスで RACADM CLI リモートコマンドを実行します。個々のデバイスでのリモート RACADM および IPMI コマンドの実行 、p. 68 を参照してください。
  - OpenManage Enterprise からデバイスを削除します。OpenManage Enterprise からのデバイスの削除 、p. 60 を参照してください。
  - すべてのデバイスにデータをエクスポートします。参照先： すべてまたは選択したデータのエクスポート 、p. 64
  - 選択したデバイスにデータをエクスポートします。参照先： すべてまたは選択したデータのエクスポート 、p. 64

OpenManage Enterprise からのデバイスの削除

次の手順では OpenManage Enterprise で検出されたデバイスを削除およびオフボードにする方法について説明します。

メモ:
- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。「OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15」を参照してください。
- プロファイルが割り当てられているデバイスは、プロファイルの割り当てを解除しない限り削除できません。詳細については、プロファイルの割り当て解除 、p. 103 を参照してください。
- デバイスは、そこでタスクが実行中でも、削除できます。タスクの完了前にデバイスが削除された場合、そのデバイスで開始されたタスクは失敗します。

検出されたデバイスを削除するには、以下の手順を実行します。

1. [OpenManage Enterprise] > [デバイス] の順にクリックして、[すべてのデバイス] ページに移動します。
2. デバイス リストから、削除するデバイスに対応するチェック ボックスを選択します。
3. [その他のアクション] ドロップダウン メニューをクリックして、[デバイスの削除] をクリックします。
4. OpenManage Enterprise からデバイスが削除およびオフボードされることを示すプロンプトが表示されたら、[はい] をクリックします。

選択したデバイスは OpenManage Enterprise から完全に削除されます。デバイスの削除後は、削除したデバイスに対応するすべてのオンボード情報は削除されます。ユーザー資格情報は、他のデバイスと共有していない場合は自動的に削除されます。OpenManage Enterprise が削除されたデバイス上でトラップの宛先として設定されていた場合、デバイスから OpenManage Enterprise コンソール IP をトラップの宛先として削除する必要があります。

関連情報

デバイスのグループ化 、p. 52

OpenManage Enterprise からのデバイスの除外

デバイスは、ファームウェアのアップデート、設定のアップデート、インベントリー生成、およびアラートの監視などの繰り返しタスクを効率的に処理するために、OpenManage Enterprise で検出およびグループ化されます。ただし、すべての OpenManage Enterprise の検出、監視、および管理アクティビティからデバイスを除外することもできます。次の手順では、OpenManage Enterprise から既に検出されたデバイスを除外する方法について説明します。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

1. [OpenManage Enterprise] > [デバイス] の順にクリックして、[すべてのデバイス] ページに移動します。
2. 左側のペインで、デバイスを除外する必要があるシステム グループまたはカスタム グループを選択します。
3. デバイス リストで、デバイスに対応するチェック ボックスを選択し、[検出] ドロップダウン メニューから [デバイスの除外] をクリックします。
4. デバイスが完全に削除され、グローバル除外リストに追加されることを示すプロンプトが表示されたら、[はい] をクリックします。

デバイスは除外され、グローバル除外リストに追加され、以降は OpenManage Enterprise によって監視されません。

メモ: デバイスをグローバル除外から削除して OpenManage Enterprise がデバイスを再び監視するようにするには、デバイスをグローバル除外範囲から削除してから、再検出する必要があります。

デバイスでのインベントリーの実行

次の手順では、検出されたデバイスでインベントリー収集を開始する方法について説明します。

OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。参照先： OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15

1. [OpenManage Enterprise] > [デバイス] の順にクリックして、[すべてのデバイス] ページに移動します。
2. デバイスのリストから、デバイスに対応するチェック ボックスを選択します。
3. [インベントリー] ドロップダウンから、[デバイスでのインベントリーの実行] をクリックします。

選択したデバイスのインベントリー収集のインベントリー ジョブが作成されます。[インベントリー] ページで、このジョブのステータスを確認することができます ([OpenManage Enterprise] > [監視] > [インベントリー])。

ベースラインを使用したデバイス ファームウェア/ドライバーのアップデート

[すべてのデバイス] ページまたは [ファームウェア/ドライバーのコンプライアンス] ページからデバイスのファームウェア/ドライバーのバージョンをアップデートすることができます (ベースライン コンプライアンス レポートを使用したデバイスのファームウェア/ドライバーのアップデート 、p. 80 を参照)。単一デバイスのファームウェア/ドライバーをアップデートする場合は、[すべてのデバイス] ページの使用をお勧めします。

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- ドライバーのアップデートは、64 ビット版 Windows に関連付けられているデバイスにのみ適用されます。
- デバイス上のドライバーのアップデートをロールバックすることはできません。
- ファームウェア アップデートが [**次のサーバー再起動のためのステージ**] オプションを使用して実行されている場合は、リモート デバイスにパッケージをインストールした後でインベントリーとベースラインのチェックを手動で実行する必要があります。
- デバイスがどのベースラインにも関連付けられていない場合、[ベースライン] ドロップダウンメニューにデータが投入されません。デバイスをベースラインに関連付けるには、「ファームウェアのベースラインの作成」を参照してください。
- 複数のデバイスを選択すると、選択したベースラインに関連付けられているデバイスのみが表にリストされます。

1. [すべてのデバイス] ページの [**デバイス**] リストからデバイスを選択し、[その他のアクション] > [アップデート] をクリックします。

メモ: デバイスを選択する際は、デバイスが 1 つまたは複数のファームウェアベースラインに関連付けられていることを確認してください。そうしないと、デバイスがコンプライアンスレポートに表示されず、アップデートできません。

2. [デバイスのアップデート] ダイアログ ボックスで、次のように実行します。
   a. [アップデート ソースの選択] 画面で、次のいずれかを選択します。
      - [ベースライン] ドロップダウン メニューから、ベースラインを選択します。選択したファームウェア ベースラインに関連付けられているデバイスのリストが表示されます。各デバイスのコンプライアンス レベルは、[コンプライアンス] 列に表示されます。コンプライアンス レベルに基づいて、ファームウェア/ドライバーのバージョンをアップデートすることができます。このページのフィールドの説明についての詳細は、「デバイスファームウェアコンプライアンスレポートの表示」を参照してください。
        i. アップデートが必要なデバイスに対応するチェックボックスを選択します。
        ii. [次へ] をクリックします。
      - 個々のアップデート パッケージを使用して、ファームウェア/ドライバーをアップデートすることもできます。[個々のパッケージ] をクリックして画面の手順を完了します。**次へ**をクリックします。
   b. **スケジュール** セクションで :
      - [**アップデートのスケジュール**] の下で、[追加情報] をクリックして重要な情報を表示し、次のいずれかを選択します。
        a. [今すぐアップデート]: ファームウェア/ドライバーのアップデートをすぐに適用します。
        b. [実行日時を指定]: ファームウェア/ドライバーのバージョンをアップデートする日時を指定します。このモードは、現在のタスクに影響を与えたくない場合に推奨します。
      - [**サーバー オプション**] で、次のオプションのいずれかを選択します。
        a. ファームウェア/ドライバーのアップデート直後にサーバーを再起動するには、[サーバーをただちに再起動] を選択し、ドロップダウン メニューから次のいずれかのオプションを選択します。
           i. **正常な再起動 (強制シャットダウンなし)**
           ii. **正常な再起動 (強制シャットダウンあり)**
           iii. デバイスをハード リセットする**パワーサイクル。**
        b. 次のサーバー再起動時に、ファームウェア/ドライバーのアップデートをトリガーするには、[次のサーバー再起動のためのステージ] を選択します。このオプションが選択されている場合は、リモート デバイスにパッケージをインストールした後で、インベントリーとベースラインのチェックを手動で実行する必要があります。
3. [終了] をクリックします。

ファームウェア/ドライバー アップデート ジョブが作成されてジョブ リストにリストされます。デバイスコントロール用ジョブの使い方 、p. 124 を参照してください。

デバイス グループのデバイス正常性の更新

デフォルトでは、すべてのデバイスとデバイス グループの正常性は 1 時間ごとにアプライアンスによって自動的に更新されます。ただし、デバイスやデバイス グループの正常性は、いつでも更新できます。次の手順では、[すべてのデバイス] ページで選択したデバイス グループの正常性およびオンライン ステータスを更新する方法について説明します。

1. 左ペインで、デバイスが属するグループを選択します。
   グループに関連付けられているデバイスがリストされます。
2. デバイスに対応するチェック ボックスを選択し、[グループでの正常性の更新] をクリックします。
   ジョブが作成されてジョブリストに一覧表示され、ジョブステータス 列に **新規** と示されます。

選択したデバイス (複数可) の最新の作業ステータスが収集され、ダッシュボードと OpenManage Enterprise のその他関連セクションに表示されます。デバイスインベントリをダウンロードするには、「1 台のデバイスのインベントリのエクスポート 、p. 63」を参照してください。

関連情報

デバイスのグループ化 、p. 52

デバイスでの正常性の更新

デフォルトでは、すべてのデバイスとデバイス グループの正常性は 1 時間ごとにアプライアンスによって自動的に更新されます。ただし、デバイスやデバイス グループの正常性は、いつでも更新できます。次の手順では、[すべてのデバイス] ページで選択されたデバイスの正常性およびオンライン ステータスを更新する方法について説明します。

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- ESXi および Linux オペレーティング システムを使用して検出されたインバンド デバイスの場合、正常性状態 ( ) は不明 ( ) として表示されます。

1. [OpenManage Enterprise] > [デバイス] の順にクリックして、[すべてのデバイス] ページに移動します。
2. 正常性を更新するデバイスのリストからデバイスを選択します。
3. [正常性の更新] ドロップダウン メニューをクリックし、[デバイスでの正常性の更新] をクリックします。

選択したデバイスの正常性タスクが開始されます。正常性タスクのステータスは、[ジョブ] ページ ([OpenManage] > [監視] > [ジョブ]) で確認することができます。

個々のデバイスのファームウェア バージョンのロールバック

関連付けられているベースラインのファームウェアバージョンよりも新しいデバイスのファームウェアバージョンをロールバックすることができます。この機能は、個々のデバイスのプロパティを表示し、設定する場合にのみ使用できます。「個々のデバイスの表示と設定 、p. 65」を参照してください。個々のデバイスのファームウェアバージョンをアップグレードするかまたはロールバックすることができます。一度に 1 つのデバイスのみのファームウェアバージョンをロールバックすることができます。

メモ:
- ロールバックは、ファームウェアにのみ適用されます。アップデート後のデバイス ドライバーを以前のバージョンにロールバックすることはできません。
- ロールバックは、OME コンソールからアップデートされたデバイスにのみ適用されます (ベースラインと単一 DUP アップデートの両方に適用)。
- インストールされた iDRAC のいずれかが準備完了状態でない場合は、ファームウェアのアップデート ジョブは、ファームウェアが正常に適用されていても、失敗を示す場合があります。準備完了状態でない iDRAC を確認し、サーバの起動中に F1 を押して続行します。

iDRAC GUI を使用してアップデートしたデバイス ファームウェアはここにリストされず、アップデートできません。ベースラインの作成については、「ファームウェア/ドライバーのベースラインの作成 、p. 77」を参照してください。

1. 左ペインで、グループを選択して、リスト内のデバイス名をクリックします。
2. **<デバイス名>**ページで、[**ファームウェア/ドライバー**] をクリックします。
3. [ベースライン] ドロップダウンメニューで、デバイスが属するベースラインを選択します。
   選択したベースラインに関連付けられているすべてのデバイスがリストされます。表内のフィールドの説明については、「ベースライン コンプライアンス レポートの表示 、p. 79」を参照してください。
4. で示された、ファームウェア バージョンをロールバックする必要があるデバイスの、対応するチェック ボックスをオンにします。
5. **ファームウェアのロールバック** をクリックします。
6. **ファームウェアのロールバック** ダイアログボックスに、次の情報が表示されます。
   - **コンポーネント名** : ファームウェアバージョンが、ベースラインバージョンより新しいデバイスの上のコンポーネント。
   - **現在のバージョン** : コンポーネントの現在のバージョン。
   - **ロールバックバージョン** : コンポーネントをダウングレードできる推奨ファームウェアバージョン。
   - **ロールバックのソース** : [参照] をクリックし、ファームウェアのバージョンをダウンロードできるソースを選択します。
7. [**終了**] をクリックします。ファームウェアのバージョンがロールバックされます。

   メモ: 現在、ロールバック機能は、ファームウェアがロールバックされたバージョン番号のみを追跡します。ロールバックは、(バージョンをロールバックすることで) ロールバック機能を使用してインストールされたファームウェアのバージョンを考慮しません。

1 台のデバイスのインベントリのエクスポート

一度にインベントリデータをエクスポートできるデバイスは、1 台のみであり、エクスポート形式は .csv 形式のみです。

1. 左側のペインで、デバイスグループを選択します。グループ内のデバイスのリストは デバイス リストに表示されます。
   作業中のペインのドーナツグラフに、デバイスのステータスが示されます。「ドーナツグラフ」を参照してください。表には、選択したデバイスのプロパティが一覧表示されます。「デバイスリスト」を参照してください。
2. デバイスリストで対象のデバイスに対応するチェックボックスを選択し、**インベントリのエクスポート** をクリックします。

3. [名前を付けて保存] ダイアログボックスで、想定している場所に保存します。

メモ: .csv 形式にエクスポートした場合、GUI に表示される一部のデータが説明の文字列に列挙されないことがあります。

シャーシとサーバにおける追加アクションの実行

[追加アクション] ドロップダウンメニューを使用すると、すべてのデバイス ページで次のアクションを実行できます。デバイスを選択し、次のいずれかをクリックします。

- **LED をオンにする**：デバイスの LED を点灯して、データセンター内のデバイスグループ間でデバイスを識別します。
- **LED をオフにする**：デバイスの LED を消灯します。
- **電源オン**：デバイスの電源を入れます。
- **電源オフ**：デバイスの電源を切ります。
- **正常なシャットダウン**：クリックすると、ターゲットシステムがシャットダウンします。
- **システムのパワーサイクル (コールドブート)** - クリックしてシステムの電源をオフにした後、再起動します。
- **システムリセット (ウォームブート)**: クリックすると、ターゲットシステムを強制的にオフにしてオペレーティングシステムをシャットダウンし、再起動します。
- **プロキシ使用**：MX7000 シャーシのみに表示されます。マルチシャーシ管理 (MCM) の場合、MX7000 リードシャーシを通してデバイスが検出されたことを示します。
- **IPMI CLI**：クリックすると、IMPI コマンドが実行されます。「デバイスの管理用リモートコマンドジョブの作成 、p. 129」を参照してください。
- **RACADM CLI**：クリックすると、RACADM コマンドが実行されます。「デバイスの管理用リモートコマンドジョブの作成 、p. 129」を参照してください。
- **ファームウェアのアップデート**：「ベースラインを使用したデバイス ファームウェア/ドライバーのアップデート 、p. 61」を参照してください。
- **オンボーディング**：「デバイスのオンボーディング 、p. 43」を参照してください。
- **すべてをエクスポート / 選択したものをエクスポート**：「すべてまたは選択したデータのエクスポート 、p. 64」を参照してください。

MX7000 シャーシに対して表示されるハードウェア情報

- **シャーシ電源** - スレッドやその他のコンポーネントで使用している電源ユニット (PSU) の情報。
- **シャーシスロット** - シャーシで使用可能なスロットおよびスロットに取り付けられているコンポーネント (ある場合) の情報。
- **シャーシコントローラ** - シャーシ管理コントローラ (CMC) とそのバージョン。
- **ファン** - シャーシで使用されるファンの情報とその動作ステータス。
- **温度** - シャーシの温度ステータスと閾値。
- **FRU** - シャーシに搭載可能なコンポーネントまたはフィールド交換可能ユニット (FRU)。

すべてまたは選択したデータのエクスポート

データをエクスポートできます。

- デバイスグループに表示されるデバイスについて、戦略分析と統計分析を実行します。
- 最大で 1000 台のデバイスについて実行します。
- システム アラート、レポート、監査ログ、グループ インベントリー、デバイス リスト、保証情報、OpenManage Enterprise Services などに関連。
- HTML、CSV、PDF ファイル形式へのエクスポート。

メモ:

- 長い文字列を持つ列または多数の列を含む「幅の広い」表を PDF にエクスポートしないでください。PDFMaker ライブラリーの制限により、エクスポートされたデータの一番右のセクションに文字切れが発生します。
- 1 台のデバイスのインベントリーのエクスポートは.csv 形式のみです。参照先：1 台のデバイスのインベントリのエクスポート 、p. 63
- レポートの場合のみ、一度にすべてのレポートではなく、選択したレポートだけをエクスポートできます。選択したレポートのエクスポート 、p. 138 を参照してください。

。

1. データをエクスポートするには、**すべてをエクスポート** または **選択したものをエクスポート** を選択します。

ジョブが作成され、データが選択した場所にエクスポートされます。

2. データをダウンロードし、必要に応じて、戦略分析および統計分析を実行します。
選択肢に基づいて、データが表示されるか、あるいは正常に保存されます。

メモ: .csv フォーマットでデータをエクスポートする場合は、ファイルを開くために管理者レベルの資格情報が必要です。

個々のデバイスの表示と設定

メモ: 「デバイスリスト」で、デバイス名または IP アドレスをクリックしてデバイスの設定データを表示したら、この項の説明に従ってデバイス設定を編集します。

[OpenManage Enterprise] > [デバイス] > [デバイス リストのデバイスを選択] > [詳細の表示] の順にクリックして、次の操作を実行します。

- 正常性および電源状態、デバイス IP、サービス タグに関する情報を表示します。
- デバイスに関する一般情報を表示し、デバイス制御およびトラブルシューティングタスクを実行します。
- RAID、PSU、OS、NIC、メモリ、プロセッサ、およびストレージエンクロージャなどのデバイス情報を表示します。OpenManage Enterprise には、OpenManage Enterprise の監視対象デバイス上で使用されている NIC、BIOS、物理ディスク、仮想ディスクについての概要を示す組み込みレポート機能があります。[OpenManage Enterprise] > [監視] > [レポート] の順にクリックします。
- ファームウェアのベースラインに関連付けられたデバイスに含まれるコンポーネントのファームウェアバージョンをアップデートまたはロールバックします。デバイスのファームウェアおよびドライバーの管理 、p. 73 を参照してください。

  メモ: 個別のパッケージ ワークフローを使用してデバイスをアップデートする場合は、実行可能ファイル (EXE) ベースの Dell Update Packages のみがサポートされます。FX2 CMC をアップデートする場合、実行可能 DUP は、シャーシ内のいずれかのスレッド経由で取り付ける必要があります。
- デバイスに関するアラートを承認、エクスポート、削除、または無視します。「デバイスのアラートの管理」を参照してください。
- デバイスのハードウェアログデータを表示およびエクスポートします。個々のデバイスのハードウェアログの管理 、p. 68 を参照してください。
- 設定コンプライアンスの目的のために、デバイスの設定インベントリを表示および管理します。デバイスに対して設定インベントリが実行されると、コンプライアンスの比較が開始されます。
- デバイスに関連した設定コンプライアンスベースラインに対するそのデバイスのコンプライアンスレベルを表示します。デバイス設定コンプライアンスの管理 、p. 105 を参照してください。

デバイス概要

- [<デバイス名>] ページの **概要** に、デバイスの正常性、電源状態、およびサービス タグが表示されます。IP アドレスをクリックして、iDRAC ログインページを開きます。Dell サポート サイトにある『*iDRAC ユーザーズ ガイド*』を参照してください。
  - **情報** : サービス タグ、DIMM スロット、iDRAC DNS 名、プロセッサ、シャーシ、オペレーティング システム、データ センター名など、デバイスの情報。デバイスに関連付けられた管理 IP アドレスが複数リストされ、クリックすると該当するインターフェイスがアクティブになります。
  - **最近のアラート** : デバイスに対して最近生成されたアラート。
  - **最近のアクティビティ** : デバイス上で最近実行されたジョブのリスト。**すべて表示** をクリックすると、すべてのジョブを表示します。デバイスコントロール用ジョブの使い方 、p. 124 を参照してください。
  - **リモートコンソール** : [iDRAC の起動] をクリックすると、iDRAC アプリケーションが始動します。**仮想コンソールの始動** をクリックすると、仮想コンソールが起動します。**プレビューの更新** 記号をクリックして、**概要** ページを更新します。
  - **サーバサブシステム** : PSU、ファン、CPU、バッテリなど、デバイスのその他のコンポーネントの正常性状態を表示します。

    メモ: IPMI を使用して検出されたセンサー コンポーネントのサブシステム データを収集するのにかかる時間は、ネットワーク接続、ターゲット サーバー、およびターゲット ファームウェアによって異なります。センサー データの収集中にタイムアウトが発生した場合は、ターゲット サーバーを再起動します。
  - [最終更新日] セクションは、デバイスインベントリのステータスがアップデートされた最後の時刻を示します。[更新] ボタンをクリックして、ステータスを更新します。インベントリジョブが開始され、そのページのステータスが更新されます。
- **電源制御** を使用して、電源のオン / オフ、電源サイクル、デバイスの正常なシャットダウンを実行します。
- **トラブルシューティング** を使用して、以下を実行します。
  - 診断レポートを実行してダウンロードします。診断レポートの実行とダウンロード 、p. 66 を参照してください。
  - iDRAC をリセットします。

- Services (SupportAssist) レポートを解凍およびダウンロードします。Services (SupportAssist) レポートの解凍とダウンロード 、p. 67 を参照してください。
- デバイスステータスを更新します。
- デバイスインベントリを更新します。
- [インベントリの更新] をクリックして収集したデバイスインベントリをエクスポートします。すべてまたは選択したデータのエクスポート 、p. 64 を参照してください。
- デバイスで、リモート RACADM、および IPMI コマンドを実行します。個々のデバイスでのリモート RACADM および IPMI コマンドの実行 、p. 68 を参照してください。

OpenManage Enterprise は、OpenManage Enterprise の監視対象デバイスについての概要を取得するためのビルトインレポートを提供します。[OpenManage Enterprise] > [監視] > [レポート] > [デバイスの概要レポート] の順にクリックします。**実行** をクリックします。レポートの実行 、p. 135 を参照してください。

デバイスのハードウェア情報

OpenManage Enterprise では、コンポーネントとファームウェアコンプライアンスベースラインに対するそのコンプライアンスに関するビルトインレポートを提供しています。[OpenManage Enterprise] > [監視] > [レポート] > [コンポーネントごとのファームウェアコンプライアンスレポート] の順にクリックします。**実行** をクリックします。レポートの実行 、p. 135 を参照してください。

- **デバイスカード情報** — デバイスで使用されるカードに関する情報。
- **インストールされているソフトウェア** — デバイスの別のコンポーネントにインストールされているファームウェアおよびソフトウェアのリスト。
- **プロセッサ** — ソケット、シリーズ、速度、コア、モデルなどのプロセッサに関する情報。
- **RAID コントローラー情報** — ストレージデバイスで使用されている PERC および RAID コントローラー。ロールアップ状態は、重大度の高い RAID のステータスと同じです。ロールアップ正常性状態の詳細については、Dell TechCenter のホワイトペーパー『*第 14 世代以降の Dell EMC PowerEdge サーバーで iDRAC を使用してロールアップ正常性状態を管理する*』を参照してください。
- **NIC 情報** — デバイスで使用されている NIC に関する情報。
- **メモリ情報** — デバイスで使用されている DIMM に関するデータ。
- **アレイディスク** : デバイスにインストールされているドライブについての情報です。OpenManage Enterprise は、OpenManage Enterprise の監視対象デバイス上で使用できる HDD または仮想ドライブについてのビルトインレポートを提供します。[OpenManage Enterprise] > [監視] > [レポート] > [物理ディスクレポート] をクリックします。**実行** をクリックします。レポートの実行 、p. 135 を参照してください。
- **ストレージコントローラ** : デバイスにインストールされているストレージコントローラ。個々のコントローラのデータを表示するには、プラス記号をクリックします。
- **電源装置情報** : デバイスにインストールされている PSU についての情報。
- **オペレーティング システム** — デバイスにインストールされている OS。
- **ライセンス** — デバイスにインストールされた異なるライセンスの正常性状態。
- **ストレージエンクロージャ** — ストレージエンクロージャステータスと EMM のバージョン。
- **仮想フラッシュ** - 仮想フラッシュドライブとその技術仕様のリスト。
- **FRU** — 現場技術者のみが処理および修復できる、フィールド交換可能ユニット (FRU) のリスト。OpenManage Enterprise は、OpenManage Enterprise の監視対象デバイスに取り付けられているフィールド交換可能ユニット (FRU) についてのビルトインレポートを提供します。[OpenManage Enterprise] > [監視] > [レポート] > [FRU レポート] をクリックします。**実行** をクリックします。レポートの実行 、p. 135 を参照してください。
- **デバイス管理情報** — サーバデバイスの場合にのみインストールされる iDRAC の IP アドレス情報。
- **ゲストの情報** — OpenManage Enterprise で監視するゲストデバイスを表示します。UUID は、デバイスの汎用の固有識別子です。**ゲストの状態** 列は、ゲストデバイスの動作ステータスを示します。

診断レポートの実行とダウンロード

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。参照先：OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15

メモ: シャーシや、iDRAC バージョン 2.50.50.50 以前が動作している PowerEdge YX2X および YX3X サーバーとの通信が必要なファームウェア タスクを開始するには、事前に [SMB 設定] で SMBv1 を有効にしておく必要があります。詳細については、「コンソールプリファレンスの管理 、p. 158」および「Dell EMC PowerEdge サーバーの汎用命名規則 、p. 179」を参照してください。

1. **<デバイス名>** ページで、**トラブルシューティング** ドロップダウンメニューから、**診断を実行する** を選択します。
2. **リモート診断タイプ** ダイアログボックスの **リモート診断タイプ** ドロップダウンメニューで、次のいずれかを選択してレポートを生成します。
   - **急速**：可能な限り最短の時間で生成。
   - **延長**：公称速度で生成。
   - **長時間**：遅いペースで生成。

   メモ: https://en.community.dell.com/techcenter/extras/m/white_papers/20438187 でテクニカル ホワイトペーパー『*WS-MAN コマンドと RACADM コマンドを使用して自動診断をリモートで実行する*』を参照してください。
3. 診断レポートを今すぐ生成するには、**今すぐ実行** を選択します。
4. **OK** をクリックします。プロンプトが表示されたら、**はい** をクリックします。

   警告: 診断レポートを実行すると、自動的にサーバが再起動します。

   ジョブが作成され、**ジョブ** ページに表示されます。ジョブについての情報を表示するには、右ペインで、**詳細の表示** をクリックします。ジョブ リストの表示 、p. 124 を参照してください。ジョブステータスも、**最近のアクティビティ** セクションに表示されます。ジョブが正常に実行された後、ジョブのステータスは **診断完了** と示され、**ダウンロード** リンクが **最近のアクティビティ** セクションに表示されます。
5. レポートをダウンロードするには、**ダウンロード** リンクをクリックし、*<サービスタグ-ジョブ ID>*.TXT 診断レポートファイルをダウンロードします。
   - それ以外の場合は、[トラブルシューティング] > [診断レポートのダウンロード] をクリックして、ファイルをダウンロードします。
6. **リモート診断ファイルのダウンロード** ダイアログボックスで、.TXT ファイルのリンクをクリックし、レポートをダウンロードします。
7. **OK** をクリックします。

Services（SupportAssist）レポートの解凍とダウンロード

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。参照先： OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15

メモ: シャーシや、iDRAC バージョン 2.50.50.50 以前が動作している PowerEdge YX2X および YX3X サーバーとの通信が必要なファームウェア タスクを開始するには、事前に [SMB 設定] で SMBv1 を有効にしておく必要があります。詳細については、コンソールプリファレンスの管理 、p. 158 および Dell EMC PowerEdge サーバーの汎用命名規則 、p. 179 を参照してください。

1. **<デバイス名>** ページで、**トラブルシューティング** ドロップダウンメニューから、**SupportAssist レポートの解凍** を選択します。
2. **SupportAssist レポートの解凍** ダイアログボックスで、次の手順を実行します。
   a. SupportAssist のレポートを保存するファイル名を入力します。
   b. SupportAssist のレポートを解凍するログの種類に対応するチェックボックスを選択します。
3. **OK** をクリックします。
   ジョブが作成され、**ジョブ** ページに表示されます。ジョブについての情報を表示するには、右ペインで、**詳細の表示** をクリックします。ジョブ リストの表示 、p. 124 を参照してください。ジョブステータスも、**最近のアクティビティ** セクションに表示されます。ジョブが正常に実行された後、ジョブのステータスは **診断完了** と示され、**ダウンロード** リンクが **最近のアクティビティ** セクションに表示されます。
4. レポートをダウンロードするには、**ダウンロード** リンクをクリックして、*<サービスタグ>.<時刻>*.TXT SupportAssist レポートファイルをダウンロードします。
   - それ以外の場合は、[トラブルシューティング] > [SupportAssist レポートをダウンロード] をクリックします。
5. **SupportAssist ファイルのダウンロード** ダイアログボックスで、.TXT ファイルのリンクをクリックし、レポートをダウンロードします。各リンクは、選択したログタイプを表します。
6. **OK** をクリックします。

個々のデバイスのハードウェアログの管理

メモ: ハードウェア ログは、YX4X サーバー、MX7000 シャーシ、スレッドで使用できます。詳細については、「Dell EMC PowerEdge サーバーの汎用命名規則 、p. 179」を参照してください。

- [<デバイス名>] ページで、[ハードウェアログ] をクリックします。デバイスに生成されたすべてのイベントとエラーメッセージが一覧表示されます。フィールドの説明については、「監査ログのモニター 、p. 122」を参照してください。
- シャーシの場合、ハードウェアログに関するリアルタイムデータがシャーシから取得されます。
- コメントを追加するには、[コメントの追加] をクリックします。
- ダイアログボックスに、コメントを入力し、[保存] をクリックします。コメントが保存され、[コメント] 行の記号によって識別されます。
- 選択したログデータを .CSV ファイルにエクスポートするには、対応するチェックボックスを選択し、[エクスポート] > [選択したものをエクスポート] の順にクリックします。
- ページ上のすべてのログをエクスポートするには、[エクスポート] > [現在のページをエクスポート] の順にクリックします。

個々のデバイスでのリモート RACADM および IPMI コマンドの実行

[デバイス名] ページからデバイスの iDRAC に RACADM コマンドと IPMI コマンドを送信して、それぞれのデバイスをリモートで管理することができます。

メモ:

- RACADM CLI では、一度に 1 つのコマンドのみが許可されます。
- 次の特殊文字は、RACADM および IPMI の CLI パラメーターとしての使用はサポートされていません：**[**、**;**、**|**、**$**、**>**、**<**、**&**、**'**、**]**、**.**、*、**'**。

1. デバイスに対応するチェックボックスを選択し、**詳細の表示** をクリックします。
2. **<デバイス名>** ページで、**リモートコマンドライン** をクリックし、**RACADM CLI** または **IPMI CLI** を選択します。

   メモ: MX740c、MX840c、MX5016S などのデバイスパックでは、対応するタスクを使用できないため、次のサーバでは RACADM CLI タブは表示されません。

3. **リモートコマンドの送信** ダイアログボックスに、コマンドを入力します。コマンドは 100 個まで入力でき、それぞれ改行して入力します。同じダイアログボックスに結果を表示するには、**送信後に結果を表示する** チェックボックスを選択します。

   メモ: 次の構文で IPMI コマンドを入力します。`-I lanplus <command>`コマンドを終了するには、「Exit」と入力します。

4. **送信** をクリックします。
   ジョブが作成され、ダイアログボックスに表示されます。ジョブは、ジョブの詳細 にも一覧表示されます。ジョブ リストの表示 、p. 124 を参照してください。
5. **終了** をクリックします。
   最近のアラート セクションに、ジョブの完了ステータスが表示されます。

デバイスの管理アプリケーション iDRAC の開始

1. デバイスに対応するチェックボックスを選択します。
   デバイスの稼働状態、名前、タイプ、IP、サービスタグが表示されます。
2. 右ペインで、[管理アプリケーションの起動] をクリックします。
   iDRAC ログインページが表示されます。iDRAC 資格情報を使用してログインします。

   iDRAC 使用の詳細については、Dell.com/idracmanuals にアクセスしてください。

   メモ: デバイス リスト内の IP アドレスをクリックして、管理アプリケーションを起動することもできます。「デバイスリスト 、p. 59」を参照してください。

仮想コンソールの起動

仮想コンソール リンクは、YX4X サーバーの iDRAC Enterprise ライセンスで機能します。YX2X および YX3X サーバーの場合、このリンクは 2.52.52.52 以降のバージョンの iDRAC Enterprise ライセンスで機能します。仮想コンソールの現在のプラグイン タイプが Active X の場合にリンクをクリックすると、ユーザー エクスペリエンス向上のために、コンソールを HTML 5 にアップデートす

るよう求めるメッセージが示されます。詳細については、「仮想コンソール プラグイン タイプを変更するジョブの作成 、p. 130」および「Dell EMC PowerEdge サーバーの汎用命名規則 、p. 179」を参照してください。

1. デバイスに対応するチェックボックスを選択します。
   デバイスの稼働状態、名前、タイプ、IP、サービスタグが表示されます。
2. 右ペインで、[仮想コンソールの起動] をクリックします。
   サーバにリモートコンソールページが表示されます。

単一デバイスのデバイス インベントリーの更新

デフォルトでは、デバイスまたはデバイス グループ内のソフトウェアおよびハードウェア コンポーネントのインベントリーは、24 時間ごと (つまり毎日深夜 00:00) に自動的に収集されます。ただし、次の手順により、任意の時点で、1 つのデバイスのインベントリー レポートを収集できます。

1. [すべてのデバイス] ページのデバイス ([OpenManage Enterprise] > [デバイス]) で対応するチェック ボックスを選択し、右ペインの [詳細の表示] をクリックします。デバイスの [概要] ページが表示されます。
2. [**インベントリーの更新]** をクリックして、インベントリー ジョブを開始します。
   インベントリー ジョブのステータスは、[インベントリー] ページ ([OpenManage Enterprise] > [監視] > [インベントリー]) で確認できます。インベントリー ジョブを選択し、[詳細の表示] をクリックして、選択したデバイスの収集済みインベントリーを表示します。更新されたインベントリデータの表示についての詳細は、「個々のデバイスの表示と設定 、p. 65」を参照してください。デバイスインベントリをダウンロードするには、「1 台のデバイスのインベントリのエクスポート 、p. 63」を参照してください。

関連情報

デバイスのグループ化 、p. 52

9

デバイスインベントリの管理

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

[OpenManage Enterprise] > [監視] > [インベントリ] をクリックして、デバイスインベントリレポートを生成すると、データセンターの管理を向上してメンテナンスを減らし、最小在庫を維持して運用コストを削減することができます。OpenManage Enterprise のインベントリスケジュール機能を使用すると、事前に定義された時刻にジョブを実行するようにスケジュールしてレポートを生成できます。第 12 世代以降の PowerEdge サーバ、ネットワークデバイス、PowerEdge シャーシ、EqualLogic アレイ、Compellent アレイ、および PowerVault デバイスで、インベントリジョブをスケジュールできます。

このページでは、インベントリスケジュールを作成、編集、実行、停止、または削除できます。既存のインベントリスケジュールジョブのリストが表示されます。

- [名前]: インベントリスケジュールの名前。
- [スケジュール]: ジョブを今すぐ実行するか、または後で実行するかを示します。
- [最終実行]: ジョブが最後に実行された時刻を示します。
- [ステータス]: ジョブのステータスが実行中、完了、または失敗のいずれであるかを示します。

メモ: [検出] と [インベントリのスケジュール] ページに、スケジュール済みジョブのステータスは [待機] と [ステータス] 列に示されています。ただし、[ジョブ] ページでは、[スケジュール済み] として同じステータスが示されます。

ジョブ情報をプレビューするには、対象のジョブに対応する列をクリックします。右ペインには、インベントリタスクに関連したジョブデータとターゲットグループが表示されます。ジョブについての情報を表示するには、[詳細の表示] をクリックします。[ジョブの詳細] ページに、詳細情報が表示されます。個々のジョブ情報の表示 、p. 128 を参照してください。

関連タスク

インベントリジョブを今すぐ実行する 、p. 71
インベントリジョブの停止 、p. 71
インベントリジョブの削除 、p. 72
インベントリジョブの作成 、p. 70

トピック：

インベントリジョブの作成

次の手順では、検出されたグループでインベントリーの収集を開始する方法について説明します。

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- シャーシ ストレージ スレッドのインベントリー収集がシャーシのデバイス管理を使用して管理される場合、OpenManage Enterprise では、シャーシ ストレージ スレッドのインベントリー収集はサポートされません。

1. [インベントリー] ウィザードを開始するには、次のいずれかを実行します。

a. [すべてのデバイス] ページ ([OpenManage Enterprise] > [デバイス]) の左ペインでグループを選択し、[インベントリー] ドロップダウン メニューから [グループでのインベントリーの実行] をクリックします。
b. [インベントリー] ページ ([OpenManage Enterprise] > [監視] > [インベントリー]) で、[作成] をクリックします。

2. [インベントリ] ダイアログボックスで、[インベントリジョブ名] にデフォルトのインベントリジョブ名を入力します。変更するには、インベントリジョブ名を入力します。
3. [グループの選択] ドロップダウンメニューから、インベントリを実行する必要があるデバイスグループを選択します。
グループを選択した後に [すべてのデバイス] ページからインベントリー ジョブを開始した場合、選択したグループ名が [グループの選択] に入力されます。デバイス グループの詳細については、デバイスのグループ化 、p. 52 を参照してください。
4. [スケジュール] セクションで、ジョブをただちに実行するか、後の時点で実行するようにスケジュールします。
スケジュールジョブフィールドの定義 、p. 174 を参照してください。
5. インベントリー ジョブの実行中に、次の [追加オプション] を選択できます。
- [設定インベントリーの収集] チェック ボックスを選択して、設定コンプライアンス ベースラインのインベントリーを生成します。
- [ドライバー インベントリーの収集] チェック ボックスを選択して、Windows サーバーからドライバー インベントリー情報を収集します。また、Windows サーバーでインベントリー コレクターと Dell System Update を使用できない場合に、これらのコンポーネントをサーバーにインストールするときにも、同様に選択します。

メモ:
- [ドライバー インベントリーの収集] は、64 ビット版 Windows サーバーとして検出されたデバイスにのみ適用されます。
- Windows ベースのデバイス インベントリーの収集は、OpenSSH を使用した場合にのみサポートされます。CygWin SSH のようなその他の Windows SSH 実装はサポートされていません。

設定コンプライアンス ベースラインの詳細については、デバイス設定コンプライアンスの管理 、p. 105 を参照してください。
6. **終了**をクリックします。
7. ジョブが作成され、キュー内に一覧表示されます。
インベントリジョブが作成され、インベントリジョブのリストに表示されます。[スケジュール] 行には、ジョブがスケジュールされているか、スケジュールされていないかどうかが指定されます。インベントリジョブを今すぐ実行する 、p. 71 を参照してください。

関連情報

デバイスインベントリの管理 、p. 70

インベントリジョブを今すぐ実行する

メモ: すでに実行中のジョブを再実行できません。

1. 既存のインベントリスケジュールジョブのリストで、直ちに実行するインベントリジョブに対応するチェックボックスを選択します。
2. [今すぐ実行] をクリックします。
ジョブがただちに開始され、メッセージが右下隅に表示されます。

関連情報

デバイスインベントリの管理 、p. 70

インベントリジョブの停止

ジョブを実行中にのみ停止できます。完了または失敗したインベントリジョブは停止できません。ジョブを停止するには次の手順を実行します。

1. 既存のインベントリスケジュールジョブのリストで、停止したいインベントリスケジュールジョブに対応するチェックボックスを選択します。
2. [停止] をクリックします。
ジョブが停止され、メッセージが右下隅に表示されます。

関連情報

デバイスインベントリの管理 、p. 70

インベントリジョブの削除

メモ: ジョブが実行中の場合は、削除できません。

1. 既存のインベントリスケジュールジョブのリストで、削除するインベントリジョブに対応するチェックボックスを選択します。
2. [削除] をクリックします。
   ジョブが削除され、メッセージが右下隅に表示されます。

関連情報

デバイスインベントリの管理 、p. 70

インベントリスケジュールジョブの編集

1. [編集] をクリックします。
2. [インベントリスケジュール] ダイアログボックスで、[インベントリジョブ名] のインベントリジョブ名を編集します。「インベントリジョブの作成 、p. 70」を参照してください。
   インベントリスケジュールジョブがアップデートされ、表に示されます。

10

デバイスのファームウェアおよびドライバーの管理

[OpenManage Enterprise] > [設定] > [ファームウェア/ドライバーのコンプライアンス] ページでは、すべての「管理」デバイスのファームウェアを管理することができます。64 ビット Windows ベースのデバイスのドライバーをアップデートすることもできます。

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- ベースライン バージョンより前のデバイスのファームウェア/ドライバーのバージョンは自動的にアップデートされないため、ユーザーはアップデートを開始する必要があります。
- デバイスまたは環境が勤務時間中にオフラインになってしまうのを防ぐため、メンテナンス時にデバイスのファームウェア/ドライバーをアップデートすることをお勧めします。
- デバイスのファームウェア/ドライバーを管理するには、システムのオンボード ステータスが「管理」または「アラートで管理」のいずれかである必要があります。参照先： デバイスのオンボーディング 、p. 43
- 現在、カタログには 64 ビット版 Windows ベースのデバイスのみのドライバーが含まれています。

[ファームウェア/ドライバー] 機能を使用すると、次の操作を実行できます。

- ファームウェア/ドライバーのカタログを Dell.com から直接、またはネットワーク パスに保存した後に使用します。Dell.com を使用したカタログの追加 、p. 74 または「ローカルネットワーク使用によるファームウェアカタログの作成」を参照してください。
- 使用可能なカタログを使用して、ファームウェア/ドライバーのベースラインを作成します。これらのベースラインは、デバイスのファームウェア/ドライバーのバージョンをカタログのバージョンと比較するためのベンチマークとして機能します。「ファームウェアのベースラインの作成」を参照。
- ベースラインに関連付けられたデバイスがベースライン ファームウェアおよびドライバーのバージョンに準拠しているかどうかを確認するには、コンプライアンス レポートを実行します。「ファームウェアのコンプライアンスチェック」を参照。[コンプライアンス] 列が表示されます。
  - **OK** - ターゲット デバイス ファームウェア/ドライバーのバージョンがベースラインと一致している場合。
  - **アップグレード** - ターゲット デバイスにベースラインのファームウェア/ドライバーよりも以前のバージョンがいくつか存在する場合。「デバイスのファームウェア バージョンのアップデート」を参照してください。
  - **重要** - デバイスがベースラインに準拠していない場合に、これが重要なアップグレードであることおよび、適切に機能させるにはデバイス ファームウェア/ドライバーのアップグレードが必要であることを示します。
  - **警告** - デバイスのファームウェア/ドライバーがベースラインに準拠していない場合に、デバイス ファームウェアのアップグレードによって機能を強化できることを示します。
  - **ダウングレード** - デバイスのファームウェア/ドライバーがベースラインより後のバージョンの場合。
  - 統計や分析のためにコンプライアンスレポートをエクスポート。
  - ベースラインを使用して、デバイスのファームウェア/ドライバーのバージョンをアップデートします。ベースラインを使用したデバイス ファームウェア/ドライバーのアップデート 、p. 61 を参照してください。

メモ:

- 多くのデバイスを含むファームウェア/ドライバーのベースラインの準拠について確認する場合、アラート ページの警告アラート CDEV9000 は、そのベースラインからランダムに抽出された 1 個の非準拠デバイス対してのみログに記録されます。
- ネットワーク スイッチ、モジュラー型 IOA、Dell ストレージ デバイスのファームウェアまたはドライバーは Dell カタログを使用してアップデートできないため、コンプライアンス ステータスが「**不明**」として表示されます。これらのデバイスについては、個々のアップデート パッケージを用いて、ファームウェアまたはドライバーのアップデートを個別に実行することをお勧めします。ファームウェアまたはドライバーのアップデートを個別に実行するには、[すべてのデバイス] ページでデバイスを選択し、[詳細表示] > [ファームウェア/ドライバー] をクリックして、個々のパッケージ オプション

を選択します。サポート対象外デバイスのリストの詳細については、ファームウェア/ドライバー コンプライアンス ベースライン レポート—「不明」コンプライアンス ステータスのデバイス 、p. 178 を参照してください。

以下でもデバイスのファームウェアのバージョンをアップデートできます。

- すべてのデバイス ページ。「デバイスのファームウェアバージョンのアップデート」を参照。
- デバイスの詳細 ページ。デバイス リストで、デバイス名または IP アドレスをクリックしてデバイスの設定データを表示し、次に編集します。個々のデバイスの表示と設定 、p. 65 を参照してください。

  メモ: 個別のパッケージ ワークフローを使用してデバイスをアップデートする場合は、実行可能ファイル (EXE) ベースの Dell Update Packages のみがサポートされます。FX2 CMC をアップデートする場合、実行可能 DUP は、シャーシ内のいずれかのスレッド経由で取り付ける必要があります。

すべてのベースラインの概要が作業中のペインに表示され、選択したベースラインのコンプライアンスがドーナツグラフによって右ペインに表示されます。ドーナツ グラフおよび項目リストは、ベースライン リストから選択したベースラインに基づいて変更されます。「ドーナツグラフ」を参照してください。

トピック：

- ファームウェア カタログおよびドライバー カタログの管理
- ファームウェア/ドライバーのベースラインの作成
- 設定コンプライアンス ベースラインの削除
- ベースラインの編集
- デバイス ファームウェア/ドライバーのコンプライアンスの確認

ファームウェア カタログおよびドライバー カタログの管理

カタログは、デバイス タイプに基づいてファームウェア/ドライバーにバンドルされています。利用可能なすべてのカタログ (アップデートパッケージ) が検証され、Dell.com に掲載されています。オンライン リポジトリから直接カタログを使用するか、またはネットワーク共有にダウンロードすることができます。

これらのカタログを使用して、検出されたデバイスのファームウェア/ドライバーのベースラインを作成し、コンプライアンスを確認することができます。これにより、管理者やデバイス管理者への負荷が軽減し、全体的なアップデート作業やメンテナンスの時間を削減できます。

管理者ユーザーは OpenManage コンソールのすべてのカタログを表示してアクセスできますが、デバイス マネージャーは、自分が作成して、所有するカタログのみを表示および管理できます。「OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15」を参照してください。

カタログ管理 ページのフィールド定義については、「カタログの管理フィールドの定義 、p. 178」を参照してください。現在のアクセス可能なカタログソースは、次のとおりです。

メモ:

- Dell.com またはローカル ネットワーク パスを使用したファームウェア カタログの管理は、Enterprise Server カタログのみに限定されます。
- 「Downloads.dell.com」をポイントするベース ロケーションを持つカタログは、ネットワーク共有から OpenManage Enterprise バージョン 3.5 でカタログをインポートするときに、Dell Update Packages (DUP) なしで使用できます。ファームウェアのアップグレード プロセス中に、https://downloads.dell.com から直接 DUP がダウンロードされます。

- [Dell.com の最新コンポーネント バージョン]: デバイスの最新のファームウェアおよびドライバー (64 ビット版 Windows) バージョンをリストします。たとえば、厳しくテストおよびリリースされ、Dell.com に掲載された iDRAC、BIOS、PSU、および HDD。「Dell.com 使用によるファームウェアカタログの作成」を参照。
- [ネットワーク パス]: ファームウェア/ドライバーのカタログが、Dell Repository Manager (DRM) によってダウンロードされ、ネットワーク共有に保存される場所です。「ローカルネットワーク使用によるファームウェアカタログの作成」を参照。

Dell.com を使用したカタログの追加

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

メモ: シャーシや、iDRAC バージョン 2.50.50.50 以前が動作している PowerEdge YX2X および YX3X サーバーとの通信が必要なファームウェア タスクを開始するには、事前に [SMB 設定] で SMBv1 を有効にしておく必要があります。詳細については、コンソールプリファレンスの管理 、p. 158 および Dell EMC PowerEdge サーバーの汎用命名規則 、p. 179 を参照してください。

1. [カタログ管理] ページで、[追加] をクリックします。
2. [カタログのアップデートの追加] ダイアログ ボックスで、次の手順を実行します。
   a. [名前] ボックスに、ファームウェア カタログの名前を入力します。
   b. [カタログ ソース] で、[Dell.com の最新コンポーネント バージョン] を選択します。
   c. [カタログのアップデート] ボックスで、[手動] または [自動] を選択します。
   d. [カタログのアップデート] ボックスで [自動] を選択した場合、[更新頻度] を [毎日] または [毎週] のいずれかに選択して、時刻を AM/PM の 12 時間形式で指定します。
   e. [終了] をクリックします。
   [終了] ボタンは、ダイアログ ボックスのすべてのフィールドが入力し終わるまで表示されません。

   新しいファームウェアカタログが [カタログの管理] ページのカタログテーブルに作成され、表示されます。
3. [ファームウェア/ドライバーのコンプライアンス] ページに戻るには、[ファームウェア/ドライバーのコンプライアンスに戻る] をクリックします。

ローカル ネットワークへのカタログの追加

ファームウェアおよびドライバー (64 ビット版 Windows) を含むカタログは、Dell Repository Manager (DRM) を使用してダウンロードし、ネットワーク共有に保存することができます。

1. [カタログ管理] ページで、[追加] をクリックします。
2. [カタログのアップデートの追加] ダイアログ ボックスで、次の手順を実行します。
   a. [名前] ボックスに、カタログの名前を入力します。
   b. カタログ ソースの場合は、[ネットワーク パス] オプションを選択します。
   [共有タイプ] ドロップダウンメニューが表示されます。
   c. 次のいずれか 1 つを選択します。

   メモ: シャーシや、iDRAC バージョン 2.50.50.50 以前が動作している PowerEdge YX2X および YX3X サーバーとの通信が必要なファームウェア タスクを開始するには、事前に [SMB 設定] で SMBv1 を有効にしておく必要があります。詳細については、コンソールプリファレンスの管理 、p. 158 および Dell EMC PowerEdge サーバーの汎用命名規則 、p. 179 を参照してください。

   - NFS
     i. [共有アドレス] ボックスに、ネットワーク上のファームウェアカタログが保存されているシステムの IP アドレスを入力します。
     ii. [カタログファイルパス] ボックスに、カタログファイルの場所のフルファイルパスを入力します。パスの例 : *nfsshare\catalog.xml*
   - CIFS
     i. [共有アドレス] ボックスに、ネットワーク上のファームウェアカタログが保存されているシステムの IP アドレスを入力します。
     ii. [カタログファイルパス] ボックスに、カタログファイルの場所のフルファイルパスを入力します。パスの例 : *Firmware\m630sa\catalog.xml*
     iii. [ドメイン] ボックスに、デバイスのドメイン名を入力します。
     iv. [ユーザー名] ボックスに、カタログが保存されているデバイスのユーザー名を入力します。
     v. [パスワード] ボックスに、共有にアクセスするデバイスのパスワードを入力します。catalog.xml ファイルが格納されている共有フォルダのユーザー名とパスワードを入力します。
   - HTTP
     i. [共有アドレス] ボックスに、ネットワーク上のファームウェアカタログが保存されているシステムの IP アドレスを入力します。
     ii. [カタログファイルパス] ボックスに、カタログファイルの場所のフルファイルパスを入力します。パスの例 : *compute/catalog.xml*
   - HTTPS
     i. [共有アドレス] ボックスに、ネットワーク上のファームウェアカタログが保存されているシステムの IP アドレスを入力します。

ii. [カタログファイルパス] ボックスに、カタログファイルの場所のフルファイルパスを入力します。パスの例：*compute/catalog.xml*
iii. [ユーザー名] ボックスに、カタログが保存されているデバイスのユーザー名を入力します。
iv. [パスワード] ボックスに、カタログが保存されているデバイスのパスワードを入力します。
v. [証明書チェック] のチェック ボックスを選択します。

カタログファイルが保存されているデバイスの信頼性が検証され、セキュリティ証明書が生成されて [証明書情報] ダイアログボックスに表示されます。

d. [共有アドレス] と [カタログ ファイル パス] を入力すると、[今すぐテスト] リンクが表示されます。カタログへの接続を検証するには、[今すぐテストする] をクリックします。カタログへの接続が確立されると、「*接続しました*」というメッセージが表示されます。共有アドレスやカタログ ファイル パスへの接続が確立されていない場合は、「*パスに接続できませんでした*」というエラー メッセージが表示されます。これはオプションの手順です。
e. [カタログのアップデート] ボックスで、[手動] または [自動] を選択します。
[カタログのアップデート] で [自動] を選択した場合は、[毎日] か [毎週] を選択して、12 時間形式で更新頻度を入力します。

3. [終了] をクリックします。[終了] ボタンは、ダイアログ ボックスのすべてのフィールドが入力し終わるまで表示されません。
新しいファームウェアカタログが [カタログの管理] ページのカタログテーブルに作成され、表示されます。
4. [ファームウェア/ドライバーのコンプライアンス] ページに戻るには、[ファームウェア/ドライバーのコンプライアンスに戻る] をクリックします。

関連タスク

カタログの削除 、p. 77

SSL 証明書情報

ファームウェアとドライバーのアップデート用のカタログ ファイルは、Dell サポート サイト、Dell EMC Repository Manager (Repository Manager)、またはユーザーの組織ネットワーク内の Web サイトからダウンロードできます。

ユーザーの組織ネットワーク内の Web サイトからカタログファイルをダウンロードすることを選択した場合、SSL 証明書を承認または拒否することができます。SSL 証明書の詳細を [証明書情報] ウィンドウに表示できます。この情報には、有効期間、発行元の認証機関および証明書が発行されたエンティティの名前が含まれます。

メモ: [証明書情報] ウィンドウは、[ベースラインの作成] ウィザードからカタログを作成した場合のみ表示されます。

処置

[同意する]	SSL 証明書を承認して、Web サイトへのアクセスを可能にします。
[キャンセル]	SSL 証明書を承認せずに [証明書情報] ウィンドウを閉じます。

カタログのアップデート

既存のファームウェアおよびドライバー カタログは、Dell.com サイト (ベースの場所) から更新することができます。

カタログをアップデートするには、次の手順を実行します。

1. [カタログ管理] ページで、カタログを選択します。
2. [[カタログ管理]] ページの右ペインにある [[アップデートのチェック]] ボタンをクリックします。
3. [[はい]] をクリックします。
選択したカタログがオンライン カタログであることが確認されると、Dell.com のサイトにある最新バージョンに置き換えられます。ローカル ネットワーク カタログに関しては、ベースの場所で使用可能なすべての最新ファームウェア/ドライバーがベースライン コンプライアンスの計算で考慮されます。

カタログの編集

1. [カタログ管理] ページで、カタログを選択します。
カタログの詳細が、右ペインの [<カタログ名>] に表示されます。
2. 右側のペインで [編集] をクリックします。

3. [カタログのアップデートの編集] ウィザードで、プロパティを編集します。
   編集できないプロパティはグレー表示されます。フィールドの定義については、「Dell.com を使用したカタログの追加 、p. 74」および「ローカル ネットワークへのカタログの追加 、p. 75」を参照してください。
4. [共有アドレス] と [カタログ ファイル パス] を入力すると、[今すぐテストする] リンクが表示されます。カタログへの接続を検証するには、[今すぐテストする] をクリックします。カタログへの接続が確立されると、「Connection Successful」というメッセージが表示されます。共有アドレスやカタログ ファイル パスへの接続が確立されていない場合は、「Connection to path failed」というエラー メッセージが表示されます。これはオプションの手順です。
5. [カタログのアップデート] ボックスで、[手動] または [自動] を選択します。
   [カタログのアップデート] で [自動] を選択した場合は、[毎日] か [毎週] を選択して、12 時間形式で更新頻度を入力します。
6. [終了] をクリックします。
   直ちにジョブが作成され、実行されます。ジョブのステータスは、[カタログ管理] ページの [リポジトリの場所] 列に示されます。

カタログの削除

1. [カタログ管理] ページで、カタログを選択して [削除] をクリックします。
   カタログがリストから削除されます。
2. [ファームウェア/ドライバーのコンプライアンス] ページに戻るには、[ファームウェア/ドライバーのコンプライアンスに戻る] をクリックします。

   メモ: ベースラインにリンクされているカタログは削除できません。

関連情報

ローカル ネットワークへのカタログの追加 、p. 75

ファームウェア/ドライバーのベースラインの作成

ベースラインは、ファームウェア/ドライバーのカタログに関連付けられたデバイスまたはデバイスのグループのセットです。ベースラインは、そのベースラインのデバイス用のファームウェアおよびドライバーのコンプライアンス評価のために作成され、カタログで指定されたバージョンに対して使用されます。ベースラインを作成するには、次の手順を実行します。

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- デバイス マネージャー ユーザーが表示および管理できるのは、自分が作成して所有するファームウェア/ドライバーのベースラインのみです。また、ベースラインの作成中に、デバイス マネージャーの範囲内にあるターゲット グループまたはデバイス (ファームウェア アップデート対応) が表示されます。
- バージョン 3.5 またはそれ以前のバージョンからのアップグレード後、以前の OpenManage Enterprise リリースのいずれかからデバイス マネージャーによって作成されたすべてのファームウェア/ドライバー ベースラインは、管理者のみに割り当てられます。そのため、デバイス マネージャは、アップグレード後に以前のバージョンからファームウェア/ドライバーのベースラインを再作成する必要があります。
- ファームウェアやドライバーのバージョンがカタログのバージョンよりも前である非対応デバイスは、自動的にはアップデートされません。ユーザーがファームウェアのバージョンをアップデートする必要があります。デバイスまたは環境が勤務時間中にオフラインになってしまうのを防ぐため、メンテナンス時にデバイスのファームウェアをアップデートすることをお勧めします。

1. **ファームウェア** で、**ベースラインの作成** をクリックします。
2. [**アップデート ベースラインの作成**] ダイアログ ボックスで、次の手順を実行します。
   a. **ベースライン情報** セクションで、次のように実行します。
      i. **カタログ** ドロップダウンメニューから、カタログを選択します。
      ii. このリストにカタログに追加するには、[追加] をクリックします。「ファームウェアカタログの管理」を参照。
      iii. **ベースライン名** ボックスに、ベースラインの名前を入力し、説明を入力します。

iv. **次へ**をクリックします。

b. [ターゲット] セクションで次のように実行します。

- ターゲットデバイスを選択する場合：
  i. **デバイスの選択** を選択してから、**デバイスの選択** ボタンをクリックします。
  ii. **デバイスの選択** ダイアログボックスには、OpenManage Enterprise、IOM により監視されるすべてのデバイスと、静的グループまたはクエリグループの下のデバイスが各グループに表示されます。
  iii. 左側のペインで、カテゴリ名をクリックします。そのカテゴリのデバイスが、作業中のペインに表示されます。
  iv. デバイスに対応するチェックボックスを選択します。選択したデバイスは **選択済みのデバイス** タブのリストに表示されます。
- ターゲットデバイスグループを選択する場合：
  i. **グループの選択** を選択してから **グループの選択** ボタンをクリックします。
  ii. **グループの選択** ダイアログボックスには、OpenManage Enterprise、IOM により監視されるすべてのデバイスと、静的グループまたはクエリグループの下のデバイスが各カテゴリに表示されます。
  iii. 左側のペインで、カテゴリ名をクリックします。そのカテゴリのデバイスが、作業中のペインに表示されます。
  iv. グループに対応するチェックボックスを選択します。選択したグループは **選択したグループ** タブのリストに表示されます。

3. [終了] をクリックします。
ベースラインを作成するためにジョブが作成されたというメッセージが表示されます。

ベースラインの表には、デバイスとベースラインジョブに関するデータが表示されます。フィールドの定義については、「ファームウェアのベースラインフィールドの定義 、p. 174」を参照してください。

設定コンプライアンス ベースラインの削除

[設定] > [設定コンプライアンス] ページで設定コンプライアンス ベースラインを削除し、関連づけられているベースラインのデバイスとの関連づけを解除することができます。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。参照先 OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15

設定コンプライアンス ベースラインを削除するには、次のようにします。

1. [設定コンプライアンス] ページにリストされているベースラインからベースラインを選択します。
2. [削除] をクリックして、確認プロンプトで [はい] をクリックします。

削除された設定ベースラインは、[設定コンプライアンス] ページから削除されます。

ベースラインの編集

[設定] > [ファームウェア/ドライバーのコンプライアンス] ページのベースラインは、次のように編集することができます。

1. ベースラインを選択し、右側のペインで [編集] をクリックします。
2. 「ファームウェアのベースラインの作成」の説明に従ってデータを修正します。
更新された情報がベースラインリストに表示されます。
3. [ファームウェア/ドライバーのコンプライアンス] ページに戻るには、[ファームウェア/ドライバーのコンプライアンスに戻る] をクリックします。

デバイス ファームウェア/ドライバーのコンプライアンスの確認

[設定] > [ファームウェア/ドライバーのコンプライアンス] ページでは、関連付けられているカタログに対するベースライン デバイスのファームウェア/ドライバーのコンプライアンスを確認し、レポートを表示して、非対応デバイスのファームウェア/ドライバーをアップデートすることができます。

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- ベースラインの非対応デバイスのファームウェア/ドライバー (64 ビット版 Windows) は自動的にアップデートされず、ユーザーがアップデートする必要があります。デバイスまたは環境が勤務時間中にオフラインになってしまうのを防ぐため、メンテナンス時にデバイスのファームウェア/ドライバーをアップデートすることをお勧めします。
- インベントリー情報を収集するには、Windows サーバーでインベントリー コレクターと Dell System Update が使用可能である必要があります。これらのコンポーネントがサーバー上で使用できない場合は、インベントリー ジョブを開始して、[ドライバー インベントリーの収集] を選択します。検出ジョブでもドライバー インベントリー情報を収集しますが、サーバー上に必要なコンポーネントをインストールするのはインベントリー ジョブのみです。ドライバー インベントリー情報を収集するには、インベントリー ジョブを作成または編集して、[ドライバー インベントリーの収集] チェック ボックスを選択します。詳細については、インベントリジョブの作成 、p. 70 およびインベントリスケジュールジョブの編集 、p. 72 を参照してください。

1. 対象のベースラインに対応するチェック ボックスを選択し、[コンプライアンスの確認] をクリックします。
   ベースライン コンプライアンス ジョブが実行されます。

   メモ: デバイスがカタログに関連付けられていない場合は、コンプライアンスが検証されません。関連付けられて、コンプライアンス の表に一覧表示されているデバイスに対してのみ、ジョブが作成されます。デバイスをカタログに関連付ける場合は、「ファームウェアのベースラインの作成」を参照してください。

   ベースラインの表には、デバイスとベースラインジョブに関するデータが表示されます。フィールドの定義については、「ファームウェアのベースラインフィールドの定義 、p. 174」を参照してください。
2. コンプライアンス レポートを表示して、デバイス/ドライバーのファームウェア バージョンをアップグレードする場合は、右ペインで [レポートの表示] をクリックします。

   「デバイスファームウェアコンプライアンスレポートの表示」を参照してください。

   メモ: ロールバックは、ドライバーではサポートされていません。

ベースライン コンプライアンス レポートの表示

[設定] > [ファームウェア/ドライバーのコンプライアンス] ページに、ベースラインのコンプライアンス ステータスが表示されます。ドーナツ チャートには、各カタログに対するベースラインのコンプライアンスのサマリーが表示されます。複数のデバイスが 1 つのベースラインに関連付けられているときは、そのベースラインに対するコンプライアンス レベルの一番低いデバイスのステータスが、そのベースラインのコンプライアンス レベルとして示されます。たとえば、デバイスの大部分が準拠している場合でも、コンプライアンスが「重要」であるデバイスが 1 つでもあると、ベースラインのコンプライアンス レベルは、「重要」  として示されます。

ベースラインに関連付けられている各デバイスのファームウェア/ドライバーのコンプライアンスを表示し、そのデバイスのファームウェア/ドライバーのバージョンをアップグレードまたはダウングレードできます。ベースラインのコンプライアンス レポートを表示するには、次の手順を実行します。

- ベースラインに対応するチェックボックスを選択し、右ペインで [レポートの表示] をクリックします。

  [コンプライアンスレポート] ページに、ベースラインに関連付けられたデバイスリストとそれらのコンプライアンスレベルが表示されます。デフォルトでは、**重要**および**警告**ステータスにあるデバイスが表示されます。

  メモ: 各デバイスに独自のステータスがある場合、重要度が最高のステータスがグループのステータスと見なされます。ロールアップ正常性状態の詳細については、Dell TechCenter のホワイトペーパー『*第 14 世代以降の Dell EMC PowerEdge サーバーで iDRAC を使用してロールアップ正常性状態を管理する*』を参照してください。
- [コンプライアンス]: ベースラインに対するデバイスのコンプライアンスレベルを示します。デバイス ファームウェア/ドライバーのコンプライアンス レベルに使用される記号に関する詳細については、「デバイスのファームウェアおよびドライバーの管理 、p. 73」を参照してください。
- [タイプ]: コンプライアンスレポートが生成されるデバイスのタイプ。
- [デバイス名/コンポーネント]: デフォルトでは、デバイスのサービスタグが表示されます。
  1. デバイスのコンポーネントについての情報を表示するには、[>] 記号をクリックします。

     コンポーネントおよびそれらのコンポーネントのカタログに対するコンプライアンス ステータスが一覧表示されます。

     メモ: 関連付けられているファームウェア ベースラインに準拠しているすべてのデバイス (MX7000 シャーシ以外) には、[>] 記号が表示されません。

2. ファームウェアのコンプライアンス ステータスが「重要」で、アップデートが必要なデバイスに対応するチェック ボックスを 1 つまたは複数選択します。
3. [一致させる] をクリックします。「ベースライン コンプライアンス レポートを使用したデバイスのファームウェア バージョンのアップデート」を参照してください。

- [サービスタグ]: クリックすると、[<デバイス名>] ページにデバイスについての詳細情報が表示されます。このページで実行できるタスクについての詳細は、「個々のデバイスの表示と設定 、p. 65」を参照してください。
- [再起動が必要]: ファームウェアをアップデートした後でデバイスの再起動が必要であることを示します。
- [情報] : 各デバイス コンポーネントに対応する記号は、ファームウェア/ドライバーをアップデートできるサポート サイト ページにリンクしています。クリックすると、サポートサイトの対応するドライバの詳細ページが開きます。
- [現在のバージョン]: デバイスの現在のファームウェアバージョンを表示します。
- [ベースライン バージョン]: 関連カタログで使用可能なデバイスの対応ファームウェア/ドライバーのバージョンを示します。
- コンプライアンスレポートを Excel ファイルにエクスポートするには、デバイスに対応するチェックボックスを選択して、[エクスポート] を選択します。
- [ファームウェア] ページに戻るには、[ファームウェアに戻る] をクリックします。
- 列に基づいてデータを並べ替えるには、列のタイトルをクリックします。
- 表内のデバイスを検索するには、[詳細フィルタ] をクリックしてデータを選択するかフィルタボックスにデータを入力します。詳細フィルタについては、「OpenManage Enterprise グラフィカル ユーザー インターフェイスの概要 、p. 34」を参照してください。

ベースライン コンプライアンス レポートを使用したデバイスのファームウェア/ドライバーのアップデート

ファームウェアまたはドライバーのコンプライアンス レポートを実行すると、デバイスのファームウェアまたはドライバーがカタログ上のバージョンより古い場合は、コンプライアンス レポートのページでデバイスのファームウェアまたはドライバーのステータスにアップグレードが表示されます (または) と表示されます。

関連付けられているベースライン デバイスのファームウェア/ドライバーのバージョンは自動的にアップデートされないため、ユーザーはアップデートを開始する必要があります。デバイスまたは環境が勤務時間中にオフラインになってしまうのを防ぐため、メンテナンス時にデバイスのファームウェア/ドライバーをアップデートすることをお勧めします。

デバイス マネージャーは、そのスコープ内にあるデバイス上でのみ、ファームウェア/ドライバー アップデートを実行できます。

メモ: シャーシ ストレージ スレッドでのインベントリー収集とファームウェア アップデートは、シャーシのデバイス管理を使用して管理されている場合、OpenManage Enterprise ではサポートされません。

前提条件：

- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- ポート 22 との通信を許可する受信ファイアウォール ルールを作成する必要があります。
- プロキシ設定を使用して HTTP および HTTPS 共有を設定している場合は、アップデート タスクを開始する前に、これらのローカル URL がプロキシ例外リストに含まれていることを確認してください。
- 任意の時点でターゲット マシン上で開始できるアップデート タスクは 1 つのみです。

メモ:

- [iDRAC のリセット] 機能は、「プロキシ」の状態でオンボードされている MCM シャーシ配下のデバイスではサポートされていません。また、デバイスのドライバーのみをアップデートする場合にもサポートされません。オンボーディングの状態の詳細については、デバイスのオンボーディング 、p. 43 を参照してください。
- ネットワーク スイッチ、モジュラー型 IOA、Dell ストレージ デバイスのファームウェアまたはドライバーは Dell カタログを使用してアップデートできないため、コンプライアンス ステータスが「不明」として表示されます。これらのデバイスについては、個々のアップデート パッケージを用いて、ファームウェアまたはドライバーのアップデートを個別に実行することをお勧めします。ファームウェアまたはドライバーのアップデートを個別に実行するには、[すべてのデバイス] ページでデバイスを選択し、[詳細表示] > [ファームウェア/ドライバー] をクリックして、個々のパッケージ オプションを選択します。サポート対象外デバイスのリストの詳細については、次を参照： ファームウェア/ドライバー コンプライアンス ベースライン レポート—「不明」コンプライアンス ステータスのデバイス 、p. 178

マルチシャーシ管理（MCM）グループが 1.30.00 より低い OpenManage Enterprise-Modular バージョンを使用して管理されている場合は、MX7000 シャーシとスレッドのファームウェアやドライバーをアップデートする前に、次の点を考慮してください。

- シャーシとスレッドのファームウェアのアップデートは個別に行う必要があります。
- すべてのメンバー シャーシをアップデートした後に、最後のステップとしてリード シャーシを個別にアップデートする必要があります。
- ファームウェアは、一度に最大 9 個のメンバー シャーシに対してのみアップデートできます。
- ファームウェア アップデートは、オンボード状態（管理対象またはプロキシ状態）に関係なく、一度に最大 43 スレッドでサポートされています。

ドライバー アップデートは、64 ビット版の Windows サーバーとして検出されたデバイスでのみ使用できます。ドライバーをアップデートする前に、次の手順を実行します。

- ドライバー アップデートのロールバックはサポートされていないことに注意してください。
- インバンド ドライバーのアップデートは、OpenSSH を使用した Windows でのみサポートされています。CygwinSSH など、Windows でホストされているサード パーティ SSH のドライバー アップデートはサポートされていません。
- インベントリー情報を収集するには、Windows サーバーでインベントリー コレクターと Dell System Update が使用可能である必要があります。これらのコンポーネントがサーバー上で使用できない場合は、インベントリー ジョブを開始して、[ドライバー インベントリーの収集] を選択します。検出ジョブでもドライバー インベントリー情報を収集しますが、サーバー上に必要なコンポーネントをインストールするのはインベントリー ジョブのみです。ドライバー インベントリー情報を収集するには、インベントリー ジョブを作成または編集して、[ドライバー インベントリーの収集] チェック ボックスを選択します。詳細については、インベントリジョブの作成 、p. 70 およびインベントリスケジュールジョブの編集 、p. 72 を参照してください。

ベースライン コンプライアンス レポートを使用して、デバイスのファームウェアやドライバーをアップデートするには、次の手順を実行します。

1. [設定] > [ファームウェア/ドライバーのコンプライアンス] ページで、デバイスが取り付けられているベースラインに対応するチェック ボックスを選択し、右ペインで [レポートの表示] をクリックします。

   [コンプライアンス レポート] ページに、ベースラインに関連付けられたデバイス リストとそれらのコンプライアンス レベルが表示されます。フィールドの説明については、ベースライン コンプライアンス レポートの表示 、p. 79 を参照してください。
2. ファームウェアまたはドライバーのアップデートが必要なデバイスに対応するチェック ボックスを選択します。同様のプロパティを持つデバイスを複数選択できます。
3. [一致させる] をクリックします。
4. [デバイスを一致させる] ダイアログ ボックスでは、以下を実行できます。
   - [**アップデートのスケジュール**] の下で、[追加情報] をクリックして重要な情報を表示し、次のいずれかを選択します。
     a. [今すぐアップデート]: ファームウェア/ドライバーのアップデートをすぐに適用します。
     b. [実行日時を指定]: ファームウェア/ドライバーのバージョンをアップデートする日時を指定します。このモードは、現在のタスクに影響を与えたくない場合に推奨します。
   - [**サーバー オプション**] で、次のオプションのいずれかを選択します。
     a. ファームウェア/ドライバーのアップデート直後にサーバーを再起動するには、[サーバーをただちに再起動] を選択し、ドロップダウン メニューから次のいずれかのオプションを選択します。
        i. **正常な再起動（強制シャットダウンなし）**
        ii. **正常な再起動（強制シャットダウンあり）**
        iii. デバイスをハード リセットする**パワーサイクル。**
     b. 次のサーバー再起動時に、ファームウェア/ドライバーのアップデートをトリガーするには、[次のサーバー再起動のためのステージ] を選択します。

        メモ: ファームウェア/ドライバーのアップデート ジョブが [次のサーバー再起動のためのステージ] オプションを使用して作成されている場合は、リモート デバイスにパッケージをインストールした後で、インベントリーとベースラインのチェックを手動で実行する必要があります。
   - [ジョブ キューをクリア]: アップデート ジョブを開始する前に、ターゲット デバイスのすべてのジョブ（スケジュール、完了、失敗）を削除する場合に選択します。

     メモ: この機能は、ドライバーのアップデートではサポートされていません。
   - [iDRAC をリセット]: アップデート ジョブを開始する前に iDRAC を再起動する場合に選択します。

     メモ: この機能は、ドライバーのアップデートではサポートされていません。
5. [アップデート] をクリックします。

デバイスのファームウェア/ドライバーをアップデートするために、ファームウェア/ドライバーのアップデート ジョブが作成されます。ジョブのステータスは、[監視] > [ジョブ] ページに表示できます。

11

デバイス導入テンプレートの管理

OpenManage Enterprise のデバイス導入テンプレートでは、サーバーおよびシャーシの BIOS、起動、ネットワーク プロパティなどの構成プロパティを設定することができます。

導入テンプレートは、属性と呼ばれるシステム構成設定を統合したものです。導入テンプレートを使用すると、人為的なエラーのリスクなしに、複数のサーバーまたはシャーシを迅速かつ自動的に構成できます。

テンプレートを使用すると、データ センターのリソースを最適化し、クローンの作成と導入のサイクル時間を削減することができます。また、テンプレートを利用すれば、ソフトウェアデファインド インフラストラクチャを使用するコンバージド インフラストラクチャでのビジネスクリティカルな処理を強化できます。

事前に定義された導入テンプレートを使用するか、またはリファレンス デバイスまたは既存のテンプレート ファイルから導入テンプレートをインポートすることができます。既存のテンプレートのリストを表示するには、OpenManage Enterprise のメニューから、[設定] > [テンプレート] をクリックします。

OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15。

デバイス マネージャーは、デフォルト テンプレートおよび自らが所有するカスタム テンプレートのみでタスクを表示および実行できます。

トピック：

リファレンス デバイスからの導入テンプレートの作成

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

メモ: シャーシや、iDRAC バージョン 2.50.50.50 以前が動作している PowerEdge YX2X および YX3X サーバーとの通信が必要なタスクを開始するには、事前に [SMB 設定] で SMBv1 を有効にしておく必要があります。コンソールプリファレンスの管理 、p. 158 および Dell EMC PowerEdge サーバーの汎用命名規則 、p. 179 を参照してください。

リファレンス デバイスを使用するか、既存の導入テンプレートからインポートすることによって、導入テンプレートを作成または編集できます。リファレンスデバイスを使用して作成するには、次の手順を実行します。

1. [OpenManage Enterprise] メニューで、[設定] > [テンプレート] > [テンプレートの作成] の順にクリックし、[リファレンス デバイスから] を選択します。
2. [テンプレートの作成] ダイアログボックスで、次の手順を実行します。
   a. [テンプレートの情報] セクションで、導入テンプレートの名前とテンプレートの説明を入力します。
   b. 次の導入テンプレート タイプを選択します。
      - [参照サーバのクローン]: 既存サーバの設定をクローンできるようになります。
      - [参照シャーシのクローン]: 既存シャーシの設定をクローンできるようになります。
      - [参照 IOA のクローン]: 既存 M I/O アグリゲーターの設定をクローンできるようになります。

        メモ: IOA テンプレートの属性は編集できません。編集できるのは、IOA テンプレートの**名前**と**説明**のみです。
   c. [次へ] をクリックします。
   d. [リファレンス デバイス] セクションの [デバイスの選択] をクリックして、新しい導入テンプレートの作成に使用する必要がある設定プロパティを持つデバイスを選択します。デバイスの選択の詳細については、「ターゲットデバイスおよびデバイス グループの選択」を参照してください。

      メモ: 選択できる参照デバイスは、1 つだけです。

      メモ: クローンの作成には、シャーシ検出時に抽出された IOA テンプレートのみが使用できます。参照先 サーバー用にカスタマイズされたデバイス検出ジョブ プロトコルの作成 - 検出プロトコルの追加設定 、p. 47
   e. [設定要素] セクションで、クローンする必要のあるデバイス要素に対応するチェック ボックスを選択します。サーバーをデバイスとして使用して導入テンプレートを作成する場合は、iDRAC、BIOS、Lifecycle Controller、イベント フィルターなどのサーバーのプロパティをクローンすることを選択することができます。デフォルトで、すべての要素が選択されます。
   f. [終了] をクリックします。
      正常に作成された後、ジョブがリストに表示されます。導入テンプレート作成ジョブが開始され、[ステータス] 列にステータスが表示されます。

      ジョブ情報は、[監視] > [ジョブ] ページにも表示されます。ジョブの詳細を表示するには、作業ペインでジョブを選択して、[詳細の表示] をクリックします。[ジョブの詳細] ページに、ジョブの実行内容の詳細が表示されます。[結果] ペインで [詳細の表示] をクリックすると、ジョブの実行状態に関する詳細を確認できます。

テンプレート ファイルのインポートによる導入テンプレートの作成

メモ: シャーシや、iDRAC バージョン 2.50.50.50 以前が動作している PowerEdge YX2X および YX3X サーバーとの通信が必要なタスクを開始するには、事前に [SMB 設定] で SMBv1 を有効にしておく必要があります。詳細については、「コンソールプリファレンスの管理 、p. 158」および「Dell EMC PowerEdge サーバーの汎用命名規則 、p. 179」を参照してください。

1. [OpenManage Enterprise] メニューで [設定] > [テンプレート] > [テンプレートの作成] の順にクリックし、[ファイルからインポート] を選択します。
2. **テンプレートのインポート** ダイアログボックスで、次の手順を実行します。
   a. 新しい導入テンプレートの名前を入力します。
   b. **ファイルを選択** をクリックし、テンプレートファイルを選択します。
   c. テンプレート タイプとして、[**サーバー**]、[**シャーシ**]、[IOA] のいずれかを選択します。
3. **終了**をクリックします。
   既存のテンプレート ファイルのプロパティがインポートされ、新しい導入テンプレートが作成されます。

- 導入テンプレートに関する詳細情報を表示するには、チェック ボックスを選択し、右ペインの [詳細の表示] をクリックします。[テンプレートの詳細] ページで、導入テンプレートを導入または編集できます。デバイス導入テンプレートの導入 、p. 86 およびリファレンス デバイスからの導入テンプレートの作成 、p. 82 を参照してください。
- 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. 対応するチェック ボックスを選択し、**編集** をクリックします。
  2. [**テンプレートの編集**] ダイアログボックスで導入テンプレート名を編集し、[**終了**] をクリックします。更新された情報は、導入テンプレートのリストに表示されます。

導入テンプレート情報の表示

事前定義されたデバイス導入テンプレート、あるいはユーザー作成またはクローン作成したデバイス導入テンプレートのリストは、[設定] > [テンプレート] の下に表示されます。

1. 導入テンプレートのリストで、必要なデバイス テンプレートに対応するチェック ボックスを選択します。
2. 作業中のペインで、**詳細の表示** をクリックします。
   [**テンプレートの詳細**] ページには、導入テンプレートの名前、説明、導入テンプレートの作成元になったリファレンス デバイス、OpenManage Enterprise のユーザー情報別の最終更新日が表示されます。
3. 導入テンプレートの作成に使用するすべての属性を表示するには、[**設定の詳細**] セクションでエレメントを右クリックして、すべての子エレメントを展開するか折りたたみます。親エレメントに固有の子エレメントを個々に展開することもできます。たとえば、iDRAC および BIOS の要素をターゲットデバイス上でクローン作成のために使用する必要があることを選択した場合は、その要素に関連する属性のみが表示されます。

サーバー導入テンプレートの編集

ビルトイン導入テンプレートは編集できません。編集できるのは、「カスタム」として識別されるユーザーが作成した導入テンプレートのみです。導入テンプレートの属性は、テンプレート作成時に参照テンプレート ファイルを使用したかリファレンス デバイスを使用したかに関係なく、編集することができます。テンプレートの編集時、属性を選択または選択解除しても、テンプレートに格納されている属性は変更されず、エクスポートされた場合でも、すべての属性はテンプレートの一部になります。これは、導入される内容に影響します。

1. [設定] > [テンプレート] ページで、必要なカスタム テンプレートのチェック ボックスを選択し、[**編集**] をクリックします。
2. [**テンプレートの編集**] ダイアログボックスで、次の手順を実行します。
   a. [**テンプレートの情報**] セクションで、導入テンプレートの名前と説明を編集します。テンプレートのタイプは編集できません。
   b. [**次へ**] をクリックします。
   c. [**コンポーネントの編集**] セクションでは、導入テンプレートの属性が以下に表示されます。
      - [ガイド付きビュー] - この属性ビューには、機能別にグループ化された共通属性のみが表示されます。次のカテゴリーの属性が表示されます。
        i. [**BIOS 設定**] セクションで、次のいずれかを選択します。
           - **手動** : 次の BIOS プロパティを手動で定義できます。
             - **システム プロファイル** : ドロップダウン メニューから、システム プロファイルで実行するパフォーマンスの最適化のタイプを指定するために選択します。
             - **ユーザーのアクセスが可能な USB ポート** : ドロップダウンメニューから、ユーザーがアクセスできるポートを指定するために選択します。
             - デフォルトでは、論理プロセッサの使用とインバンド管理機能が有効になっています。
           - **ワークロードに基づく最適化** : ワークロードプロファイルの選択 ドロップダウンメニューから、プロファイルで実行するワークロードパフォーマンス最適化のタイプを指定するために選択します。
        ii. [**起動**] をクリックし、起動モードを定義します。
           - BIOS を起動モードとして選択する場合は、以下を入力します。
             - ブート シーケンスを再試行するには、[**有効**] チェック ボックスをオンにします。
             - 項目をドラッグして、ブート シーケンスとハード ドライブのシーケンスを設定します。
           - 起動モードとして UEFI を選択した場合は、項目をドラッグして UEFI ブート シーケンスを設定します。必要に応じて、セキュアブート機能を有効にするチェック ボックスを選択します。
        iii. [**ネットワーキング**] をクリックします。導入テンプレートに関連付けられているすべてのネットワークが [**ネットワーク インターフェイス**] の下に表示されます。
           - オプションの ID プールを導入テンプレートに関連付けるには、[**ID プール**] ドロップダウン メニューから選択します。選択した ID プールに関連付けられているネットワークが表示されます。[詳細] ビューで導入テンプレートが編集されている場合は、この導入テンプレートに対して ID プールの選択が無効になっています。
             - ネットワークのプロパティを表示するには、ネットワークを展開します。
             - プロパティを編集するには、対応するペンシンボルをクリックします。
               - 起動に使用するプロトコルを選択します。プロトコルがネットワークでサポートされている場合にのみ選択してください。
               - ネットワークに関連付けられているタグ付きネットワーク、およびタグなしネットワークを選択します。
               - パーティション、最大、最小帯域幅は、先ほど作成した導入テンプレート (プロファイル) から表示されます。
             - [**終了**] をクリックします。導入テンプレートのネットワーク設定が保存されます。

- [詳細ビュー] — このビューには、変更可能なすべての導入テンプレート属性（ガイド付きビューに表示される属性を含む）がリスト表示されます。このビューでは、属性値（ガイド付きビューなど）だけでなく、導入テンプレートがターゲット デバイスに導入されたときに各属性を含めるかどうかを指定できます。

  属性は機能的にグループ化されて表示されます。ベンダー固有属性は、[その他の属性] の下にグループ化されています。個々の属性は、その名前の前にチェック ボックスが付いた状態で表示されます。このチェック ボックスは、導入テンプレートがターゲット デバイスに導入されたときに、その属性を含めるかどうかを示します。属性の依存関係のため、特定の属性が導入されるかどうかの設定を変更すると、ターゲット デバイスで予期しない結果が発生したり、導入が失敗したりする可能性があります。各グループには、名前の左側にチェック ボックスもあります。[グループ内のアイコン] チェック ボックスには、次の 3 つの値のいずれかがあります。

  i. チェック済み - グループ内のすべての属性が導入対象として選択されていることを示します。
  ii. ハイフン - 導入用に属性の一部（すべてではない）が選択されていることを示します。
  iii. クリア — グループ内のどの属性も導入対象として選択されていないことを示します

  メモ:
  - さまざまな属性はその動作を決定するために別の属性の値に依存するため、このオプションを使用するには、属性と属性の依存関係について十分な注意を払う必要があります。
  - グループ アイコンをクリックすると、グループ内のすべての属性の導入設定を切り替えることができます。
  - パスワードなどのセキュリティ情報を含む属性は非表示にされており、初回ロード時には「空白」表示され、こうした機密性の高い属性値の変更はマスクされます。
  - プロファイルがすでに関連付けられている場合は、導入テンプレートに関連付けられている ID プールを変更することはできません。

3. [**次へ**] をクリックします。
   [**サマリー**] セクションでは、ガイド付きモードおよび詳細モードを使用して編集した属性が表示されます。
4. このフィールドは読み取り専用です。設定を確認し、[**終了**] をクリックします。
   更新されたテンプレート属性が導入テンプレートに保存されます。

シャーシ導入テンプレートの編集

OpenManage Enterprise では、シャーシ導入テンプレートの編集が可能です。テンプレートの編集時、属性を選択または選択解除しても、テンプレートに格納されている属性は変更されず、エクスポートされた場合でも、すべての属性はテンプレートの一部になります。これは、導入される内容に影響します。

メモ:
- シャーシ導入テンプレートの編集には、管理者またはデバイス マネージャーの権限が必要です。詳細については、「OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15」を参照してください。
- ユーザー パスワードは、MX7000 シャーシおよび Chassis Management Controller（CMC）導入テンプレートで設定することはできません。

シャーシ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. [OpenManage Enterprise] > [設定] > [テンプレート] の順に選択すると、導入テンプレートのリストが表示されます。
2. 必要なシャーシ テンプレートに対応するチェック ボックスを選択して、[編集] をクリックします。導入テンプレートの表示が「"カスタム"」になっていることを確認します。
3. [**テンプレート情報**] セクションで [テンプレート名] と [説明] を編集します。[**テンプレート タイプ**] を編集することはできません。
4. [次へ] をクリックします。
5. [**詳細ビュー**] の [コンポーネントの編集] セクションで、属性を導入テンプレートに入れるか入れないかを選択したり選択解除したりできます。
6. [次へ] をクリックします。
7. 属性に対する変更は [サマリー] で確認できます。変更された属性の横には円が表示されます。
8. [終了] をクリックすると、シャーシ導入テンプレートに加えられた変更が保存されます。

IOA 導入テンプレートの編集

IOA 導入テンプレートの属性は編集できません。編集できるのは、IOA 導入テンプレートの**名前**と**説明**のみです。

メモ:

IOA テンプレートの属性は、アプライアンスの外部で編集しないでください。さもないと、導入時にテンプレートが破損したファイルと見なされます。

導入テンプレートのネットワーク プロパティの編集

[設定] > [テンプレート] ページで、該当する NIC 属性を含む導入テンプレートのネットワーク設定を編集できます。

導入テンプレートを選択したら、[ネットワークの編集] をクリックし、[ネットワークの編集] ウィザードをアクティブ化して、次の手順を実行します。

メモ: MX7000 シャーシが範囲外の場合でも、デバイス マネージャーでは、範囲内の「プロキシされた」MX7000 スレッドの VLAN 設定が許可されています。

1. [IO プールの割り当て] をクリックし、[ID プール] リストから導入テンプレートの ID プールを選択します。[次へ] をクリックします。
2. [帯域幅] セクションで、関連づけられている NIC の**最小帯域幅 (%)** と**最大帯域幅 (%)** を編集して [次へ] をクリックします。

   メモ: 帯域幅の設定は、パーティション化された NIC にのみ適用されます。

3. [VLAN] セクション (モジュラー型システムにのみ適用) で、次の手順を実行します。
   a. 適切な [NIC チーミング] オプションを選択します。
   b. [VLAN 設定をすぐに反映] チェック ボックスをオンにします。そうすることで、サーバーを再起動しなくても、変更された VLAN 設定を関連付けられているモジュラー システム サーバー上ですぐに反映することができます。影響を受けるデバイスを表示するには、[詳細の表示] をクリックします。

      メモ:
      - [VLAN 設定をすぐに反映] は、導入テンプレートがすでに導入されている場合にのみ実装されます。
      - VLAN 設定を反映する前に、ファブリック内のモジュラー型システム サーバー用にネットワーク プロファイルがすでに作成されていることを確認します。
      - [VLAN 設定をすぐに反映] チェック ボックスがオンになっている場合は、変更を適用するために、「**VLAN の反映**」という名前のジョブが作成されます。このジョブのステータスは [監視] > [ジョブ] ページで確認できます。

   c. [厳密なチェックを使用] チェック ボックスを選択して、VLAN を同様の特性と照合します。選択しない場合、VLAN 名と QoS のみが照合に使用されます。

      メモ: このオプションは、モジュラー型システムのスレッドにのみ適用されます。

   d. 必要に応じて、関連づけられている NIC の [タグなしネットワーク] 属性と [タグ付きネットワーク] 属性を変更します。
4. [終了] をクリックして変更を適用します。

デバイス導入テンプレートの導入

特定のデバイスに一連の設定属性を含む導入テンプレートを導入することができます。デバイスにデバイス導入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。

メモ:
- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- デバイス マネージャーがテンプレートを導入している場合は、そのデバイス マネージャーのスコープに含まれており、導入可能なターゲット グループとデバイスのみが表示されます。

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。

- デバイス導入テンプレートの作成またはサンプル導入テンプレートのクローニングが完了している。リファレンス デバイスからの導入テンプレートの作成 、p. 82 を参照してください。
- 対象のデバイスが「OpenManage Enterprise の導入のための最小システム要件 、p. 19」に記載されている要件を満たしている。
- OpenManage Enterprise Advanced ライセンスが、ターゲット デバイスにインストールされている。

注意: 適切なデバイスだけが導入に選択されていることを確認します。再利用のベアメタル デバイスに導入テンプレートを導入すると、その後デバイスを元の設定に戻すことができなくなる可能性があります。

メモ: MX7000 シャーシテンプレートの導入時は、次の点に注意してください。

- ターゲットデバイスになれるのは、リード MX7000 シャーシのみです。
- MX7000 シャーシがグループから削除されている場合は、OpenManage Enterprise で再度検出する必要があります。
- MX7000 シャーシのユーザーは、テンプレートで設定されているユーザーで置き換えられます。
- インポートされた Active Directory の設定は、シャーシプロファイルの値に置き換えられます。

1. [ ][設定] > [テンプレート] ページの導入テンプレート一覧から、導入する導入テンプレートに対応するチェック ボックスを選択して、[テンプレートの導入] をクリックします。
2. [テンプレートの導入：<テンプレート名>] ダイアログボックスの **ターゲット** の下で、次の手順を実行します。
   a. [選択] をクリックし、[ジョブのターゲット] ダイアログボックスでデバイスを選択します。「ターゲットデバイスおよびデバイス グループの選択」を参照してください。
   b. デバイス導入テンプレートの導入時、設定変更によりサーバーの強制的な再起動が必要になる場合があります。サーバを再起動しない場合は、[ホスト OS の強制再起動をしない] オプションを選択します。
   [ホスト OS の強制再起動をしない] オプションを選択すると、サーバの正常な再起動が試行されます。再起動に失敗した場合、テンプレート導入タスクを再実行する必要があります。
   c. [厳密なチェックを使用] チェック ボックスを選択して、VLAN を同様の特性と照合します。選択しない場合、VLAN 名と QoS のみが照合に使用されます。

      メモ: このオプションは、選択したターゲット デバイスがモジュラー型システム スレッドの場合にのみ表示されます。

   d. **次へ**をクリックします。
3. 対象のデバイスがサーバの場合は、[ネットワーク ISO からの起動] セクションで次の手順を実行します。
   a. **ネットワーク ISO からの起動** チェック ボックスを選択します。
   b. 共有タイプに **CIFS** または **NFS** のいずれかを選択し、ISO イメージのファイルパスや ISO イメージファイルが格納されている共有の場所など、情報をフィールドに入力しします。ツールヒントを使用して正しい構文を入力します。
   c. [ISO 接続時間] ドロップダウン メニュー オプションを選択して、ネットワーク ISO ファイルがターゲット デバイスにマップされたままになる時間数を設定します。デフォルトでは、この値は 4 時間に設定されています。
   d. **次へ**をクリックします。
4. [iDRAC 管理 IP] セクションで、必要に応じて、ターゲットデバイスの IP 設定を変更して [次へ] をクリックします。

   メモ:

   - 静的 IP を使用して最初に検出されたターゲット デバイスへのテンプレートの導入中に DHCP 設定が割り当てられると、テンプレートの導入に失敗します。
   - IP 設定が検出された MX7000 スレッドで設定されていない場合、テンプレートの導入中に、ネットワーク ISO から起動操作は実行されません。

5. 導入テンプレートを導入する前に、[ターゲット属性] セクションで、選択したターゲット デバイスそれぞれに固有の非仮想 ID 属性 (場所の属性や IP アドレスなど) を変更することができます。テンプレートを導入すると、変更されたターゲット属性は特定のデバイスにのみ実装されます。デバイス固有の非仮想 ID 属性を変更するには、次の手順を行います。
   a. 前に選択したターゲット デバイスを表示しているリストからターゲット デバイスを選択します。
   b. 属性のカテゴリーを展開し、ターゲット デバイスでのテンプレートの導入時に含める、または除外する必要がある属性を選択またはクリアします。
   c. [次へ] をクリックします。
6. [仮想 ID] セクションで、[予約 ID] をクリックします。
   選択したターゲット デバイスの NIC カードに割り当てられた仮想 ID が表示されます。選択したターゲット デバイスの ID プールに割り当てられた ID をすべて表示するには、[すべての NIC の詳細を表示] をクリックします。

   メモ: アプライアンス以外で ID がすでに割り当てられている場合、これらの ID はクリアされない限り新しい導入環境では使用されません。詳細については、次を参照： ID プール 、p. 92
7. [スケジュール] セクションで、ジョブをただちに実行するか、またはスケジュールを設定して後で実行します。スケジュールジョブフィールドの定義 、p. 174 を参照してください。
8. **終了**をクリックします。警告メッセージを確認して、[**はい**] をクリックします。
   デバイス設定ジョブが作成されます。デバイスコントロール用ジョブの使い方 、p. 124 を参照してください。

IOA 導入テンプレートの導入

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

IOA 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。

- 導入する IOA 導入テンプレートを作成済みである。リファレンス デバイスからの導入テンプレートの作成 、p. 82 を参照してください。
- 対象のデバイスが「OpenManage Enterprise の導入のための最小システム要件 、p. 19」に記載されている要件を満たしている。
- ターゲット デバイスのファームウェア バージョンが、IOA 導入テンプレートと同じである。
- 次のクロス テンプレート導入のみがサポートされています。

表 14. サポートされているクロス テンプレート導入

IOA 導入テンプレート モード	サポートされるターゲットの IOA テンプレート モード
スタンドアロン	スタンドアロン、PMUX
PMUX (プログラム可能 MUX)	PMUX、スタンドアロン
VLT	VLT

注意: 適切なデバイスだけが導入に選択されていることを確認します。再利用のベアメタル デバイスに導入テンプレートを導入すると、その後デバイスを元の設定に戻すことができなくなる可能性があります。

1. [設定] > [テンプレート] ページの導入テンプレート一覧で、導入する IOA テンプレートに対応するチェック ボックスを選択して、[テンプレートの導入] をクリックします。
2. [テンプレートの導入 : <テンプレート名>] ダイアログボックスの **ターゲット** の下で、次の手順を実行します。
   a. [選択] をクリックし、[ジョブのターゲット] ダイアログボックスでデバイスを選択します。「ターゲットデバイスおよびデバイス グループの選択」を参照してください。
   b. **OK** をクリックします。
3. [ホスト名] ダイアログ ボックスで、ターゲット IOA デバイスの**ホスト名**を変更できます。[次へ] をクリックします。
4. [詳細オプション] ダイアログ ボックスで [プレビュー モード] を選択すると導入のシミュレートが行われ、[警告時に続行] を選択すると警告が発生してもそれを無視してテンプレートが導入されます。[次へ] をクリックします。
5. [スケジュール] セクションで、ジョブをただちに実行するか、またはスケジュールを設定して後で実行します。スケジュール ジョブフィールドの定義 、p. 174 を参照してください。
6. **終了**をクリックします。警告メッセージを確認して、[**はい**] をクリックします。
   デバイス設定ジョブは、ジョブ の下に作成されます。デバイスコントロール用ジョブの使い方 、p. 124 を参照してください。

導入テンプレートのクローン作成

1. [OpenManage Enterprise] メニューで ([設定] の下) [テンプレート] をクリックします。
   利用可能な導入テンプレートのリストが表示されます。
2. クローンを作成するテンプレートに対応するチェック ボックスを選択します。
3. [クローン] をクリックします。
4. 新しい導入テンプレートの名前を入力し、[**終了**] をクリックします。
   クローン作成された導入テンプレートが、導入テンプレートのリストに表示されます。

未検出のサーバーまたはシャーシへの設定の自動導入

OpenManage Enterprise の既存の導入テンプレートを、まだ検出されていないサーバーとシャーシに割り当てることができます。デバイスが検出されオンボードされると、導入テンプレートが自動的に各デバイスに導入されます。

[**自動導入**] ページにアクセスするには、[OpenManage Enterprise] > [設定] > [自動導入] の順にクリックします。

自動導入のターゲットと、それぞれの**識別子** (サービス タグまたはノード ID)、**テンプレート名**、**テンプレート タイプ**、**ステータス**、**ネットワーク ISO からの起動のステータス** (サーバーのみ) が表示されます。

リストの一番上にある [詳細フィルター] フィールドを使用して、**自動導入**のターゲットのリストをカスタマイズすることができます。

[自動導入] ページ右側のセクションには、選択した自動導入のターゲットの [作成日] と [作成者] の詳細が表示されます。項目を複数選択すると、最後に選択した項目の詳細がセクションに表示されます。

自動導入ターゲットが検出されると、自動導入ページのエントリーが自動的に削除され、[すべてのデバイス] ページに移動します。また、プロファイルは、デバイスの設定が含まれている [プロファイル] ページにも作成されます。

[自動導入] ページで実行できる操作は次のとおりです。

- 自動導入のためのテンプレートを [作成する]。参照先： 自動導入のターゲットの作成 、p. 89
- 必要のないテンプレートを [削除する]。参照先：自動導入のターゲットを削除 、p. 90
- 自動導入のテンプレートを別のフォーマットに [エクスポート] する。参照先： 自動導入のターゲットの詳細の別形式へのエクスポート 、p. 90

メモ:

- 自動導入テンプレートでは、管理者のみが作成、削除、エクスポートのタスクを実行できます。デバイス マネージャーは、自動導入テンプレートのみを「エクスポート」できます。詳細については、OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

自動導入のターゲットの作成

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。参照先： OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15

自動導入のターゲットを作成するには、次の手順を実行します。

1. [OpenManage Enterprise] > [設定] > [自動導入] > [作成] の順にクリックします。
   [**自動導入テンプレート**] ウィザードが表示されます。
2. [テンプレート情報] ページで、導入テンプレート タイプ ([サーバー] または [シャーシ]) を選択します。
3. [テンプレートの選択] ドロップダウン メニューで、適切なテンプレートを選択します。選択したテンプレートに割り当てられた ID 属性が仮想 ID プールと関連付けられていない場合には、「*選択したテンプレートには'ID 属性'が割り当てられていますが、'仮想 ID プール'に関連付けられていません。このテンプレートを導入しても、ターゲット デバイス上の仮想ネットワーク アドレスは変更されません。*」というメッセージが表示されます。
4. [次へ] をクリックします。
   [ターゲット情報] ページが表示されます。
5. [**ターゲット情報**] ページでターゲット デバイスを選択するには、次のような方法があります。
   - [手動で入力]: ターゲット デバイスのサービス タグまたはノード ID を入力します。ID の入力順序は任意ですが、コンマで区切る必要があります。[検証] をクリックして、値の精度を検証します。ID の検証は必須です。
   - [CSV をインポート]: [CSV をインポート] をクリックして、フォルダーを参照し、ターゲット デバイスの詳細情報が入ったそれぞれの.csv ファイルを選択します。正常にインポートされたエントリーと無効なエントリーの数のサマリーが表示されます。インポートの結果の詳細を表示するには、[詳細の表示] をクリックします。

     CSV ファイルの形式では、最初の列に ID が 1 行に 1 つずつ入力され、2 列目以降にエントリーが入力されている必要があります。テンプレートの CSV ファイルの場合は、[サンプル CSV ファイルのダウンロード] をクリックします。
6. [次へ] をクリックします。
7. [ターゲット グループ情報] ページで、[**静的グループ**] がある場合は、サブグループを指定します。デバイスのグループに関する詳細については、「デバイスのグループ化 、p. 52」を参照してください。ターゲット デバイスは、検出で指定されたターゲット グループに置かれます。
8. **次へ**をクリックします。
9. ターゲット デバイスがサーバーの場合は、[ネットワーク ISO で起動] ページで次の手順を実行します。
   - [ネットワーク ISO からの起動] チェック ボックスを選択します。
   - [CIFS] または [NFS] を選択します。
   - ISO イメージ ファイルが格納される場所を [ISO パス] に入力します。ツールヒントを使用して、正しい構文を入力します。
   - [共有 IP アドレス]、[ワークグループ]、[ユーザー名]、[パスワード] に入力します。
   - [ISO 接続時間] ドロップダウン メニュー オプションを選択して、ネットワーク ISO ファイルがターゲット デバイスにマップされたままになる時間数を設定します。デフォルトでは、この値は 4 時間に設定されています。
   - [次へ] をクリックします。

10. [仮想 ID] ページで、[予約 ID] をクリックします。
選択したターゲット デバイスの NIC カードに割り当てられた仮想 ID が表示されます。選択したターゲット デバイスの ID プールに割り当てられた ID をすべて表示するには、[すべての NIC の詳細を表示] をクリックします。
11. 導入テンプレートを導入する前に、[ターゲット属性] セクションで、選択したターゲット デバイスそれぞれに固有の非仮想 ID 属性 (場所の属性や IP アドレスなど) を変更することができます。テンプレートを導入すると、変更されたターゲット属性は特定のデバイスにのみ実装されます。デバイス固有の非仮想 ID 属性を変更するには、次の手順を行います。
    a. 前に選択したターゲット デバイスを表示しているリストからターゲット デバイスを選択します。
    b. 属性のカテゴリーを展開し、ターゲット デバイスでのテンプレートの導入時に含める、または除外する必要がある属性を選択またはクリアします。
    c. [次へ] をクリックします。
12. **終了**をクリックします。
「テンプレートを導入すると、データが失われ、デバイスを再起動する必要があります。テンプレートを導入しますか？」 が表示されます。
13. [はい] をクリックします。
自動導入のターゲットが新たに作成され、[自動導入] ページに表示されます。

自動導入のターゲットを削除

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。参照先 OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15

メモ: [OpenManage Enterprise] > [設定] > [テンプレート] ページで、自動導入のターゲットに関連付けられたテンプレートが削除されると、関連する自動導入のエントリーも状態にかかわらず削除されます。

自動導入のターゲットを**自動導入**リストから削除します。

1. [OpenManage Enterprise] > [設定] > [自動導入] の順にクリックして、[自動導入] ページにアクセスします。
2. リストから、自動導入するターゲットを選択します。
3. [削除] をクリックし、[はい] をクリックして確認します。
削除のために自動導入のターゲットを選択すると、[自動導入] ページから削除されます。

自動導入のターゲットの詳細の別形式へのエクスポート

1. [OpenManage Enterprise] > [設定] > [自動導入] の順にクリックして、[自動導入] ページにアクセスします。
2. リストで自動導入するターゲットを選択して、[エクスポート] をクリックします。
3. [すべてエクスポート] ダイアログ ボックスで、[HTML]、[CSV]、[PDF] から形式を選択します。[終了] をクリックします。
ジョブが作成され、自動導入のターゲットのデータが選択した形式でエクスポートされます。

ステートレスな導入の概要

仮想 ID 属性があるデバイス導入テンプレートをターゲット デバイスに導入するには、次の手順に従います。

1. **デバイス テンプレートの作成** — [導入] タブの下にある [テンプレートの作成] タスクをクリックして、導入テンプレートを作成します。テンプレートは、設定ファイルからでも、リファレンスデバイスからでも、作成できます。
2. **ID プールの作成** - [ID プール] タブの下にある [作成] タスクをクリックして、1 つ以上の仮想 ID タイプのプールを作成します。
3. **仮想 ID のデバイス テンプレートへの割り当て** — [テンプレート] ペインから導入テンプレートを選択し、[ネットワークの編集] をクリックして、導入テンプレートに ID プールを割り当てます。また、タグ付きおよびタグなしネットワークを選択して、ポートに最小および最大帯域幅を割り当てることもできます。
4. **ターゲット デバイスでの導入テンプレートの導入** — [導入] タブの [テンプレートの導入] タスクを使用して、導入テンプレートと仮想 ID をターゲット デバイスに導入します。

ID プールの管理 - 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 Enterprise 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 を含むデバイス導入テンプレートを使用して導入されたサーバーは、「ステートレス」と呼ばれます。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ー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。

[OpenManage Enteprise] > [設定] > [ID プール] ページでは、仮想 I/O プールを作成、編集、削除、またはエクスポートすることができます。

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。 OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15
- 範囲ベースの制限は ID プールには適用されないため、すべての ID プールはすべてのユーザー タイプで表示および使用することができます。ただし、デバイス マネージャーによって ID が割り当てられると、そのデバイス マネージャーはそれらの ID のみを表示して使用することができます。

ID プールの作成 - プール情報

ID プールは、以下のために、ネットワーク ID を仮想化するためのサーバ上のテンプレートベースの導入に使用されます。

- イーサネット
- iSCSI
- ファイバチャネルオーバーイーサネット (FCoE)
- ファイバチャネル (FC)

これらの各カテゴリで最大 5000 の ID プールを作成することができます。

サーバ導入プロセスでは、テンプレートの説明からサーバを提供しながら、プールから次に使用可能な ID をフェッチして使用します。その後、環境内でネットワークまたはストレージリソースへのアクセスを失うことなく、あるサーバから別のサーバにプロファイルを移行できます。

プール内のエントリ数を編集できます。ただし、エントリ数を割り当て済みの数または予約された数より少なくすることはできません。割り当てられていなまたは予約されていないエントリを削除することもできます。

メモ: ID の範囲が重複している場合、ID プールの編集に失敗します。Ethernet、FCoE、および iSCSI 用に設定された ID プールがあり、既存の範囲と重複している開始アドレスを編集して交換しようとすると、交換は許可されません。開始 MAC アドレスを交換するには、開始 MAC アドレスを競合している範囲から一度に 1 つのセクションずつ移動する必要があります。

[プール名] ID プールの名前を入力します。プール名の最大長は 255 文字です。

[説明] ID プールの説明を入力します。説明の最大長は 255 文字です。

処置

[次へ] [イーサネット] タブを表示します。

[完了] 変更を保存して、[ID プール] ページを表示します。

[キャンセル] 変更を保存せずに [ID プールの作成] ウィザードを閉じます。

ID プール

ID プールは、ネットワーク通信に必要な 1 つ以上の仮想 ID タイプの集合です。ID プールには、次の仮想 ID タイプの組み合わせを含めることができます。

- Ethernet ID

  メディア アクセス制御（MAC）アドレスによって定義される ID。MAC address は Ethernet（LAN）通信に必要です。

- iSCSI ID

  iSCSI 修飾名（IQN）によって定義される 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。

- ファイバー チャネル（FC）ID

  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 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。

- Fibre Channel over Ethernet（FCoE）ID

  FCoE を操作するための一意の仮想 ID。MAC アドレスおよび FC アドレス（WWNN および WWPN）で定義される ID。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。

OpenManage Enterprise では ID プールを利用して、サーバー導入に使用したデバイス導入テンプレートに仮想 ID を自動的に割り当てます。

メモ:
- 既存の ID プールに属しているが、OpenManage Enterprise 以外に導入されていた ID については、新しい設定インベントリー ジョブを識別し、アプライアンスで「割り当て済み」として指定する必要があります。
- すでに割り当てられている仮想 ID は、これらの ID がクリアされない限り、新しい導入環境では使用されません。

ID プールの作成

1 つ以上の仮想 ID タイプで構成される ID プールを作成することができます。管理者によって作成された共通プールは、すべてのデバイス マネージャーで使用できます。また、管理者は、使用されているすべての ID を表示することができます。デバイス マネージャーはすべての ID プールを表示し、そのプールに対するすべての操作を実行します（RBAC で指定されています）。ただし、[使用状況] では、デバイス マネージャーはそのスコープ内のデバイスに関連付けられた ID のみを表示することができます。

仮想 ID タイプのプールは、次の手順で作成します。

1. [設定] ページで、[ID プール] をクリックします。
2. [作成] をクリックします。
3. [ID プールの作成] ダイアログボックスの [プール情報] で、次の手順を実行します。
   a. ID プールの固有の名前と適切な説明を入力します。
   b. [次へ] をクリックします。
4. [イーサネット] セクションで、次の手順を実行します。
   a. MAC アドレスを含めるには、[イーサネット仮想 MAC アドレスを含める] チェックボックスをオンにします。
   b. 開始 MAC アドレスを入力し、作成する仮想 MAC ID の数を指定します。
5. [iSCSI] セクションで、次の手順を実行します。
   a. iSCSI MAC アドレスを含めるには、[iSCSI MAC アドレスを含める] チェックボックスをオンにします。
   b. 開始 MAC アドレスを入力し、作成する iSCSI MAC アドレスの数を指定します。
   c. [iSCSI イニシエータの設定] を選択し、IQN プレフィックスを入力します。
   d. [iSCSI イニシエータ IP プールを有効にする] を選択し、ネットワークの詳細を入力します。

      メモ: iSCSI イニシエータ IP プールは IPv6 アドレスをサポートしていません。

6. [FCoE] セクションの場合で、以下の手順を実行します。
   a. FCoE ID を含めるには、[FCoE ID を含める] チェックボックスをオンにします。
   b. 開始 MAC アドレスを入力し、作成する FCoE ID の数を指定します。

メモ: WWPN および WWNN アドレスは、それぞれ MAC アドレスに 0x2001 および 0x2000 をプレフィックスとして付けることによって生成されます。

7. [Fibre Channel] セクションで、以下の手順を実行します。
   a. FC ID を含めるには、[FC ID を含める] チェックボックスをオンにします。
   b. ポストフィックスオクテット (6 オクテット) とともに、作成する WWPN アドレスと WWNN アドレスの数を入力します。

      メモ: WWPN および WWNN アドレスは、用意されたポストフィックスに、それぞれ 0x2001 および 0x2000 をプレフィックスとして付けることによって生成されます。

ID プールが作成され、[ID プール] タブにリストされます。

ID プールの作成 - ファイバチャネル

ファイバチャネル (FC) アドレスを ID プールに追加できます。FC は WWPN/WWNN アドレスで構成されています。

[FC ID を含める] FC アドレスを ID プールに追加するには、このチェックボックスを選択します。

[Postfix (6 オクテット)] Postfix の入力は次のいずれかの形式で行います。
- `AA:BB:CC:DD:EE:FF`
- `AA-BB-CC-DD-EE-FF`
- `AABB.CCDD.EEFF`

Postfix の最大長は 50 文字です。このオプションは、[FC ID を含める] チェックボックスが選択されている場合にのみ表示されます。

[WWPN/WWNN アドレスの数] WWPN または WWNN アドレスの数を選択します。アドレスは、1 ~ 5000 の間で設定できます。

このオプションは、[FC ID を含める] チェックボックスが選択されている場合にのみ表示されます。

処置

[前へ] [FCoE] タブを表示します。

[完了] 変更を保存して、[設定] ページを表示します。

[キャンセル] 変更を保存せずに [ID プールの作成] ウィザードを閉じます。

ID プールの作成 - iSCSI

iSCSI タブで、必要な数の iSCSI MAC アドレスを設定できます。

メモ: iSCSI 属性は、iSCSI イニシエータ用の DHCP オプションがソースのテンプレートで無効の場合にのみ適用されます。

[仮想 iSCSI MAC アドレスを含める] iSCSI MAC アドレスを ID プールに追加するには、このチェックボックスを選択します。

[開始仮想 MAC アドレス] 次のいずれかの形式で ID プールの開始 MAC アドレスを入力します。
- `AA:BB:CC:DD:EE:FF`
- `AA-BB-CC-DD-EE-FF`
- `AABB.CCDD.EEFF`

MAC アドレスの最大長は 50 文字です。このオプションは、[iSCSI MAC アドレスを含める] チェックボックスが選択されている場合にのみ表示されます。

[iSCSI MAC アドレスの数] iSCSI MAC アドレスの数を入力します。MAC アドレスは 1 ~ 5000 の間で設定できます。このオプションは、[iSCSI MAC アドレスを含める] チェックボックスが選択されている場合にのみ表示されます。

[iSCSI イニシエータの設定] iSCSI イニシエータを設定するには、このチェックボックスを選択します。このオプションは、[iSCSI MAC アドレスを含める] チェックボックスが選択されている場合にのみ表示されます。

[IQN プレフィックス] iSCSI の ID プールの IQN プレフィックスを入力します。IQN プレフィックスの最大長は 200 文字です。システムは、生成された番号をプレフィックスに追加し、IQN アドレスのプールを自動的に生成します。例：`<IQN Prefix>.<number>`

このオプションは、[iSCSI イニシエータの設定] チェックボックスが選択されている場合にのみ表示されます。

メモ: ID プールで設定された IQN は、起動モードが「BIOS」の場合、ターゲットシステムに展開されません。

メモ: [ID プール] > [使用状況] > [iSCSI IQN] フィールドの別の行に iSCSI イニシエータ名が表示される場合は、iSCSI IQN が NIC パーティションでのみ有効になっていることを示します。

[iSCSI イニシエータの IP プールの有効化] チェックボックスを選択して、iSCSI イニシエータ ID のプールを設定します。このオプションは、[iSCSI MAC アドレスを含める] チェックボックスが選択されている場合にのみ表示されます。

[IP アドレス / 範囲] iSCSI イニシエータプールの IP アドレス範囲を、次のいずれかの形式で入力します。

- `A.B.C.D - W.X.Y.Z`
- `A.B.C.D/E`

[サブネットマスク] ドロップダウンリストから、iSCSI プールのサブネットマスクアドレスを選択します。

[ゲートウェイ] iSCSI プールのゲートウェイアドレスを入力します。

[プライマリー DNS サーバー] プライマリ DNS サーバアドレスを入力します。

[セカンダリー DNS サーバー] セカンダリー DNS サーバー アドレスを入力します。

メモ: [IP アドレスの範囲]、[ゲートウェイ]、[プライマリ DNS サーバ]、[セカンダリ DNS サーバ] は、有効な IPv4 アドレスである必要があります。

処置

[前へ] [イーサネット] タブを表示します。

[次へ] [FCoE] タブを表示します。

[完了] 変更を保存して、[設定] ページを表示します。

[キャンセル] 変更を保存せずに [ID プールの作成] ウィザードを閉じます。

ID プールの作成 - Fibre Channel over Ethernet

必要な数の Fibre Channel over Ethernet（FCoE）初期化プロトコル（FIP）MAC アドレスを ID プールに追加できます。World Wide Port Name（WWPN）/ ワールドワイドノード名（WWNN）の値は、これらの MAC アドレスから生成されます。

[FCoE ID を含める] FCoE MAC アドレスを ID プールに含めるには、このチェックボックスを選択します。

[FIP MAC アドレス] ID プールの FCoE 初期化プロトコル（FIP）開始 MAC アドレスを、次のいずれかの形式で入力します。

- `AA:BB:CC:DD:EE:FF`
- `AA-BB-CC-DD-EE-FF`
- `AABB.CCDD.EEFF`

MAC アドレスの最大長は 50 文字です。このオプションは、[FCoE ID を含める] チェックボックスが選択されている場合にのみ表示されます。

WWPN/WWNN の値は、MAC アドレスから生成されます。

[FCoE ID の数]　必要な FCoE ID の数を選択します。この ID は 1 ~ 5000 の間で設定できます。

処置

[前へ]　[iSCSI] タブを表示します。

[次へ]　[ファイバチャネル] タブを表示します。

[完了]　変更を保存して、[ID プール] ページを表示します。

[キャンセル]　変更を保存せずに [ID プールの作成] ウィザードを閉じます。

ID プールの作成 - Ethernet

[イーサネット] タブでは、必要な数の MAC アドレスを ID プールに追加できます。

[イーサネット仮想 MAC アドレスを含める]　仮想 MAC アドレスを ID プールに追加するには、このチェックボックスを選択します。

[開始仮想 MAC アドレス]　次のいずれかの形式で、開始仮想 MAC アドレスを入力します。

- `AA:BB:CC:DD:EE:FF`
- `AA-BB-CC-DD-EE-FF`
- `AABB.CCDD.EEFF`

MAC アドレスの最大長は 50 文字です。このオプションは、[イーサネット仮想 MAC アドレスを含める] チェックボックスが選択されている場合にのみ表示されます。

[仮想 MAC ID の合計数]　仮想 MAC ID の合計数を選択します。ID の合計数は 1~50 に設定できます。このオプションは、[イーサネット仮想 MAC アドレスを含める] チェックボックスが選択されている場合にのみ表示されます。

処置

[前へ]　[プール情報] タブを表示します。

[次へ]　[iSCSI] タブを表示します。

[完了]　変更を保存して、[ID プール] ページを表示します。

[キャンセル]　変更を保存せずに [ID プールの作成] ウィザードを閉じます。

ID プールの定義の表示

ID プールの定義を表示するには、次の手順を実行します。

1. [設定] ページで、[ID プール] をクリックします。
2. ID プールを選択して、[サマリ] をクリックします。
   ID プールのさまざまな ID 定義がリストされます。
3. これらの ID 定義の使用状況を表示するには、[使用状況] タブをクリックし、[表示条件] フィルタオプションを選択します。

ID 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 ID タイプを追加したり、ID タイプの範囲を削除したりするために ID プールを編集できます。

ID プールの定義を編集するには、次の手順を実行します。

1. [設定] ページで、[ID プール] をクリックします。

2. ID プールを選択し、[編集] をクリックします。
   [ID プールの編集] ダイアログボックスが表示されます。
3. 該当するセクションの定義に変更を行い、[終了] をクリックします。

これで ID プールが変更されました。

ID プールの削除

ID が予約されているか、導入テンプレートに割り当てられている場合は、ID プールを削除することはできません。

ID プールを削除するには、次の手順を実行します。

1. [設定] ページで、[ID プール] をクリックします。
2. ID プールを選択して、[削除] をクリックします。
3. [はい] をクリックします。

ID プールが削除され、1 つ以上の導入テンプレートに関連付けられていた予約済みの ID が削除されます。

ネットワークの定義

VLAN ページでは、デバイスがアクセスできる環境で現在構成されているネットワークの情報を入力することができます。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

1. [設定] > [VLAN] > [定義] の順に選択します。
2. [ネットワークの定義] ダイアログボックスで、名前と適切な説明を入力します。
3. VLAN ID を入力し、ネットワークタイプを選択します。
   ネットワークタイプを選択できるのは MX7000 シャーシのみです。ネットワークタイプの詳細については「ネットワークタイプ 、p. 96」を参照してください。
4. [終了] をクリックします。

これで、ご使用の環境に現在設定されているネットワークが定義され、リソースがネットワークにアクセスできるようになります。

メモ: 範囲ベースの制限は、共通のリソース プールであるため、VLAN に適用されません。VLAN が管理者によって定義されると、すべてのデバイス マネージャーが使用できるようになります。

ネットワークタイプ

メモ: ネットワークタイプを選択できるのは MX7000 シャーシのみです。

表 15. ネットワークタイプ

ネットワークタイプ	説明
[汎用 (ブロンズ)]	優先度の低いデータトラフィックに使用されます。
[汎用 (シルバー)]	標準またはデフォルトの優先度のデータトラフィックに使用されます
[汎用 (ゴールド)]	優先度の高いデータトラフィックに使用されます。
[汎用 (プラチナ)]	優先度が非常に高いデータトラフィックに使用されます
[クラスタ相互接続]	クラスタハートビート VLAN に使用されます
[ハイパーバイザ管理]	ESXi management VLAN などのハイパーバイザ管理接続用に使用されます

表 15. ネットワークタイプ（続き）

ネットワークタイプ	説明
[ストレージ - iSCSI]	iSCSI VLAN に使用されます
[ストレージ - FCoE]	FCoE VLAN に使用されます
[ストレージ - データレプリケーション]	VMware 仮想ストレージエリアネットワーク（VSAN）など、ストレージのデータレプリケーションをサポートする VLAN に使用されます
[VM の移行]	vMotion および同様のテクノロジをサポートする VLAN に使用されます
[VMWare FT ロギング]	VMware フォールトトレランスをサポートする VLAN に使用されます

設定済みネットワークの編集または削除

1. [設定] > [VLAN] をクリックして、[VLAN] ページに移動します。
2. リストからネットワークを選択し、右側のペインで [編集] をクリックして名前、説明、VLAN ID、またはネットワークタイプを変更します。

   メモ: M I/O アグリゲーター（IOA）および FN I/O モジュールでは IPv6 アドレス指定はサポートされないため、IPv6 インフラストラクチャーでは M1000e および FX2 シャーシでの VLAN 設定はサポートされません。

   メモ: ステートレス導入タスクを実行すると、変更された VLAN 名と ID はターゲット MX7000 シャーシでアップデートされません。

3. ネットワークを削除するには、ネットワークを選択し、[削除] をクリックします。
4. [はい] をクリックします。

VLAN 定義のエクスポート

OpenManage Enterprise で使用可能なネットワーク定義は、CSV または JSON ファイルのいずれかの形式でダウンロードできます。

1. CSV ファイルとしてダウンロードするには、次のように操作します。
   a. [設定] > [VLAN] > [エクスポート] をクリックして、[すべて CSV としてエクスポート] を選択します。
2. JSON ファイルとしてダウンロードするには、次のように操作します。
   a. [設定] > [VLAN] > [エクスポート] をクリックして、[すべて JSON としてエクスポート] を選択します。

ネットワーク定義のインポート

ネットワーク定義をインポートするには、次のオプションを使用できます。

1. **VLAN 定義をファイルからインポート**

   VLAN 定義をファイルからインポートするには、次のようにします。

   a. [設定] > [VLAN] をクリックします。
   b. [インポート] をクリックして [ファイルからインポート] を選択します。
   c. ファイルのある場所に移動し、VLAN 定義を含んだ既存の.json または.csv ファイルを選択して、[開く] をクリックします。

   メモ:
   - ファイル内にある無効なエントリーやコンテンツ タイプについては、フラグが付けられ、インポートされません。
   - .csv および.json ファイルの VLAN 定義は、次のフォーマットで入力する必要があります。

表 16. CSV ファイルの VLAN 定義フォーマット

名前	説明	VLANMin	VLANMax	タイプ
VLAN1	単一 ID の VLAN	1	1	1
VLAN2 (Range)	ID の範囲が指定された VLAN	2	10	2

および

表 17. JSON ファイルの VLAN 定義フォーマット

```
[{"Name":"VLAN1","Description":"VLAN with single ID
","VlanMinimum":1,"VlanMaximum":1,"Type":1},
{"Name":"VLAN2 (Range)","Description":"VLAN with an ID Range
","VlanMinimum":2,"VlanMaximum":10,"Type":2}]
```

d. [終了] をクリックします。選択したファイルからネットワークをインポートするためのジョブが **ImportVLANDefinitionsTask** という名前で作成されます。

2. **VLAN 定義のシャーシからのインポート**

VLAN 定義を既存の MX7000 シャーシからインポートするには、次のようにします。

メモ: MX7000 には、OpenManage Enterprise-Modular バージョン 1.2 がインストールされている必要があります。

a. [設定] > [VLAN] をクリックします。
b. [インポート] をクリックして、[VLAN をシャーシからインポート] を選択します。
c. [**ジョブのターゲット**] 画面で、VLAN の定義をインポートするシャーシを選択し、[OK] をクリックします。選択したシャーシからネットワークをインポートするためのジョブが、**ImportVLANDefinitionsTask** という名前で作成されます。

ジョブが完了したら、[構成] > [VLAN] ページを更新して、インポートされた VLAN 定義を表示します。

ジョブの実行の詳細と、シャーシからインポートされた各ネットワークのステータスを表示させるには、[監視] > [ジョブ] をクリックして [**ジョブ**] ページに移動し、該当するジョブを選択して [詳細の表示] をクリックします。

12

プロファイルの管理

「プロファイル」は、既存の導入テンプレートの特定インスタンスであり、個々のデバイスに固有の属性を用いてカスタマイズしたものです。プロファイルの作成は、テンプレートの導入/自動導入時に暗黙的に行われるか、あるいは既存のテンプレートを基にユーザーが作成することができます。プロファイルは、ターゲット固有の属性値と、BootToISO の選択、およびターゲット デバイスに関する iDRAC 管理 IP の詳細によって構成されます。また該当する場合は、サーバー NIC ポートのネットワーク帯域幅や VLAN 割り当てを含めることもできます。プロファイルは、作成元であるソース テンプレートにリンクされています。

[設定] > [プロファイル] ページで、ログインしているユーザーのスコープ内にあるすべてのプロファイルが表示されます。たとえば、管理者がすべてのプロファイルを表示して管理することはできますが、制限されたスコープのデバイス マネージャーでは、作成および所有するプロファイルのみを表示して使用できます。

リストされたプロファイルの次の詳細情報が表示されます。

表 18. プロファイルの管理 - フィールドの定義

フィールド名	説明
変更済み	最初の割り当て後に、関連するプロファイルやテンプレート属性に変更や修正が生じた場合、その通知として「変更済み」シンボル⚠が表示されます。変更後のプロファイルがデバイスに再導入されると、このシンボルは表示されなくなります。
プロファイル名	プロファイルの名前
テンプレート名	リンクされたソース テンプレートの名前
ターゲット	プロファイルが割り当てられたデバイスのサービス タグまたは IP アドレス。プロファイルがどのデバイスにも割り当てられていない場合、ターゲットは空白にされます。
ターゲット タイプ	プロファイルが割り当てられたデバイスのタイプ (サーバーまたはシャーシ)
シャーシ	ターゲット サーバーがシャーシの一部として検出された場合のシャーシ名
プロファイルの状態	プロファイルの状態についての表示は、プロファイルが割り当てられている場合は「デバイスに割り当て済み」、プロファイルが割り当てられていない場合は「未割り当て」、導入済みプロファイルの場合は「導入済み」とされます。
最後のアクションのステータス	プロファイルの最後のアクションのステータスとして、「中止」、「キャンセル」、「完了」、「失敗」、「新規」、「未実行」、「一時停止」、「キュー済み」、「実行中」、「スケジュール済み」、「開始中」、「停止済み」、「エラーが発生して完了」などが表示されます。

[詳細フィルター] を使用して、プロファイル リストをカスタマイズすることができます。

右側 — 選択したプロファイルに関する説明、最終導入時刻、最終更新時刻、作成日、作成者が表示されます。[ID の表示] をクリックすると、プロファイルにタグ付けされている NIC 設定および仮想 ID が表示されます。

さまざまなプロファイルの状態に応じて、次に説明するように、[設定] > [プロファイル] ページで次のアクションを実行できます。

メモ: 作成および削除操作は、テーブルの一部としては表示されません。

表 19. プロファイルの状態と可能な操作

プロファイルの状態	編集	ターゲットの割り当て	ターゲットの割り当て解除	再導入	移行
割り当て解除済みプロファイル	はい	はい	いいえ	いいえ	いいえ

表 19. プロファイルの状態と可能な操作（続き）

プロファイルの状態	編集	ターゲットの割り当て	ターゲットの割り当て解除	再導入	移行
デバイスに割り当て済み	はい	いいえ	はい	いいえ	いいえ
導入済み	はい	いいえ	はい	はい	はい

- プロファイル作成と仮想 ID の事前予約。参照： プロファイルの作成 、p. 100
- プロファイルの詳細表示。参照： プロファイルの詳細の表示 、p. 101
- プロファイルの属性と設定の編集。参照： プロファイルの編集 、p. 101
- デバイスまたはサービス タグへのプロファイルの割り当て（自動導入を使用 ）。参照： プロファイルの割り当て 、p. 102
- デバイスまたはサービス タグからのプロファイルの割り当て解除。参照： プロファイルの割り当て解除 、p. 103
- 関連するターゲット デバイスへのプロファイル変更の再導入。参照： プロファイルの再導入 、p. 103
- 1 つのターゲット（デバイスまたはサービス タグ）から別のターゲットへのプロファイルの移行。
- プロファイルの削除。参照： プロファイルの削除 、p. 104
- HTML、CSV、または PDF へのプロファイル データのエクスポートとダウンロード。参照： プロファイル データの HTML、CSV、PDF としてのエクスポート 、p. 104

トピック：

- プロファイルの作成
- プロファイルの詳細の表示
- プロファイル - ネットワークの表示
- プロファイルの編集
- プロファイルの割り当て
- プロファイルの割り当て解除
- プロファイルの再導入
- プロファイルの移行
- プロファイルの削除
- プロファイル データの HTML、CSV、PDF としてのエクスポート

プロファイルの作成

既存の導入テンプレートを使用してプロファイルを作成すると、既存のターゲット デバイスにプロファイルを導入することができます。また、プロファイルを予約することにより、未検出のデバイスで自動的に導入することもできます。

メモ:

- プロファイル管理のタスクを実行できるのは OpenManage Enterprise 管理者またはデバイス マネージャーの権限を持つユーザーのみです。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- バージョン 3.5 またはそれ以前のバージョンからのアップグレード後、以前の OpenManage Enterprise リリースのいずれかから AD/LDAP および OIDC（PingFederate または KeyCloak）デバイス マネージャーによって作成されたプロファイルは、管理者のみに割り当てられます。そのため、デバイス マネージャーは、アップグレード後にプロファイルを再作成する必要があります。

既存の導入テンプレートからプロファイルを作成するには、次の手順を実行します。

1. [設定] > [プロファイル] をクリックして、[プロファイル] ページに移動します。
2. [作成] をクリックして、[プロファイルの作成] ウィザードを有効にします。
3. [テンプレート] セクションの [テンプレート タイプ] で [サーバー] または [シャーシ] を選択し、[テンプレートの選択] ドロップダウン リストから導入テンプレートを選択します。[次へ] をクリックします。
4. [詳細] ページで、[名前のプレフィックス] を変更し、必要に応じて [説明] ボックスに説明を入力します。[プロファイル数] ボックスに、プロファイルの数を入力します。[次へ] をクリックします。
5. オプションとして、[ネットワーク ISO からの起動] ページで、[ネットワーク ISO からの起動] チェック ボックスを選択します。ISO のフル パスとファイル共有の場所を指定し、[ISO 接続時間] オプションを選択して、ネットワーク ISO ファイルがターゲット デバイスにマップされたままになる時間を設定します。
6. [終了] をクリックします。

プロファイルは、入力された導入テンプレート名と数に基づいて作成されます。作成されたプロファイルは [プロファイル] ページの一覧に表示されます。

プロファイルの詳細の表示

編集せずに既存のプロファイルの詳細をただ表示するには、次の手順を実行します。

1. [設定] > [プロファイル] ページで、プロファイルのリストからプロファイルを選択します。
2. [表示] をクリックして、[プロファイルの表示] ウィザードを有効にします。
3. ウィザードの [詳細] ページに、ソース テンプレート、名前、説明、ターゲットの情報が表示されます。
4. [次へ] をクリックします。そのプリファレンスでプロファイルが最初に設定されていた場合には、[ネットワーク ISO からの起動] ページに、ISO イメージ ファイルのパス、ISO イメージ ファイルの共有の場所、および [ISO 接続時間] の値が表示されます。

プロファイル - ネットワークの表示

プロファイルに関連付けられている NIC ポートのネットワーク帯域幅と VLAN 割り当てを表示するには、次のようにします。

1. [設定] > [プロファイル] ページでプロファイルを選択します。
2. [表示] > [ネットワークの表示] をクリックして、[ネットワークの表示] ウィザードを有効にします。
3. [**帯域幅**] セクションには、領域確保された NIC の帯域幅設定 (NIC 識別子、ポート、パーティション、最小帯域幅 (%)、最大帯域幅 (%)) が表示されます。[次へ] をクリックします。
4. [**VLAN**] セクションには、プロファイルの VLAN 詳細 (NIC チーミング、NIC 識別子、ポート、チーム、タグなしネットワーク、タグ付きネットワーク) が表示されます。
5. [終了] をクリックして、[ネットワークの表示] ウィザードを閉じます。

プロファイルの編集

[設定] > [プロファイル] ページで、既存のプロファイルを編集することができます。プロファイルを変更しても、関連づけられているターゲットシ ステムが自動的に影響を受けることはありません。変更を有効にするには、変更されたプロファイルをターゲット デバイスに導入しなおす必要があります。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。参照先： OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15

既存のプロファイルの名前の変更、ネットワークの編集、または属性の編集を行うには、[プロファイル] ページでプロファイルを選択して、[編集] をクリックします。次の編集オプションが選択可能です。

1. [名前の変更] を選択し、[プロファイルの名前変更] ウィザードの [名前] ボックスでプロファイル名を編集します。
2. [プロファイルの編集] を選択して [プロファイルの編集] ウィザードをアクティブ化し、次の項目を編集します。
   a. [詳細] ページでは、[名前] と [説明] を編集できます。[次へ] をクリックします。
   b. [ネットワーク ISO で起動] ページで、[ネットワーク ISO で起動] チェック ボックスを選択し、ISO のフルパスと共有の場所を指定して、次の手順を実行します。
      - [共有タイプ] で CIFS または NFS を選択します。
      - [ISO パス] ボックスに、ISO のフル パスを入力します。ツールヒントを使用して正しい構文を入力します。
      - [共有 IP アドレス]、[ユーザー名]、および [パスワード] ボックスに詳細情報を入力します。
      - [ISO 接続時間] ドロップダウン メニュー オプションを選択して、ネットワーク ISO ファイルがターゲット デバイスにマップされたままになる時間数を設定します。デフォルトでは、この値は 4 時間に設定されています。
      - [次へ] をクリックします。
   c. [iDRAC 管理 IP] ページで、以下のいずれかを選択します。
      - IP 設定を変更しない
      - DHCP として設定
      - 静的 IP を設定して、関連する管理 IP、サブネットマスク、およびゲートウェイの詳細情報を入力する
   d. [ターゲット属性] ページでは、プロファイルの BIOS、システム、NIC、iDRAC、および仮想 ID 属性を選択して編集することができます。
   e. [終了] をクリックし、設定を保存します。

プロファイルの割り当て

[設定] > [プロファイル] ページでは、未割り当てプロファイルに対する操作として、既存サーバーへの導入、または未検出サーバーへの自動導入の予約のいずれかが行えます。

メモ:
- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- ターゲット サーバーに既存の属性がある場合、これらはプロファイルが導入された時点で上書きされます。
- どのプロファイルにも関連付けられていないデバイスのみが導入または自動導入に使用できます。

1. **プロファイルの導入**をするには、次のように操作します。
   a. [設定] > [プロファイル] ページで未割り当てプロファイルを選択し、[割り当て] > [導入] をクリックして、プロファイルの導入ウィザードをアクティブにします。
   b. [詳細] ページに、ソース テンプレート、プロファイル名、および説明が表示されます。[次へ] をクリックします。
   c. [ターゲット] ページで、次のように操作します。
      - デバイスのリストから [選択] をクリックし、ターゲット デバイスを選択します。
        メモ: プロファイルが割り当て済みのデバイスはグレー表示され、ターゲット リストでは選択できません。
      - 導入後に再起動が必要な場合は、[正常な再起動に失敗した場合、強制的にホスト OS を再起動させない] チェック ボックスを選択します。
      - [次へ] をクリックします。
   d. (オプション)[ネットワーク ISO からの起動] ページで、[ネットワーク ISO からの起動] チェック ボックスを選択して、関連する ISO パス、共有する位置の詳細、[ISO 接続時間] の値を指定します。[次へ] をクリックします。
   e. [iDRAC 管理 IP] ページで、次のいずれかのオプションを選択し、関連する詳細情報を指定します。
      - IP 設定を変更しない
      - DHCP として設定
      - 静的 IP を設定
   f. [ターゲット属性] ページで、BIOS、システム、NIC、iDRAC の各セクションに属性が表示されます。導入の実行前に、属性の選択、選択解除、または編集を行えます。
   g. [仮想 ID] ページで、[予約 ID] をクリックします。選択したターゲット デバイスの NIC カードに割り当てられた仮想 ID が表示されます。選択したターゲット デバイスの ID プールに割り当てられた ID をすべて表示するには、[すべての NIC の詳細を表示] をクリックします。
   h. [スケジュール] ページでは、[今すぐ実行] を選択してプロファイルをただちに導入するか、あるいは [スケジュールの有効化] を選択してプロファイルを展開する都合のよい日時を選択できます。
   i. [終了] をクリックします。

   メモ: アプライアンス以外で ID がすでに割り当てられている場合、これらの ID はクリアされない限り新しい導入環境では使用されません。詳細については、次を参照： ID プール 、p. 92

2. **プロファイルの自動導入**を行うには、次を実行します。

   メモ: モジュラー デバイスの場合、デフォルトで VLAN 定義の厳密なチェックが有効になっています。

   a. [設定] > [プロファイル] ページで未割り当てプロファイルを選択し、[割り当て] > [自動導入] をクリックして、自動導入ウィザードをアクティブにします。
   b. [詳細] ページには、プロファイルのソース テンプレート、名前、および説明 (存在する場合) が表示されます。[次へ] をクリックします。
   c. [ターゲット] ページで、未検出デバイスのノード ID またはサービス タグを [識別子] ボックスに指定します。[次へ] をクリックします。
   d. (オプション)[ネットワーク ISO からの起動] ページで、[ネットワーク ISO からの起動] チェック ボックスを選択し、ISO のフル パスおよび共有する位置を指定します。
      - [共有タイプ] として CIFS または NFS のいずれかを選択します。
      - [ISO パス] ボックスに、ISO のフル パスを入力します。ツールヒントを使用して、正しい構文を入力します。
      - [共有 IP アドレス]、[ユーザー名]、[パスワード] ボックスに詳細を入力します。
      - [ISO 接続時間] ドロップダウン メニュー オプションを選択して、ネットワーク ISO ファイルがターゲット デバイスにマップされたままになる時間数を設定します。デフォルトでは、この値は 4 時間に設定されています。
   e. [終了] をクリックします。

プロファイルの割り当て解除

[設定] > [プロファイル] > [割り当て解除] を使用して、導入されたプロファイルまたは自動導入されたプロファイルと、それぞれのターゲットとの関連付けを解除することができます。。

プロファイルの割り当てを解除するには、次の手順を実行します。

1. [設定] > [プロファイル] ページの [プロファイル] リストからプロファイルを選択します。
2. [割り当て解除] をクリックします。
3. [終了] をクリックすると [確認] ダイアログボックスが表示されます。

選択したプロファイルの割り当てが解除され、それぞれのターゲットからの識別情報が削除されます。

メモ: 導入済みのターゲット デバイスについては、プロファイルの割り当てを解除すると、工場出荷時に割り当てられた ID に戻ります。

プロファイルの再導入

すでに導入されているプロファイルの属性を変更して、関連するターゲットデバイスに適用するには、プロファイルを再導入する必要があります。モジュラー デバイスの場合、再導入時に VLAN の定義を設定することができます。ただし、VLAN 属性の照合での厳格なチェックは無効になります。

メモ:「VLAN 設定をただちに伝播」オプションを使用してテンプレートの導入中に VLAN 属性が MX7000 スレッドに最初に導入されなかった場合、VLAN 属性の変更はプロファイルの再導入中にターゲット MX7000 スレッドで失敗します。

プロファイルを再導入するには、次の手順を実行します。

1. [設定] > [プロファイル] ページで、「導入済み」または「変更済み」(⚠) のプロファイルを選択し、[再導入] をクリックします。
2. 再導入ウィザードの [属性導入オプション] ページで、次のいずれかの属性導入オプションを選択し、[次へ] をクリックします。
   - [変更された属性のみ]: ターゲット デバイス上で変更された属性のみを再導入します。
   - [すべての属性]: すべての属性を、ターゲット デバイス上の変更された属性とともに再導入します。
3. [スケジュール] ページで、次から選択します。
   - [今すぐ実行] を選択すると変更をただちに実装します。
   - [スケジュールの有効化] を選択し、再導入をスケジュールする日時を選択します。
4. [終了] をクリックして続行します。

プロファイルを再導入すると、**プロファイルの再展開**ジョブが実行されます。ジョブ状態は、[監視] > [ジョブ] ページで見ることができます。

プロファイルの移行

導入済みまたは自動導入済みのプロファイルは、既存のターゲット デバイスまたはサービス タグから、別の同一のターゲット デバイスまたはサービス タグに移行することができます。

移行が正常に完了すると、プロファイル ターゲットの割り当てに新しいターゲットが反映されます。ターゲット デバイスからまだ表示されていないサービス タグへの移行の場合、プロファイルの状態は「割り当て済み」に変更されます。

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- プロファイルの移行は、プロファイル (導入された仮想 ID を含む) によって定義された設定をソースからターゲットに移動します。
- ソース デバイスに接続できない場合でも、プロファイルの移行を強制することができます。この場合、仮想 ID の競合がないことを確認してください。
- 真のターゲット固有の属性は、移行の一環として「ソース」サーバーからは再利用されません。これにより、移行後の 2 台のサーバーで同じインベントリーの詳細が存在することがあります。

プロファイルを移行するには、次の手順を実行します。

1. [設定] > [プロファイル ページ] でプロファイルを選択し、[移行] をクリックして [プロファイルの移行] ウィザードをアクティブにします。
2. 選択ページで、次の手順を実行します。
   a. [ソース プロファイルの選択] ドロップダウン メニューから、移行するプロファイルを選択します。
   b. [ターゲットの選択] をクリックし、ジョブのターゲット ダイアログ ボックスでターゲット デバイスを選択して [Ok] をクリックします。
   c. 必要に応じて、[ソース デバイスに接続できない場合でも移行を強制する] チェック ボックスを選択します。

      メモ: 仮想 ID の競合がないことを確認してください。

   d. [次へ] をクリックします。
3. [スケジュール] ページで、以下のいずれかを選択します。
   a. [今すぐアップデート] を選択して、プロファイル設定をただちにターゲットに移行します。
   b. 移行をスケジュールする [日付] と [時刻] を選択します。
4. [終了] をクリックします。

プロファイルの設定を新しいターゲット デバイスに移行するためのジョブが作成されます。ジョブのステータスは、[監視] > [ジョブ] ページに表示できます。

プロファイルの削除

[設定] > [プロファイル] ページで、「未割り当て」のプロファイルを削除することができます。

メモ:

- 割り当て済みまたは導入済みのプロファイルは、割り当てられていない場合にのみ、[プロファイル ポータル] から削除できます。
- ID が予約されている未割り当てプロファイルを削除すると、それらの ID は元の ID プールに返されます。これらの回収された ID を将来の予約および導入に使用するには、10 分間待つことをお勧めします。

未割り当てのプロファイルを削除するには、次の手順を行います。

1. [プロファイル] ページで、未割り当てのプロファイルを選択します。
2. [削除] をクリックし、プロンプトが表示されたら、[はい] をクリックして確認します。

プロファイル データの HTML、CSV、PDF としてのエクスポート

プロファイル データを HTML、CSV、または PDF ファイルとしてエクスポートするには、次の手順を実行します。

1. [設定] > [プロファイル] ページで、プロファイルを選択します。
2. [エクスポート] をクリックし、[選択項目のエクスポート] ダイアログ ボックスで、HTML、CSV、または PDF を選択します。
3. [終了] をクリックします。プロファイル データが、選択されたフォーマットでダウンロードされます。

13

デバイス設定コンプライアンスの管理

[OpenManage Enterprise] > [設定] > [設定コンプライアンス] の順に選択すると、ビルトインまたはユーザーが作成したコンプライアンス テンプレートを使用して設定 - コンプライアンス ベースラインを作成できます。コンプライアンス テンプレートは、既存の導入テンプレートやリファレンス デバイスから作成することもできれば、ファイルからインポートして作成することもできます。この機能を使用するには、サーバに OpenManage Enterprise および iDRAC のエンタープライズレベルのライセンスが必要です。Chassis Management Controller にライセンスは必要ありません。特定の権限を持つユーザーでのみ、この機能の使用を許可されます。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

コンプライアンス テンプレートを使用して設定ベースラインが作成された後に、各ベースラインのコンプライアンス レベルの概要が表にリストされます。ただし、ベースラインに関連付けられた各デバイスには独自のステータスがあり、重要度が最高のステータスがベースラインのステータスと見なされます。ロールアップ正常性状態の詳細については、サポート サイトにあるホワイトペーパー『*第 14 世代以降の Dell EMC PowerEdge サーバーで iDRAC を使用してロールアップ正常性状態を管理する*』を参照してください。

メモ: 複数のデバイスがあるベースラインは、一部の属性値がすべてのターゲットで必ずしも同じである必要はないため、永続的に非準拠と表示されることがあります。例えば、すべてのターゲットで同一でない、iSCSI ターゲット IQN、LUN ID、FCoE ターゲット WWPN などの起動制御属性は、そのベースラインで永続的に非準拠であると表示されることがあります。

全体的なコンプライアンスのサマリレポートには、次のフィールドが表示されます。

- **コンプライアンス**：設定コンプライアンスのベースラインに添付されるデバイスのロールアップコンプライアンスレベル。最もコンプライアンスが低い (重要) デバイスのステータスが全体のベースラインのステータスとして示されます。
- **名前**：設定コンプライアンスのベースラインの名前。
- **テンプレート**：ベースラインで使用されるコンプライアンステンプレートの名前。
- [**最終実行時間**]: コンプライアンス ベースラインが実行された最新の日付と時刻。

ベースラインの設定コンプライアンスのレポートを表示するには、対応するチェック ボックスを選択して、右ペインで [レポートの表示] をクリックします。

クエリビルダの機能を使用して、選択したベースラインに対するデバイスレベルのコンプライアンスを生成します。クエリ条件の選択 、p. 55 を参照してください。

OpenManage Enterprise は、監視対象デバイスのリストおよび設定コンプライアンスベースラインに対するコンプライアンスを表示するビルトインレポートを提供します。[OpenManage Enterprise] > [監視] > [レポート] > [デバイス (テンプレートコンプライアンスベースライン別)] の順に選択して、**実行** をクリックします。レポートの実行 、p. 135 を参照してください。

関連タスク

設定コンプライアンスベースラインの作成 、p. 108
設定コンプライアンスベースラインの編集 、p. 109
設定コンプライアンスベースラインの削除 、p. 111
コンプライアンス テンプレートの管理 、p. 106
クエリ条件の選択 、p. 55

トピック：

コンプライアンス テンプレートの管理

コンプライアンステンプレートを使用してコンプライアンスベースラインを作成したら、ベースラインに関連付けられているデバイスの設定コンプライアンス状態を定期的に確認します。デバイス設定コンプライアンスの管理 、p. 105 を参照してください。

導入テンプレートまたはリファレンス デバイスを使用するか、ファイルからインポートしてコンプライアンス テンプレートを作成できます。コンプライアンス テンプレートの管理 、p. 106 を参照してください。

メモ:
- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

[設定] > [設定コンプライアンス] > [テンプレートの管理] の順に選択すると、OpenManage Enterprise にある範囲ベースのアクセス権に基づいて、コンプライアンス テンプレートのリストを表示することができます。たとえば、管理者はすべてのコンプライアンス テンプレートを表示および管理できます。ただし、デバイス マネージャーは、作成および所有するテンプレートの表示と管理のみを行うことができます。このページでできること :

- 次の方法でコンプライアンステンプレートを作成する。
  - 導入用テンプレートを使用する。導入テンプレートからのコンプライアンス テンプレートの作成 、p. 106 を参照してください。
  - リファレンスデバイスを使用する。リファレンス デバイスからのコンプライアンス テンプレートの作成 、p. 107 を参照してください。
  - テンプレートファイルからインポートする。ファイルからのインポートによるコンプライアンス テンプレートの作成 、p. 107 を参照してください。
- コンプライアンステンプレートを編集する。コンプライアンス テンプレートの編集 、p. 108 を参照してください。
- コンプライアンステンプレートのクローンを作成する。コンプライアンス テンプレートのクローン作成 、p. 107 を参照してください。
- コンプライアンステンプレートについてのレポートをエクスポートする。[コンプライアンステンプレート] ページで、対応するチェック ボックスを選択してから [エクスポート] をクリックします。すべてまたは選択したデータのエクスポート 、p. 64 を参照してください。
- コンプライアンステンプレートを削除します。[コンプライアンステンプレート] ページで、対応するチェック ボックスを選択してから [削除] をクリックします。

設定コンプライアンスは、最大 6,000 台のデバイスに拡張できます。大規模な設定コンプライアンス アクティビティを効率的に管理するには、次の手順を実行します。
- 自動的にトリガーされるデフォルトの設定インベントリー タスクを無効にし、必要に応じて手動で実行します。
- デバイス数が少ないコンプライアンス ベースラインを作成します。例えば、6,000 台のデバイスは、それぞれ 1,500 台のデバイスを含む 4 つの個別ベースラインに分類される必要があります。
- すべてのベースラインのコンプライアンスを同時に確認することはできません。

メモ: コンプライアンス テンプレートを編集する場合、設定コンプライアンスは関連付けられているすべてのベースラインで自動的にトリガーされます。頻繁にテンプレートを編集するユース ケースでは、前述の拡張環境はサポートされないため、最適なパフォーマンスを得るためには、ベースラインごとに最大 100 のデバイスを関連付けることをお勧めします。

関連情報

デバイス設定コンプライアンスの管理 、p. 105
設定コンプライアンスベースラインの編集 、p. 109
設定コンプライアンスベースラインの削除 、p. 111
導入テンプレートからのコンプライアンス テンプレートの作成 、p. 106
コンプライアンス テンプレートの編集 、p. 108

導入テンプレートからのコンプライアンス テンプレートの作成

1. [設定] > [設定コンプライアンス] > [テンプレート管理] > [作成] > [導入テンプレートから] の順にクリックします。

2. [導入テンプレートのクローン] ダイアログボックスの [テンプレート] ドロップダウン メニューで、新しいテンプレートのリファレンスとして使用する必要がある導入テンプレートを選択します。
3. コンプライアンス テンプレートの名前と説明を入力します。
4. [終了] をクリックします。
   コンプライアンス テンプレートが作成され、コンプライアンス テンプレートのリストに表示されます。

関連タスク

コンプライアンス テンプレートの管理 、p. 106
コンプライアンス テンプレートのクローン作成 、p. 107

リファレンス デバイスからのコンプライアンス テンプレートの作成

設定ベースラインを作成するためのテンプレートとしてデバイスの設定プロパティを使用するには、デバイスがすでに登録されている必要があります。「デバイスのオンボーディング 、p. 43」を参照してください。

1. [[設定]] > [[設定コンプライアンス]] > [[テンプレート管理]] > [[作成]] > [[リファレンス デバイスから]] の順にクリックします。
2. [[コンプライアンス テンプレートの作成]] ダイアログボックスに、コンプライアンス テンプレートの名前と説明を入力します。
3. サーバーまたはシャーシのいずれかのプロパティをクローンすることによってコンプライアンス テンプレートを作成するオプションを選択します。
4. [[次へ]] をクリックします。
5. [[リファレンス デバイス]] セクションで、コンプライアンス テンプレートを作成するために「リファレンス」として使用する必要があるデバイスを選択します。「ターゲットデバイスおよびデバイス グループの選択 、p. 130」を参照してください。
   a. リファレンスとしてサーバーを選択した場合は、クローニングする必要のあるサーバー構成のプロパティを選択します。
6. [[終了]] をクリックします。
   テンプレート作成ジョブが作成され、実行されます。新しく作成されたコンプライアンス テンプレートは、[[コンプライアンス テンプレート]] ページにリストされています。

ファイルからのインポートによるコンプライアンス テンプレートの作成

1. [設定] > [設定コンプライアンス] > [テンプレートの管理] > [作成] > [ファイルからインポート] の順にクリックします。
2. [コンプライアンス テンプレートのインポート] ダイアログ ボックスに、コンプライアンス テンプレートの名前を入力します。
3. サーバまたはシャーシテンプレートタイプのいずれかを選択し、[ファイルを選択] をクリックしてファイルをブラウズして選択します。
4. **終了**をクリックします。
   コンプライアンス テンプレートが作成され、リストされます。

コンプライアンス テンプレートのクローン作成

1. [設定] > [設定コンプライアンス] > [テンプレートの管理] の順にクリックします。
2. クローンを作成するコンプライアンステンプレートを選択してから [クローン] をクリックします。
3. [クローン テンプレート] ダイアログボックスに、新しいコンプライアンス テンプレートの名前を入力します。
4. [終了] をクリックします。
   新しいコンプライアンス テンプレートが作成され、[コンプライアンス テンプレート] の下にリストされます。

関連情報

導入テンプレートからのコンプライアンス テンプレートの作成 、p. 106
コンプライアンス テンプレートの編集 、p. 108

コンプライアンス テンプレートの編集

コンプライアンス テンプレートは、[設定コンプライアンス] > [コンプライアンス テンプレート] ページで編集することができます。テンプレート属性を編集、選択、または選択解除しても、テンプレートに格納されている属性は変更されず、エクスポートされた場合でも、すべての属性はテンプレートの一部になります。これは、導入される内容に影響します。

メモ:

- その他のベースラインとすでに関連づけられているコンプライアンス テンプレートを編集すると、そのテンプレートを使用するすべてのベースラインのすべてのデバイスに対して、自動的に設定コンプライアンスがトリガーされます。
- 多数のデバイスを持つ複数のベースラインにリンクされているコンプライアンス テンプレートを編集すると、関連付けられているすべてのデバイスに対する設定コンプライアンス チェックに数分かかる場合があるため、セッション タイムアウトが発生する可能性があります。セッション タイムアウトは、コンプライアンス テンプレートに加えられた変更に問題があることを示すものではありません。
- 1,000 台で構成される大規模システムのコンプライアンス テンプレート、または最大 6,000 台の管理対象デバイスの設定インベントリーを編集する場合は、その他の設定インベントリーまたはコンプライアンス操作が同時に実行されていないことを確認します。さらに [監視] > [ジョブ] ページで、デフォルトでシステムに生成された設定インベントリー ジョブを**無効**にします (ソースをシステム生成に設定)。
- 最適なパフォーマンスを実現するには、ベースラインごとに最大 1,500 のデバイスを関連づけることをお勧めします。
- テンプレートの編集を頻繁に行うユース ケースでは、最適なパフォーマンスを実現するために、ベースラインごとに最大 100 のデバイスを関連付けることをお勧めします。

1. [コンプライアンステンプレート] ページで、対応するチェック ボックスを選択し、[編集] をクリックします。
2. [テンプレートの詳細] ページに、コンプライアンス テンプレートの設定プロパティがリストされます。
3. 編集するプロパティを展開し、フィールドにデータを入力するか、選択します。
   a. 無効になっているプロパティを有効にするには、チェック ボックスを選択します。
4. [保存] または [破棄] をクリックして、変更を適用または拒否します。
   コンプライアンス テンプレートが編集され、更新情報が保存されます。

関連タスク

コンプライアンス テンプレートの管理 、p. 106
コンプライアンス テンプレートのクローン作成 、p. 107

設定コンプライアンスベースラインの作成

設定コンプライアンス ベースラインは、コンプライアンス テンプレートに関連付けられているデバイスのリストです。OpenManage Enterprise のデバイスは、10 のベースラインに割り当てることができます。一度に最大 250 台のデバイスのコンプライアンスを確認することができます。。

ベースラインのリストを表示するには、[OpenManage Enterprise] > [設定] > [設定コンプライアンス] の順にクリックします。

使用できるコンプライアンス ベースラインのリストは、OpenManage Enteprise でのロール ベースと範囲ベースのアクセス権限によって異なります。たとえば、管理者はすべてのコンプライアンス ベースラインを表示して管理できますが、デバイス マネージャーは、そのデバイス マネージャーによって作成および所有されたコンプライアンス ベースラインの表示と管理のみを行うことができます。また、デバイス マネージャーで使用可能なターゲット デバイスは、それぞれのスコープ内にあるデバイス/デバイス グループによって制限されます。

コンプライアンスのベースラインは、次の方法によって作成できます。

- 既存の展開テンプレートを使用する。デバイス設定コンプライアンスの管理 、p. 105 を参照してください。
- サポートデバイスから取得されたテンプレートを使用する。リファレンス デバイスからのコンプライアンス テンプレートの作成 、p. 107 を参照してください。
- ファイルからインポートされたテンプレートを使用する。ファイルからのインポートによるコンプライアンス テンプレートの作成 、p. 107 を参照してください。

ベースラインの作成用のテンプレートを選択した場合は、テンプレートに関連付けられた属性も選択されます。ただし、ベースラインのプロパティは編集できます。設定コンプライアンスベースラインの編集 、p. 109 を参照してください。

注意: ベースラインに使用されているコンプライアンス テンプレートに別のベースラインが関連付けられている場合は、テンプレートのプロパティを編集することにより、既に関連付けられているデバイスのベースライン コンプライアンス レベルを変更できます。表示されたエラーおよびイベントメッセージを読み、適切に対応します。エラーおよびイベント メッセージの

詳細については、サポート サイトから入手できる『*エラーおよびイベント メッセージ リファレンス ガイド*』を参照してください。

メモ: 設定コンプライアンスベースラインを作成する前に、適切なコンプライアンステンプレートを作成したことを確認します。

1. [設定] > [設定コンプライアンス] > [ベースラインの作成] の順に選択します。
2. [コンプラインベースラインの作成] ダイアログボックスで、次の手順を実行します。
   - [ベースライン情報] セクションで、次のように実行します。
   a. [テンプレート] ドロップダウンメニューから、コンプライアンステンプレートを選択します。テンプレートの詳細については、「デバイス設定コンプライアンスの管理 、p. 105」を参照してください。
   b. コンプライアンスのベースラインの名前と説明を入力します。
   c. [次へ] をクリックします。
   - [ターゲット] セクションで次のように実行します。
   a. デバイスまたはデバイスグループを選択します。互換性があるデバイスのみが表示されます。ターゲットデバイスおよびデバイス グループの選択 、p. 130 を参照してください。

     メモ: 互換性があるデバイスのみがリストされます。グループを選択する場合は、コンプライアンス テンプレートと互換性がないデバイスまたは設定コンプライアンスのベースライン機能をサポートしないデバイスは識別されて除外され、効果的に選択できます。

3. [終了] をクリックします。
   コンプライアンスのベースラインが作成され、リストされます。コンプライアンスの比較は、ベースラインが作成または更新されると開始されます。[コンプライアンス] 列には、ベースラインの全体的なコンプライアンスレベルが示されます。リスト内のフィールドの詳細については、「デバイス設定コンプライアンスの管理 、p. 105」を参照してください。

   メモ: 設定ベースラインが作成されるたびに、アプライアンスによって設定インベントリー ジョブが自動的に作成され、実行されて、インベントリー データを利用できないベースラインに関連付けられているデバイスのインベントリーが収集されます。この新規作成された設定インベントリー ジョブの名前は、インベントリーが収集されるベースラインと同じです。また、[設定コンプライアンス] ページでは、インベントリー ジョブの進行状況を示す [プログレス] バーが、それぞれのベースラインの横に表示されます。

関連情報

デバイス設定コンプライアンスの管理 、p. 105
設定コンプライアンスベースラインの削除 、p. 111

設定コンプライアンスベースラインの編集

設定ベースラインに関連付けられているデバイス、名前、およびその他のプロパティを編集できます。リストに表示されるフィールドの説明については、デバイス設定コンプライアンスの管理 、p. 105 を参照してください。

注意: ベースラインに使用されているコンプライアンス テンプレートに別のベースラインが関連付けられている場合は、テンプレートのプロパティを編集することにより、既に関連付けられているデバイスのベースライン コンプライアンス レベルを変更できます。コンプライアンス テンプレートの編集 、p. 108 を参照してください。表示されたエラーおよびイベントメッセージを読み、適切に対応します。エラーおよびイベント メッセージの詳細については、サポート サイトから入手できる『*エラーおよびイベント メッセージ リファレンス ガイド*』を参照してください。

1. [設定] > [設定コンプライアンス] を選択します。
2. 設定コンプライアンスベースラインのリストで、対応するチェック ボックスを選択し、[編集] をクリックします。
3. [コンプライアンスベースラインの編集] ダイアログボックスで、情報を更新します。設定コンプライアンスベースラインの作成 、p. 108 を参照してください。

   メモ: 設定ベースラインが編集されるたびに、設定インベントリー ジョブが自動的にトリガーされ、インベントリー データを利用できないベースラインに関連付けられているデバイスのインベントリーが収集されます。この新規作成された設定インベントリー ジョブの名前は、インベントリーが収集されるベースラインと同じです。また、[設定コンプライアンス] ページでは、インベントリー ジョブの進行状況を示す [プログレス] バーが、それぞれのベースラインの横に表示されます。

関連タスク

コンプライアンス テンプレートの管理 、p. 106
クエリ条件の選択 、p. 55

関連情報

デバイス設定コンプライアンスの管理 、p. 105
設定コンプライアンスベースラインの削除 、p. 111

設定コンプライアンス ベースラインの削除

[設定] > [設定コンプライアンス] ページで設定コンプライアンス ベースラインを削除し、関連づけられているベースラインのデバイスとの関連づけを解除することができます。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。参照先 OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15

設定コンプライアンス ベースラインを削除するには、次のようにします。

1. [設定コンプライアンス] ページにリストされているベースラインからベースラインを選択します。
2. [削除] をクリックして、確認プロンプトで [はい] をクリックします。

削除された設定ベースラインは、[設定コンプライアンス] ページから削除されます。

設定コンプライアンス ベースラインのコンプライアンスの更新

ベースライン参照テンプレートの属性に変更が加えられた場合、またはベースラインに関連付けられているデバイスの設定インベントリーに変更がある場合、コンプライアンス ベースラインのコンプライアンス ステータスのチェックが自動的にトリガーされます。

設定コンプライアンス ベースラインのコンプライアンス ステータスは、その設定コンプライアンス ベースラインに接続されているデバイスのコンプライアンス レベルをロールアップしたものです。最もコンプライアンスが低い (重要) デバイスのステータスが全体のベースラインのステータスとして示されます。

すべての設定ベースラインの全体的なコンプライアンスの概要は、ベースライン グリッドの上にあるドーナツ グラフに表示されます。コンプライアンスの最終実行日時がチャートの下に表示されます。

大規模なベースラインのコンプライアンス ステータスの確認には数分かかる場合がありますが、[コンプライアンスの更新] をクリックすると、大規模なベースライン コンプライアンスのジョブが実行されている間に、必要に応じてデバイスの全体的なコンプライアンスの概要を取得できます。

メモ: 設定コンプライアンスが「実行中」ステータスの場合、コンプライアンス テンプレートやベースラインの編集など、ベースラインに影響する新しいジョブを開始することはできません。

すべてのベースラインのコンプライアンス概要全体の更新を開始するには、次の手順を実行します。

1. [設定] > [設定コンプライアンス] をクリックすると、[設定コンプライアンス] ページが表示されます。
2. [コンプライアンスの更新] をクリックします。

コンプライアンス更新ジョブ (コンプライアンス概要の読み込み) が開始され、その時点でのコンプライアンス全体の概要が表示され、コンプライアンスの最終実行時間が更新されます。

非対応デバイスの修正

ベースラインの [コンプライアンス レポート] ページでは、関連づけられているベースラインに一致するように属性値を変更することによって、関連するベースラインと一致しないデバイスを修正することができます。

[コンプライアンス レポート] ページには、コンプライアンス テンプレートのベースラインに関連付けられているターゲット デバイスの次のフィールドが表示されます。

- **コンプライアンス**：最もコンプライアンスが低い (例：重要) デバイスのステータスがデバイスのステータスとして示されます。

- **デバイス名**：ベースラインに関連付けられているターゲット デバイスの名前です。
- **IP アドレス**：ターゲット デバイスの IP アドレスを表示します。
- **タイプ**：関連付けられているターゲット デバイスのタイプです。
- **モデル**：ターゲット デバイスのモデル名です。
- **サービス タグ**：ターゲット デバイスのサービス タグです。
- [**最終実行時間**]：コンプライアンス ベースラインが実行された最新の日付と時刻。

[詳細フィルター] を使用して、非準拠デバイスを迅速に表示することができます。また、[すべて選択] および並び替えのサポートは、設定コンプライアンスの結果で使用できます。フィルターを取り消す場合は、[フィルターのクリア] をクリックします。

非準拠ターゲット デバイスのドリフトした属性を表示するには、デバイスを選択し、[レポートの表示] をクリックします。それぞれのターゲット デバイスの [コンプライアンス レポート] には、属性名、その属性の予想される属性値、および現在の属性値が表示されます。

1 つまたは複数の非対応デバイスを修正するには、次の手順を実行します。

1. [設定] > [設定コンプライアンス] を選択します。
2. 設定コンプライアンスベースラインのリストから対応するチェック ボックスを選択し、[レポートの表示] をクリックします。
3. 非対応デバイスのリストから、1 つまたは複数のデバイスを選択して [遵守させる] をクリックします。
4. 設定の変更をすぐに実行するようにスケジュールして、[完了] をクリックします。
   次のサーバの再起動後に設定の変更を適用するには [次の再起動時にデバイスへの設定の変更をステージングする] オプションを選択できます。

新しい設定インベントリタスクが実行され、ベースラインのコンプライアンスステータスが [コンプライアンス] ページでアップデートされます。

コンプライアンス ベースライン レポートのエクスポート

コンプライアンス テンプレート ベースラインに関連付けられているデバイスの完全または一部のリストを CSV ファイルにエクスポートすることができます。

設定ベースラインの [コンプライアンス レポート] ページで、次を実行します。

1. [すべてエクスポート] をクリックして、コンプライアンス ベースライン内のすべてのデバイスの詳細をエクスポートします。
   または、
2. レポートから個々のデバイスを選択した後、[選択した項目をエクスポート] をクリックします。

設定コンプライアンスベースラインの削除

設定ベースラインに関連付けられたデバイスの設定コンプライアンスレベルを削除できます。リストに表示されるフィールドの説明については、デバイス設定コンプライアンスの管理 、p. 105 を参照してください。

注意: コンプライアンスベースラインを削除したり、コンプライアンスベースラインからのデバイスの削除する場合：

- **ベースラインおよび / またはデバイスのコンプライアンスデータは、OpenManage Enterprise データから削除されます。**
- **デバイスが削除されると、その設定インベントリは取得されず、インベントリがインベントリジョブに関連付けられていない限り、既に取得された情報も削除されます。**

デバイスに関連付けられている場合は、コンプライアンス ベースラインとして使用されるコンプライアンス テンプレートは削除することができません。そのような場合は、適切なメッセージが表示されます。表示されるエラーおよびイベントメッセージを確認し、適切に対応します。エラーおよびイベント メッセージの詳細については、サポート サイトから入手できる『*エラーおよびイベント メッセージ リファレンス ガイド*』を参照してください。

1. [設定] > [設定コンプライアンス] の順にクリックします。
2. 設定コンプライアンスベースラインのリストで、対応するチェックボックスを選択し、[削除] をクリックします。
3. 削除するかどうかを確認するプロンプトが表示されたら、[はい] をクリックします。
   コンプライアンスベースラインが削除され、ベースラインの [全体的なコンプライアンスのサマリ] 表が更新されます。

関連タスク

設定コンプライアンスベースラインの作成 、p. 108
クエリ条件の選択 、p. 55
コンプライアンス テンプレートの管理 、p. 106

設定コンプライアンスベースラインの編集 、p. 109

関連情報

デバイス設定コンプライアンスの管理 、p. 105

14

デバイス アラートのモニターと管理

[OpenManage Enterprise] > [アラート] の順に選択すると、管理システム環境でデバイスによって生成されたアラートを表示し、管理することができます。[アラート] ページに次のタブが表示されます。

- [アラート ログ]: ターゲット デバイス上で生成されたすべてのアラートを表示し、管理することができます。
- [アラート ポリシー]: E メール、モバイル、syslog サーバーなどの宛先にターゲット デバイスで生成されたアラートを送信するためのアラート ポリシーを作成することができます。
- [アラート定義]: エラーまたは情報目的で生成されたアラートを表示することができます。

メモ:

- OpenManage Enterprise でデバイス アラートを管理および監視するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- アラート ポリシーとアラート ログは、OpenManage Enterprise で設定された範囲ベースのアクセス権によって管理されます。たとえば、管理者はすべてのアラート ポリシーを表示して管理できますが、デバイス マネージャーは、デフォルトのアラート ポリシーと作成および所有するポリシーのみを表示および管理できます。また、デバイス マネージャーは、そのスコープ内にあるデバイスのアラートのみを表示することができます。
- OpenManage Enterprise が受信する SNMPv1 および SNMPv2 アラートの送信元となる PowerEdge サーバーは、現時点では MX840c と MX5016s のみです。
- OpenManage Enterprise にはビルトインレポートが備わっており、OpenManage Enterprise の監視対象デバイスのリスト、および各デバイスに対して生成されたアラートが表示されます。[OpenManage Enterprise] > [監視] > [レポート] > [デバイスレポートあたりのアラート数] の順にクリックします。**実行** をクリックします。参照先： レポートの実行 、p. 135

関連概念

アラート ログの表示 、p. 113

トピック：

アラート ログの表示

[**アラート ログ**] ページには、デバイスで発生しているイベントのアラート ログのリストが表示されます。OpenManage Enterprise で、[アラート] > [アラート ログ] をクリックします。**アラートログ** ページが表示されます。

デフォルトでは、未確認アラートのみが表示されます。アラート リストは、アラート リストの左上にある [詳細フィルター] を使用するか、[アプリケーション設定] ページで [アラート表示設定] を変更してカスタマイズできます。アラート表示のカスタマイズ 、p. 160 を参照してください。アラートの詳細を表示するには、次の手順を実行します。

- [確認]: アラートが確認された場合は、[確認] にチェックマークが表示されます。[確認] の下にある角かっこの間をクリックして、アラートを確認または未確認にします。
- [時刻]: アラートが生成された時刻。
- [ソース名]: アラートを生成したデバイスのオペレーティング システム ホスト名です。デバイスのプロパティを表示および設定するには、ソース名をクリックします。

  メモ: 未検出デバイスからアラートが生成された場合、または内部アラートが生成された場合は、IP アドレス (ソース名) に基づいてアラートをフィルタリングすることはできません。
- [カテゴリー]: カテゴリーはアラートのタイプを示します。たとえば、システムの正常性や監査などです。
- [メッセージ ID]: 生成されたアラートの ID。
- [メッセージ]: 生成されたアラート。

- 右側のボックスには、選択したアラートの詳細説明や推奨処置などの追加情報が表示されます

メモ: OpenManage Enterprise バージョン 3.2 以上では [**最終更新者**] に表示されたデータを追跡しますが、旧バージョンではこれは追跡されませんでした。このため、[ユーザー] 詳細フィルター フィールドを使用してアラート ログを絞り込むと、旧バージョンで確認したアラートは表示されないため、注意してください。

アラートを選択すると、[アラート ログ] ページの右側に詳細な説明や推奨処置などの追加情報が表示されます。アラートログ ページで、次のタスクも実行できます。

- アラートの確認
- アラートの確認の解除
- アラートの無視
- アラートのエクスポート
- アラートの削除
- アーカイブされたアラート

関連情報

デバイス アラートのモニターと管理 、p. 113

アラート ログの管理

アラート ログが生成され、[アラート ログ] ページに表示された後、それらのアラート ログを確認、確認解除、無視、エクスポート、削除、アーカイブを行うことができます。

アラートの確認

アラートを表示してその内容を理解したら、アラートメッセージに目を通したことを確認することができます。アラートを確認すると、システムに同じイベントを保存することができなくなります。たとえば、デバイスにノイズが多く、同じイベントを複数回生成している場合は、デバイスから受信したイベントを確認することで、アラートの記録を無視することができます。また、同じタイプのイベントはそれ以上記録されません。

アラートを確認するには、[アラート ログ] ページで、アラートに対応するチェック ボックスを選択して、[確認] をクリックします。

[確認] 列にチェック マークが表示されます。アラートを確認すると、[アラートの詳細] セクションの [最終更新者] フィールドに更新者のユーザー名が表示されます。

アラートの確認の解除

確認済みのアラートログを未確認にできます。アラートを未確認にすると、同じイベントが頻繁に繰り返される場合でも、すべてのデバイスからのすべてのイベントが記録されることを意味します。デフォルトでは、すべてのアラートが未確認にされます。

アラートの確認を解除するには、アラートに対応するチェック ボックスを選択して、[確認を解除] をクリックします。または、各アラートに対応するチェックマークをクリックしても、確認を解除することができます。

メモ: [アラートの詳細] セクションの [最終更新者] フィールドに、最後にアラートを確認したユーザーのユーザー名が保存されます。

アラートの無視

アラートを無視すると、有効にされているアラートのポリシーが作成され、そのアラートの以後の発生を破棄します。アラートに対応するチェック ボックスを選択して、[無視] をクリックします。選択したアラートを無視するためにジョブを作成中であるというメッセージが表示されます。OpenManage Enterprise のヘッダー列に表示されているアラートの合計数が減ります。

アラートのエクスポート

ネットワーク共有またはお使いのシステムのローカルドライブに、アラートログを .csv 形式でエクスポートできます。

アラート ログページで、エクスポートするアラート ログを選択し、[エクスポート] > [選択した項目のエクスポート] をクリックします。[エクスポート] > [すべてエクスポート] をクリックすると、すべてのアラート ログをエクスポートすることができます。アラートログは、.csv 形式でエクスポートされます。

アラートの削除

アラートを削除して、コンソールからそのアラートが永久に発生しないようにすることができます。

対象のアラートに対応するチェックボックスを選択し、[削除] をクリックします。削除プロセスの確認を求めるメッセージが表示されます。[はい] をクリックしてアラートを削除します。OpenManage Enterprise のヘッダー列に表示されているアラートの合計数が減ります。

アーカイブされたアラートの表示

OpenManage Enterprise 内では、最大 5 万のアラートを生成し、表示することができます。上限の 50,000 件の 95 % (47,500 件) に達すると、OpenManage Enterprise は内部メッセージを生成し、アラート数が 50,000 件に達すると OpenManage Enterprise はアーカイブされたアラートの 10 % (5,000 件) を自動的にパージすることを通知します。次の表では、アラートのパージに関連するさまざまなシナリオを示します。

表 20. アラートのパージ

ワークフロー	説明	結果
パージタスク	コンソールで 30 分ごとに実行されます。	アラートがその最大容量 (つまり、50,000)に達した場合、パージアーカイブにチェックを入れて生成します。
パージアラート警告	内部パージアラート警告を生成します。	アラートが 95% (つまり、475000 件) を超えた場合は、アラートの 10% をパージするために内部パージアラートを生成します。
パージアラート	アラートログからパージされたアラートです。	アラートの数が 100% を超えると、古いアラートの 10% がパージされて 90% (45,000 件) に戻ります。
パージアラートのダウンロード	パージされたアラートをダウンロードします。	パージされたアラートのうち最近の 5 件のアーカイブは、アーカイブアラートからダウンロードできます。

アーカイブされたアラートのダウンロード

アーカイブされたアラートは、アラートの数が 50,000 個を超えるとき、古い順にアラートの 10 % (5,000 個) がパージされたものです。これらの古い 5,000 個のアラートは表から削除され、.csv ファイルに保存されてアーカイブされます。アーカイブされたアラートファイルをダウンロードするには、次の手順を実行します。

1. [アーカイブされたアラート] をクリックします。

   [アーカイブされたアラート] ダイアログボックスに、最後にパージされた 5 回分のアーカイブ済みアラートが表示されます。ファイルサイズ、ファイル名、およびアーカイブされた日付が示されます。

2. 対象のアラートファイルに対応するチェック ボックスを選択し、[終了] をクリックします。.CSV ファイルが、選択した場所にダウンロードされます。

メモ: アーカイブされたアラートをダウンロードするには、必要な権限を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

アラートポリシー

このトピックでは、アラート ポリシーの概念とアラート ポリシーがどのように役に立つかについて説明します。アラート ポリシーの作成、編集、有効化、無効化、削除の手順については、[*アラート ポリシーの設定と管理*] を参照してください。

アラートポリシーを使用すると、特定のデバイスまたはコンポーネントの特定のアラートを設定して、E メール、モバイル、syslog サーバーなどの特定の宛先に送信できます。アラートは、デバイスを効果的にモニターおよび管理するために役立ちます。

アラート ポリシーを使用して、次の機能を実行します。

- アラートからの入力に基づいて自動的にアクションをトリガします。
- アラートを E メール アドレスに送信します。
- SMS または通知を介してアラートを電話に送信します。

- SNMP トラップを介してアラートを送信します。
- アラートを syslog サーバーに送信します。
- 事前定義されたカテゴリーのアラートが生成されたときに、デバイスの電源をオンまたはオフにするなどのデバイス電源制御アクションを実行します。
- リモート スクリプトを実行します。

アラート ポリシーの表示、作成、編集、有効化、無効化、削除を行うには、[アラート] > [アラート ポリシー] をクリックします。

関連タスク

アラート ポリシーの作成と管理 、p. 116

アラート ポリシーの作成と管理

このトピックでは、アラート ポリシーを作成、編集、有効化、無効化、削除する方法について説明します。

メモ:
- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

関連情報

アラートポリシー 、p. 115
監査ログのリモート Syslog サーバへの転送 、p. 117

アラート ポリシーの作成

アラート ポリシーを作成し有効化して、E メール アドレス、電話、SNMP トラップにアラートを送信し、事前定義されたカテゴリーのアラートが生成されたときのデバイスのオン/オフ、電源の入れ直し、正常なシャットダウンなどのデバイス制御アクションを実行できるようにすることができます。

メモ: バージョン 3.5 またはそれ以前のバージョンからのアップグレード後、以前の OpenManage Enterprise リリースのいずれかからデバイス マネージャーによって作成されたすべてのアラート ポリシーは、管理者のみに割り当てられます。したがって、アラートを引き続き受信するには、デバイス マネージャーはアップグレード後にアラート ポリシーを再作成する必要があります。

[アラート] > [アラート ポリシー] ページで、[作成] をクリックして、次の操作を実行します。

1. アラート ポリシーの名前と説明を入力して、[次へ] をクリックします。[ポリシーの有効化] チェック ボックスは、デフォルトでオンになっています。
2. 組み込みおよびインポートされたサード パーティー製管理情報ベース (MIB) カテゴリーを選択して、アラート カテゴリーを選択します。
   各カテゴリーを展開して、サブカテゴリーを表示して選択することができます。カテゴリーとサブカテゴリーの詳細については、アラートの定義 、p. 120 を参照してください。
3. アラートが必要なデバイスまたはグループを選択し、[次へ] をクリックします。アラートは次に対して適用できます。
   - 1 つまたは複数のデバイス
   - 1 つまたは複数のデバイス グループ
   - IP アドレスまたはホスト名を入力して指定された未検出のデバイス
   - 未検出のデバイス

     メモ: 未検出のデバイスでは、リモート スクリプトの実行および電源アクションのタスクを実行できません。

     メモ: このような未検出 (外部) デバイスによって送信された SNMPv1、SNMPv2、SNMPv3 プロトコルのアラートは、OpenManage Enterprise によって認識されます。
4. (オプション)[日付範囲]、[時間間隔]、[日数] に必要な値を選択し、[次へ] をクリックして、アラート ポリシーが適用される期間を指定します。
5. アラートの重大度を選択し、[次へ] をクリックします。
   すべての重要度カテゴリを選択する場合は、[すべて] チェックボックスを選択します。

6. 1 つまたは複数のアラート アクションを選択し、[次へ] をクリックします。使用可能なオプションは次のとおりです。
   - E メール - 各フィールドの情報を指定し、件名とメッセージに必要な場合はトークンを使用して、E メールを指定した受信者に送信します。参照先： リモート スクリプトおよびアラート ポリシーでのトークン代用 、p. 176

     メモ: 同じカテゴリー、メッセージ ID、およびコンテンツの複数のアラートに対する E メールは、受信トレイでの繰り返しまたは冗長なアラート メッセージを回避するため、2 分ごとに 1 回のみトリガーされます。
   - SNMP トラップ転送 (有効) —有効 をクリックして、SNMP 設定 ウィンドウを表示し、アラートの SNMP 設定を行うことができます。SMTP、SNMP、Syslog アラートの設定 、p. 118 を参照してください。
   - Syslog (有効) — [有効] をクリックして、[Syslog 設定] ウィンドウを表示し、アラートのシステム ログ設定を行うことができます。SMTP、SNMP、Syslog アラートの設定 、p. 118 を参照してください。
   - アラートメッセージを無視する場合は 無視する チェックボックスを選択し、アラートポリシーをアクティブにしません。
   - 指定された電話番号に SMS を送信します。
   - 電源制御 - デバイスの電源のオン、オフ、電源の入れ直し、または正常なシャットダウンを行うことができる処置を表示するには、[電源制御] チェック ボックスを選択します。電源制御処置を実行する前にオペレーティング システムをシャットダウンするには、[最初にオペレーティング システムをシャットダウンする] チェック ボックスを選択します。
   - リモート スクリプトの実行 (有効化) - [有効化] をクリックすると、リモート ノードでリモート コマンドを追加して実行できる [リモート コマンド設定] ウィンドウが表示されます。リモート コマンドの追加に関する詳細については、リモートコマンドとスクリプトの実行 、p. 119 を参照してください。

     ドロップダウン メニューから、このアラート ポリシーの実行時に実行するスクリプトを選択します。リモート コマンドを実行してセットアップすることもできます。これについては、OpenManage Enterprise アプライアンス設定の管理 、p. 142 で説明されています。
   - OpenManage Enterprise に登録されている携帯電話に通知を送信します。OpenManage Mobile の設定 、p. 169 を参照してください。
7. [概要] タブで作成されたアラート ポリシーの詳細を確認し、[終了] をクリックします。
   アラートポリシーが正常に作成され、[アラートポリシー] セクションに一覧表示されます。

アラート ポリシーの管理

[アラート ポリシー] ページでアラート ポリシーが作成された後、それらを編集、有効化、無効化、削除することができます。さらに、OME は、アラートを受信したときに関連するアクションをトリガーする組み込みのアラート ポリシーを提供します。組み込みのアラート ポリシーを編集または削除することはできませんが、有効または無効にすることはできます。

作成されたアラート ポリシーを表示するには、[アラート] > [アラート ポリシー] をクリックします。

すべてのアラート ポリシーを選択するには、[有効] の左側にあるチェック ボックスを選択します。アラート ポリシーの横にある 1 つ以上のチェック ボックスを選択して、次のアクションを実行します。

- **アラート ポリシーの編集**：アラート ポリシーを選択し、[編集] をクリックしてアラート ポリシーの作成と管理 、p. 116 ダイアログ ボックスで必要な情報を編集します。

  メモ: 一度に編集できるアラート ポリシーは 1 つだけです。

  メモ: バージョン 3.3.1 より前の OpenManage Enterprise バージョンのアラート ポリシーでは、[時間間隔] チェック ボックスがデフォルトで無効になっています。アップグレード後に、[時間間隔] を有効化してフィールドを更新し、ポリシーを再アクティブ化します。
- **アラート ポリシーの有効化**：アラート ポリシーを選択し、[有効] をクリックします。アラート ポリシーが有効になっている場合、[有効] 列の下にチェックマークが表示されます。すでに有効化されているアラートポリシーは、[有効にする] ボタンがグレー表示されています。
- **アラート ポリシーの無効化**：アラート ポリシーを選択し、[無効] をクリックします。アラート ポリシーが無効になり、[有効] 列のチェックマークが削除されます。

  アラート ポリシーの作成中に [名前と説明] セクションの [ポリシーの有効化] チェック ボックスをクリアすると、アラートポリシーが無効になります。
- **アラート ポリシーの削除**：アラート ポリシーを選択し、[削除] をクリックします。

  対応するチェックボックスをそれぞれ選択することで、一度に複数のアラートポリシーを削除できます。すべてのチェックボックスを選択またはクリアする場合は、[有効] の横にあるヘッダー列のチェックボックスを選択します。

監査ログのリモート Syslog サーバへの転送

OpenManage Enterprise のすべての監査ログを Syslog サーバから監視するには、アラートポリシーを作成します。ユーザーログインの試行、アラートポリシーの作成、さまざまなジョブの実行などの監査ログは、すべて Syslog サーバに転送できます。

監査ログを Syslog サーバに転送するアラートポリシーを作成するには、次の手順を実行します。

1. [アラート] > [アラートポリシー] > [作成] の順に選択します。
2. [アラートポリシーの作成] ダイアログボックスの [名前と説明] セクションに、アラートポリシーの名前と説明を入力します。
   a. デフォルトでは [ポリシーの有効化] チェックボックスが選択されており、これは作成したアラートポリシーが有効になることを意味します。アラートポリシーを無効にするには、チェックボックスをクリアします。後でアラートポリシーを有効にする場合の詳細については「アラート ポリシーの作成と管理 、p. 116」を参照してください。
   b. [次へ] をクリックします。
3. [カテゴリ] セクションで、[アプリケーション] を展開し、アプライアンスログのカテゴリとサブカテゴリを選択します。[次へ] をクリックします。
4. [ターゲット] セクションでは、[デバイスの選択] オプションがデフォルトで選択されています。[デバイスの選択] をクリックし、左側のペインでデバイスを選択します。[次へ] をクリックします。

   メモ: ターゲットデバイスやグループの選択は、監査ログの Syslog サーバへの転送には適用されません。

5. (オプション) デフォルトでは、アラートポリシーは常にアクティブです。アクティビティに期限をつけるには、[日付と時刻] セクションで、開始日と終了日を選択してタイムフレームを選択します。
   a. アラートポリシーを実行する必要がある日付に対応するチェックボックスを選択します。
   b. [次へ] をクリックします。
6. [重大度] セクションでは、このポリシーをアクティブにする必要のあるアラートの重要度レベルを選択します。
   a. すべての重要度カテゴリを選択する場合は、[すべて] チェックボックスを選択します。
   b. [次へ] をクリックします。
7. [アクション] セクションで、[Syslog] を選択します。
   Syslog サーバが OpenManage Enterprise で設定されていない場合は、[有効化] をクリックし、宛先 IP アドレスまたは Syslog サーバのホスト名を入力します。Syslog サーバの設定の詳細に関しては、「SMTP、SNMP、Syslog アラートの設定 、p. 118」を参照してください。
8. [次へ] をクリックします。
9. [概要] セクションに、定義したアラートポリシーの詳細が表示されます。注意深く情報に目を通してください。
10. [終了] をクリックします。

アラートポリシーが正常に作成され、[アラートポリシー] セクションに一覧表示されます。

関連タスク

アラート ポリシーの作成と管理 、p. 116
監査ログのモニター 、p. 122

SMTP、SNMP、Syslog アラートの設定

[OpenManage Enterprise] > [アプリケーションの設定] > [アラート] の順にクリックすると、システム アラートを受信する E メール (SMTP) アドレス、SNMP アラートの転送先、Syslog の転送プロパティを設定できます。これらの設定を管理するには、OpenManage Enterprise 管理者レベルの資格情報が必要です。

ユーザーおよび OpenManage Enterprise 間の E メールの通信を管理する SMTP サーバーを設定し認証するには、次の手順を実行します。

メモ: OpenManage Enterprise は、内部ルート CA によって発行された証明書を持つ内部 SMTP サーバーに E メールを送信することはできません。

1. [電子メールの設定] を展開します。
2. 電子メールメッセージを送信する SMTP サーバのネットワークアドレスを入力します。
3. SMTP サーバーを認証するには、[認証を有効にする] チェック ボックスをオンにし、ユーザー名とパスワードを入力します。
4. デフォルトでは、アクセスする SMTP ポート番号は 25 です。必要に応じて編集します。
5. SMTP トランザクションを固定するには、[SSL を使用する] チェックボックスを選択します。
6. SMTP サーバーが正常に動作しているかどうかをテストするには、[テスト E メールの送信] チェック ボックスをクリックして、[E メール受信者] を入力します。
7. [適用] をクリックします。
8. 設定をデフォルトの属性にリセットするには、[破棄] をクリックします。

SNMP アラートの転送を設定するには、次の手順を実行します。

1. [SNMP アラート転送設定] を展開します。

2. 事前定義されたイベント発生時にアラートを送信する各 SNMP トラップを有効にするには、[有効] チェックボックスを選択します。
3. [送信先アドレス] ボックスに、アラートを受信すべき宛先デバイスの IP アドレスを入力します。

   メモ: コンソール IP の入力は、アラートの重複を回避するために許可されません。
4. [SNMP バージョン] メニューから、SNMP バージョン タイプを SNMPv1、SNMPv2、または SNMPv3 として選択し、次のフィールドに入力します。
   a. コミュニティ文字列 ボックスに、アラートを受信すべき宛先デバイスの SNMP コミュニティ文字列を入力します。
   b. 必要に応じてポート番号を編集します。SNMP トラップのデフォルトのポート番号は 162 です。OpenManage Enterprise でサポートされるプロトコルおよびポート 、p. 31 を参照してください。
   c. SNMPv3 が選択されている場合は、次の追加の詳細を入力します。
      i. ユーザー名：ユーザー名を入力します。
      ii. 認証タイプ：ドロップダウン リストから [SHA]、[MD_5]、または [なし] を選択します。
      iii. 認証パスフレーズ：8 文字以上の認証パスフレーズを入力します。
      iv. プライバシー タイプ：ドロップダウン リストから [DES]、[AES_128]、または [なし] を選択します。
      v. プライバシー パスフレーズ：8 文字以上のプライバシー パスフレーズを入力します。
5. SNMP メッセージをテストするには、対応するトラップの [送信] ボタンをクリックします。
6. [適用] をクリックします。設定をデフォルトの属性にリセットするには、[破棄] をクリックします。

Syslog 転送設定をアップデートするには、次の手順を実行します。

1. [Syslog 転送設定] を展開します。
2. [サーバー] 列の各サーバーのチェックボックスを選択して、Syslog 機能を有効化します。
3. [送信先アドレス/ホスト名] ボックスに、Syslog メッセージを受信するデバイスの IP アドレスを入力します。
4. UDP を使用するデフォルトのポート番号は 514 です。必要に応じてボックスから選択するか入力して編集します。OpenManage Enterprise でサポートされるプロトコルおよびポート 、p. 31 を参照してください。
5. [適用] をクリックします。
6. 設定をデフォルトの属性にリセットするには、[破棄] をクリックします。

リモートコマンドとスクリプトの実行

SNMP トラップを取得すると、OpenManage Enterprise でスクリプトを実行できます。これにより、アラート管理用にサード パーティーのチケット システムでチケットを開くポリシーが設定されます。最大 **4 つ**のリモート コマンドを作成して保存できます。

メモ: 次の特殊文字は、RACADM および IPMI の CLI パラメーターとしての使用はサポートされていません：**[**、**;**、**|**、**$**、**>**、**<**、**&**、**'**、**]**、**.**、*、**'**。

1. [アプリケーションの設定] > [スクリプトの実行] の順にクリックします。
2. [リモート コマンドの設定] セクションで、次の手順を実行します。
   a. リモート コマンドを追加するには [作成] をクリックします。
   b. [コマンド名] ボックスにコマンド名を入力します。
   c. 次のいずれかのコマンド タイプを選択します。
      i. スクリプト
      ii. RACADM
      iii. IPMI ツール
   d. [スクリプト] を選択した場合は、次の手順を実行します。
      i. [IP アドレス] ボックスに IP アドレスを入力します。
      ii. 認証方法として、[パスワード] または [SSH キー] を選択します。
      iii. [ユーザー名] および [パスワード] または [SSH キー] を入力します。
      iv. [コマンド] ボックスにコマンドを入力します。
         - コマンドは 100 個まで入力でき、それぞれ改行して入力します。
         - スクリプトではトークンの代用が可能です。参照先：リモート スクリプトおよびアラート ポリシーでのトークン代用 、p. 176
      v. [終了] をクリックします。
   e. [RACADM] を選択した場合は、次の手順を実行します。
      i. [コマンド名] ボックスにコマンド名を入力します。
      ii. [コマンド] ボックスにコマンドを入力します。コマンドは 100 個まで入力でき、それぞれ改行して入力します。
      iii. [終了] をクリックします。
   f. [IPMI ツール] を選択した場合は、次の手順を実行します。

i. [コマンド名] ボックスにコマンド名を入力します。
ii. [コマンド] ボックスにコマンドを入力します。コマンドは 100 個まで入力でき、それぞれ改行して入力します。
iii. [終了] をクリックします。

3. リモート コマンドの設定を編集するには、コマンドを選択して [編集] をクリックします。
4. リモート コマンドの設定を削除するには、コマンドを選択して [削除] をクリックします。

MX7000 シャーシの挿入と取り外しでのスレッドの自動更新

OpenManage Enterprise では、スタンドアロンまたはリード MX7000 シャーシが検出されたりオンボードされたりした後のスレッドの追加や削除をほぼ瞬時に反映できます。

OpenManage Enterprise (バージョン 3.4 以降) を使用してスタンドアロンまたはリード MX7000 シャーシを検出またはオンボードすると、MX7000 シャーシにアラート ポリシーが同時に作成されます。OpenManage Enterprise でのデバイスの検出およびオンボードの詳細については、「デバイス検出ジョブの作成 、p. 42」および「デバイスのオンボーディング 、p. 43」を参照してください。

MX7000 OpenManage Enterprise-Modular アプライアンスで自動生成されたアラート ポリシーにより、MX7000 シャーシ内のスレッドの挿入、取り外し、または交換のたびに、OpenManage Enterprise に「**シャーシ インベントリーの更新**」という名前のシャーシ インベントリー更新ジョブがトリガーされます。

シャーシ インベントリー更新ジョブの完了後、MX7000 に対するスレッド関連の変更が [すべてのデバイス] ページに表示されます。

自動アラートポリシーが正常に作成されるよう、MX7000 シャーシをオンボードする際には次の前提条件を満たす必要があります。

- MX7000 には、OpenManage Enterprise-Modular バージョン 1.2 がインストールされている必要があります。
- MX7000 シャーシをオンボードする際に、[検出された iDRAC サーバーと MX7000 シャーシからのトラップ受信を有効にする] オプションと、[アプリケーション設定からトラップの宛先のコミュニティー文字列を設定する] オプションを設定する必要があります。
- OpenManage Enterprise アプライアンスの IP が、新しくオンボード MX7000 で使用可能な 4 つのアラート送信先の 1 つとして正常に登録される必要があります。MX7000 のアラート送信先がオンボード時にすでにすべて構成されていると、自動アラートポリシーの作成が失敗します。

メモ:

- MX7000 のアラート ポリシーはスレッドのみに固有のものであり、IOM などシャーシの他のコンポーネントには適用されません。
- MX7000 のアラートのプリファレンスは、OpenManage Enterprise で、すべてのアラートを受信するか、MX7000 シャーシからのシャーシ カテゴリーのアラートのみを受信するように設定できます。詳細については、コンソールプリファレンスの管理 、p. 158 を参照してください。
- スレッドの実際の動作と OpenManage Enterprise でのシャーシ インベントリー更新のトリガーの間に若干遅延があることが予想されます。
- MX7000 シャーシが OpenManage Enterprise のデバイス インベントリーから削除されると、自動的に作成されたアラートポリシーが削除されます。
- [すべてのデバイス] ページに、正常にオンボードされた MX7000 シャーシの [**管理状態**] が表示されます。ここでは、アラート転送ポリシーが自動的に「アラートで管理」となります。オンボーディングの詳細については、次のセクションを参照： デバイスのオンボーディング 、p. 43

アラートの定義

[OpenManage Enterprise] > [アラート] > [アラート定義] をクリックすると、エラーまたは情報目的で生成されたアラートを表示できます。これらのメッセージは

- イベントおよびエラーメッセージとして呼び出されます。
- グラフィカルユーザーインタフェース (GUI) と、RACADM および WS-Man のコマンドラインインタフェース (CLI) に表示されます。
- 情報のみを目的としてログファイルに保存されます。
- 番号が付けられており、対応措置と予防措置を効率的に実装できるように明確に定義されています。

エラーおよびイベントメッセージには、次のものが含まれます。

- **メッセージ ID**：メッセージは、BIOS、電源 (PSU)、ストレージ (STR)、ログデータ (LOG)、およびシャーシ管理コントローラ (CMC) などのコンポーネントに基づいて分類されます。

- **メッセージ**：イベントの実際の原因。イベントは、情報のみを目的としてトリガされるか、またはタスクの実行でエラーが発生したときにトリガされます。
- **カテゴリ**：エラーメッセージが属しているクラス。カテゴリについては、サポートサイトで利用可能な『*Event and Error Message Reference Guide for Dell EMC PowerEdge Servers*』（Dell EMC PowerEdge サーバのイベントおよびエラーメッセージリファレンスガイド）を参照してください。
- **推奨処置**：GUI、RACADM、または WS-MAN コマンドを使用した、エラーの解決策。必要に応じて、サポートサイトまたは TechCenter のドキュメントで詳細を参照することをお勧めします。
- **詳細な説明**：不具合の簡単かつ迅速な解決策に関する詳細情報。

メッセージ ID、メッセージテキスト、カテゴリ、およびサブカテゴリなどのフィルタを使用して、アラートに関する詳細情報を表示できます。アラートの定義を表示するには、次の手順を実行します。

1. [OpenManage Enterprise] メニューの [アラート] の下で、[アラートの定義] をクリックします。

   [アラートの定義] の下に、標準のアラートメッセージのリストが表示されます。

2. エラーメッセージを素早く検索するには、[詳細フィルタ] をクリックします。

右ペインに、表で選択したメッセージ ID のエラーおよびイベントメッセージの情報が表示されます。

15

監査ログのモニター

[OpenManage Enterprise] > [監視] > [監査ログ] ページには、お客様や Dell EMC サポート チームのトラブルシューティングと分析に役立つログ データがリストされます。監査ログは、次のときに記録されます。

- グループが割り当てられた、またはアクセス許可が変更された。
- ユーザーの役割が変更された。
- OpenManage Enterprise によって監視されているデバイスで実行されたアクション。

監査ログファイルは CSV ファイルフォーマットにエクスポートできます。すべてまたは選択したデータのエクスポート 、p. 64 を参照してください。

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- 監査ログには、範囲ベースの制限は適用されません。

1. 監査ログを表示するには、[モニター] > [監査ログ] を選択します。
   ここで表示される監査ログは、アプライアンスを用いて実行されたタスクを OpenManage Enterprise が保存して表示するものです。たとえば、ユーザーログインの試行、アラートポリシーの作成、異なるジョブの実行などです。
2. 任意の行でデータを並べ替えるには、行タイトルをクリックします。
3. 監査ログに関する情報を素早く検索するには、[高度なフィルター] をクリックします。
   情報を素早く検索するためのフィルタとして機能する、次のフィールドが表示されます。
4. 次のフィールドで、データを入力または選択します。
   - [重要度]: ログデータの重要度レベルを選択します。使用可能なオプションは、情報、警告、および重要です。
     - 重要：異常なアクションが発生しました。早急な対応が必要です。
     - 警告：イベントは重要ですが、早急な対応は不要です。
     - 情報：アクションが正常に実行されました。
   - [開始時刻] と [終了時刻]: 指定された期間の監査ログを表示します。
   - [ユーザー]: 特定のユーザーからの監査ログを表示します (例：管理者、システム、デバイス マネージャー、ビューアー)。
   - [ソース アドレス]: 特定のシステムからの監査ログを表示します (例：ユーザーが OpenManage Enterprise にログインしているシステム)。
   - [カテゴリー]: 監査タイプまたは構成タイプの監査ログを表示します。
     - 監査：ユーザーが OpenManage Enterprise アプライアンスにログインまたはログアウトしたときに生成されます。
     - 設定：ターゲット デバイス上で何らかのアクションが実行されると生成されます。
   - [含まれる説明]: 検索するログデータに含まれるテキストまたはフレーズを入力します。選択したテキストが含まれるすべてのログが表示されます。たとえば、`warningSizeLimit` と入力すると、このテキストが含まれるすべてのログが表示されます。
   - [メッセージ ID]: メッセージ ID を入力します。検索条件が一致した場合は、メッセージ ID の一致する項目のみが表示されます。
5. フィルタを削除する場合は、[すべてのフィルタのクリア] をクリックします。
6. 単一の監査ログまたはすべての監査ログをエクスポートするには、それぞれ [エクスポート] > [選択した項目をエクスポート] または [エクスポート] > [すべての監査ログをエクスポート] の順に選択します。監査ログのエクスポートの詳細については、すべてまたは選択したデータのエクスポート 、p. 64 を参照してください。
7. 最新のコンソール ログをすべて取得し、ダウンロード可能なアーカイブを作成するには、[トラブルシューティング] > [コンソール ログ アーカイブの作成] をクリックします。
8. コンソール ログ アーカイブをダウンロードするには、[トラブルシューティング] > [アーカイブされたコンソール ログのダウンロード] をクリックします。

メモ:

- 現在、シャーシ ファームウェアのバージョン 5.1x 以前で検出される M1000e シャーシでは、ハードウェア ログのタイムスタンプ列にある日付が「JAN 12, 2013」と表示されます。ただし、FX2 シャーシおよび VRTX のすべてのシャーシバージョンでは、正確な日付が表示されます。
- 特に大量のログが収集されている場合、ファイルはすぐにはダウンロードできません。収集プロセスはバックグラウンドで実行され、動作が完了するとファイル保存プロンプトが表示されます。

関連情報

監査ログのリモート Syslog サーバへの転送 、p. 117

トピック：

- 監査ログのリモート Syslog サーバへの転送

監査ログのリモート Syslog サーバへの転送

OpenManage Enterprise のすべての監査ログを Syslog サーバから監視するには、アラートポリシーを作成します。ユーザーログインの試行、アラートポリシーの作成、さまざまなジョブの実行などの監査ログは、すべて Syslog サーバに転送できます。

監査ログを Syslog サーバに転送するアラートポリシーを作成するには、次の手順を実行します。

1. [アラート] > [アラートポリシー] > [作成] の順に選択します。
2. [アラートポリシーの作成] ダイアログボックスの [名前と説明] セクションに、アラートポリシーの名前と説明を入力します。
   a. デフォルトでは [ポリシーの有効化] チェックボックスが選択されており、これは作成したアラートポリシーが有効になることを意味します。アラートポリシーを無効にするには、チェックボックスをクリアします。後でアラートポリシーを有効にする場合の詳細については「アラート ポリシーの作成と管理 、p. 116」を参照してください。
   b. [次へ] をクリックします。
3. [カテゴリ] セクションで、[アプリケーション] を展開し、アプライアンスログのカテゴリとサブカテゴリを選択します。[次へ] をクリックします。
4. [ターゲット] セクションでは、[デバイスの選択] オプションがデフォルトで選択されています。[デバイスの選択] をクリックし、左側のペインでデバイスを選択します。[次へ] をクリックします。

   メモ: ターゲットデバイスやグループの選択は、監査ログの Syslog サーバへの転送には適用されません。

5. (オプション) デフォルトでは、アラートポリシーは常にアクティブです。アクティビティに期限をつけるには、[日付と時刻] セクションで、開始日と終了日を選択してタイムフレームを選択します。
   a. アラートポリシーを実行する必要がある日付に対応するチェックボックスを選択します。
   b. [次へ] をクリックします。
6. [重大度] セクションでは、このポリシーをアクティブにする必要のあるアラートの重要度レベルを選択します。
   a. すべての重要度カテゴリを選択する場合は、[すべて] チェックボックスを選択します。
   b. [次へ] をクリックします。
7. [アクション] セクションで、[Syslog] を選択します。
   Syslog サーバが OpenManage Enterprise で設定されていない場合は、[有効化] をクリックし、宛先 IP アドレスまたは Syslog サーバのホスト名を入力します。Syslog サーバの設定の詳細に関しては、「SMTP、SNMP、Syslog アラートの設定 、p. 118」を参照してください。
8. [次へ] をクリックします。
9. [概要] セクションに、定義したアラートポリシーの詳細が表示されます。注意深く情報に目を通してください。
10. [終了] をクリックします。

アラートポリシーが正常に作成され、[アラートポリシー] セクションに一覧表示されます。

関連タスク

アラート ポリシーの作成と管理 、p. 116
監査ログのモニター 、p. 122

16

デバイスコントロール用ジョブの使い方

ジョブは、1つまたは複数のデバイスでタスクを実行するための一連の手順です。ジョブには、デバイスの検出、ファームウェア アップデート、インベントリー更新、保証などが含まれます。デバイスおよびそのサブコンポーネントで開始されたジョブのステータスおよび詳細は、[ジョブ] ページに表示できます。OpenManage Enterprise には、設定されたスケジュールに基づいてアプライアンスによってトリガーされる多くの内部メンテナンス ジョブがあります。「デフォルト」ジョブとそのスケジュールの詳細については、OpenManage Enterprise のデフォルト ジョブおよびスケジュール 、p. 126 を参照してください。

前提条件：

点滅、電源制御、ファームウェア ベースラインの管理、設定コンプライアンス ベースラインの管理などの、デバイスの選択タスクが関係するジョブを作成して管理する場合、以下が当てはまります。

- 必要なユーザー権限を持っている必要があります。参照先： OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15
- 各ジョブ タイプは、以下を持つデバイスに限定されます。
  - アクセス権限。
  - 必要なアクションを実行する能力。

ジョブを作成および管理するには、[OpenManage Enterprise] > [モニター] > [ジョブ] を選択します。[ジョブ] ページでは、次のタスクを実行できます。

- 現在実行中のジョブ、失敗したジョブ、正常に完了したジョブを示すジョブのリストを表示します。
- デバイスの LED を点滅させるジョブ、デバイスの電源を制御するジョブ、およびデバイスでリモートコマンドを実行するジョブを作成します。デバイスの管理用リモートコマンドジョブの作成 、p. 129、「電源管理のためのジョブの作成」、および「デバイスの LED を点滅させるジョブの作成」を参照してください。デバイスの詳細ページのサーバ上で同様のアクションを実行できます。個々のデバイスの表示と設定 、p. 65 を参照してください。
- ジョブの実行、停止、有効化、無効化、削除など、ジョブを管理します。

ジョブに関する詳細情報を表示するには、ジョブに対応するチェックボックスを選択し、右ペインの [詳細の表示] をクリックします。「ジョブ情報の表示」を参照してください。

トピック：

ジョブ リストの表示

OpenManage Enterprise から [モニター] > [ジョブ] をクリックして、既存のジョブのリストを表示します。ジョブに関する情報が、次の列に表示されます。

- [ジョブのステータス]: ジョブの実行ステータスを示します。

  ジョブのステータスとジョブ タイプの説明 、p. 125 を参照してください。

- [状態]: ジョブの状態を示します。使用可能なオプションは、[有効] と [無効] です。
- [ジョブ名]: ジョブの名前です。
- [ジョブの種類]: ジョブの種類を示します。

  ジョブのステータスとジョブ タイプの説明 、p. 125 を参照してください。

- [説明]: ジョブの詳細な説明です。
- [最終実行]: ジョブの最後の実行期間です。

ジョブは、[詳細フィルター] セクションで値を入力または選択してフィルタリングすることもできます。アラートのフィルタリングには、次の追加情報を使用できます。

- [最終実行開始日]: ジョブの最終実行の開始日。
- [最終実行終了日]: ジョブの最終実行の終了日。
- [ソース]: 使用可能なオプションは、[すべて]、[ユーザー生成](デフォルト)、[システム] です。

ジョブについての詳細情報を表示するには、右ペインでジョブを選択し、[詳細の表示] をクリックします。個々のジョブ情報の表示 、p. 128 を参照してください。

OpenManage Enterprise は、スケジュールされたジョブのリストを表示するビルトインレポートを提供します。[OpenManage Enterprise] > [監視] > [レポート] > [スケジュールされたジョブレポート] をクリックしてください。**実行** をクリックします。レポートの実行 、p. 135 を参照してください。

メモ: [検出とインベントリのスケジュール] ページに、スケジュール済みジョブのステータスは [ステータス] 列に [待機] と示されています。ただし、[ジョブ] ページでは、[スケジュール済み] として同じステータスが示されます。

ジョブのステータスとジョブ タイプの説明

表 21. ジョブのステータスと説明

ジョブ状態	説明
スケジュール済み	ジョブは指定した日付または時刻に実行されるようにスケジュールされています。
キューに登録済み	実行を待機しているジョブです。
開始	
実行中	ジョブは [今すぐ実行] で実行を開始しています。
完了	ジョブが実行されました。
失敗	ジョブの実行は失敗しました。
新規	ジョブは作成されましたが、実行されていません。
エラーで終了	ジョブの実行は部分的に成功しましたが、エラーで終了しました。
中断	ジョブの実行がユーザーによって一時停止されました。
一時停止	ジョブの実行がユーザーによって停止されました。
停止	ジョブの実行がユーザーによって中断されました。
キャンセル	
未実行	ジョブが「キューに登録済み」か「スケジュール済み」で、まだ実行されていません。

ジョブは次のタイプのいずれかに属します。

表 22. ジョブのタイプと説明

ジョブタイプ	説明
正常性	デバイスの正常性状態を表示します。デバイスの正常性状態 、p. 38 を参照してください。
インベントリ	デバイスのインベントリ レポートを作成します。デバイスインベントリの管理 、p. 70 を参照してください。
デバイス設定	デバイス設定コンプライアンス ベースラインを作成します。デバイス設定コンプライアンスの管理 、p. 105 を参照してください。
レポート タスク	組み込みまたはカスタマイズ データ フィールドを使用してデバイスについてのレポートを作成します。レポート 、p. 134 を参照してください。
保証	デバイスの保証ステータスについてのデータを生成します。デバイス保証の管理 、p. 132 を参照してください。
オンボード タスク	検出デバイスをオンボードします。デバイスのオンボーディング 、p. 43 を参照してください。

表 22. ジョブのタイプと説明（続き）

ジョブタイプ	説明
検出	デバイスを検出します。監視または管理のためのデバイスの検出 、p. 39 を参照してください。
コンソールのアップデートの実行タスク	このタスクを使用してコンソール アップグレード ジョブがトラッキングされています。このタスクは、アップグレードが完了したか失敗したかを特定するのに役立ちます。
バックアップ	
シャーシ プロファイル	
デバッグログ	アプリケーション モニタリング タスク、イベント、およびタスク実行履歴のデバッグ ログを収集します。
デバイスアクション	LED のオン/オフ、IPMI CLI、RACADM CLI などのデバイスに対するアクションを作成します。
診断タスク	診断/TSR または Services（SupportAssist）タスクのダウンロード/実行は、診断タスクに関連しています。「診断レポートの実行とダウンロード」を参照してください。
VLAN 定義のインポート	Excel または MSM から VLAN 定義をインポートします。
OpenID Connect プロバイダー	OpenID 接続の設定です。「OpenID Connect プロバイダーを使用した OpenManage Enterprise ログイン」を参照してください。OpenID Connect プロバイダーを使用した OpenManage Enterprise ログイン 、p. 154
プラグインのダウンロード タスク	プラグインのダウンロード タスクがトラッキングされています。このタスクは、RPM プラグインのダウンロードが完了しており、インストールの準備ができているかを特定するのに役立ちます。「OpenManage Enterprise のバージョンと使用可能なプラグインの確認とアップデート」を参照してください。
アップグレード後タスク	アップグレード後タスクは、N-1 または N-2 バージョンで行われるアプライアンス設定を設定するためにトラッキングされます。また、以前のバージョンで作成された検出タスクも実行して、すべてのデバイスがリストされていることを確認します。
レポート タスク	ユーザーがレポートを実行したときにレポート タスクがトラッキングされます（既定の場合もカスタムの場合も同様）。
復元	
設定のアップデート	ユーザーが [アプリケーションの設定] タブの下に新しい設定を適用したときに「設定のアップデート」タスクがトラッキングされます。
ソフトウェアのロールバック	ロールバックは、ユーザーがターゲット デバイス上でロールバック操作を実行するときにトラッキングされるタスクです。
アップデート	ユーザーがターゲット デバイスでファームウェアまたはドライバーのアップデートを実行したときに、アップデート タスクがトラッキングされます。
アップグレード バンドルのダウンロード タスク	アップグレード バンドルのダウンロード タスクがトラッキングされています。このタスクは、OMEnterprise RPM のダウンロードが完了し、インストールの準備ができているかどうかを特定するのに役立ちます。

OpenManage Enterprise のデフォルト ジョブおよびスケジュール

OpenManage Enterprise には、設定されたスケジュールでアプライアンスによって自動的にトリガーされる多くの内部メンテナンス ジョブがあります。

表 23. 次の表に、OpenManage Enterprise のデフォルト ジョブ名とそのスケジュールのリストを示します。

ジョブ名	Cron 式	Cron 式の説明	例
設定インベントリ	0 0 0 1/1 * ? *	毎月 1 日から毎日、00:00:00am に	• Tue May 18 00:00:00 UTC 2021 • Wed May 19 00:00:00 UTC 2021

表 23. 次の表に、OpenManage Enterprise のデフォルト ジョブ名とそのスケジュールのリストを示します。（続き）

ジョブ名	Cron 式	Cron 式の説明	例
デフォルト コンソール アップデート タスク	0 0 12 ? * MON *	毎月、毎週月曜日、12:00:00pm に	• Mon May 24 12:00:00 UTC 2021 • Mon May 31 12:00:00 UTC 2021
デフォルト インベントリー タスク	0 0 5 * * ? *	毎日 05:00:00am に	• Tue May 18 05:00:00 UTC 2021 • Wed May 19 05:00:00 UTC 2021
クリーンアップのためのデバイス構成パージ タスク	0 0/1 * * * ? *	毎時、00 分から毎分、00 秒に	• Mon May 17 18:39:00 UTC 2021 • Mon May 17 18:40:00 UTC 2021
共有使用のためのファイル パージ タスク	0 0 0 1/1 * ? *	毎月 1 日から毎日、00:00:00am に	• Tue May 18 00:00:00 UTC 2021 • Wed May 19 00:00:00 UTC 2021
単一 DUP ファイルのためのファイル パージ タスク	0 0 0/4 1/1 * ? *	毎月 1 日から毎日、午前 0 時から 4 時間ごと、00 分 00 秒に	• Mon May 17 20:00:00 UTC 2021 • Tue May 18 00:00:00 UTC 2021 • Tue May 18 04:00:00 UTC 2021 • Tue May 18 04:00:00 UTC 2021
グローバル正常性タスク	0 0 0/1 1/1 * ? *	毎月 1 日から毎日、午前 0 時から 1 時間ごと、00 分 00 秒に	• Mon May 17 19:00:00 UTC 2021 • Mon May 17 20:00:00 UTC 2021
内部同期タスク	0 0/5 * 1/1 * ? *	毎月 1 日から毎日、毎時、00 分から 5 分ごと、00 秒に	• Mon May 17 18:45:00 UTC 2021 • Mon May 17 18:50:00 UTC 2021
メトリック パージ タスク	0 0 * ? * *	毎時 00 分の 00 秒に	• Mon May 17 19:00:00 UTC 2021 • Mon May 17 20:00:00 UTC 2021 • Mon May 17 21:00:00 UTC 2021
メトリック タスク	0 0/15 * 1/1 * ? *	毎月 1 日から毎日、毎時、00 分から 15 分ごと、00 秒に	• Mon May 17 18:45:00 UTC 2021 • Mon May 17 19:00:00 UTC 2021
モバイル サブスクリプション タスク	0 0/2 * 1/1 * ? *	毎月 1 日から毎日、毎時、00 分から 2 分ごと、00 秒に	• Mon May 17 18:54:00 UTC 2021 • Mon May 17 18:56:00 UTC 2021
ノードから開始される検出タスク	0 0/10 * 1/1 * ? *	毎月 1 日から毎日、毎時、00 分から 10 分ごと、00 秒に	• Mon May 17 19:00:00 UTC 2021 • Mon May 17 19:10:00 UTC 2021
パスワード ローテーション タスク	0 0 0/6 1/1 * ? *	毎月 1 日から毎日、午前 0 時から 6 時間ごと、00 分 00 秒に	• Tue May 18 00:00:00 UTC 2021 • Tue May 18 06:00:00 UTC 2021 • Tue May 18 12:00:00 UTC 2021
定期的なメトリックの登録	0 0 3 * * ?	毎日 03:00:00am に	• Tue May 18 03:00:00 UTC 2021 • Wed May 19 03:00:00 UTC 2021
テーブルのパージ オンデマンド正常性タスク：タスク	0 0 0/5 1/1 * ? *	毎月 1 日から毎日、午前 0 時から 5 時間ごと、00 分 00 秒に	• Tue May 18 00:00:00 UTC 2021 • Tue May 18 05:00:00 UTC 2021 • Tue May 18 10:00:00 UTC 2021
パージ タスク テーブル：Event_Archive	0 0 18/12 ? * * *	毎日午後 18 時から 12 時間ごと、00 分 00 秒に	• Tue May 18 18:00:00 UTC 2021 • Wed May 19 18:00:00 UTC 2021 • Thu May 20 18:00:00 UTC 2021
パージ タスク テーブル：Group_Audit	0 0 0 1/1 * ? *	毎月 1 日から毎日、00:00:00am に	• Tue May 18 00:00:00 UTC 2021 • Wed May 19 00:00:00 UTC 2021 • Thu May 20 00:00:00 UTC 2021
パージ タスク テーブル：タスク	0 0 0 1/1 * ? *	毎月 1 日から毎日、00:00:00am に	• Tue May 18 00:00:00 UTC 2021 • Wed May 19 00:00:00 UTC 2021 • Thu May 20 00:00:00 UTC 2021
パージ タスク テーブル：announced_target	0 0 0 1/1 * ? *	毎月 1 日から毎日、00:00:00am に	• Tue May 18 00:00:00 UTC 2021

表 23. 次の表に、OpenManage Enterprise のデフォルト ジョブ名とそのスケジュールのリストを示します。（続き）

ジョブ名	Cron 式	Cron 式の説明	例
			• Wed May 19 00:00:00 UTC 2021 • Thu May 20 00:00:00 UTC 2021
テーブルのパージ タスク：コア アプリケーション ログ	0 0 0/5 1/1 * ? *	毎月 1 日から毎日、午前 0 時から 5 時間ごと、00 分 00 秒に	• Tue May 18 00:00:00 UTC 2021 • Tue May 18 05:00:00 UTC 2021
テーブルのパージタスク：イベント	0 0/30 * 1/1 * ? *	毎月 1 日から毎日、毎時、00 分から 30 分ごと、00 秒に	• Mon May 17 19:30:00 UTC 2021 • Mon May 17 20:00:00 UTC 2021 • Mon May 17 20:30:00 UTC 2021
テーブルのパージ タスク：インフラストラクチャ デバイス	0 0/30 * 1/1 * ? *	毎月 1 日から毎日、毎時、00 分から 30 分ごと、00 秒に	• Mon May 17 19:30:00 UTC 2021 • Mon May 17 20:00:00 UTC 2021 • Mon May 17 20:30:00 UTC 2021
サブスクリプションの呼び出しタスク	0 0/30 * 1/1 * ? *	毎月 1 日から毎日、毎時、00 分から 30 分ごと、00 秒に	• Mon May 17 19:30:00 UTC 2021 • Mon May 17 20:00:00 UTC 2021 • Mon May 17 20:30:00 UTC 2021

個々のジョブ情報の表示

1. [ジョブ] ページで、対象のジョブに対応するチェックボックスを選択します。
2. 右ペインで、[詳細の表示] をクリックします。
   [ジョブの詳細] ページに、そのジョブ情報が表示されます。
3. ジョブのステータスが停止、失敗、または新規のいずれかである場合は、[ジョブの再スタート] をクリックします。
   ジョブの実行が開始されたことを示すメッセージが表示されます。

   [実行履歴] セクションには、ジョブが正常に実行された場合の情報が一覧表示されます。[実行の詳細] セクションには、ジョブが実行されたデバイスと、ジョブの実行時刻が一覧表示されます。

   メモ: 設定の修正タスクが停止した場合、タスク全体のステータスは「停止しました」と表示されますが、タスクは実行し続けます。ただし、ステータスは **実行履歴** セクションでは実行中であることを示しています。
4. Excel ファイルにデータをエクスポートする場合は、対応するチェックボックスまたはすべてのチェックボックスを選択して [エクスポート] をクリックします。「すべてまたは選択したデータのエクスポート 、p. 64」を参照してください。

デバイスの LED を点灯させるジョブの作成

次の手順では、デバイスの点滅ウィザードを使用して、指定したデバイスの LED を点滅させる方法について説明します。

OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。参照先： OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15

1. デバイスの点滅ウィザードは、次の方法で有効にすることができます。
   a. [ジョブ] ページ ([OpenManage Enterprise] > [監視] > [ジョブ]) から [作成] をクリックし、[デバイスの点滅] を選択します。
   b. [すべてのデバイス] ページ ([OpenManage Enterprise] > [デバイス]) からデバイスを選択し、[その他のアクション] ドロップダウンをクリックして、[LED をオンにする] または [LED をオフにする] をクリックします。
2. [デバイスの点滅ウィザード] ダイアログボックスで、次の手順を実行します。
   a. [オプション] セクションで、次の手順を実行します。
      i. [ジョブ名] ボックスにジョブ名を入力します。
      ii. [LED の点滅期間] ドロップダウンメニューで、設定した期間 LED を点滅させる、オンにする、オフにするのいずれかのオプションを選択します。
      iii. [次へ] をクリックします。
   b. [ターゲット] セクションで、ターゲット デバイスまたはターゲット グループを選択し、[次へ] をクリックします。ターゲットデバイスおよびデバイス グループの選択 、p. 130 を参照してください。

c. [スケジュール] ドロップダウンで、[今すぐ実行]、[後で実行]、または [スケジュールに従って実行] を選択します。スケジュールジョブフィールドの定義 、p. 174 を参照してください。

3. [終了] をクリックします。
LED の点滅ジョブが作成され、[ジョブ] ページ ([OpenManage Enterprise] > [監視] > [ジョブ]) の [ジョブ ステータス] 列に一覧表示されます。

電源デバイス管理のためのジョブの作成

メモ: 電源制御処置は、iDRAC (帯域外) を使用して検出および管理されるデバイスでのみ実行できます。

1. [作成] をクリックして [電源制御デバイス] を選択します。
2. [電源制御デバイスウィザード] ダイアログボックスで次の手順を実行します。
   a. [オプション] セクションで、次の手順を実行します。
      i. [ジョブ名] にジョブ名を入力します。
      ii. [電源オプション] ドロップダウンメニューから、次のいずれかのタスクを選択します :[電源オン]、[電源オフ] または [電源サイクル]
      iii. [次へ] をクリックします。
   b. [ターゲット] セクションで、ターゲットデバイスを選択し、[次へ] をクリックします。ターゲットデバイスおよびデバイス グループの選択 、p. 130 を参照してください。
   c. [スケジュール] セクションでは、ジョブをただちに実行するか、後の時点で実行するようにスケジュールします。スケジュールジョブフィールドの定義 、p. 174 を参照してください。
3. [終了] をクリックします。
ジョブが作成されてジョブリストに一覧表示され、[ジョブステータス] 行に適切なステータスで示されます。
4. このジョブが後の時点にスケジュールされているが、ジョブをただちに実行する場合は、次の操作を実行します。
   - ジョブ ページで、スケジュールされたジョブに対応するチェックボックスを選択します。
   - **今すぐ実行** をクリックします。ジョブが実行され、ステータスが更新されます。
   - ジョブデータを表示するには、右ペインの **詳細の表示** をクリックします。個々のジョブ情報の表示 、p. 128 を参照してください。

デバイスの管理用リモートコマンドジョブの作成

コマンド ライン ジョブ ウィザードを使用して、リモート コマンド ジョブを作成し、ターゲット デバイスをリモートで管理することができます。

1. [作成] をクリックして [デバイスのリモートコマンド] を選択します。
2. [コマンドラインジョブウィザード] ダイアログボックスの [オプション] セクションで、次の手順を実行します。
   a. [ジョブ名] にジョブ名を入力します。
   b. インターフェイス ドロップダウン メニューから、管理するターゲット デバイスに応じて、インターフェイスのいずれかを選択します。
      - [IPMI CLI] - iDRAC と非 Dell サーバー
      - [RACADM CLI] - WSMAN プロトコルを使用して検出された iDRAC
      - [SSH CLI] - SSH プロトコルを使用して検出された Linux サーバー
   c. [引数] ボックスにコマンドを入力します。コマンドは 100 個まで入力でき、それぞれ改行して入力します。

      メモ: [引数] ボックスのコマンドは、一度に 1 つずつ実行されます。

   d. [次へ] をクリックします。
   [オプション] の横に表示される緑色のチェックマークは、必要なデータが提供されていることを示します。
3. [ターゲット] セクションで、ターゲットデバイスを選択し、[次へ] をクリックします。ターゲットデバイスおよびデバイス グループの選択 、p. 130 を参照してください。
4. [スケジュール] セクションで、ジョブをただちに実行するか、またはスケジュールを設定して後で実行します。スケジュールジョブフィールドの定義 、p. 174 を参照してください。
5. [終了] をクリックします。
ジョブが作成されてジョブリストに一覧表示され、[ジョブステータス] 行に適切なステータスで示されます。
6. 後で実行するようにスケジュールされているジョブを、直ちに実行する場合は、次の操作を実行します。

- ジョブ ページで、スケジュールされたジョブに対応するチェックボックスを選択します。
- **今すぐ実行** をクリックします。ジョブが実行され、ステータスが更新されます。
- ジョブデータを表示するには、右ペインの **詳細の表示** をクリックします。個々のジョブ情報の表示 、p. 128 を参照してください。

仮想コンソール プラグイン タイプを変更するジョブの作成

複数のデバイスで、仮想コンソール プラグイン タイプを HTML5 に変更できます。HTML5 にアップデートすると、ブラウザーのユーザー エクスペリエンスが向上します。アップデートするには、次の手順を実行します。

1. [OpenManage Enterprise] > [監視] > [ジョブ] の順にクリックします。
2. [作成] をクリックして [デバイスの仮想コンソールプラグインの変更] を選択します。
3. [仮想コンソールプラグインの変更ウィザード] ダイアログボックスの [オプション] セクションで、次の手順を実行します。
   a. [ジョブ名] にジョブ名を入力します。デフォルトでは、プラグインタイプは HTML5 として表示されます。
   b. [次へ] をクリックします。
4. [ジョブのターゲット] セクションでは、ターゲットデバイスを選択し、[次へ] をクリックします。ターゲットデバイスおよびデバイス グループの選択 、p. 130 を参照してください。
   a. [次へ] をクリックします。
5. [スケジュール] セクションでは、ジョブをただちに実行するか、後の時点で実行するようにスケジュールします。スケジュールジョブフィールドの定義 、p. 174 を参照してください。
6. [終了] をクリックします。
   ジョブが作成されてジョブリストに一覧表示され、[ジョブステータス] 行に適切なステータスで示されます。
7. このジョブが後の時点にスケジュールされているが、ジョブをただちに実行する場合は、次の操作を実行します。
   - ジョブ ページで、スケジュールされたジョブに対応するチェックボックスを選択します。
   - **今すぐ実行** をクリックします。ジョブが実行され、ステータスが更新されます。
   - ジョブデータを表示するには、右ペインの **詳細の表示** をクリックします。個々のジョブ情報の表示 、p. 128 を参照してください。

ターゲットデバイスおよびデバイス グループの選択

デフォルトでは、[デバイスの選択] が選択され、デバイスでジョブを実行できることを示します。[デバイスグループ] を選択することにより、デバイスグループでジョブを実行することもできます。

メモ: 表示されるデバイス グループとデバイスは、ユーザーがデバイスに対して持っている範囲ベースの操作アクセス権によって管理されます。詳細については、OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

1. [デバイスの選択] をクリックします。
   [ジョブのターゲット] ダイアログボックスの左ペインに、OpenManage Enterprise で監視されるデバイスリストが表示されます。作業中のペインに、各グループに関連付けられたデバイスリスト、およびデバイスの詳細が表示されます。フィールドの説明については、デバイスリスト 、p. 59 を参照してください。デバイス グループの詳細については、デバイスのグループ化 、p. 52 を参照してください。
2. デバイスに対応するチェックボックスを選択し、[OK] をクリックします。
   選択したデバイスが、選択したグループの **選択されたすべてのデバイス** セクションに表示されます。

ジョブの管理

作成されて [ジョブ] ページに表示されたジョブは、次のように管理することができます。

- **ジョブの実行** : ジョブに対応するチェック ボックスを選択し、[今すぐ実行] をクリックして、対象のデバイスでタスクを実行します。ジョブはステータスが有効の場合に実行することができます。
- **ジョブの有効化** : ジョブに対応するチェック ボックスを選択して、[有効化] をクリックします。
- **ジョブの無効化** : ジョブに対応するチェック ボックスを選択して、[無効化] をクリックします。

メモ: 実行を無効にできるのは「スケジュール済み」ジョブのみです。アクティブで「実行中」状態のジョブは、途中で無効にすることはできません。

- **ジョブの停止**：ジョブに対応するチェック ボックスを選択して、[停止] をクリックします。ジョブはステータスが実行中の場合に停止することができます。
- **削除**：ジョブに対応するチェック ボックスを選択して、[削除] をクリックします。

17

デバイス保証の管理

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

[OpenManage Enterprise] > [監視] > [保証] の順にクリックすると、OpenManage Enterprise によって監視されているすべての範囲内のデバイスの保証ステータスを表示できます。たとえば、すべてのデバイス グループへのアクセス権を持つ管理者にはすべてのデバイスの保証の詳細が表示されますが、デバイス マネージャーには、それぞれの範囲内にあるデバイスについての保証の詳細のみが表示されます。

統計または分析目的で、選択したデータまたはすべてのデータを Excel シートにエクスポートすることもできます。保証ページには、次の詳細情報が表示されます。

- 保証の**ステータス**

  メモ: 保証ステータスは、管理者が選択した設定によって決まります。参照先： 保証設定の管理 、p. 162

  - **重要**を意味し、保証の期限が切れていることを示します。
  - **警告**を意味し、保証の期限が近づいていることを示します。
  - **正常**を意味し、保証が有効であることを示します。
- **サービスタグ**
- **デバイス モデル**
- **デバイスタイプ**
- **保証タイプ**：
  - 初期：OpenManage Enterprise 購入時に提供される保証です。
  - 延長：初期保証期間の終了後に、保証が延長されています。
- **サービス レベルの説明**：デバイス保証に関連するサービス レベル アグリーメント（SLA）を示します。
- **残りの日数** - 保証が期限切れになるまでの残り日数です。警告を受けるまでの日数を設定できます。保証設定の管理 、p. 162 を参照してください。

OpenManage Enterprise は、次の 30 日で期限切れになる保証に関するビルトインレポートを提供します。[OpenManage Enterprise] > [監視] > [レポート] > [次の 30 日で期限切れする保証] をクリックします。**実行** をクリックします。レポートの実行 、p. 135 を参照してください。

表に表示されるデータをフィルタするには、[詳細フィルタ] をクリックします。詳細フィルタのセクションについては、「OpenManage Enterprise グラフィカル ユーザー インターフェイスの概要 、p. 34」を参照してください。

検出されたすべてのデバイスの保証ステータスは、ビルトインの保証ジョブによって、週に 1 回自動的に収集されます。保証ジョブは、右上隅にある [保証の更新] をクリックして、手動で開始することもできます。

すべてまたは選択した保証データをエクスポートするには、[エクスポート] をクリックしてください。すべてまたは選択したデータのエクスポート 、p. 64 を参照してください。

関連タスク

デバイス保証の表示と更新 、p. 132

トピック：

デバイス保証の表示と更新

[OpenManage Enterprise] > [監視] > [保証] の順にクリックすると、OpenManage Enterprise によって監視されているすべてのデバイスの保証ステータスのリストと、それらのサービス タグ、モデル名、デバイス タイプ、関連する保証、サービス レベル情報のリストが表示されます。フィールドの説明については、デバイス保証の管理 、p. 132 を参照してください。

保証情報を表示して、デバイスの保証を更新するには、次の手順を実行します。

- デバイスに対応するチェックボックスを選択します。右ペインにデバイスの保証ステータスなどの重要詳細情報として、サービス レベル コード、サービス プロバイダー、保証開始日、保証終了日などが表示されます。
- 期限が切れた保証の更新をするには、[デバイスの Dell 保証の更新] をクリックすると、Dell EMC サポート サイトにリダイレクトされ、保証の管理ができます。
- 右上にある [保証の更新] をクリックすると、保証のテーブルが更新されます。保証が更新されたすべてのデバイス保障のステータスが、重要 ( から正常 ( に自動的に変わります。[保障の更新] をクリックするたびに、デバイスの保証アラート ログが生成されて、保証期限切れの合計数がコンソールに表示されます。アラート ログの詳細については「アラート ログの表示」を参照してください。
- 列に基づいて表のデータを並べ替えるには、列のタイトルをクリックします。
- [詳細フィルター] ボタンをクリックするとカスタマイズできます。

関連情報

デバイス保証の管理 、p. 132

18

レポート

[OpenManage Enterprise] > [監視] > [レポート] の順にクリックすると、デバイスの詳細を掘り下げたカスタマイズレポートを作成することができます。レポートでは、データセンターのデバイス、ジョブ、アラート、その他の要素に関するデータを表示できます。レポートは、ビルトインとユーザー定義です。ユーザー定義のレポートのみを編集または削除できます。ビルトインレポートで使用される定義と条件は、編集または削除できません。レポートのリストから選択したレポートのプレビューが右ペインに表示されます。

[レポート]ページに表示されるレポートとデータは、OpenManage Enterprise での範囲ベースのユーザー権限に応じて異なります。たとえば、デバイス マネージャは、ビルトイン レポートに加えて、自分が作成したレポートのみにアクセスできます。また、ユーザーによって生成されたレポートには、そのユーザーの範囲に含まれるデバイスからのデータのみが含まれることになります。たとえば、管理者と「制限なし」のデバイス マネージャーによって生成されたレポートにはすべてのデバイス グループのデータが含まれますが、範囲が制限されているデバイス マネージャーによって生成されたレポートには、その範囲内にあるデバイスおよび/またはデバイス グループに関連するデータのみが含まれます。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

表 24. OpenManage Enterprise レポートを管理するためのロール ベースのアクセス権限

ユーザー役割...	許可されているレポートタスク...
管理者とデバイス マネージャー	実行、作成、編集、コピー、電子メール、ダウンロード、およびエクスポート
閲覧者	実行、電子メール、エクスポート、表示、およびダウンロード

レポート機能のメリット：

- 最大 20 のフィルタを使用し、レポートの条件を構築
- 任意の列名でデータをフィルタリングしたり並べ替えが可能
- レポートは、表示、ダウンロード、および電子メールメッセージで送信可能
- 一度に最大で 20 ~ 30% の受信者にレポートを送信
- レポートの生成に時間がかかっていると思われる場合は、プロセスを停止できます
- OpenManage Enterprise のインストール中、生成されたレポートは設定されている言語に自動的に翻訳されます。
- レポート定義が生成、編集、削除、コピーされるたびに、監査ログエントリが作成されます。

現時点では、次についての情報を抽出するために、次のビルトインレポートを生成できます。

- デバイス カテゴリー：資産、FRU、ファームウェア、ファームウェア/ドライバーのコンプライアンス、スケジュールされたジョブ、アラートの概要、ハード ドライブ、モジュラー エンクロージャ、NIC、仮想ドライブ、保証、およびライセンス。
- アラートカテゴリ：週次アラート

関連タスク

レポートの実行 、p. 135
レポートの実行と電子メール送信 、p. 135
レポートの編集 、p. 136
レポートの削除 、p. 136

トピック：

- レポートの作成
- 選択したレポートのエクスポート

レポートの実行

[レポート] ページ ([OpenManage Enterprise] > [監視] > [レポート]) からは、ビルトイン レポートまたは作成したレポートを実行、表示、ダウンロードすることができます。

レポートを実行すると最初の 20 行が表示され、以降ページごとに改ページされて表示されます。一度にすべての行を表示するには、レポートをダウンロードしてください。この値を編集するには、「すべてまたは選択したデータのエクスポート 、p. 64」を参照してください。出力で表示されたデータは、レポートの構築に使用するクエリで定義されているため、並べ替えられません。データを並べ替えるには、レポートのクエリを編集するか、Excel シートにエクスポートします。レポートはシステムのリソースを消費するため、一度に 5 つ以上のレポートを実行しないことをお勧めします。ただし、この 5 つのレポートという値は、検出されるデバイス、使用されるフィールド、レポートを生成するために結合されるテーブルの数によって異なります。レポートの生成が要求されると、レポートジョブが作成され、実行されます。ロール ベースの権限のレポートを生成するには、レポートの作成 、p. 137 を参照してください。

メモ:
- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- デバイス マネージャーによって生成されたレポートには、そのスコープ内にあるデバイスに関するデータのみが含まれます。
- プロセスとデータリソースリソースが消費されるため、レポートを頻繁に実行しないことをお勧めします。
- レポートのカテゴリが「デバイス」の場合は、最初の列はデフォルトで、デバイスの名、デバイスモデル、デバイスのサービスタグになります。レポートをカスタマイズする場合、列を除外することができます。

レポートを実行するには、レポートを選択し、[実行] をクリックします。[<レポート名> レポート] ページでは、レポートはレポートを作成するために定義されたフィールドを使用した表になります。

レポートをダウンロードするには、次の手順に従います。

1. [ダウンロード] をクリックします。
2. **レポートのダウンロード** ダイアログボックスで、出力ファイルのタイプを選択し、**終了** をクリックします。選択した出力ファイルが表示されます。現在、XML、PDF、Excel、および CSV ファイル形式にレポートをエクスポートできます。レポート定義を生成、編集、削除、またはコピーするたびに、監査ログエントリが生成されます。

レポートを電子メールで送信するには、次の手順に従います。

1. **電子メール** をクリックします。
2. **レポートの電子メール送信** ダイアログボックスで、ファイル形式を選択し、受信者の電子メールアドレスを入力し、**終了** をクリックします。レポートが電子メールで送信されます。一度に 20~30 の受信者へのレポートを電子メールで送信できます。
3. 電子メールアドレスが設定されていない場合は、**SMTP 設定に進む** をクリックします。SMTP プロパティの設定の詳細については、「SNMP 資格情報の設定 、p. 162」を参照してください。

メモ: すでに生成されたレポートをダウンロードまたは実行しており、別のユーザーが同時にそのレポートを削除しようとした場合は、両方のタスクが正常に完了します。

関連情報

レポート 、p. 134

レポートの実行と電子メール送信

レポートを実行して、一度に 20 ~ 30 人の受信者に E メールで送信することができます。

メモ: メッセージ サイズが SMTP サーバーで設定された固定メッセージ サイズを超えると、E メール操作が大きなレポートで失敗する可能性があります。そのような場合は、SMTP サーバーのメッセージ サイズ制限をリセットして再試行することを考慮してください。

1. レポートを選択して [実行と電子メール送信] をクリックします。
2. [レポートの電子メール送信] ダイアログボックスで、次の手順を実行します。

a. [フォーマット] ドロップダウンメニューで、生成する必要があるレポートのファイルフォーマットを HTML、CSV、PDF、または MS-Excel の中から 1 つ選択します。
b. [宛先] ボックスに、受信者の電子メールアドレスを入力します。電子メールアドレスが設定されていない場合は、**SMTP 設定に進む** をクリックします。SMTP プロパティの設定の詳細については、「SNMP 資格情報の設定 、p. 162」を参照してください。
c. **終了** をクリックします。
レポートが電子メールで送信され、監査ログに記録されます。

関連情報

レポート 、p. 134

レポートの編集

編集できるのは、ユーザーが作成したレポートのみです。

1. レポートを選択し、[編集] をクリックします。
2. [レポート定義] ダイアログボックスで、設定を編集します。「レポートの作成」を参照。
3. [保存] をクリックします。
アップデートされた情報が保存されます。レポート定義を生成、編集、削除、またはコピーするたびに、監査ログエントリが生成されます。

メモ: カスタマイズしたレポートを編集する際に、カテゴリを変更すると、関連フィールドも削除されます。

関連情報

レポート 、p. 134

レポートのコピー

コピーできるのは、ユーザーが作成したレポートのみです。

1. レポートを選択して、[追加アクション] > [コピー] の順にクリックします。
2. [レポート定義のコピー] ダイアログボックスに、コピーされるレポートの新しい名前を入力します。
3. [保存] をクリックします。
アップデートされた情報が保存されます。レポート定義を生成、編集、削除、またはコピーするたびに、監査ログエントリが生成されます。

レポートの削除

削除できるのは、ユーザーが作成したレポートのみです。レポート定義が削除されると、関連するレポートの履歴が削除され、そのレポート定義を使用して実行されているレポートも停止されます。

1. [OpenManage Enterprise] メニューの [モニター] の下で、[レポート] を選択します。
デバイスの利用可能なレポートのリストが表示されます。
2. レポートを選択して、[追加アクション] > [削除] の順にクリックします。

メモ: すでに生成されたレポートをダウンロードまたは実行しており、別のユーザーが同時にそのレポートを削除しようとした場合は、両方のタスクが正常に完了します。

3. [レポート定義の削除] ダイアログボックスで、そのレポートを削除する必要があるかどうか表示されたら、[はい] をクリックします。
対象のレポートがレポートのリストから削除され、表がアップデートされます。レポート定義を生成、編集、削除、またはコピーするたびに、監査ログエントリが生成されます。

関連情報

レポート 、p. 134

レポートの作成

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- デバイス マネージャーによって生成されたレポートには、その範囲内にあるデバイス グループに関するデータのみが含まれます。
- デバイス タイプ別にデータが入っている表もあり、そのデバイス タイプのレポートを効果的にロックすることができます。タイプの異なる (サーバーとシャーシなど) の複数のデバイス別の表の列を混在させると、レポートが無効になり、結果は表示されません。

ビルトインレポートには、レポートを生成するためのデフォルトの定義 (フィルタ条件) がありますが、条件をカスタマイズして、自分の定義を作成し、カスタマイズされたレポートを生成できます。レポートに表示されるフィールドまたは列は、選択したカテゴリによって異なります。一度に選択できるカテゴリは 1 つだけです。レポート内の列の配置は、ドラッグして配置することで変更できます。また、次の設定が必要です。

- レポート名は固有でなければなりません。
- レポート定義には、少なくとも 1 つのフィールドと 1 つのカテゴリが必要です。
- カテゴリがデバイスおよび警告のレポートでは、デバイス名またはデバイスグループを必須フィールドにする必要があります。

デフォルトでは、**デバイス** が、カテゴリ、デバイス名、デバイスサービスタグとして選択され、デバイスモデル列が、作業中のペインに表示されます。レポート条件の編集中に他のカテゴリを選択すると、デフォルトのフィールドが削除されることを示すメッセージが表示されます。すべてのカテゴリに事前に定義されたプロパティがあり、定義した条件を使用してデータがフィルタ処理される列のタイトルとして使用することができます。カテゴリタイプの例 :

- ジョブ : タスク名、タスクのタイプ、タスクのステータス、タスクの内部。
- グループ : グループのステータス、グループの説明、グループメンバーシップのタイプ、グループ名、グループのタイプ。
- アラート : アラートのステータス、アラートの重大度、カタログ名、アラートのタイプ、アラートのサブカテゴリ、デバイス情報。
- デバイス : アラート、アラートのカタログ、シャーシファン、デバイスソフトウェアなど。これらの条件は、フィルタ処理されたデータや生成されたレポートに基づいて、さらに分類されます。

表 25. OpenManage Enterprise のレポートを生成するためのロール ベースのアクセス権限

ユーザー役割...	許可されているレポートタスク...
管理者とデバイス マネージャー	実行、作成、編集、コピー、電子メール、ダウンロード、およびエクスポート
閲覧者	実行、電子メール、エクスポート、表示、およびダウンロード

1. [レポート] > [作成] の順にクリックします。
2. [レポート定義] ダイアログボックスで、次の手順を実行します。
   a. 定義する新しいレポートの名前と説明を入力します。
   b. [次へ] をクリックします。
3. **レポートビルダー** セクションで、次の手順を実行します。
   a. **カテゴリ** ドロップダウンメニューから、レポートカテゴリを選択します。
      - デバイスをカテゴリに選択した場合は、デバイスグループも選択します。
      - 必要な場合は、フィルタ条件を編集します。クエリ条件の選択 、p. 55 を参照してください。

   b. [**列の選択**] セクションで、レポート列として表示する必要のあるフィールドのチェックボックスを選択します。
   選択したフィールド名は、[**列の順序**] セクションに表示されます。
   c. 次のようにして、レポートをカスタマイズすることができます。
      - [並べ替え列] および [並べ替え方向] ボックスを使用します。
      - [**列の順序**] セクションで、上または下にフィールドをドラッグします。
4. **終了**をクリックします。
   レポートが生成され、レポートのリストに表示されます分析のためにレポートをエクスポートできます。すべてまたは選択したデータのエクスポート 、p. 64 を参照してください。レポート定義を生成、編集、削除、またはコピーするたびに、監査ログエントリが生成されます。

レポート作成するときのクエリ条件の選択

クエリ条件を作成中に以下のためのフィルタを定義します。

- カスタマイズしたレポートの生成。「レポートの作成 、p. 137」を参照してください。
- カスタムグループ の下のクエリベースのデバイスグループの作成。「クエリデバイスグループの作成 、p. 55」を参照してください。

次の 2 つのオプションを使用してクエリ条件を定義します。

- **コピーする既存のクエリを選択**：デフォルトで OpenManage Enterprise では、自身のクエリ条件をコピーおよび構築可能な組み込みクエリテンプレートのリストを提供しています。クエリの定義中に最大 20 件の条件 (フィルター) を使用できます。フィルタを追加するには、**タイプの選択** ドロップダウンメニューから選択する必要があります。
- **タイプの選択**：このドロップダウン メニューに一覧表示されている属性を使用して、一からクエリ条件を構築します。メニュー内の項目は、OpenManage Enterprise によって監視されているデバイスによって異なります。クエリタイプを選択するときには、=、>、<、null などの適切な演算子のみがクエリタイプに基づいて表示されます。このメソッドは、カスタマイズされたレポートの構築において、クエリ条件を定義するために推奨されます。

  メモ: 複数の条件でクエリを評価する場合、評価順序は SQL と同じです。条件の評価に特定の順序を指定するには、クエリを定義するときに括弧を追加または削除します。

メモ: 選択すると、既存のクエリ条件のフィルタは、新しいクエリ条件を構築するためにのみ仮想的にコピーされます。既存のクエリに関連付けられたデフォルトのフィルタは変更されません。組み込みクエリ条件の定義 (フィルタ) は、カスタマイズされたクエリ条件を構築するための開始点として使用されます。たとえば、次のとおりです。

1. *Query1* は、次の事前定義されたフィルターを持つ組み込みクエリ条件です：`Task Enabled=Yes`
2. *Query1* のフィルター プロパティをコピーし、*Query2* を作成してから、別のフィルターを追加してクエリ条件をカスタマイズします：`Task Enabled=Yes` および `(Task Type=Discovery)`
3. その後、*Query1* を開きます。そのフィルター条件は、`Task Enabled=Yes` のままです。

1. **クエリ条件の選択** ダイアログボックスで、クエリグループ用か、またはレポート生成用にクエリ条件を作成したいかどうかに基づいて、ドロップダウンメニューから選択します。
2. プラス記号またはゴミ箱記号をそれぞれクリックしてフィルタを追加または削除します。
3. [**終了**] をクリックします。
   クエリ条件が生成され、既存のクエリのリストに保存されます。監査ログエントリが作成され、監査ログのリストに表示されます。「監査ログのモニター 、p. 122」を参照してください。

選択したレポートのエクスポート

1. エクスポートするレポートに対応したチェックボックスを選択して [追加アクション] をクリックし、[選択したものをエクスポート] をクリックします。
   現在、すべてのレポートを一度にエクスポートすることはできません。
2. [選択したレポートをエクスポート] ダイアログボックスで、エクスポートする必要があるレポートのファイルフォーマットを HTML、CSV、または PDF の中から 1 つ選択します。
3. [終了] をクリックします。
   このダイアログボックスで、分析および統計目的でファイルを開くか、既知の場所にそのファイルを保存します。

19

MIB ファイルの管理

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

データセンターの他社製ツールがあなたの操作に不可欠なアラートを生成する場合があります。そのようなアラートは、各ベンダーツールが定義および理解する管理情報ベース (MIB) ファイルに保存されます。ただし、OpenManage Enterprise ではこのような MIB の管理も可能になるため、Dell EMC 以外の MIB を OpenManage Enterprise がデバイス管理用にインポート、解析、使用できるようになります。OpenManage Enterprise は SMI1 と SMI2 をサポートします。OpenManage Enterprise は、Dell EMC デバイスに使用できるビルトイン MIB ファイルを提供します。これらは読み取り専用の MIB で編集できません。

メモ: トラップがある有効な MIB のみ OpenManage Enterprise が処理します。

MIB の管理の仕方：

- MIB ファイルのインポート 、p. 139
- MIB ファイルの削除 、p. 141
- MIB タイプの解決 、p. 141

[OpenManage Enterprise] > [監視] > [MIB] を選択すると、OpenManage Enterprise およびデータセンター内のその他のシステム管理ツールが使用する MIB ファイルを管理できます。表には、次のプロパティで使用可能な MIB ファイルが一覧表示されます。列見出しをクリックしてデータを並べ替えます。

表 26. OpenManage Enterprise での MIB ファイルへのロール ベースのアクセス

OpenManage Enterprise の機能	MIB ファイルに対するロール ベースのアクセス制御		
	管理者	デバイス マネージャー	閲覧者
トラップまたは MIB の表示	Y	Y	Y
MIB のインポートトラップの編集	Y	無	無
MIB を削除	Y	無	無
トラップの編集	Y	無	無

OpenManage Enterprise からビルトイン MIB ファイルをダウンロードするには、**MIB のダウンロード** をクリックします。ファイルは指定したフォルダに保存されます。

トピック：

- MIB ファイルのインポート
- MIB トラップの編集
- MIB ファイルの削除
- MIB タイプの解決
- OpenManage Enterprise MIB ファイルのダウンロード

MIB ファイルのインポート

MIB インポートの最適なプロセス フローは、[ユーザーが OpenManage Enterprise を MIB にアップロード] > [OpenManage Enterprise が MIB を解析] > [OpenManage Enterprise がすでに使用可能になっている同種のトラップをデータベースで検索] > [OpenManage Enterprise が MIB ファイル データを表示] です。インポートできる MIB の最大ファイルサイズは 3 MB です。OpenManage Enterprise の監査ログ履歴は、MIB のインポートと削除をそれぞれ記録します。

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なロール ベースのユーザー権限と、デバイスへの範囲ベースの操作アクセス権を持っている必要があります。参照先： OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15
- 一度に 1 つの MIB ファイルだけをインポートすることができます。

1. [MIB] > [MIB のインポート] の順にクリックします。
2. [MIB のインポート] ダイアログボックスの [MIB ファイルのアップロード] セクションで、[ファイルの選択] をクリックして MIB ファイルを選択します。

   MIB に外部の MIB によって解決されるインポートステートメントがある場合は、メッセージが表示されます。

   a. **タイプの解決** をクリックします。MIB タイプの解決 MIB ファイルの削除 、p. 141 を参照してください。
   b. **終了** をクリックします。MIB ファイルが Dell EMC 所有の場合は、MIB は製品に付属のもので変更できないことを示すメッセージが表示されます。
3. [次へ] をクリックします。
4. [トラップの表示] セクションには、MIB ファイルのリストが次の情報と共に表示されます。
   - トラップの警告カテゴリ。OpenManage Enterprise カテゴリの定義に合わせてカテゴリを編集することができます。MIB トラップの編集 、p. 140 を参照してください。
   - トラップ名は読み取り専用です。他社製のデバイスによって定義されます。
   - 警告の重大度は重要、警告、情報、および正常です。
   - 警告に関連する警告メッセージです。
   - トラップ OID は読み取り専用で、固有のものです。
   - 「新規」は、トラップが OpenManage Enterprise によって初めてインポートされたことを示します。すでにインポートされたトラップは、「インポート済み」として示されます。「上書き」は、インポート操作のためにその定義が上書きされたトラップを示します。

   MIB ファイルの警告カテゴリまたは重大度レベルのデフォルト設定を編集するには、「MIB トラップの編集 、p. 140」を参照してください。MIB ファイルを削除するには、対応するチェックボックスを選択し、**トラップの削除** をクリックします。MIB ファイルは削除され、MIB ファイルのリストが更新されます。
5. **終了** をクリックします。MIB ファイルが解析され、OpenManage Enterprise にインポートされたら、**最小** タブの下に表示されます。

メモ: MIB をインポートし、再度インポートする場合は、MIB のステータスは [インポート済み] として表示されます。ただし、削除された MIB ファイルを再度インポートする場合は、トラップのステータスは [新規] で示されます。

メモ: すでに OpenManage Enterprise にインポートされたトラップはインポートできません。

メモ: OpenManage Enterprise とともにデフォルトで出荷された MIB ファイルはインポートできません。

メモ: トラップのインポート後に生成されたイベントは、新しい定義に従ってフォーマットされ、表示されます。

MIB トラップの編集

1. レポートを選択し、[編集] をクリックします。
2. [MIB トラップの編集] ダイアログボックスで、次の手順を実行します。
   a. フィールドでデータを選択するか入力します。
      - アラートに割り当てる新しいアラートのカテゴリを選択します。デフォルトの場合、OpenManage Enterprise で表示されるビルトインのアラートカテゴリは数種類です。
      - アラートコンポーネントを入力します。
      - トラップ名は、他社製ツールで生成されているため読み取り専用です。
      - アラートに割り当てる重大度を選択します。デフォルトの場合、OpenManage Enterprise で表示されるビルトインのアラートカテゴリは数種類です。
      - アラートを説明するメッセージを入力します。
   b. [終了] をクリックします。
      トラップが編集され、更新されたトラップのリストが表示されます。

      メモ: 一度に複数のアラートを編集することはできません。OpenManage Enterprise にインポートされたトラップは編集できません。

3. [レポート定義] ダイアログボックスで、設定を編集します。「レポートの作成」を参照。
4. [保存] をクリックします。
   アップデートされた情報が保存されます。

MIB ファイルの削除

メモ: いずれかのアラートポリシーによって使用されているトラップ定義を持つ MIB ファイルを削除することはできません。「アラートポリシー 、p. 115」を参照してください。

メモ: MIB を削除する前に受信したイベントは、関連付けられた MIB の削除による影響を受けません。ただし、削除後に生成されたイベントは、未フォーマットのトラップを持ちます。

1. [MIB ファイル名] 行で、フォルダを展開して MIB ファイルを選択します。
2. [MIB の削除] をクリックします。
3. [MIB の削除] ダイアログボックスで、削除する MIB のチェックボックスを選択します。
4. [削除] をクリックします。
   MIB ファイルは削除され、MIB の表が更新されます。

MIB タイプの解決

1. 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 、p. 139」を参照してください。
   MIB タイプが未解決の場合、**未解決のタイプ** ダイアログボックスに MIB タイプがリストされ、解決された場合のみ MIB タイプがインポートされることを示します。
2. **タイプの解決** をクリックします。
3. **タイプの解決** ダイアログボックスで、**ファイルの選択** をクリックし、欠落しているファイル (複数可) を選択します。
4. **MIB のインポート** ダイアログボックスで、**次へ** をクリックします。まだ見つからない MIB タイプがある場合は、**未解決のタイプ** ダイアログボックスに欠落している MIB タイプが再度表示されます。手順 1~3 を繰り返します。
5. すべての未解決の MIB タイプが解決された後、**終了** をクリックします。インポートプロセスを完了します。「MIB ファイルのインポート 、p. 139」を参照してください。

OpenManage Enterprise MIB ファイルのダウンロード

1. [監視] ページで、[MIB] をクリックします。
2. OpenManage Enterprise MIB ファイルを解凍して選択し、[MIB のダウンロード] をクリックします。

   メモ: ダウンロードできるのは、OpenManage Enterprise 関連の MIB ファイルのみです。

20

OpenManage Enterprise アプライアンス設定の管理

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

メモ: 対応するブラウザーの詳細については、サポート サイトで入手できる『*OpenManage Enterprise サポート マトリックス*』を参照してください。

[OpenManage Enterprise] > [アプリケーションの設定] の順にクリックすると、次の作業を行うことができます。

- IPv4、IPv6、時刻、プロキシ設定などの OpenManage Enterprise のネットワーク設定を指定して管理します。「ネットワークの設定」を参照。
- ユーザーを追加、有効化、編集、および削除します。「ユーザーの管理」を参照。
- デバイスの正常性およびダッシュボードの監視プロパティを設定します。「コンソールプリファレンスの管理」を参照してください。
- ユーザーのログインおよびロックアウトのポリシーを管理します。「ログインセキュリティのプロパティの設定」を参照してください。
- 現在の SSL 証明書を表示して、CSR 要求を生成します。証明書署名要求を生成してダウンロードする 、p. 157 を参照してください。
- 電子メール、SNMP、アラート管理用のシスログプロパティを設定します。SMTP、SNMP、Syslog アラートの設定 、p. 118 を参照してください。
- SNMP リスナーとトラップの転送の設定を行います。「着信アラートの管理」を参照してください。
- 資格情報と、保証期限に関する通知を受け取るタイミングを設定します。「保証設定の管理」を参照してください。
- アップデートされたバージョンの可用性をチェックするプロパティを設定してから、OpenManage Enterprise のバージョンをアップデートします。OpenManage Enterprise のバージョンと使用可能なプラグインの確認とアップデート 、p. 163 を参照してください。
- ユーザー資格情報を設定し、RACADM と IPMI を使用してリモート コマンドを実行します。「リモートコマンドとスクリプトの実行」を参照してください。
- 携帯電話のアラート通知を設定および受信します。OpenManage Mobile の設定 、p. 169 を参照してください。

関連タスク

ディレクトリサービスの削除 、p. 153

トピック：

OpenManage Enterprise のネットワーク設定

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

1. DNS ドメイン名、FQDN、IPv4 および IPv6 設定など、OpenManage Enterprise のすべてのアクティブなネットワーク接続の現在のネットワーク設定のみを表示するには、[現在の設定] を展開します。
2. OpenManage Enterprise API のセッション タイムアウトおよび最大セッション数と Web インターフェイス ユーザーを設定するには、[セッションの非アクティブ タイムアウト設定] を展開して、次の操作を実行します。
   a. [有効にする] チェック ボックスにチェックを入れて [ユニバーサル タイムアウト] を有効にして、[非アクティブ タイムアウト (1 ~ 1440)] に値を入力します。タイムアウト値は、1 分から 1440 分 (24 時間) の範囲で設定できます。デフォルトでは、[ユニバーサル タイムアウト] はグレー表示されています。[ユニバーサル タイムアウト] を有効にすると、[API] および [Web インターフェイス] フィールドは無効になります。
   b. API の [非アクティブ タイムアウト (1 ~ 1440)] と [最大セッション数 (1 ~ 100)] の値を変更します。デフォルトでは、それぞれ 30 分と 100 分に設定されています。
   c. Web インターフェイスの [非アクティブ タイムアウト (1 ~ 1440)] と [最大セッション数 (1 ~ 100)] の値を変更します。デフォルトでは、それぞれ 30 分と 100 分に設定されています。
   d. 変更を保存するには [適用] を、デフォルト値を使用するには [破棄] をクリックします。
3. 現在のシステム時間とソース (ローカルのタイムゾーンまたは NTP サーバの IP) が表示されます。システムのタイムゾーン、日付、時刻、および NTP サーバとの同期を設定するには、[時刻設定] を展開します。
   a. ドロップダウンリストからタイムゾーンを選択します。
   b. 日付を入力するか、[カレンダー] アイコンをクリックして日付を選択します。
   c. 時刻を hh:mm:ss 形式で入力します。
   d. NTP サーバと同期するには、[NTP を使用] チェック ボックスを選択して、プライマリ NTP サーバのサーバアドレスを入力します。

      OpenManage Enterprise では、最大 3 つの NTP サーバを指定できます。

      メモ: [NTP を使用] オプションを選択している場合、[日付] および [時刻] のオプションは指定できません。
   e. [適用] をクリックします。
   f. 設定をデフォルトの属性にリセットするには、[破棄] をクリックします。
4. OpenManage Enterprise のプロキシ設定を行うには、[プロキシ設定] を展開します。
   a. [HTTP プロキシ設定を有効にする] チェック ボックスを選択して HTTP プロキシを設定してから、HTTP プロキシアドレスと HTTP ポート番号を入力します。
   b. [プロキシ認証の有効化] チェック ボックスをオンにして、プロキシ資格情報を有効化し、ユーザー名とパスワードを入力します。
   c. 構成されたプロキシが SSL トラフィックを傍受し、信頼できるサードパーティー証明書を使用しない場合は、[証明書の検証を無視]チェック ボックスを選択します。このオプションを使用すると、保証およびカタログ同期に使用される組み込み型証明書の確認は無視されます。
   d. [適用] をクリックします。
   e. 設定をデフォルトの属性にリセットするには、[破棄] をクリックします。

アプリケーションの設定機能を使用して実行できるすべてのタスクを理解するには、「OpenManage Enterprise アプライアンス設定の管理 、p. 142」を参照してください。

OpenManage Enterprise ユーザーの管理

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- ユーザーの役割を変更しても、影響を受けるユーザーのアクティブなセッションには影響しません。その後のログインから有効になります。
- デバイス マネージャー ユーザーがビューアーに降格された場合、その DM は、ジョブ、ファームウェアまたは設定テンプレート、ベースライン、アラート ポリシー、プロファイルなど、所有しているすべてのエンティティにアクセスできなくなります。これらのエンティティは管理者のみが管理でき、同じユーザーがビューアーから DM に対して「昇格」された場合でも復元できません。

[OpenManage Enterprise] > [アプリケーションの設定] > [ユーザー] の順にクリックすると、以下を実行できます。

- OpenManage Enterprise ローカル ユーザーの表示、追加、有効化、編集、無効化、削除。詳細については、「OpenManage Enterprise ローカル ユーザーの追加と編集」を参照。
- ディレクトリー グループをインポートすることによって Active Directory ユーザーに OpenManage Enterprise の役割を割り当て。AD および LDAP ディレクトリー ユーザーには、OpenManage Enterprise の管理者、デバイス マネージャー、ビューアーのいずれかの役割を割り当てることができます。詳細については、次を参照： AD および LDAP グループのインポート 、p. 149
- ログインしたユーザーに関する詳細を表示して、ユーザーセッションを終了。
- ディレクトリサービスの管理。詳細については、次を参照： ディレクトリサービスで使用する Active Directory グループの追加または編集 、p. 152
- OpenID Connect プロバイダーの表示、追加、有効化、編集、無効化、削除（PingFederate や Key Cloak ）。詳細については、次を参照： OpenID Connect プロバイダーを使用した OpenManage Enterprise ログイン 、p. 154

デフォルトでは、ユーザーリストは [ユーザー] に表示されます。右ペインに、作業中のペインで選択したユーザー名のプロパティが表示されます。

- [ユーザー名]: ユーザーの作成に伴い、OpenManage Enterprise はデフォルトのユーザー役割（管理者、システム、ルート）を表示しますが、これは編集 / 削除できません。ただし、ログイン資格情報は、デフォルトのユーザー名を選択して [編集] をクリックすると編集することができます。OpenManage Enterprise ユーザーを有効にする 、p. 148 を参照してください。ユーザー名に推奨される文字は、次のとおりです。
  - 0 ~ 9
  - A–Z
  - a–z
  - - ! # $ % & ( ) * / ; ? @ [\ ] ^ _ ` { | } ~ + < = >
  - パスワードに推奨される文字は、次のとおりです。
    - 0 ~ 9
    - A–Z
    - a–z
    - ' - ! " # $ % & ( ) * , ./ : ; ? @ [\ ] ^ _ ` { | } ~ + < = >
- [ユーザータイプ]: ユーザーがローカルでログインしたかリモートでログインしたかを示します。
- [有効]: ユーザーが OpenManage Enterprise 管理タスクを実行する権限がある場合、チェックマークで示します。OpenManage Enterprise ユーザーを有効にする 、p. 148 および OpenManage Enterprise ユーザーを無効にする 、p. 148 を参照してください。
- [役割]: OpenManage Enterprise 使用時のユーザー役割を示します。たとえば、OpenManage Enterprise の管理者とデバイスマネージャ。OpenManage Enterprise ユーザーの役割タイプ 、p. 14 を参照してください。

関連参照文献

OpenManage Enterprise ユーザーを無効にする 、p. 148
OpenManage Enterprise ユーザーを有効にする 、p. 148

関連タスク

ディレクトリサービスの削除 、p. 153
OpenManage Enterprise ユーザーの削除 、p. 148
ユーザーセッションの終了 、p. 150

OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御

OpenManage Enterprise には、3 つの組み込みの役割（管理者、デバイス マネージャー、ビューアー）のユーザー権限を明確に定義するロール ベースのアクセス制御（RBAC ）があります。さらに、範囲ベースのアクセス制御（SBAC ）を使用すると、管理者はデバイス マネージャーがアクセスできるデバイス グループを制限することができます。次のトピックでは、RBAC 機能と SBAC 機能について説明します。

OpenManage Enterprise のロール ベースのアクセス制御（RBAC ）権限

アプライアンス設定およびデバイス管理機能へのアクセスレベルを指定する役割をユーザーに割り当てます。この機能は、ロールベースのアクセス制御（RBAC ）と呼ばれています。コンソールは、アクションを許可する前に、特定のアクションに必要な権限を適用します。OpenManage Enterprise でのユーザー管理の詳細については、OpenManage Enterprise ユーザーの管理 、p. 143 を参照してください。

この表は、役割ごとに有効なさまざまな権限のリストです。

表 27. OpenManage Enterprise でのロール ベースのユーザー権限

OpenManage Enterprise の機能	権限の説明	OpenManage Enterprise にアクセスするためのユーザーレベル		
		管理者	デバイス マネージャー	閲覧者
アプライアンスのセットアップ	アプライアンスの設定を含むグローバル アプライアンスの設定。	Y	無	無
セキュリティ設定	アプライアンスのセキュリティ設定	Y	無	無
アラート管理	アラート アクション/管理	Y	無	無
ファブリック管理	ファブリック アクション/管理	Y	無	無
ネットワーク管理	ネットワーク アクション/管理	Y	無	無
グループ管理	静的および動的グループの作成、読み取り、アップデート、削除 (CRUD)	Y	無	無
検出管理	検出タスクのための CRUD、検出タスクの実行	Y	無	無
インベントリー管理	インベントリー タスクのための CRUD、インベントリー タスクの実行	Y	無	無
トラップ管理	MIB のインポート、トラップの編集	Y	無	無
自動導入管理	自動導入設定操作の管理	Y	無	無
セットアップのモニタリング	アラート ポリシー、転送、SupportAssist など	Y	Y	無
電源ボタン	デバイス電源の再起動/サイクル	Y	Y	無
デバイス設定	デバイスの設定、テンプレートの適用、IO ID の管理/移行、ストレージ マッピング (ストレージ デバイス用) など	Y	Y	無
オペレーティングシステムの導入	オペレーティング システムの導入、LUN へのマッピングなど	Y	Y	無
デバイスのアップデート	デバイス ファームウェアのアップデート、アップデートされたベースラインのアプリケーションなど	Y	Y	無
テンプレートの管理	テンプレートの作成/管理	Y	Y	無
ベースラインの管理	ファームウェア/設定ベースライン ポリシーの作成/管理	Y	Y	無
電源管理	電力予算の設定	Y	Y	無
ジョブ管理	ジョブの実行/管理	Y	Y	無
レポート管理	レポートでの CRUD 操作	Y	Y	無
レポート実行	レポートの実行	Y	Y	Y
表示	すべてのデータの表示、レポートの実行/管理など	Y	Y	Y

OpenManage Enterprise の範囲ベースのアクセス制御（SBAC）

ロール ベースのアクセス制御（RBAC）機能を使用すると、管理者はユーザーの作成時に役割を割り当てることができます。役割は、アプライアンス設定およびデバイス管理機能へのアクセス レベルを決定します。範囲ベースのアクセス制御（SBAC）は、管理者がデバイス マネージャーの役割を範囲と呼ばれるデバイス グループのサブセットに制限できるようにする RBAC 機能の拡張です。

デバイス マネージャー（DM）ユーザーを作成またはアップデートする際に、管理者は、1 つまたは複数のシステム グループ、カスタム グループ、プラグイン グループに DM の操作アクセスを制限するための範囲を割り当てることができます。

管理者とビューアーの役割の範囲には制限はありません。つまり、すべてのデバイスおよびグループ エンティティへの RBAC 権限によって指定された操作アクセスが可能であることを意味します。

範囲は次のように実装できます。

1. ユーザーの作成または編集
2. DM 役割の割り当て
3. 操作アクセスを制限するための範囲の割り当て

ユーザーの管理の詳細については、OpenManage Enterprise ユーザーの管理 、p. 143 を参照してください。

割り当てられた範囲を持つデバイス マネージャー（DM）ユーザーがログインしている場合、DM はスコープされたデバイスのみを表示および管理できます。また、DM は、ジョブ、ファームウェアまたは設定テンプレートやベースライン、アラート ポリシー、プロファイルなど、対象デバイスに関連づけられたエンティティを表示および管理できます（DM はそのエンティティを作成しているか、そのエンティティの所有権が割り当てられています）。DM が作成できるエンティティの詳細については、「*OpenManage Enteprise のロール ベースのアクセス制御（RBAC）権限*」を参照してください。

たとえば、[設定] > [テンプレート] の順にクリックすると、DM ユーザーは、デフォルト テンプレートおよび自分が所有するカスタム テンプレートを表示できます。また、DM ユーザーは、所有するテンプレートに対する RBAC 権限によってその他のタスクを実行できます。

[設定] > [ID プール] をクリックすると、DM ユーザーは、管理者または DM ユーザーによって作成されたすべての ID を確認できます。DM は RBAC 権限によって指定されたユーザーに対してアクションを実行することもできます。ただし、DM は、DM の範囲にあるデバイスに関連づけられている ID の使用のみを表示できます。

同様に、[設定] > [VLAN プール] の順にクリックすると、管理者によって作成されたすべての VLAN が表示され、エクスポートすることができます。DM はその他の操作を実行することはできません。DM がテンプレートを所有している場合は、テンプレートを編集して VLAN ネットワークを使用できますが、VLAN ネットワークを編集することはできません。

OpenManage Enterprise では、ローカル ユーザーの作成時または AD/LDAP ユーザーのインポート時に、範囲を割り当てることができます。OIDC ユーザーの範囲の割り当ては、Open ID Connect（OIDC）プロバイダーでのみ実行できます。

ローカル ユーザー向け SBAC：

DM の役割を持つローカル ユーザーを作成または編集する際に、管理者は DM の範囲を定義する 1 つまたは複数のデバイス グループを選択できます。

たとえば、（管理者として）「dm1」という名前の DM ユーザーを作成し、カスタム グループの下に存在するグループ *g1* を割り当てます。その後、dm1 は、*g1* 内のすべてのデバイスに対してのみ操作アクセス権を持ちます。ユーザー dm1 は、他のデバイスに関連する他のグループやエンティティにアクセスすることはできません。

さらに、SBAC を使用すると、dm1 は、同じグループ *g1* で他の DM（例：dm2）によって作成されたエンティティを表示することもできません。つまり、DM ユーザーは、自分が所有するエンティティのみを表示できます。

たとえば、（管理者として）別の DM ユーザー（dm2）を作成し、カスタム グループの下に存在する同じグループ *g1* を割り当てます。dm2 が *g1* でデバイスの設定テンプレート、設定ベースライン、またはプロファイルを作成した場合、dm1 はそれらのエンティティにアクセスできません。その逆も同様です。

すべてのデバイスへの範囲を持つ DM は、DM が所有するすべてのデバイスおよびグループ エンティティに対して RBAC 権限によって指定された操作アクセス権を持ちます。

AD/LDAP ユーザー向け SBAC：

管理者は、AD/LDAP グループをインポートまたは編集するときに、DM の役割を持つユーザー グループに範囲を割り当てることができます。ユーザーが DM の役割を持つ複数の AD グループのメンバーであり、各 AD グループに個別の範囲が割り当てられている場合、そのユーザーの範囲はこれらの AD グループの範囲の結合になります。

例：

- ユーザー dm1 は、2 つの AD グループ（*RR5-Floor1-labadmins* および *RR5-Floor3-labadmins*）のメンバーです。両方の AD グループには DM の役割が割り当てられていて、AD グループの範囲の割り当ては次のようになります。*RR5-Floor1-LabAdmins* は *ptlab-servers* を取得し、*RR5-Floor3-LabAdmins* は *smdlab-servers* を取得します。DM dm1 の範囲は、*ptlab-servers* と *smdlab-servers* の結合になります。

- ユーザー dm1 は、2 つの AD グループ（*adg1* と *adg2*）のメンバーです。両方の AD グループには DM の役割が割り当てられていて、範囲の割り当ては次のようになります。*adg1* には *g1* へのアクセス権が与えられており、*adg2* には *g2* へのアクセス権が与えられています。*g1* が *g2* の上位集合である場合、dm1 の範囲は、より大きな範囲（*g1*、すべての子グループ、およびすべてのリーフ デバイス）になります。

ユーザーが、異なる役割を持つ複数の AD グループのメンバーである場合は、より高い機能の役割が優先されます（管理者、DM、ビューアーの順）。

制限のない範囲を持つ DM は、すべてのデバイスおよびグループ エンティティに対する RBAC 権限によって指定された操作アクセス権を持ちます。

メモ: OpenManage Enterprise をバージョン 3.5 またはそれ以前のバージョンからアップグレードした後、AD/LDAP および OIDC（PingFederate または KeyCloak）デバイス マネージャーは、以前のバージョンのエンティティをすべて再作成する必要があります。これは、それらのエンティティがアップグレード後は管理者のみが使用できる状態であるためです。詳細については、https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs にあるリリース ノートを参照してください。

OIDC ユーザー向け SBAC：

OIDC ユーザーの範囲の割り当ては、OME コンソール内では発生しません。ユーザーの設定中に OIDC プロバイダーの OIDC ユーザーの範囲を割り当てることができます。ユーザーが OIDC プロバイダーの認証情報を使用してログインすると、役割と範囲の割り当てが OME に使用可能になります。ユーザーの役割と範囲の設定の詳細については OpenManage Enterprise へのロール ベースのアクセスのための PingFederate での OpenID Connect プロバイダー ポリシーの設定、p. 155 を参照してください。

メモ: PingFederate が OIDC プロバイダーとして使用されている場合は、管理者ロールのみを使用できます。詳細については、OpenManage Enterprise へのロール ベースのアクセスのための PingFederate での OpenID Connect プロバイダー ポリシーの設定、p. 155、および https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs にあるリリース ノートを参照してください。

所有権の移行：管理者は、所有するリソースをデバイス マネージャー（ソース）から別のデバイス マネージャーに移行することができます。たとえば、管理者は、ソース dm1 からのすべてのリソースを dm2 に移行することができます。ファームウェアおよび/または設定ベースライン、設定テンプレート、アラート ポリシー、プロファイルなどのエンティティを所有するデバイス マネージャーは、適格なソース ユーザーと見なされます。所有権の移行は、デバイス マネージャーによって所有されている、デバイス グループ（範囲）ではなく、エンティティのみを別のデバイス マネージャーに移行します。詳細については、デバイス マネージャー エンティティの所有権の移行、p. 150 を参照してください。

関連参照文献

OpenManage Enterprise ユーザーの役割タイプ、p. 14

OpenManage Enterprise ローカル ユーザーの追加と編集

この手順は、ローカルユーザーの追加と編集のみに固有です。ローカルユーザーの編集中は、すべてのユーザープロパティを編集できます。ただし、ディレクトリー ユーザーについては、役割とデバイス グループ（デバイス マネージャーの場合）のみが編集できます。OpenManage Enterprise でディレクトリー サービスを統合し、ディレクトリー ユーザーをインポートするには、OpenManage Enterprise でのディレクトリサービスの統合、p. 150 および AD および LDAP グループのインポート、p. 149 を参照してください。

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御、p. 15 を参照してください。
- 管理者 / システム / root ユーザーを有効化、無効化、または削除できません。パスワードは、右のペインで [編集] をクリックしてのみ変更できます。

1. [アプリケーションの設定] > [ユーザー] > [ユーザー] > [追加] を選択します。
2. [新規ユーザーの追加] ダイアログボックスで、次の手順を実行します。
   a. [**ユーザーの詳細**] の下で、[ユーザーの役割] ドロップダウン メニューから [管理者]、[デバイス マネージャー]、または [ビューアー] を選択します。

      詳細については、OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御、p. 15 を参照してください。

      デフォルトでは、[有効] チェックボックスが選択され、ユーザーに現在セットアップが有効であるユーザー権限が示されます。

b. デバイス マネージャーの役割では、範囲が [すべてのデバイス](制限なし範囲) にデフォルト設定されます。ただし、管理者は、[グループの選択] オプションを選択し、次にデバイス グループを選択することによって範囲を制限することができます。
c. [**ユーザー資格情報**] で、[ユーザー名] と [パスワード] を入力して、[パスワードの確認] フィールドにパスワードを再入力します。

メモ: ユーザー名は英数字のみ (アンダースコアは許可) で構成する必要があり、パスワードは大文字、小文字、数字、特殊文字を 1 文字以上を含める必要があります。

3. [終了] をクリックします。
ユーザーが正常に保存されたことを示すメッセージが表示されます。新しいユーザーを作成するジョブが開始されます。ジョブの実行後、新規ユーザーが作成され、ユーザーのリストに表示されます。

OpenManage Enterprise ユーザーのプロパティの編集

1. **アプリケーションの設定** ページの **ユーザー** で、ユーザーに対応するチェックボックスを選択します。
2. 「OpenManage Enterprise ローカル ユーザーの追加と編集 、p. 147」のタスクを完了します。
アップデートされたデータが保存されます。

メモ: ユーザーの役割を変更する場合は、新しい役割に対して利用可能な権限が自動的に適用されます。たとえば、デバイス管理者を管理者に変更すると、管理者に提供されるアクセス権と権限がそのデバイス管理者に対して自動的に有効になります。

OpenManage Enterprise ユーザーを有効にする

ユーザー名に対応するチェックボックスを選択して、[有効にする] をクリックします。ユーザーが有効になり、[有効] 列の対応するセルにチェックマークが表示されます。ユーザー名の作成中に、ユーザーがすでに有効になっている場合は、[有効化] ボタンはグレー表示されます。

関連タスク

ディレクトリサービスの削除 、p. 153
OpenManage Enterprise ユーザーの削除 、p. 148
ユーザーセッションの終了 、p. 150

関連情報

OpenManage Enterprise ユーザーの管理 、p. 143

OpenManage Enterprise ユーザーを無効にする

ユーザー名に対応するチェックボックスを選択して、[無効] をクリックします。ユーザーは無効になり、[有効] 列の対応するセルのチェックマークが消えます。ユーザー名の作成中にユーザーが無効になると、[無効] ボタンがグレー表示されます。

関連タスク

ディレクトリサービスの削除 、p. 153
OpenManage Enterprise ユーザーの削除 、p. 148
ユーザーセッションの終了 、p. 150

関連情報

OpenManage Enterprise ユーザーの管理 、p. 143

OpenManage Enterprise ユーザーの削除

1. ユーザー名に対応するチェックボックスを選択し、[削除] をクリックします。
2. プロンプトが表示されたら、[はい] をクリックします。

関連参照文献

OpenManage Enterprise ユーザーを無効にする 、p. 148
OpenManage Enterprise ユーザーを有効にする 、p. 148

関連情報

OpenManage Enterprise ユーザーの管理 、p. 143

AD および LDAP グループのインポート

メモ:

- 管理者権限のないユーザーは、Active Directory (AD) および Lightweight Directory Access Protocol (LDAP) ユーザーを有効または無効にすることはできません。
- OpenManage Enterprise で AD をインポートする場合は、事前に AD の設定時に、ユーザーグループをユニバーサルグループに含めておく必要があります。
- AD および LDAP ディレクトリー ユーザーをインポートし、OpenManage Enterprise の役割 (管理者、デバイス マネージャー、閲覧者) のいずれかを割り当てることができます。シングルサインオン (SSO) 機能は、コンソールへのログイン時に停止します。デバイス上で操作を実行する場合、そのデバイスの特権アカウントを必要とします。
- OpenManage Enterprise をバージョン 3.5 またはそれ以前のバージョンからアップグレードした後、AD/LDAP および OIDC (PingFederate または KeyCloak) デバイス マネージャーは、以前のバージョンのエンティティをすべて再作成する必要があります。これは、それらのエンティティがアップグレード後は管理者のみが使用できる状態であるためです。詳細については、次のサイトにあるリリース ノートを参照してください : https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs

1. [ディレクトリグループのインポート] をクリックします。
2. [Active Directory のインポート] ダイアログボックスで、次の手順を実行します。
   a. [ディレクトリソース] ドロップダウンメニューから、グループを追加するためにインポートすべき AD または LDAP ソースを選択します。ディレクトリの追加については、「ディレクトリサービスで使用する Active Directory グループの追加または編集 、p. 152」を参照してください。
   b. **資格情報の入力** をクリックします。
   c. ダイアログボックスで、ディレクトリが保存されているドメインのユーザー名とパスワードを入力します。ツールヒントを使用して、正しい構文を入力します。
   d. **終了**をクリックします。
3. **使用可能なグループ** セクションで、次の操作を実行します。
   a. **グループの検索** ボックスに、テスト済みディレクトリで使用できるグループ名の最初の数文字を入力します。入力したテキストで始まるすべてのグループ名が、グループ名 の下に表示されます。
   b. インポートするグループに対応するチェックボックスを選択し、**>>** または **<<** ボタンをクリックして、グループを追加または削除します。
4. **インポートするグループ** セクションで、次の操作を実行します。
   a. グループのチェックボックスを選択し、グループ役割の割り当て ドロップダウンメニューから役割を選択します。ロールベースのアクセスの詳細については、OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
   b. [ロールの割り当て] をクリックします。
   選択したディレクトリサービスの下にあるグループのユーザーが、選択したユーザー役割に割り当てられます。
   c. デバイス マネージャーの役割では、範囲が [すべてのデバイス] にデフォルト設定されます。ただし、管理者は、[範囲の割り当て] オプションを選択し、次にデバイス グループを選択することによって範囲を制限することができます。
5. 必要に応じて、手順 3 と 4 を繰り返します。
6. **インポート** をクリックします。
   ディレクトリグループがインポートされ、ユーザーのリストに表示されます。ただし、これらのグループ内のすべてのユーザーがそれぞれのドメインユーザー名と資格情報を使用して OpenManage Enterprise へログインします。

たとえば john_smith というドメインユーザーは、複数のディレクトリグループのメンバーになることも、別の役割を割り当てられているグループのメンバーになることもできます。この例では、アプライアンスのマストヘッドの右上隅にあるユーザー名にカーソルを移動させると、デバイス マネージャーやビューアーなどの複数の役割が表示されます。このようなユーザーは、ユーザーがメンバーになっているすべてのディレクトリー グループの最高レベルの役割を受け取ります。

- 例 1 : ユーザーは管理者、DM、および閲覧者役割を持つ 3 つのグループのメンバーです。この場合、ユーザーは管理者になります。

- 例 2 : ユーザーは 3 つの DM グループと 1 つの閲覧者グループのメンバーです。この場合、ユーザーは、3 つの DM 役割全体にわたるデバイスグループのユニオンにアクセスできる DM になります。

デバイス マネージャー エンティティの所有権の移行

このトピックでは、管理者が、1 つのデバイス マネージャーによって作成されたジョブ、ファームウェアまたは設定テンプレートやベースライン、アラート ポリシー、プロファイルなどのエンティティを別のデバイス マネージャーに移行する方法について説明します。管理者は、デバイス マネージャーが組織から離脱するときに、「所有権の移行」を開始できます。

メモ:
- OpenManage Enterprise でこのタスクを実行するには、管理者ユーザー権限が必要です。OpenManage Enterprise のロールベースと範囲ベースのアクセス制御 、p. 15。
- 「所有権の移行」は、デバイス マネージャーによって所有されている、デバイス グループ (スコープ) ではなく、エンティティのみを別のデバイス マネージャーに移行します。
- エンティティの所有権の移行を開始する前に、管理者は最初に、以前のデバイス マネージャーによって所有されているデバイス グループを、引き継ぐデバイス マネージャーに再割り当てする必要があります。
- エンティティの所有権が Active Directory ユーザー グループに移行されると、所有権はその AD グループのすべてのメンバーに移行されます。

ジョブ、ファームウェアまたは設定テンプレートやベースライン、アラート ポリシー、プロファイルなどのエンティティの所有権を、あるデバイス マネージャーから別のデバイス マネージャーに移行するには、次の手順を実行します。

1. [OpenManage Enterprise] > [アプリケーションの設定] > [ユーザー] > [所有権の移行] の順にクリックして、[所有権の移行] ウィザードを開始します。
2. [ソース ユーザー] ドロップダウン リストから、エンティティの所有権を移行する必要があるデバイス マネージャーを選択します。

   メモ: ソース ユーザーは、ジョブ、FW または設定テンプレート、アラート ポリシー、それらに関連づけられたプロファイルなどのエンティティを持つ、ローカル、Active Directory、OIDC、または削除されたデバイス マネージャーのみを一覧表示します。

3. [ターゲット ユーザー] ドロップダウン リストから、エンティティの移行先となるデバイス マネージャーを選択します。
4. [完了] をクリックし、プロンプト メッセージで [はい] をクリックします。

ジョブ、ファームウェアまたは設定テンプレート、アラート ポリシー、プロファイルなどの所有されているすべてのエンティティは、「ソース」デバイス マネージャーから「ターゲット」デバイス マネージャーに移行されます。

ユーザーセッションの終了

1. ユーザー名に対応するチェックボックスを選択し、[終了] をクリックします。
2. 確認を促すプロンプトが表示されたら、[はい] をクリックします。
   選択したユーザーセッションは終了し、ユーザーはログアウトされます。

関連参照文献

OpenManage Enterprise ユーザーを無効にする 、p. 148
OpenManage Enterprise ユーザーを有効にする 、p. 148

関連情報

OpenManage Enterprise ユーザーの管理 、p. 143

OpenManage Enterprise でのディレクトリサービスの統合

ディレクトリー サービスでは、コンソールで使用するために、AD または LDAP からディレクトリー グループをインポートすることができます。OpenManage Enterprise は、次のディレクトリー サービスの統合をサポートします。

1. Windows Active Directory
2. Windows AD/LDS
3. OpenLDAP
4. PHP LDAP

LDAP 統合での前提条件/対応属性

表 28. OpenManage Enterprise における LDAP 統合での前提条件/対応属性

	ユーザーログインの属性	グループメンバーシップの属性	証明書の要件
AD/LDAP	Cn、sAMAccountName	メンバー	• ドメイン コントローラー証明書によっては、FQDN が必要です。[SAN]フィールドには、IPv4 や IPv6 または FQDN を入力できます。 • Base64 証明書形式のみがサポートされています。
OpenLDAP	uid、sn	Uniquemember	PEM 証明書形式のみがサポートされています。
PHP LDAP	uid	MemberUid	

ディレクトリー サービス統合でのユーザー前提条件

ディレクトリー サービスの統合を開始する前に、次のユーザー前提条件が満たされていることを確認する必要があります。

1. BindDN ユーザーと「テスト接続」に使用されるユーザーは、同じである必要があります。
2. ユーザー ログインの属性が入力された場合、アプライアンスのログインには属性に割り当てられた対応するユーザー名の値のみが許可されます。
3. テスト接続に使用されるユーザーは、LDAP でデフォルト以外のグループの一員である必要があります。
4. グループ メンバーシップの属性には、「userDN」またはそのユーザーの短縮名（ログインに使用）のいずれかが含まれる必要があります。
5. MemberUid を「グループ メンバーシップの属性」として使用する場合、アプライアンスのログインで使用されるユーザー名は、一部の LDAP 設定で大文字と小文字が区別されると考えられます。
6. LDAP 設定で検索フィルターを使用する場合、ユーザー ログインは、前述の検索条件に含まれていないユーザーに対して許可されません。
7. グループ検索は、指定されたグループ メンバーシップの属性を持つユーザーがグループに割り当てられている場合にのみ機能します。

メモ: OpenManage Enterprise が IPv6 ネットワーク上でホストされている場合、DNS で IPv4 が優先アドレスとして設定されていると、FQDN を使用するドメイン コントローラーに対する SSL 認証は失敗します。この問題を回避するには、次の操作のいずれかを実行します。

- FQDN でクエリした場合は、IPv6 を優先アドレスとして返すように DSN を設定する必要があります。
- DC 証明書の [SAN] フィールドは IPv6 になっている必要があります。

ディレクトリー サービスを使用するには、次の手順に従います。

- ディレクトリ接続を追加します。「ディレクトリサービスで使用する Active Directory グループの追加または編集 、p. 152」を参照してください。
- ディレクトリグループをインポートし、グループ内のすべてのユーザーに特定の役割をマッピングします。「AD および LDAP グループのインポート 、p. 149」を参照してください。
- DM ユーザーの場合は、ディレクトリグループを編集して、DM が管理できるグループを追加します。「OpenManage Enterprise ローカル ユーザーの追加と編集 、p. 147」を参照してください。

ディレクトリサービスで使用する Active Directory グループの追加または編集

1. [アプリケーションの設定] > [ユーザー] > [ディレクトリサービス] の順にクリックして、[追加] をクリックします。
2. [ディレクトリサービスへの接続] ダイアログボックスでは、デフォルトで **AD** が選択されており、ディレクトリタイプが Active Directory (AD) であることが示されます。

   メモ: ディレクトリサービスを使用して LDAP ユーザーグループを作成する場合は、「ディレクトリサービスで使用する Lightweight Directory Access Protocol (LDAP) グループの追加または編集 、p. 152」を参照してください。

   a. AD ディレクトリーの所要の名前を入力します。
   b. ドメインコントローラの検索方法を選択します。
      - **DNS：メソッド** ボックスには、ドメインコントローラの DNS のクエリのためのドメイン名を入力します。
      - **手動**：**メソッド** ボックスに、ドメインコントローラの FQDN または IP アドレスを入力します。複数サーバの場合は、カンマで区切ったリストで、最大 3 台のサーバをサポートできます。
   c. ツールヒントの構文にしたがって、**グループドメイン** ボックスにグループドメインを入力します。
3. **詳細オプション** セクションの場合：
   a. デフォルトでは、グローバルカタログアドレスのポート番号 3269 が入力されています。ドメインコントローラアクセスの場合は、ポート番号として 636 を入力します。

      メモ: サポートされているのは LDAPS ポートのみです。

   b. ネットワークタイムアウト時間と検索タイムアウト時間を秒単位で入力します。サポートされているタイムアウト時間の最大値は 300 秒です。
   c. SSL 証明書をアップロードするには、[証明書の検証] を選択し、[ファイルの選択] をクリックします。Base64 フォーマットでエンコードされたルート CA 証明書を使用する必要があります。

   接続のテスト タブが表示されます。
4. **接続のテスト** をクリックします。
5. ダイアログ ボックスで、接続先のドメインの [ユーザー名] と [パスワード] を入力します。

   メモ: [ユーザー名] は、UPN (ユーザー名@ドメイン) または NetBIOS (ドメイン\ユーザー名) のどちらかの形式で入力する必要があります。
6. **接続のテスト** をクリックします。
   ディレクトリサービス情報 ダイアログボックスに、正常に接続したことを通知するメッセージが表示されます。
7. [**OK**] をクリックします。
8. **終了**をクリックします。
   ジョブの作成と実行により、ディレクトリサービスリストに目的のディレクトリが追加されます。

1. **ディレクトリ名** 列で、ディレクトリを選択します。ディレクトリサービスプロパティが右ペインに表示されます。
2. **編集** をクリックします。
3. **ディレクトリサービスへの接続** ダイアログボックスで、データを編集して **終了** をクリックします。データはアップデートされ、保存されます。

ディレクトリサービスで使用する Lightweight Directory Access Protocol (LDAP) グループの追加または編集

1. [アプリケーションの設定] > [ユーザー] > [ディレクトリサービス] の順にクリックして、[追加] をクリックします。
2. [ディレクトリサービスへの接続] ダイアログボックスで、ディレクトリのタイプとして **LDAP** を選択します。

   メモ: ディレクトリサービスを使用して AD ユーザーグループを作成する場合は、「ディレクトリサービスで使用する Active Directory グループの追加または編集 、p. 152」を参照してください。

   a. LDAP ディレクトリーの名前を入力します。
   b. ドメインコントローラの検索方法を選択します。
      - **DNS：メソッド** ボックスには、ドメインコントローラの DNS のクエリのためのドメイン名を入力します。

- **手動**：**メソッド** ボックスに、ドメインコントローラの FQDN または IP アドレスを入力します。複数サーバの場合は、カンマで区切ったリストで、最大 3 台のサーバをサポートできます。

c. LDAP バインド識別名（DN）とパスワードを入力します。

メモ: AD LDS には、匿名のバインドはサポートされません。

3. **詳細オプション** セクションの場合：
   a. デフォルトでは、LDAP ポート番号は 636 に設定されています。変更するには、ポート番号を入力します。

   メモ: サポートされているのは LDAPS ポートのみです。

   b. サーバの LDAP 設定に一致させるには、検索するグループベース DN を入力します。
   c. LDAP システムで設定済みの**ユーザー属性**を入力します。これは選択されたベース DN 内で一意であることを推奨します。そうでない場合は、一意になるように検索フィルタを設定してください。属性と検索フィルタを使った検索の組み合わせでユーザー DN を一意に識別できない場合、ログイン操作は失敗します。

   メモ: ユーザー属性は、ディレクトリー サービスの統合前に、クエリーに用いる LDAP システムに設定しておく必要があります。

   メモ: ユーザー属性の入力は、AD LDS 設定の場合は **cn** または **sAMAccountName** とし、LDAP 設定の場合は **UID** とします。

   d. [グループメンバーシップの属性] ボックスに、グループとメンバーの情報をディレクトリに保存する属性を入力します。
   e. ネットワークタイムアウト時間と検索タイムアウト時間を秒単位で入力します。サポートされているタイムアウト時間の最大値は 300 秒です。
   f. SSL 証明書をアップロードするには、[証明書の検証] を選択し、[ファイルの選択] をクリックします。Base64 フォーマットでエンコードされたルート CA 証明書を使用する必要があります。

   [**接続のテスト**] ボタンが有効になります。
4. [**接続のテスト**] をクリックして、接続先ドメインのバインド ユーザー認証情報を入力します。

   メモ: 接続のテストを行う場合は、[[テスト ユーザー名]] に、事前に入力した [[ユーザー ログインの属性]] が使用されていることを確認してください。
5. **接続のテスト** をクリックします。
   ディレクトリサービス情報 ダイアログボックスに、正常に接続したことを通知するメッセージが表示されます。
6. [**OK**] をクリックします。
7. [**終了**] をクリックします。
   ジョブの作成と実行により、ディレクトリサービスリストに目的のディレクトリが追加されます。

1. **ディレクトリ名** 列で、ディレクトリを選択します。ディレクトリサービスプロパティが右ペインに表示されます。
2. **編集** をクリックします。
3. **ディレクトリサービスへの接続** ダイアログボックスで、データを編集して **終了** をクリックします。データはアップデートされ、保存されます。

ディレクトリサービスの削除

削除するディレクトリサービスに対応するチェックボックスを選択し、[削除] をクリックします。

関連参照文献

OpenManage Enterprise ユーザーを無効にする 、p. 148
OpenManage Enterprise ユーザーを有効にする 、p. 148

関連情報

OpenManage Enterprise アプライアンス設定の管理 、p. 142
OpenManage Enterprise ユーザーの管理 、p. 143

OpenID Connect プロバイダーを使用した OpenManage Enterprise ログイン

OpenID Connect（OIDC）プロバイダーを使用してログインすることができます。OpenID Connect プロバイダーは、ユーザーがアプリケーションに安全にアクセスできるようにする、ID およびユーザー管理ソフトウェアです。現在、OpenManage Enterprise は PingFederate と Keycloak のサポートを提供しています。

警告: OIDC プロバイダー PingFederate（PingIdentity）を使用してクライアントを再登録すると、ユーザーの役割と範囲が「デフォルト」にリセットされます。この問題により、管理者以外の役割（DM およびビューアー）の権限と範囲が管理者の権限と範囲にリセットされる原因になる場合があります。OIDC プロバイダーを使用したアプライアンス コンソールの再登録は、アプライアンスのアップグレード時、ネットワーク構成の変更時、SSL 証明書の変更時にトリガーされます。

前述の再登録イベントのいずれかの後のセキュリティ上の懸念を回避するために、管理者は PingFederate サイトですべての OpenManage Enterprise クライアント ID を再構成する必要があります。また、この問題が解決されるまで、PingFederate を使用している管理者ユーザーのみにクライアント ID を作成することを強くお勧めします。

メモ:

- OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。
- アプライアンスには、OpenID Connect プロバイダー ID を最大 4 つまで追加できます。
- OpenManage Enterprise をバージョン 3.5 またはそれ以前のバージョンからアップグレードした後、AD/LDAP および OIDC（PingFederate または KeyCloak）デバイス マネージャーは、以前のバージョンのエンティティをすべて再作成する必要があります。これは、それらのエンティティがアップグレード後は管理者のみが使用できる状態であるためです。詳細については、次のサイトにあるリリース ノートを参照してください：https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs

前提条件：

OpenID Connect プロバイダー ログインを有効にする前に、次の操作を行う必要があります。

1. **OpenManage Enterprise で OIDC プロバイダーを追加**：OpenManage Enterprise アプリケーション設定で、OpenID Connect プロバイダーを追加します。OpenID Connect プロバイダーを追加すると、OpenID Connect プロバイダー用の**クライアント ID** が生成されます。詳細については、「OpenManage Enterprise への OpenID Connect プロバイダーの追加 、p. 155」を参照してください。
2. **クライアント ID を使用して OpenID Connect プロバイダーを設定：**OpenID Connect プロバイダーで、クライアント ID を見つけて、**dxcua**（ユーザー認証の Dell 拡張要求）と呼ばれるスコープを追加およびマッピングして、ログイン ロール（管理者、デバイス マネージャー、または閲覧者）を定義します。詳細については、次を参照してください。
   - OpenManage Enterprise へのロール ベースのアクセスのための PingFederate での OpenID Connect プロバイダー ポリシーの設定 、p. 155
   - OpenManage Enterprise へのロール ベースのアクセスのための Keycloak での OpenID Connect プロバイダー ポリシーの設定 、p. 156

OpenManage Enterprise で OpenID Connect プロバイダーを追加すると、[アプリケーション設定] > [ユーザー] > [OpenID Connect プロバイダー] ページにリストされます。次の OIDC プロバイダーの詳細が表示されます。

- [名前] - アプライアンスに追加されたときの OpenID Connect プロバイダーの名前
- [有効] - このフィールドの「チェック」は、アプライアンスで OpenID Connect プロバイダーが有効になっていることを示します
- [検出 URI] - OpenID Connect プロバイダーの URI（統一リソース識別子）
- [登録ステータス] - 次のいずれかになります。
  - [成功] - OpenID Connect プロバイダーへの登録が成功したことを示します。
  - [失敗] - OpenID Connect プロバイダーへの登録が失敗したことを示します。「失敗」の OpenID Connect プロバイダーの登録は、有効になっている場合でも許可されません。
  - [進行中] - アプライアンスが OpenID Connect プロバイダーに登録しようとすると、このステータスが表示されます。

右ペインに、選択した OpenID Connect プロバイダーのクライアント ID、登録ステータス、検出 URI が表示されます。[詳細を表示] をクリックして、OpenID Connect プロバイダーの証明書の詳細を表示することができます。

[アプリケーション設定] > [ユーザー] > [OpenID Connect プロバイダー] ページで、次の操作を実行できます。

- OpenManage Enterprise への OpenID Connect プロバイダーの追加 、p. 155
- OpenManage Enterprise での OpenID Connect プロバイダーの詳細の編集 、p. 157
- OpenID Connect プロバイダーを使用した OpenManage Enterprise の登録ステータスのテスト 、p. 156
- OpenID Connect プロバイダーの有効化 、p. 157

- OpenID Connect プロバイダーの無効化 、p. 157
- OpenID Connect プロバイダーの削除 、p. 157

OpenManage Enterprise への OpenID Connect プロバイダーの追加

OpenID Connect プロバイダー (Keycloak または PingFederate) を追加、有効化、および登録することで、OpenManage Enterprise に対して認証済みのクライアント ログインを行うことができます。これにより、クライアント ID が生成されます。

OpenManage Enterprise に OpenID Connect プロバイダーを追加するには、[[アプリケーション設定]] > [[ユーザー]] > [[OpenID Connect プロバイダー]] ページに移動し、次の手順を実行します。

メモ: OpenID Connect プロバイダー クライアントを最大 4 つまで追加できます。

1. [[追加]] をクリックして、[新しい OpenID Connect プロバイダーの追加] ページをアクティブにします。
2. それぞれのフィールドに以下の情報を入力します。
   a. [名前] - OIDC クライアントの名前。
   b. [検出 URI] - OIDC プロバイダーの統一リソース識別子
   c. [認証タイプ] - アプライアンスへのアクセスにアクセス トークンが使用する必要がある方法を、以下から 1 つ選択します。
      i. [初期アクセス トークン] - 初期アクセス トークンを入力します
      ii. [ユーザー名とパスワード] - ユーザー名とパスワードを入力します。
   d. (オプション)[証明書の検証] チェック ボックス - このチェック ボックスを選択すると、[[参照]] をクリックして証明書を検索するか、または証明書を「破線の」ボックスにドラッグ アンド ドロップして、OIDC プロバイダーの証明書をアップロードできます。
   e. (オプション)[テスト接続] - [[URI および SSL 接続のテスト]] をクリックして、OpenID Connect プロバイダーとの接続をテストします。
      メモ: テスト接続は、ユーザー名とパスワード、または最初のアクセス トークンの詳細には依存しません。これは、テストでは指定された検出 URI の正当性を確認するだけであるからです。
   f. (オプション)[有効] チェック ボックス - このチェック ボックスを選択すると、認証済みのクライアント アクセス トークンを使用してアプライアンスにログインできます。
3. [終了] をクリックします。

新たに追加された OpenID Connect プロバイダーが、[アプリケーション設定] > [ユーザー] > [OpenID Connect プロバイダー] ページに表示され、右ペインにクライアント ID を配置することができます。

次の手順：

OpenManage Enterprise へのロール ベースのアクセスのための PingFederate での OpenID Connect プロバイダー ポリシーの設定 、p. 155

OpenManage Enterprise へのロール ベースのアクセスのための Keycloak での OpenID Connect プロバイダー ポリシーの設定 、p. 156

OpenManage Enterprise へのロール ベースのアクセスのための PingFederate での OpenID Connect プロバイダー ポリシーの設定

PingFederate を使用する OpenManage Enterprise OpenID Connect ログインを有効にするには、スコープ **dxcua**(ユーザー認証の Dell 拡張要求) をクライアント ID に追加してマッピングし、次のようにユーザー権限を定義する必要があります。

警告: OIDC プロバイダー PingFederate (PingIdentity) を使用してクライアントを再登録すると、ユーザーの役割と範囲が「デフォルト」にリセットされます。この問題により、管理者以外の役割 (DM およびビューアー) の権限と範囲が管理者の権限と範囲にリセットされる可能性があります。OIDC プロバイダーを使用したアプライアンス コンソールの再登録は、アプライアンスのアップグレード時、ネットワーク構成の変更時、SSL 証明書の変更時にトリガーされます。

前述の再登録イベントのいずれかの後のセキュリティ上の懸念を回避するために、管理者は PingFederate サイトですべての OpenManage Enterprise クライアント ID を再構成する必要があります。また、この問題が解決されるまで、PingFederate を使用している管理者ユーザーのみにクライアント ID を作成することを強くお勧めします。

メモ:

- デフォルトの割り当てアルゴリズムは RS256 (SHA-256 使用の RSA 署名) にする必要があります。

1. [OAuth 設定] の [スコープ管理] で、**dxcua** という名前の「排他的」または「デフォルト」のスコープを追加します。

2. 次の手順を実行して、[OpenID Connect ポリシー管理] > [ポリシー] で作成されたスコープをマッピングします。
   a. [トークンにユーザー情報を含める] を有効にします
   b. [属性スコープ] で、スコープと属性値を **dxcua** として追加します。
   c. [契約の履行] で、dxcua を追加し、タイプは [テキスト] として選択します。次に、以下の属性のいずれかを使用して OpenManage Enterprise OpenID Connect プロバイダー ログインのユーザー権限を定義します。
      i. 管理者：`dxcua : [{"Role": "AD"}]`
      ii. デバイス マネージャー：`dxcua : [{"Role": "DM"}]`
      メモ: OpenManage Enterprise でデバイス グループ (G1 や G2 など) を選択するためのデバイス マネージャーのアクセスを制限するには、`dxcua : [{"Role": "DM", "Entity":"G1, G2"}]` を使用します
      iii. 閲覧者：`dxcua : [{"Role": "VE"}]`
   d. OpenManage Enterprise でクライアントを登録した後に「排他的」スコープが設定されている場合は、PingFederate で設定されているクライアントを編集し、作成された「dxcua」排他的スコープを有効にします。
3. [**動的クライアント登録**] は、OpenManage Enterprise クライアント登録のために、PingFederate で有効にする必要があります。OpenID Connect プロバイダー クライアント設定で [初期アクセス トークンを要求する] オプションが選択されていない場合は、ユーザー名とパスワードを使用して登録を行います。このオプションが有効化されている場合、登録は初期アクセス トークンでのみ機能します。

OpenManage Enterprise へのロール ベースのアクセスのための Keycloak での OpenID Connect プロバイダー ポリシーの設定

Keycloak を使用する OpenManage Enterprise OpenID Connect ログインを有効にするには、まずスコープ **dxcua** をクライアント ID に追加してマッピングし、次のようにユーザー権限を定義する必要があります。

メモ: OpenID Connect プロバイダー設定ウィザードで指定された検出 URI には、プロバイダーの有効なエンドポイントが表示されている必要があります。

1. Keycloak ユーザーの [属性] セクションで、次の属性のいずれかを使用して OpenManage Enterprise ログイン ロールの「キーと値」を定義します。
   - 管理者：`dxcua : [{"Role": "AD"}]`
   - デバイス マネージャー：`dxcua : [{"Role": "DM"}]`
     メモ: OpenManage Enterprise でデバイス グループ (G1 や G2 など) を選択するためのデバイス マネージャーのアクセスを制限するには、`dxcua : [{"Role": "DM", "Entity":"G1, G2"}]` を使用します
   - 閲覧者： `dxcua : [{"Role": "VE"}]`
2. クライアントが Keycloak で登録されたら、[マッパー] セクションで、「ユーザー属性」マッパー タイプと以下の値を追加します。
   - [名前]: dxcua
   - [マッパー タイプ]: ユーザー属性
   - [ユーザー属性]: dxcua
   - [トークン要求名]: dxcua
   - [要求の Json 型]: 文字列
   - [ID トークンへの追加]: 有効
   - [アクセス トークンへの追加]: 有効
   - [ユーザー情報への追加]: 有効

OpenID Connect プロバイダーを使用した OpenManage Enterprise の登録ステータスのテスト

[[アプリケーション設定]] > [[ユーザー]] > [[OpenID Connect プロバイダー]] ページで、次の手順を実行します。

1. OpenID Connect プロバイダーを選択します。
2. 右ペインで [[登録ステータスのテスト]] をクリックします。
   メモ: テスト接続は、ユーザー名とパスワード、または最初のアクセス トークンの詳細には依存しません。これは、テストでは検出 URI の正当性を確認するだけであるからです。

OIDC プロバイダーを使用した最新の登録ステータス (「成功」または「失敗」) が更新されました。

OpenManage Enterprise での OpenID Connect プロバイダーの詳細の編集

[[アプリケーション設定]] > [[ユーザー]] > [[OpenID Connect プロバイダー]] ページで、次の手順を実行します。

1. OpenID Connect プロバイダーを選択します。
2. 右側のペインで [[編集]] をクリックします。
3. OpenID Connect プロバイダー クライアントの登録ステータスに応じて、次の操作を実行できます。
   a. 登録ステータスが「成功」の場合は、[証明書の検証]、[テスト接続]、および [有効] チェック ボックスのみを編集できます。
   b. 登録ステータスが「失敗」の場合は、[ユーザー名]、[パスワード]、[証明書の検証]、[テスト接続]、[有効] チェック ボックスを編集できます。
4. [[終了]] をクリックして変更を実装するか、[[キャンセル]] をクリックして変更を破棄します。

OpenID Connect プロバイダーの有効化

OpenID Connect プロバイダーのログインがアプライアンスに追加された時点で有効化されていない場合、ログインをアクティブ化するには、アプライアンスで「有効」にする必要があります。

[[アプリケーション設定]] > [[ユーザー]] > [[OpenID Connect プロバイダー]] ページで、次の手順を実行します。

1. OpenID Connect プロバイダーを選択します。
2. [[有効にする]] をクリックします。

OpenManage Enterprise で OpenID Connect プロバイダーを有効にすると、認証済みのクライアント アクセス トークンでアプライアンスにログインできるようになります。

OpenID Connect プロバイダーの削除

[[アプリケーション設定]] > [[ユーザー]] > [[OpenID Connect プロバイダー]] ページで、次の手順を実行します。

1. OpenID Connect プロバイダーを選択します。
2. [削除] をクリックします。

OpenID Connect プロバイダーの無効化

[[アプリケーション設定]] > [[ユーザー]] > [[OpenID Connect プロバイダー]] ページで、次の手順を実行します。

1. OpenID Connect プロバイダーを選択します。
2. [[無効にする]] をクリックします。

「無効な」OIDC プロバイダーからのクライアント アクセス トークンは、アプライアンスによって拒否されます。

セキュリティ証明書

[アプリケーションの設定セキュリティ証明書] の順にクリックすると、デバイスに対して現在利用可能な SSL 証明書についての情報を表示できます。

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。「OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15」を参照してください。

証明書署名要求 (CSR) を生成するには、「証明書署名要求を生成してダウンロードする 、p. 157」を参照してください。

証明書署名要求を生成してダウンロードする

お使いのデバイス用の証明書署名要求 (CSR) を生成し、SSL を適用するには、次の手順を実行します。

メモ: CSR の生成は、OpenManage Enterprise Appliance 内でのみ行えます。

1. [証明書署名要求の生成] をクリックします。
2. [証明書署名要求の生成] ダイアログボックスで、フィールドに情報を入力します。
3. [生成] をクリックします。
   CSR が作成され、**証明書署名要求** ダイアログボックスに表示されます。また、CSR のコピーが要求で指定された電子メールアドレスに送信されます。
4. SSL 証明書の申請中に、**証明書署名要求** ダイアログボックスで CSR データをコピーし、認証局 (CA) に送信します。
   - CSR をダウンロードするには、**証明書署名要求のダウンロード** をクリックします。
   - **終了** をクリックします。

Microsoft 証明書サービスによる OpenManage Enterprise への Web サーバー証明書の割り当て

1. OpenManage Enterprise で証明書署名要求 (CSR) を生成してダウンロードします。参照先 証明書署名要求を生成してダウンロードする 、p. 157
2. 証明書サーバー (https://x.x.x.x/certsrv) への Web セッションを開いて、[証明書を要求] リンクをクリックします。
3. [証明書を要求] ページで、[詳細証明書要求を送信] リンクをクリックします。
4. [詳細証明書要求] ページで、[Base64 エンコード 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 Base64 エンコード 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。
5. [証明書要求または更新要求の送信] ページで、次の手順を実行します。
   a. [Base64 エンコード証明書要求 (CMC または PKCS#10 ファイルまたは PKCS#7)] フィールドに、ダウンロードした CSR の内容全体をコピーして貼り付けます。
   b. [証明書テンプレート] には [**Web サーバー**] を選択します。
   c. [送信] をクリックして証明書を発行します。
6. [発行済み証明書] ページで、[Base64 エンコード] オプションを選択し、[証明書をダウンロード] リンクをクリックして証明書をダウンロードします。
7. [アプリケーション設定] > [セキュリティ] > [証明書] ページに移動し、[アップロード] をクリックして OpenManage に証明書をアップロードします。

コンソールプリファレンスの管理

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。
OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

[OpenManage Enterprise] > [アプリケーションの設定] > [コンソールプリファレンス] の順にクリックし、OpenManage Enterprise GUI のデフォルトプロパティを設定できます。たとえば、ダッシュボードのデバイスの正常性が自動的にチェックされて更新されるデフォルトの時刻や、デバイスの検出で優先的に使用される設定などです。次のオプションがあります。

1. [レポート設定]: OpenManage Enterprise のレポート上に表示できる行の最大数を設定するには、次の手順を実行します。
   a. **レポート設定** を展開します。
   b. **レポートの行数の制限** ボックスに数字を入力します。デフォルトの制限は 1,000 行に設定されていますが、許可される最大行数は 20 億です。
   c. **適用** をクリックします。ジョブが実行され、設定が適用されます。
2. [デバイスの正常性]: OpenManage Enterprise ダッシュボードのデバイスの正常性が自動的に監視およびアップデートされる必要がある時刻を設定するには、次の手順を実行します。
   a. [デバイスの正常性] を展開します。
   b. デバイスの正常性を記録してデータを保存する必要がある頻度を入力します。
   c. 次を選択します。
      - [最後の状態]: 電源接続が失われたときに、最後に記録されたデバイスの正常性を表示します。
      - [不明]: デバイスのステータスが「不明」になった際に最後に記録されたデバイスの正常性を表示します。iDRAC との接続は失われ、デバイスが OpenManage Enterprise で今後は監視されなくなると、デバイスは OpenManage Enterprise に対して「不明」となります。
   d. 変更を設定に保存するには [適用] を、デフォルトの属性にリセットするには [破棄] をクリックします。

3. [検出の設定]:[検出の設定] を展開して、[**一般的なデバイス ネーミング**] 設定と [**サーバーのデバイス ネーミング**] 設定を行います。このデバイス ネーミングは、検出した iDRAC やその他のデバイスを特定するために、OpenManage Enterprise によって使用されます。

   メモ: デバイス ネーミングで選択する一般的なデバイス ネーミングとサーバーのデバイス ネーミングの選択は独立しており、互いに影響をおよぼすことはありません。

   a. **一般的なデバイス ネーミング**は、iDRAC 以外のすべての検出デバイスに適用されます。次のネーミング モードのいずれかを選択します。
      - DNS 名を使用する場合は [DNS]。
      - NetBIOS 名を使用する場合は [Instrumentation (NetBIOS)]。

      メモ:
      - 一般的なデバイス ネーミングのデフォルト設定は [DNS] です。
      - 検出されたデバイスに、上記の設定に対応する DNS 名も NetBIOS 名も設定されていない場合は、アプライアンスは IP アドレスを使用してデバイスを特定します。
      - [一般的なデバイス ネーミング] で [Instrumentation (NetBIOS)] オプションを選択すると、シャーシ デバイスの場合、[すべてのデバイス] ページでデバイス名エントリーとしてその**シャーシ名**が表示されます。

   b. **サーバーのデバイス ネーミング**は iDRAC にのみ適用されます。検出した iDRAC に対して、次のいずれかのネーミング モードを選択します。
      - iDRAC ホスト名を使用する場合は [iDRAC ホスト名]。
      - システム ホスト名を使用する場合は [**システム ホスト名**]。

      メモ:
      - iDRAC デバイスに対するデフォルトのネーミング設定は [システム ホスト名] です。
      - iDRAC に、上記の設定に対応する iDRAC ホスト名もシステム ホスト名も設定されていない場合は、アプライアンスは IP アドレスを使用して iDRAC を特定します。

   c. 無効なデバイスのホスト名と共通の MAC アドレスを指定するには、[詳細設定] を展開します。
      i. [無効なデバイスのホスト名] に、カンマで区切って 1 つ以上の無効なホスト名を入力します。デフォルトでは、無効なデバイスのホスト名のリストが設定されます。
      ii. [共通の MAC アドレス] で、カンマで区切って共通の MAC アドレスを入力します。デフォルトでは、共通の MAC アドレスのリストが設定されます。

   d. 変更を設定に保存するには [適用] を、デフォルトの属性にリセットするには [破棄] をクリックします。

4. [サーバーから開始される検出]。次のいずれかの検出承認ポリシーを選択します。
   - [自動]: iDRAC ファームウェア バージョン 4.00.00.00 がインストールされた、コンソールと同じネットワーク上にあるサーバーを、コンソールが自動的に検出できるように設定します。
   - [手動]: サーバーをユーザーが手動で検出するように設定します。
   - 変更内容を保存するには [適用] を、デフォルトの属性にリセットするには [破棄] をクリックします。
5. [MX7000 のオンボード プリファレンス]:コンソール プリファレンスがオンボードの場合の MX7000 シャーシでのアラート転送動作を、次のうちから 1 つ指定します。
   - すべてのアラートを受信
   - 「シャーシ」カテゴリーのアラートのみを受信
6. [SMB 設定]: ネットワーク通信用に使用する必要がある Server Message Block (SMB) バージョンを、次のうちから 1 つ選択します。
   - [V1 を無効化]: SMBv1 が無効化されます。アプライアンスではこれがデフォルトで選択されています。
   - [V1 を有効化]: SMBv1 が有効化されます。

   メモ: シャーシや、iDRAC バージョン 2.50.50.50 以前が動作している PowerEdge YX2X および YX3X サーバーとの通信が必要なタスクを開始するには、事前に [SMB 設定] で SMBv1 を有効にしておく必要があります。詳細については、コンソール プリファレンスの管理 、p. 158 および Dell EMC PowerEdge サーバーの汎用命名規則 、p. 179 を参照してください。
7. [E メール送信者設定]: E メール メッセージを送信しているユーザーのアドレスを設定するには、次の手順を実行します。
   a. [送信者の E メール ID] ボックスに E メール アドレスを入力します。
   b. 変更内容を保存するには [適用] を、デフォルトの属性にリセットするには [破棄] をクリックします。
8. [トラップ転送形式]: 次の手順でトラップ転送形式を設定します。
   a. 次のオプションのいずれかを選択します。
      - [元の形式 (SNMP トラップのみ有効)]: トラップ データをそのまま保持します。
      - [正規化 (すべてのイベントに対して有効)]: トラップ データの正規化を行います。トラップ転送形式が「正規化」に設定されている場合、Syslog などの受信エージェントは、アラート転送元のデバイス IP を含むタグを受け取ります。
   b. 変更内容を保存するには [適用] を、デフォルトの属性にリセットするには [破棄] をクリックします。
9. [指標収集の設定]: PowerManager 拡張機能データのメンテナンスとパージの頻度を設定するには、次の手順を実行します。
   a. [データ パージ間隔] ボックスに、PowerManager データを削除する頻度を入力します。30～365 日の値を入力できます。

b. 変更内容を保存するには [適用] を、設定をデフォルトの属性にリセットするには [破棄] をクリックします。

ログインセキュリティのプロパティの設定

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。「OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15」を参照してください。

メモ: AD および LDAP ディレクトリユーザーをインポートし、OpenManage Enterprise の役割 (管理者、デバイス管理者、閲覧者) のいずれかを割り当てることができます。

[OpenManage Enterprise] > [アプリケーションの設定] > [セキュリティ] の順にクリックすると、[許可する IP 範囲を制限する] または [ログイン ロックアウト ポリシー] を指定することにより、OpenManage Enterprise のセキュリティを保護することができます。

- [許可する IP 範囲を制限する] を展開します。

  メモ: [許可する IP 範囲を制限する] がアプライアンスで構成されている場合、指定された範囲外のデバイスに対しては、アラートの受信、ファームウェアのアップデート、およびネットワークの識別情報など、アプライアンスへのインバウンド接続はブロックされます。ただし、アプライアンスからの接続はすべてのデバイスで機能します。

  1. OpenManage Enterprise へのアクセスを許可する必要がある IP アドレス範囲を指定するには、**IP 範囲を有効にする** チェックボックスを選択します。
  2. **IP 範囲のアドレス (CIDR)** ボックスで、IP アドレスの範囲を入力します。

     メモ: 1 つの IP 範囲のみが許可されます。
  3. **適用** をクリックします。デフォルトのプロパティにリセットするには、**破棄** をクリックします。

     メモ: 複数の IP 範囲が [IP 範囲アドレス (CIDR)] ボックスに入力されている場合、[適用] ボタンは有効になりません。
- [ログインロックアウトポリシー] を展開します。
  1. 特定のユーザー名が OpenManage Enterprise にログインすることを防止するには、[ユーザー名による] チェックボックスを選択します。
  2. 特定の IP アドレスが OpenManage Enterprise にログインすることを防止するには、[IP アドレスによる] チェックボックスを選択します。
  3. [ロックアウト失敗回数] ボックスには、OpenManage Enterprise がユーザーをログインできなくするまでの失敗した試行の数を入力します。デフォルトでは 3 回です。
  4. [ロックアウト失敗時間枠] ボックスでは、OpenManage Enterprise が失敗した試行に関する情報を表示する必要がある期間を入力します。
  5. [ロックアウトペナルティ時間] ボックスに、ユーザーが複数回失敗した後に、ログイン操作を再試行できるまでの時間の長さを入力します。
  6. [適用] をクリックします。設定をデフォルトの属性にリセットするには、[破棄] をクリックします。

アラート表示のカスタマイズ

1. [OpenManage Enterprise] > [アプリケーション設定] > [アラート] の順にクリックし、[アラート表示設定] を展開します。
2. 次のいずれか 1 つを選択します。
   a. [すべて]: 確認済みアラートと未確認アラートの両方の表示を有効にします。
   b. [未確認]: 未確認アラートの表示のみを有効にします。

      メモ: デフォルトでは、[**アラート表示設定**] は [未確認] に設定されています。

   c. [確認済み]: 確認済みアラートの表示のみを有効にします。
3. [適用] をクリックします。

   アラート表示設定の変更は、次の OpenManage Enterprise ページに影響します。
   - すべての OpenManage Enterprise ページの右上隅。OpenManage Enterprise グラフィカル ユーザー インターフェイスの概要 、p. 34 を参照してください。
   - [ダッシュボード] ページ。OpenManage Enterprise ダッシュボードを使用したデバイスの監視 、p. 36 を参照してください。
   - [デバイス] ページ。ドーナツグラフ 、p. 37 を参照してください。
   - [アラート] ページの [**アラート ログ**] テーブル。アラート ログの表示 、p. 113 を参照してください。

SMTP、SNMP、Syslog アラートの設定

[OpenManage Enterprise] > [アプリケーションの設定] > [アラート] の順にクリックすると、システム アラートを受信する E メール (SMTP) アドレス、SNMP アラートの転送先、Syslog の転送プロパティを設定できます。これらの設定を管理するには、OpenManage Enterprise 管理者レベルの資格情報が必要です。

ユーザーおよび OpenManage Enterprise 間の E メールの通信を管理する SMTP サーバーを設定し認証するには、次の手順を実行します。

メモ: OpenManage Enterprise は、内部ルート CA によって発行された証明書を持つ内部 SMTP サーバーに E メールを送信することはできません。

1. [電子メールの設定] を展開します。
2. 電子メールメッセージを送信する SMTP サーバのネットワークアドレスを入力します。
3. SMTP サーバーを認証するには、[認証を有効にする] チェック ボックスをオンにし、ユーザー名とパスワードを入力します。
4. デフォルトでは、アクセスする SMTP ポート番号は 25 です。必要に応じて編集します。
5. SMTP トランザクションを固定するには、[SSL を使用する] チェックボックスを選択します。
6. SMTP サーバーが正常に動作しているかどうかをテストするには、[テスト E メールの送信] チェック ボックスをクリックして、[E メール受信者] を入力します。
7. [適用] をクリックします。
8. 設定をデフォルトの属性にリセットするには、[破棄] をクリックします。

SNMP アラートの転送を設定するには、次の手順を実行します。

1. [SNMP アラート転送設定] を展開します。
2. 事前定義されたイベント発生時にアラートを送信する各 SNMP トラップを有効にするには、[有効] チェックボックスを選択します。
3. [送信先アドレス] ボックスに、アラートを受信すべき宛先デバイスの IP アドレスを入力します。

   メモ: コンソール IP の入力は、アラートの重複を回避するために許可されません。
4. [SNMP バージョン] メニューから、SNMP バージョン タイプを SNMPv1、SNMPv2、または SNMPv3 として選択し、次のフィールドに入力します。
   a. コミュニティ文字列 ボックスに、アラートを受信すべき宛先デバイスの SNMP コミュニティ文字列を入力します。
   b. 必要に応じてポート番号を編集します。SNMP トラップのデフォルトのポート番号は 162 です。OpenManage Enterprise でサポートされるプロトコルおよびポート 、p. 31 を参照してください。
   c. SNMPv3 が選択されている場合は、次の追加の詳細を入力します。
      i. ユーザー名：ユーザー名を入力します。
      ii. 認証タイプ：ドロップダウン リストから [SHA]、[MD_5]、または [なし] を選択します。
      iii. 認証パスフレーズ：8 文字以上の認証パスフレーズを入力します。
      iv. プライバシー タイプ：ドロップダウン リストから [DES]、[AES_128]、または [なし] を選択します。
      v. プライバシー パスフレーズ：8 文字以上のプライバシー パスフレーズを入力します。
5. SNMP メッセージをテストするには、対応するトラップの [送信] ボタンをクリックします。
6. [適用] をクリックします。設定をデフォルトの属性にリセットするには、[破棄] をクリックします。

Syslog 転送設定をアップデートするには、次の手順を実行します。

1. [Syslog 転送設定] を展開します。
2. [サーバー] 列の各サーバーのチェックボックスを選択して、Syslog 機能を有効化します。
3. [送信先アドレス/ホスト名] ボックスに、Syslog メッセージを受信するデバイスの IP アドレスを入力します。
4. UDP を使用するデフォルトのポート番号は 514 です。必要に応じてボックスから選択するか入力して編集します。OpenManage Enterprise でサポートされるプロトコルおよびポート 、p. 31 を参照してください。
5. [適用] をクリックします。
6. 設定をデフォルトの属性にリセットするには、[破棄] をクリックします。

着信アラートの管理

メモ: OpenManage Enterprise で任意のタスクを実行するには、必要なユーザー権限を持っている必要があります。OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15 を参照してください。

[OpenManage Enterprise] > [アプリケーションの設定] > [着信アラート] をクリックすると、TrapForward のプロパティを設定し、着信 SNMPv3 アラートを受信するユーザーを定義することができます。

- 着信アラートの SNMP 資格情報を設定するには、次の手順を実行します。

1. [SNMPV3 の有効化] チェックボックスを選択します。
2. [資格情報] をクリックします。
3. **SNMP 資格情報** ダイアログボックスで、次の手順を実行します。
   a. [ユーザー名] ボックスに、OpenManage Enterprise 設定を管理するユーザーのログイン ID を入力します。
   b. [認証タイプ] ドロップダウンメニューから、[SHA] または [MD_5] アルゴリズムを認証タイプとして選択します。
   c. [認証パスフレーズ] ボックスに、選択した内容に基づいて SHA または MD_5 に関連するパスフレーズを入力します。
   d. [プライバシータイプ] ドロップダウンメニューから、DES または AES_128 のいずれかを暗号化標準として選択します。
   e. [プライバシーパスフレーズ] ボックスに、プライバシータイプに基づいてパスフレーズを入力します。
   f. [保存] をクリックします。
4. [コミュニティ] ボックスには、SNMP トラップを受信するコミュニティ文字列を入力します。
5. デフォルトでは、着信トラップの SNMP ポート番号は 162 です。ポート番号を変更するには編集します。
6. [適用] をクリックします。
   SNMP 資格情報と設定が保存されます。
7. 設定をデフォルトの属性にリセットするには、[破棄] をクリックします。

   メモ: アプライアンスをアップグレードする前に SNMPv3 アラートを引き続き受信するには、ユーザー名、認証パスフレーズ、プライバシー パスフレーズを入力して再設定を行う必要があります。問題が解決しない場合は、テキスト ユーザー インターフェイス (TUI) を使用してサービスを再起動します。

8. [適用] をクリックして変更を保存するか、[破棄] をクリックしてキャンセルに設定し直します。

SNMP 資格情報の設定

1. [資格情報] をクリックします。
2. [SNMP 資格情報] ダイアログボックスで、次の手順を実行します。
   a. [ユーザー名] ボックスに、OpenManage Enterprise 設定を管理するユーザーのログイン ID を入力します。
   b. [認証タイプ] ドロップダウンメニューから、認証タイプとして [SHA] または [MD_5] アルゴリズムを選択します。
   c. [認証パスフレーズ] ボックスに、選択した内容に基づいて SHA または MD_5 に関連するパスフレーズを入力します。
   d. [プライバシータイプ] ドロップダウンメニューから、暗号化標準として DES または AES_128 を選択します。
   e. [プライバシーパスフレーズ] ボックスに、プライバシータイプに基づいてパスフレーズを入力します。
3. [保存] をクリックします。

保証設定の管理

[保証の設定] で、ホーム ページの [アラート] ウィジェット、全ページにまたがるスコアボード、[保証] ページ、レポートに、OpenManage Enterprise が表示する保証統計情報を設定します。

保証の設定を変更するには、次の手順を実行します。

1. [OpenManage Enterprise] > [アプリケーションの設定] > [保証] の順にクリックします。
2. [保証の設定] をクリックして、ダイアログ ボックスを開きます。
3. [保証期限が切れる前に警告の表示を開始する日数] ボックスに、日数を入力します。0 ~ 1000 (両端を含む) の値が入力できます。デフォルトでは 90 日に設定されています。保証期間終了が近づくと、この設定に基づいて、「⚠」とレポートとウィジェットに表示されます。
4. [期限切れの保証の非表示] オプションから、以下のいずれかを選択できます。
   a. [すべて]: すべての期限切れの「初期」保証と「延長」保証の表示を非表示にします。
   b. [初期のみ]: 期限切れの「初期」保証のみを非表示にします。
   c. [なし]: すべての期限切れの保証を表示します。
5. [適用] または [破棄] をクリックして、保証の設定を保存するか、変更を破棄して古い設定を残します。

OpenManage Enterprise のバージョンと使用可能なプラグインの確認とアップデート

[コンソールとプラグイン] ページでは、OpenManage Enterprise のバージョンを確認およびアップデートし、プラグインをインストールおよびアップデートすることができます。[コンソールとプラグイン] ページに移動するには、[アプリケーションの設定] > [コンソールとプラグイン] をクリックします。

[コンソールとプラグイン] ページでは、次の操作を実行できます。

- お使いの OpenManage Enterprise の現在のバージョンを表示し、アップデートが利用可能かどうかを確認してから、新しいバージョンにアップグレードします。[アップデート設定] ボタンをクリックすると、次の操作を実行できます。
  - 自動または手動でアップデートを確認することを選択します。
  - アプライアンスをアップデートする Dell.com (オンライン) またはネットワーク共有 (オフライン) モードから選択します。

    Dell.com またはネットワーク共有からのアップグレードに関する詳細については、「オンライン方式を使用した OpenManage Enterprise の構成とアップグレード 、p. 164」または「ネットワーク共有を使用して OpenManage Enterprise を構成し、オフライン アップグレードを実行する 、p. 165」を参照してください。
- インストールするプラグインの [インストール] をクリックして、アプライアンスの機能を強化します。プラグインのインストールの詳細については、「プラグイン」を参照してください。

  メモ:
  - プラグインをインストール後に完全に機能させるには、OpenManage Enterprise Advanced ライセンスが必要です。プラグインの詳細については、Dell サポート サイトで入手可能な各マニュアルを参照してください。
  - OpenManage Enterprise のプラグインをインストールすると、アプライアンス サービスが再起動します。
- すでにインストールされているプラグインを使用して、次の操作を実行できます。
  - プラグインを無効にします。参照先： プラグインの無効化 、p. 167
  - プラグインを有効にします。参照先： プラグインの有効化 、p. 168
  - プラグインをアンインストールします。参照先： プラグインのアンインストール 、p. 168

アップグレードの推奨事項と前提条件

管理者は、最新バージョンにアップデートする前に、次の点を考慮する必要があります。

- 予期しない何らかの問題が発生する場合のバックアップとして、コンソールの VM スナップショットを取ります。必要に応じて、余分のダウンタイムの時間を確保してください。
- アップデートプロセスには少なくとも 1 時間を割り当てます。低速なネットワーク接続でアップデートをダウンロードしなければならない場合は、時間を余分に確保してください。
- デバイス構成、導入、または拡張 (プラグイン) タスクが実行中でないこと、あるいは計画ダウンタイム中に実行するようにスケジュールが設定されていないことを確認してください。アクティブまたはスケジュールされたタスクまたはポリシーは、更新中に追加の警告なしで終了します。
- 差し迫ったスケジュールされたアップデートについてその他のコンソールユーザーに通知します。
- アップグレードが失敗した場合、アプライアンスが再起動します。VM スナップショットを元に戻して、再度アップグレードすることをお勧めします。

メモ:
- [自動] > [オンライン] を使用して OpenManage Enterprise バージョン 3.7 に直接アップデートできるのは、3.5 以降の OpenManage Enterprise バージョンのみです。
- バージョン 3.4 より前の OpenManage Enterprise のバージョン (たとえば、バージョン 3.3.x、バージョン 3.2) については、3.7 へのアップグレードを検討する前に、まずバージョン 3.4 に、次にバージョン 3.5 にアップデートする必要があります。
- OpenManage Enterprise — Tech Release バージョンをまず OpenManage Enterprise バージョン 3.0 または 3.1 にアップグレードする必要があります。
- デバイス検出数が 8000 台を超えている OpenManage Enterprise をアップデートする場合、アップデート タスクの完了までに 2 ~ 3 時間かかります。その間は、サービスが応答しなくなる場合があります。完了したら、アプライアンスを正常に再起動することをお勧めします。再起動後は、アプライアンスの通常の機能が回復します。
- 2 番目のネットワーク インターフェイスの追加は、コンソールのアップグレード後のタスクが完了してから行うようにしてください。アップグレード後タスクの進行中に 2 番目の NIC を追加しようとしても効果はありません。

- アプライアンスのアップデート後はすぐにログインできます。インベントリー全体が検出されるまで待つ必要はありません。アップデート後、検出タスクがバックグラウンドで実行され、進行状況を随時確認できます。
- [**アップデート**] をクリックすると、アップグレード バンドルのダウンロード ジョブが開始されます。このジョブは、すべてのアップデート ファイルがダウンロードされた後に自動的に終了し、ユーザーが終了することはできません。
- OpenManage Enterprise をバージョン 3.7 にアップグレードした後、移行されたデバイス マネージャー ユーザーは無制限の範囲を持ち、デフォルトですべてのデバイスにアクセスできます。必要に応じて、管理者は SBAC 機能を使用してスコープを割り当てることができます。SBAC 機能の詳細については、「OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15」を参照してください。

オンライン方式を使用した OpenManage Enterprise の構成とアップグレード

既存の OpenManage Enterprise は、Dell.com (https://downloads.dell.com/openmanage_enterprise) からオンラインで、自動または手動でアップグレードできます。

- アップグレードを実行するには、Administrator 権限が必要です。権限の詳細については、「OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15」を参照してください。
- OpenManage Enterprise アプライアンスから Dell.com および予定されたアップデートへのアクセスが可能であることの確認が必要です。

OpenManage Enterprise のアップグレードは、2 ステップのプロセスです。まず、オンライン アップデート用のアプライアンスの構成 、p. 164 して、アップデートの取得方法とアップデート方法を指定します。次に、[コンソールとプラグイン] ページから、オンライン方式を使用した OpenManage Enterprise のアップグレード 、p. 164 します。アップデート設定の構成は、1 回限りのプロセスです。アップデート設定が構成されたら、[アップデート] セクションの [更新] アイコンをクリックして、アップデートされたバージョンをダウンロードできるかどうかを確認できます。

オンライン アップデート用のアプライアンスの構成

1. [アプリケーションの設定] > [コンソールと拡張機能] > [アップデート設定] をクリックします。
2. [アップデートのチェック方法] で、次のいずれかのオプションを選択します。
   - [[自動]]: アプライアンスによる利用可能なアップデートの確認が、[[アップデートのチェック先]] に指定されたソースに対し、毎週月曜日に自動的に実施されます。
   - [手動]: ユーザーは、[コンソールとプラグイン] ページの [アップデート] セクションにある [更新リスト] アイコンをクリックして、[アップデートのチェック先] で指定されたソースからアップデートの可用性を手動で確認する必要があります。
3. [アップデートのチェック先] で、[dell.com] を選択して、アプライアンスがアップデートをチェックする場所を指定します。
4. オプション: [ダウンロードが完了したら自動的にコンソールのアップデートを開始する] チェック ボックスを選択しておくと、アップデート パッケージのダウンロードが完了すると即座にコンソール アップデートのインストールが開始されます。それ以外の場合、アップデートは手動で開始できます。
5. [適用] をクリックします。

   アプライアンスは、https://downloads.dell.com/openmanage_enterprise から直接アップデートをチェックします。

オンライン方式を使用してアプライアンスをアップデートします。

オンライン方式を使用した OpenManage Enterprise のアップグレード

Dell.com からアップデートを開始する前に、次のことを確認してください。

- アップデート設定がオンライン アップデート用に構成されていることを確認します。オンライン方式を使用した OpenManage Enterprise の構成とアップグレード 、p. 164 を参照してください。
- 「アップグレードの推奨事項と前提条件 、p. 163」に記載されているように、すべてのアップグレードの前提条件と推奨事項を確認してください。
- 予期しない何らかの問題が発生する場合のバックアップとして、コンソールの VM スナップショットを必ず作成してください。必要に応じて、余分のダウンタイムの時間を確保してください。

1. アプライアンスによる利用可能なアップデートの確認や、新バージョンが利用可能な場合のバナーによる新規アップグレード バージョンに関する情報表示は、アップデートの設定に基づいて実施されます。バナーに対して管理者は、通知を閉じるか、後で通知させるかを選択でき、また [今すぐ表示] をクリックすれば、[アプリケーションの設定] > [コンソールとプラグイ

ン] ページで利用可能なアップデートのバージョンとサイズなどの詳細を確認できます。[コンソールとプラグイン] ページの [OpenManage Enterprise] セクションには、利用可能なアップデートでのすべての新機能および機能拡張が表示されます。

2. [アップデート] をクリックし、[コンソールのダウンロード] をクリックして、指定したソースからパッケージをダウンロードします。

メモ:
- [アップデート] をクリックすると、アップグレード バンドルのダウンロード ジョブが開始されます。このジョブは、すべてのアップデート ファイルがダウンロードされた後に自動的に終了し、ユーザーの操作で終了することはできません。
- アップグレードが失敗した場合、アプライアンスが再起動します。VM スナップショットを元に戻して、再度アップグレードすることをお勧めします。

3. [アップデート設定] で、[ダウンロードが完了したら自動的にコンソールのアップデートを開始する] チェック ボックスが選択されている場合、アップデート パッケージのダウンロード後にアップグレードが自動的に開始されます。それ以外の場合は、[コンソールのアップデート] をクリックしてアップデートを実行します。

ネットワーク共有を使用して OpenManage Enterprise を構成し、オフライン アップグレードを実行する

Dell.com に自動接続されない場合は、ローカル ネットワーク共有を設定して、アップデート パッケージを手動でダウンロードしてください。手動でアップデートを検索するたびに監査ログが作成されます。

ネットワーク共有からアップデートを開始する前に、次の手順を実行します。

- アップグレードを実行するには、Administrator 権限が必要です。権限の詳細については、「OpenManage Enterprise のロール ベースと範囲ベースのアクセス制御 、p. 15」を参照してください。
- 「アップグレードの推奨事項と前提条件 、p. 163」に記載されている一般的なアップグレードの推奨事項と前提条件を必ず読んでください。
- オフライン アップデート (ネットワーク共有) の場合、管理者は最小限または完全なアップグレードが必要かどうかに応じて適切なフォルダー構造を作成し、該当するファイルを https://downloads.dell.com からダウンロードしてネットワーク共有に保存する必要があります。OpenManage Enterprise の最新バージョンへのアップデートおよびアップデートで許容されるフォルダー構造の詳細については、サポート サイトにあるテクニカル ホワイト ペーパー『Dell EMC OpenManage Enterprise アプライアンス バージョンのアップグレード』(https://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/dell-openmanage-enterprise-v321_white-papers10_en-us.pdf) を参照してください。
- 予期しない何らかの問題が発生する場合のバックアップとして、コンソールの VM スナップショットを取ります。(必要に応じて、ダウンタイムの時間を余分に確保してください。)
- アップグレードが失敗した場合、アプライアンスが再起動します。VM スナップショットを元に戻して、再度アップグレードすることをお勧めします。
- 2 番目のネットワーク インターフェイスの追加は、コンソールのアップグレード後のタスクが完了してから行うようにしてください。アップグレード後タスクの進行中に 2 番目の NIC を追加しようとしても効果はありません。
- HTTPS 方式でアップデートする場合は、セキュリティ証明書に信頼されたサードパーティの認証局による署名がされていることを確認する必要があります。

メモ:
- バージョン 3.4 より前の OpenManage Enterprise のバージョン (たとえば、バージョン 3.3x、バージョン 3.2) については、共有されたネットワーク ファイル共有 (NFS) を介した 3.7 へのアップグレードを検討する前に、まずバージョン 3.4 に、次にバージョン 3.5 にアップデートする必要があります。
- OpenManage Enterprise—Tech Release バージョンからの直接のアップデートはサポートされていません。Tech Release バージョンをまず OpenManage Enterprise バージョン 3.0 または 3.1 にアップグレードする必要があります。
- 拡張機能/プラグインがインストールされていないバージョン (3.1 や 3.2 など) を手動でアップグレードするためにローカル共有を更新すると、監査ログに「ファイルが存在しないため拡張機能カタログ タイプのソース ファイルを取得できません」および「拡張機能カタログのダウンロードのステータスは「失敗」です」などの警告エントリーが表示されます。これらのエラー メッセージは、アップグレード プロセスに機能的な影響を与えることはなく、無視してかまいません。

ネットワーク共有からの OpenManage Enterprise のアップグレードは、2 ステップのプロセスです。まず、ネットワーク共有からアップデートするようにアプライアンスを構成する 、p. 166 して、アップデートの取得方法とアップデート方法を指定します。次に、[コンソールとプラグイン] ページから、ネットワーク共有からのアプライアンスのアップデート 、p. 166 します。

ネットワーク共有からアップデートするようにアプライアンスを構成する

1. 該当ファイルを https://downloads.dell.com からダウンロードし、コンソールがアクセス可能な同じフォルダ構造にしてネットワーク共有に保存します。

   OpenManage Enterprise の最新バージョンへのアップデートおよびアップデートで許容されるフォルダー構造の詳細については、サポート サイトにあるテクニカル ホワイト ペーパー『Dell EMC OpenManage Enterprise アプライアンス バージョンのアップグレード』(https://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/dell-openmanage-enterprise-v321_white-papers10_en-us.pdf) を参照してください。
2. [アプリケーションの設定] > [コンソールと拡張機能] > [アップデート設定] をクリックします。
3. [アップデートのチェック方法] で、次のいずれかのオプションを選択します。
   - [[自動]]: アプライアンスによる利用可能なアップデートの確認が、[[アップデートのチェック先]] に指定されたソースに対し、毎週月曜日に自動的に実施されます。
   - [手動]: ユーザーは、[コンソールとプラグイン] ページの [アップデート] セクションにある [更新リスト] アイコンをクリックして、[アップデートのチェック先] で指定されたソースからアップデートの可用性を手動で確認する必要があります。
4. [アップデートのチェック先] で、[ネットワーク共有] オプションを選択して、アプライアンスがアップデートをチェックする場所を指定します。
   a. [ローカル パス] で、ダウンロードしたファイルを含む NFS、HTTP、または HTTPS パスを指定します。ネットワーク共有の形式は、`nfs://<IP Address>/<Folder_Name>`, `http://<IP Address>/<Folder_Name>`, or `https://<IP Address>/<Folder_Name>`です。
   b. 指定したネットワーク共有への接続を確認するには、[今すぐテスト] をクリックします。
5. オプション: [ダウンロードが完了したら自動的にコンソールのアップデートを開始する] チェック ボックスを選択しておくと、アップデート パッケージのダウンロードが完了すると即座にコンソール アップデートのインストールが開始されます。それ以外の場合、アップデートは手動で開始できます。
6. [適用] をクリックします。

ネットワーク共有からのアプライアンスのアップデート

- 「アップグレードの推奨事項と前提条件 、p. 163」に記載されている前提条件と推奨事項を必ず読んでください。
- ネットワーク共有からのアップデート用に、アップデート設定が構成されていることを確認します。「*ネットワーク共有からアップデートするようにアプライアンスを構成する*」を参照してください。

1. アプライアンスによる利用可能なアップデートの確認や、新バージョンが利用可能な場合のバナーによる新規アップグレードバージョンに関する情報表示は、アップデートの設定に基づいて実施されます。バナーに対して管理者は、通知を閉じるか、後で通知させるかを選択でき、また [今すぐ表示] をクリックすれば、[アプリケーションの設定] > [コンソールとプラグイン] ページで利用可能なアップデートのバージョンとサイズなどの詳細を確認できます。[コンソールとプラグイン] ページの [OpenManage Enterprise] セクションには、利用可能なアップデートでのすべての新機能および機能拡張が表示されます。
2. [アップデート] をクリックし、[コンソールのダウンロード] をクリックして、指定したソースからパッケージをダウンロードします。

   メモ:
   - [アップデート] をクリックすると、アップグレード バンドルのダウンロード ジョブが開始されます。このジョブは、すべてのアップデート ファイルがダウンロードされた後に自動的に終了し、ユーザーの操作で終了することはできません。
   - アップグレードのダウンロード時にプロキシ経由の接続に問題が発生する場合は、プロキシ設定のチェックを外してダウンロードしてください。
3. [アップデート設定] で [ダウンロードが完了したら自動的にコンソールのアップデートを開始する] チェック ボックスが選択されている場合、アップデート パッケージのダウンロード後にアップグレードが自動的に開始されます。それ以外の場合は、[コンソールのアップデート] をクリックしてアップデートを実行します。

アップデート後にログインし、製品が想定どおりに機能することを確認します。アップデートに関連した警告やエラーがないか、監査ログを確認します。エラーがある場合は、監査ログをエクスポートして、テクニカルサポート用に保存します。

アプライアンスのアップデート後：

- ブラウザのキャッシュをクリアします。ブラウザのキャッシュをクリアしないと、アップデート後に新しいタスクが失敗する可能性があります。
- OpenManage Enterprise バージョン 3.1 からアップグレードする場合は、パフォーマンスの向上のため、Active Directory グループを再構成またはインポートすることをお勧めします。

- アプライアンスのアップデート後はすぐにログインできます。インベントリー全体が検出されるまで待つ必要はありません。アップデート後、検出タスクがバックグラウンドで実行され、進行状況を随時確認できます。

プラグインのインストール

お客様の要件に基づいて CloudIQ、Power Manager、OpenManage Enterprise Services (旧 SupportAssist-Enterprise)、Update Manager プラグインをインストールし、OpenManage Enterprise の機能を強化できます。

- OpenManage Enterprise プラグインを Dell.com からインストールするには、OpenManage Enterprise アプライアンスが downloads.dell.com にアクセスできることを確認してください。
- ローカル ネットワーク共有から OpenManage Enterprise プラグインをインストールする場合、手動でパッケージをネットワーク共有にダウンロードし、OpenManage Enterprise の [アップデートの設定] ページで場所をアップデートする必要があります。

アップデートの設定の構成の詳細については、OpenManage Enterprise のバージョンと使用可能なプラグインの確認とアップデート 、p. 163 を参照してください。

メモ: OpenManage Enterprise のプラグインをインストールすると、アプライアンス サービスが再起動します。

プラグインをインストールするには、次の手順を実行します。

1. OpenManage Enterprise で、[アプリケーションの設定] > [コンソールとプラグイン] の順にクリックします
   [コンソールとプラグイン] ページが表示されます。
2. [プラグイン] セクションで、インストールするプラグインの [インストール] をクリックします。
   [プラグインのインストール] ウィザードが表示されます。
3. [使用可能なバージョン] リストから、インストールするバージョンを選択します。
4. [前提条件] セクションで説明されている前提条件のリストを確認し、満たしていることを確認し、[プラグインのダウンロード] をクリックします。

   メモ: インストールするプラグインのバージョンを選択すると、動作条件のリストが変更されます。

   インストール操作では、プラグインをインストールするための前提条件が検証されます。インストールの前提条件が満たされていない場合、エラー メッセージが表示されます。

   プラグインが正常にダウンロードされると、プラグインの上部に表示されるステータスが、[使用可能] から [ダウンロード済み] に変わります。
5. OpenManage Enterprise プラグインをインストールするには、[プラグインのインストール] ウィザードで、[プラグインのインストール] をクリックします。
6. 同意フォームが表示され、エンド ユーザー ライセンス契約 (EULA) について通知されます。[同意] をクリックして、プラグインのインストールを続行します。
   OpenManage Enterprise にログインしているユーザー数、進行中のタスク、およびスケジュール ジョブの詳細が [確認] ダイアログ ボックスに表示されます。
7. インストールを確認するには、[プラグイン アクションを実行する前に OpenManage Enterprise アプライアンスのスナップショットを取得したことに同意する] オプションを選択し、[インストールの確認] をクリックします。
   インストール操作のステータスが表示されます。プラグインのインストールが正常に完了すると、[プラグイン] セクションの上部に表示されるステータスが、[使用可能] または [ダウンロード済み] から [インストール済み] に変わります。

プラグインの無効化

OpenManage Enterprise でプラグインのすべての機能を無効にします。

メモ: OpenManage Enterprise のプラグインを無効にすると、アプライアンス サービスが再起動します。

1. OpenManage Enterprise で、[アプリケーションの設定] > [コンソールとプラグイン] をクリックします。
   [コンソールとプラグイン] タブが表示されます。
2. [プラグイン] セクションで、無効にするプラグインで [無効化] をクリックします。
   [プラグインの無効化] ウィザードが表示されます。
3. プラグインを無効にするには、[プラグインの無効化] をクリックします。
   OpenManage Enterprise にログインしているユーザー数、進行中のタスク、およびスケジュール ジョブの詳細が [確認] ダイアログ ボックスに表示されます。
4. 確認するには、[プラグイン アクションを実行する前に、OpenManage Enterprise アプライアンスのスナップショットを取得したことに同意する] オプションを選択してから、[無効化の確認] をクリックします。

メモ: プラグインを無効にした後は、OpenManage Enterprise でプラグインに関連する情報またはページを表示できなくなります。

プラグインのアンインストール

プラグインによって収集されたすべてのデータをアンインストールし、削除します。

1. OpenManage Enterprise で、[アプリケーションの設定] > [コンソールとプラグイン] をクリックします。
   [コンソールとプラグイン] タブが表示されます。
2. [プラグイン] セクションで、アンインストールするプラグインで [アンインストール] をクリックします。
   [プラグインのアンインストール] ウィザードが表示されます。
3. OpenManage Enterprise からプラグインをアンインストールするには、[プラグインのアンインストール] をクリックします。
   OpenManage Enterprise にログインしているユーザー数、進行中のタスク、およびスケジュール ジョブの詳細が [確認] ダイアログ ボックスに表示されます。
4. アンインストールを確認するには、[プラグイン アクションを実行する前に OpenManage Enterprise アプライアンスのスナップショットを取得したことに同意する] オプションを選択し、[アンインストールの確認] をクリックします。

プラグインに関連づけられているすべての機能とデータがアンインストールされます。

プラグインの有効化

すべてのプラグイン ページが OpenManage Enterprise に表示され、OpenManage Enterprise でプラグイン機能が有効になります。

メモ: OpenManage Enterprise のプラグインを有効にすると、アプライアンス サービスが再起動します。

1. OpenManage Enterprise で、[アプリケーションの設定] > [コンソールとプラグイン] をクリックします。
   [コンソールとプラグイン] タブが表示されます。
2. [プラグイン] セクションで、有効にするプラグインに対して [有効化] をクリックします。
   [プラグインの有効化] ウィザードが表示されます。
3. プラグインを有効にするには、[プラグインの有効化] をクリックします。
   OpenManage Enterprise にログインしているユーザー数、進行中のタスク、およびスケジュール ジョブの詳細が [確認] ダイアログ ボックスに表示されます。
4. 確認するには、[プラグイン アクションを実行する前に、OpenManage Enterprise アプライアンスのスナップショットを取得したことに同意する] オプションを選択してから、[有効化の確認] をクリックします。

プラグインのアップデート

アプライアンスは、アップデートの設定に基づいて、インストールされたプラグインのアップデートの有無をチェックします。新しいバージョンが使用可能な場合は、新しいアップグレード バージョン情報が記載されたバナーが表示されます。バナーに対して管理者は、通知を閉じるか、後で通知させるかを選択でき、また [今すぐ表示] をクリックすれば、[アプリケーションの設定] > [コンソールとプラグイン] ページで利用可能なアップデートのバージョンとサイズなどの詳細を確認できます。[コンソールとプラグイン] ページの [プラグイン] セクションには、利用可能なプラグイン アップデートでのすべての新機能および機能拡張が表示されます。

プラグインをアップデートする前に、OpenManage Enterprise のバージョンと使用可能なプラグインの確認とアップデート 、p. 163 の説明に従って、アップデートの設定が構成されていることを確認します。

プラグインをアップデートするには、次の手順を実行します。

1. [プラグイン] セクションで、アップデートするプラグインに対して [利用可能なアップデート] をクリックします。
   [プラグインのアップデート] ページが表示されます。
2. プラグインのバージョンを選択し、[プラグインのダウンロード] をクリックします。
   プラグインがダウンロードされ、ダウンロードのステータスが緑色のバーに表示されます。
3. プラグインをアップデートするには、[プラグインのアップデート] をクリックします。
   [確認] ウィンドウで、[プラグイン アクションの実行前に OpenManage Enterprise アプライアンスのスナップショットをキャプチャしたことに同意します] オプションを選択し、[アップデート] をクリックします。

アップデート操作が完了すると、バージョンが [プラグイン] セクションに表示されます。

リモートコマンドとスクリプトの実行

SNMP トラップを取得すると、OpenManage Enterprise でスクリプトを実行できます。これにより、アラート管理用にサード パーティーのチケット システムでチケットを開くポリシーが設定されます。最大 **4 つ**のリモート コマンドを作成して保存できます。

メモ: 次の特殊文字は、RACADM および IPMI の CLI パラメーターとしての使用はサポートされていません：**[**、**;**、**|**、**$**、**>**、**<**、**&**、**'**、**]**、**.**、*****、**'**。

1. [アプリケーションの設定] > [スクリプトの実行] の順にクリックします。
2. [リモート コマンドの設定] セクションで、次の手順を実行します。
   a. リモート コマンドを追加するには [作成] をクリックします。
   b. [コマンド名] ボックスにコマンド名を入力します。
   c. 次のいずれかのコマンド タイプを選択します。
      i. スクリプト
      ii. RACADM
      iii. IPMI ツール
   d. [スクリプト] を選択した場合は、次の手順を実行します。
      i. [IP アドレス] ボックスに IP アドレスを入力します。
      ii. 認証方法として、[パスワード] または [SSH キー] を選択します。
      iii. [ユーザー名] および [パスワード] または [SSH キー] を入力します。
      iv. [コマンド] ボックスにコマンドを入力します。
         - コマンドは 100 個まで入力でき、それぞれ改行して入力します。
         - スクリプトではトークンの代用が可能です。参照先： リモート スクリプトおよびアラート ポリシーでのトークン代用 、p. 176
      v. [終了] をクリックします。
   e. [RACADM] を選択した場合は、次の手順を実行します。
      i. [コマンド名] ボックスにコマンド名を入力します。
      ii. [コマンド] ボックスにコマンドを入力します。コマンドは 100 個まで入力でき、それぞれ改行して入力します。
      iii. [終了] をクリックします。
   f. [IPMI ツール] を選択した場合は、次の手順を実行します。
      i. [コマンド名] ボックスにコマンド名を入力します。
      ii. [コマンド] ボックスにコマンドを入力します。コマンドは 100 個まで入力でき、それぞれ改行して入力します。
      iii. [終了] をクリックします。
3. リモート コマンドの設定を編集するには、コマンドを選択して [編集] をクリックします。
4. リモート コマンドの設定を削除するには、コマンドを選択して [削除] をクリックします。

OpenManage Mobile の設定

OpenManage Mobile (OMM) は、お使いの Android を使用して、1 つ、または複数の OpenManage Enterprise 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。OMM を使用すると、次のことができます。

- OpenManage Enterprise コンソール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。
- サーバ電源のオン / オフ、またはサーバの再起動。

プッシュ通知は、すべてのアラートと重要アラートに対してデフォルトで有効になっています。この章では、OpenManage Enterprise で設定可能な OMM の設定について説明しています。また、OMM のトラブルシューティングの際に必要な情報についても紹介しています。

メモ: OMM のインストールと使用についての情報は、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。

関連タスク

OpenManage Mobile 用アラート通知の有効化または無効化 、p. 170
OpenManage Mobile サブスクライバーの有効化または無効化 、p. 170
OpenManage Mobile サブスクライバーの削除 、p. 171

アラート通知サービスステータスの表示 、p. 171
OpenManage Mobile のトラブルシューティング 、p. 172

関連情報

OpenManage Mobile 用アラート通知の有効化または無効化 、p. 170
OpenManage Mobile サブスクライバーの有効化または無効化 、p. 170
OpenManage Mobile のトラブルシューティング 、p. 172

OpenManage Mobile 用アラート通知の有効化または無効化

OpenManage Enterprise は、デフォルトで OpenManage Mobile アプリケーションに警告通知を送信するように設定されています。ただし、OpenManage Enterprise からアラート通知が送信されるのは、OpenManage Mobile ユーザーが OpenManage Enterprise を OpenManage Mobile アプリケーションに追加した場合のみです。

メモ: OpenManage Mobile 用のアラート通知の有効化または無効化には、管理者権限が必要です。

メモ: OpenManage Enterprise による OpenManage Mobile へのアラート通知の送信のため、OpenManage Enterprise サーバにアウトバウンド（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。

OpenManage Enterprise から OpenManage Mobile に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 Enterprise] > [アプリケーションの設定] > [Mobile] の順にクリックします。
2. [プッシュ通知を有効にする] チェックボックスを選択します。
3. [適用] をクリックします。

関連タスク

OpenManage Mobile の設定 、p. 169

関連情報

OpenManage Mobile の設定 、p. 169
OpenManage Mobile サブスクライバーの削除 、p. 171

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、管理者権限が必要です。
- OpenManage Mobile 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は、デバイスが恒久的に到達不可能であることを示している場合は、 OpenManage Enterprise によって自動的に無効があります。
- 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 Enterprise] > [アプリケーションの設定] > [Mobile] の順にクリックします。
2. 有効にするには、対応するチェックボックスを選択して、**有効にする** をクリックします。無効にするには、チェックボックスを選択し、**無効にする** をクリックします。
   複数のサブスクライブを一度に選択することができます。

関連タスク

OpenManage Mobile の設定 、p. 169

関連情報

OpenManage Mobile の設定 、p. 169
OpenManage Mobile サブスクライバーの削除 、p. 171

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、サブスクライバリストからユーザーが削除され、ユーザーによる OpenManage Enterprise 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管理者権限が必要です。

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 Enterprise] > [アプリケーションの設定] > [Mobile] の順にクリックします。
2. 対象のサブスクライバー名に対応するチェックボックスを選択し、[削除] をクリックします。
3. 確認のメッセージが表示されたら、[はい] をクリックします。

関連タスク

OpenManage Mobile 用アラート通知の有効化または無効化 、p. 170
OpenManage Mobile サブスクライバーの有効化または無効化 、p. 170
OpenManage Mobile サブスクライバーの削除 、p. 171
アラート通知サービスステータスの表示 、p. 171

関連情報

OpenManage Mobile の設定 、p. 169
OpenManage Mobile サブスクライバーの削除 、p. 171

アラート通知サービスステータスの表示

OpenManage Enterprise 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、[アプリケーションの設定] > [Mobile] をクリックします。

関連タスク

アラート通知サービスステータスの表示 、p. 171

関連情報

OpenManage Mobile の設定 、p. 169
OpenManage Mobile サブスクライバーの削除 、p. 171
アラート通知サービスステータスの表示 、p. 171

通知サービスステータス

次の表は、[アプリケーションの設定] > [Mobile] で、ページに表示される [通知サービスのステータス] に関する情報の表です。

表 29. 通知サービスステータス

ステータスアイコン	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

表 29. 通知サービスステータス（続き）

ステータスアイコン	ステータスの説明
	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 サブスクライバーに関する情報の表示

OpenManage Mobile ユーザーが OpenManage Enterprise を正常に追加すると、そのユーザーは OpenManage Enterprise の［Mobile サブスクライバ］表に追加されます。Mobile サブスクライバー情報を表示するには、OpenManage Enterprise で、［アプリケーションの設定］>［Mobile］の順にクリックします。

［エクスポート］ドロップダウンリストを使用して、Mobile サブスクライバーに関する情報を .CSV ファイルにエクスポートすることもできます。

OpenManage Mobile サブスクライバー情報

次の表は、［アプリケーションの設定］>［Mobile］でページに表示される［Mobile サブスクライバー］の説明の表です。

表 30. OpenManage Mobile サブスクライバー情報

フィールド	説明
［有効］	チェックボックスを選択するかクリアして、**有効にする** または **無効にする** をそれぞれクリックし、OpenManage Mobile サブスクライバに対するアラート通知を有効または無効にします。
［ステータス］	OpenManage Enterprise 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、サブスクライバのステータスを表示します。
［ステータスメッセージ］	ステータスメッセージのステータスの説明。
［ユーザー名］	OpenManage Mobile ユーザーの名前です。
［デバイス ID］	モバイルデバイスの一意の識別子です。
［説明］	携帯電話についての説明。
［フィルタ］	フィルタはサブスクライバがアラート通知のために設定したポリシーです。
［最後のエラー］	OpenManage Mobile ユーザーへのアラート通知の送信時に発生した最後のエラーの日付と時刻。
［最後のプッシュ］	OpenManage Enterprise 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。
［最後の接続］	ユーザーが最後に OpenManage Mobile 経由で OpenManage Enterprise にアクセスした日付と時間。
［登録］	ユーザーが OpenManage Mobile に OpenManage Enterprise を追加した日付と時間。

OpenManage Mobile のトラブルシューティング

OpenManage Enterprise 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 31. OpenManage Mobile のトラブルシューティング

問題	理由	解像度
OpenManage Enterprise 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。	Web 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。 接続が使用できない場合は、次のネットワークトラブルシューティングタスクを実行します。 • 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。
	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 ユーザーズ ガイド*』で説明されている OpenManage Mobile のトラブルシューティング手順に従って、デバイスを OpenManage Enterprise に再接続します。 デバイスが OpenManage Enterprise 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 Enterprise 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 Enterprise が使用されています。	新しいバージョンの OpenManage Enterprise にアップグレードしてください。

関連タスク

OpenManage Mobile の設定 、p. 169

関連情報

OpenManage Mobile の設定 、p. 169

21

その他の参照情報およびフィールドの説明

OpenManage Enterprise グラフィカルユーザーインタフェース (GUI) で一般的に表示されるフィールドの一部に関する定義については、この章でリストして定義します。また、今後の参照用に役立つその他の情報も、ここで説明します。

トピック：

スケジュールに関する参照情報

- **今すぐアップデート**：ファームウェアバージョンをアップデートし、関連するカタログで使用できるバージョンに一致させます。デバイスの次回再起動中にこのアップデートを有効にするには、[次回サーバ再起動のステージ] チェックボックスを選択します。
- **実行日時を指定**：ファームウェアバージョンをアップデートする日時を指定する場合に選択します。

ファームウェアのベースラインフィールドの定義

- **コンプライアンス**:ファームウェアベースラインの正常性状態。ファームウェアベースラインに関連付けられたデバイスが 1 つでも重要な正常性状態にある場合は、ベースラインの正常性は重要と宣言されます。これは、ロールアップ正常性状態と呼ばれ、重要度高のベースラインの状態と同じです。ロールアップ正常性状態の詳細については、Dell TechCenter のホワイトペーパー『*MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS*』(Dell EMC 第 14 世代以降の PowerEdge サーバの iDRAC を使用してロールアップ正常性状態を管理する) を参照してください。
- **名前**：ファームウェアベースラインの名前。クリックすると、**コンプライアンスレポート** ページにベースラインコンプライアンスレポートが表示されます。ファームウェアベースラインの作成の詳細については、「ファームウェア/ドライバーのベースラインの作成 、p. 77」を参照してください。
- **カタログ**：ファームウェアベースラインが属するファームウェアカタログ。「ファームウェア カタログおよびドライバー カタログの管理 、p. 74」を参照してください。
- **前回の実行時刻**：ベースラインコンプライアンスレポートが最後に実行された時刻。「デバイス ファームウェア/ドライバーのコンプライアンスの確認 、p. 78」を参照してください。

スケジュールジョブフィールドの定義

- [今すぐ実行] を選択するとジョブをただちに実行します。
- [後で実行] を選択して、後で実行する日時を指定します。

- [スケジュールどおりに実行] を選択して、選択した頻度に基づいて繰り返し実行します。[毎日] を選択し、周波数を適切に選択します。

メモ: デフォルトでは、ジョブスケジューラのクロックが毎日午前 00:00 にリセットされます。cron 形式は、ジョブの頻度の計算時に、ジョブの作成時刻を考慮しません。たとえば、ジョブが午前 10:00 時に開始され、10 時間ごとに実行される場合、次にジョブが実行される時刻は午後 08:00 時になります。ただし、次に実行される時刻は午前 06:00 時ではなく、翌日の午前 0:00 になります。これは、スケジューラのクロックが毎日午前 0:00 にリセットされるからです。

EEMI 再配置後のアラート カテゴリー

EEMI 再配置の表

表 32. OpenManage Enterprise でのアラート カテゴリー

以前のカテゴリー	以前のサブカテゴリー	新しいカテゴリー	新しいサブカテゴリー
監査	デバイス	システム正常性	デバイス
監査	デバイス	設定	デバイス
監査	デバイス	設定	デバイス
監査	デバイス	設定	デバイス
監査	デバイス	設定	デバイス
監査	アプリケーション	設定	アプリケーション
監査	アプリケーション	設定	アプリケーション
監査	アプリケーション	設定	アプリケーション
監査	アプリケーション	設定	アプリケーション
監査	デバイス	監査	ユーザー
監査	テンプレート	設定	テンプレート
監査	テンプレート	設定	テンプレート
監査	テンプレート	設定	テンプレート
監査	テンプレート	設定	テンプレート
監査	テンプレート	設定	テンプレート
設定	インベントリ	設定	ジョブ
設定	インベントリ	設定	ジョブ
設定	インベントリ	設定	ジョブ
設定	インベントリ	設定	デバイス
設定	インベントリ	設定	デバイス
設定	インベントリ	設定	デバイス
設定	ファームウェア	設定	ジョブ
設定	ファームウェア	設定	ジョブ
その他	ジョブ	設定	ジョブ
その他	ジョブ	設定	ジョブ
その他	ジョブ	設定	ジョブ
その他	Generic	設定	Generic
その他	Generic	設定	Generic

表 32. OpenManage Enterprise でのアラート カテゴリー（続き）

以前のカテゴリー	以前のサブカテゴリー	新しいカテゴリー	新しいサブカテゴリー
その他	Generic	設定	Generic
その他	Generic	設定	Generic
その他	Generic	設定	Generic
その他	Generic	設定	Generic
その他	Generic	設定	Generic
その他	Generic	設定	Generic
その他	デバイス	設定	デバイス
その他	デバイス	設定	デバイス
監査	セキュリティ	設定	セキュリティ
監査	セキュリティ	設定	セキュリティ
監査	セキュリティ	設定	セキュリティ

リモート スクリプトおよびアラート ポリシーでのトークン代用

OpenManage Enterprise では、リモート スクリプトとアラート ポリシーの作成にトークンを使用することができます。

表 33. OpenManage Enterprise でサポートされるトークン

トークン	説明
$IP	デバイスの IP アドレス
$MSG	メッセージ
$DATE	日付
$TIME	時間
$SEVERITY	重大度
$SERVICETAG	サービスタグ
$RESOLUTION	推奨される解決策
$CATEGORY	アラート カテゴリ名
$ASSETTAG	資産タグ
$MODEL	モデル名
$HOSTNAME	FQDN またはホスト名（FQDN が存在しない場合）

フィールドサービスデバッグのワークフロー

OpenManage Enterprise では、フィールドサービスデバッグ（FSD）オプションを使用して、コンソールデバッグを許可できます。

FSD を使用して、次のタスクを実行できます。

- デバッグログの有効化とコピーの許可
- リアルタイムログのコピーの許可
- VM へのデータベースのバックアップまたは復元の許可。

各タスクで参照されるトピックには詳細な手順が提供されます。FSD を有効にするには、次のタスクを実行します。

1. FSD 機能のブロック解除。「FSD 機能のブロック解除 、p. 177」を参照してください。

2. 署名済み FSD DAT.ini ファイルのインストールまたは許可。「署名済み FSD DAT.ini ファイルのインストールまたは許可 、p. 177」を参照してください。
3. FSD の呼び出し。「FSD の呼び出し 、p. 178」を参照してください。
4. FSD の無効化。「FSD の無効化 、p. 178」を参照してください。

FSD 機能のブロック解除

TUI 画面を介して FSD 機能をブロック解除することができます。

1. TUI のメインメニューに移動します。
2. TUI 画面で、FSD オプションを使用するには、[フィールドサービスデバッグ (FSD) モードを有効にする] を選択します。
3. 新しい FSD ブロック解除要求を生成するには、[FSD 機能] 画面で、[FSD 機能のブロック解除] を選択します。
4. 要求されるデバッグ機能の期間を決定するには、開始日と終了日を選択します。
5. [要求されるデバッグ機能の選択] 画面で、コンソールに一意のデバッグ機能のリストから目的のデバッグ機能を選択します。右下隅で、[生成] を選択します。

   メモ: 現在サポートされているデバッグ機能は、`RootShell.`です。

6. [DAT ファイルのダウンロード] 画面で、署名の手順と、DAT.ini ファイルが存在する共有の URL アドレスを表示します。
7. 外部クライアントを使用して、手順 6 で説明されている共有の URL アドレスから DAT.ini ファイルを抽出します。

   メモ: ダウンロード共有ディレクトリには、読み取り専用の権限があり、一度に 1 つの DAT.ini ファイルのみをサポートします。

8. 外部ユーザーであるか、内部 Dell EMC ユーザーであるかどうかに応じて、次のタスクのいずれかを実行します。
   - 外部ユーザーである場合は、DAT.ini ファイルを Dell EMC の問い合わせ先に送信します。
   - DAT.ini ファイルを適切な Dell Field Service Debug Authentication Facility (FSDAF) にアップロードして、送信します。
9. Dell EMC が署名し承認した DAT.ini ファイルが返されるのを待機します。

署名済み FSD DAT.ini ファイルのインストールまたは許可

Dell EMC によって署名および承認されている DAT.ini ファイルを受信していることを確認します。

メモ: Dell EMC が DAT.ini ファイルを承認した後で、元のブロック解除コマンドを生成したコンソールアプライアンスにファイルをアップロードする必要があります。

1. 署名されている DAT.ini ファイルをアップロードするには、[FSD 機能] 画面で、[署名済み FSD DAT.ファイルのインストール / 許可] を選択します。

   メモ: アップロード共有ディレクトリには、書き込み専用の権限があり、一度に 1 つの DAT.ini ファイルのみをサポートします。DAT.ini ファイルサイズの制限は、4 KB です。

2. [署名済み DAT ファイルのアップロード] 画面で、指定されたファイル共有 URL に DAT.ini ファイルをアップロードする方法についての手順に従ってください。
3. 外部クライアントを使用して、共有の場所に DAT.ini ファイルをアップロードします。
4. [署名済み DAT ファイルのアップロード] 画面で、[FSD DAT ファイルをアップロードしました] を選択します。

DAT.ini ファイルのアップロード中にエラーがない場合は、証明書のインストールが成功したことを確認するメッセージが表示されます。続行するには、[OK] をクリックします。

DAT.ini ファイルのアップロードは、次の理由のいずれかにより、失敗する可能性があります。

- アップロード共有ディレクトリに十分なディスク容量がない。
- アップロードされた DAT.ini ファイルが以前のデバッグ機能要求に対応していない。
- DAT.ini ファイルに対して DELL EMC によって提供された署名が無効である。

FSD の呼び出し

DAT.ini ファイルが署名されていて、Dell EMC によって返され、OpenManage Enterprise にアップロードされていることを確認します。

1. デバッグ機能を呼び出すには、[FSD 機能] 画面で、[FSD 機能を呼び出す] を選択します。
2. [要求されたデバッグ機能を呼び出す] 画面で、Dell EMC が署名した DAT.ini ファイルで承認されているデバッグ機能のリストからデバッグ機能を選択します。右下隅で、[呼び出す] をクリックします。

   メモ: 現在サポートされているデバッグ機能は、`RootShell` です。

`invoke` コマンドが実行されている間に、OpenManage Enterprise は SSH デーモンを起動することができます。外部 SSH クライアントは、デバッグの目的で OpenManage Enterprise に添付できます。

FSD の無効化

コンソールでデバッグ機能を呼び出した後で、コンソールが再起動するまで動作が継続されるか、またはデバッグ機能が停止します。それ以外の場合は、開始日と終了日から決定された期間が超過します。

1. デバッグ機能を停止するには、[FSD 機能] 画面で、[デバッグ機能を無効にする] を選択します。
2. [呼び出されているデバッグ機能を無効にする] 画面で、デバッグ機能を選択するか、現在呼び出されているデバッグ機能のリストから機能を選択します。画面の右下隅から、[無効にする] を選択します。

デバッグ機能を現在使用している SSH デーモンまたは SSH セッションを停止していることを確認します。

カタログの管理フィールドの定義

[カタログ名]: カタログの名前。ビルトインカタログは編集できません。

[ダウンロード]: リポジトリフォルダからのカタログのダウンロードステータスを示します。ステータスには、完了、実行中、および 失敗 があります。

[リポジトリ]: Dell.com、CIFS、NFS などのリポジトリのタイプ。

[リポジトリの場所]: カタログが保存されている場所。Dell.com、CIFS、NFS などです。また、カタログで実行されているジョブの完了ステータスを示します。

[カタログファイル]: カタログファイルのタイプ。

[作成日]: カタログ ファイルが作成された日。

ファームウェア/ドライバー コンプライアンス ベースライン レポート— 「不明」コンプライアンス ステータスのデバイス

次のストレージ、ネットワーク、ハイパーコンバージド インフラストラクチャ (HCI) デバイスについては、Dell ファームウェア/ドライバー カタログがこれらのデバイスのファームウェアまたはソフトウェア アップデートをサポートしていないため、ファームウェア/ドライバーのベースライン コンプライアンス レポート内でファームウェアまたはドライバーのコンプライアンス ステータスが「不明」と表示されます。

表 34. ファームウェア/ドライバー コンプライアンス ベースライン レポート — 「false」準拠デバイス

デバイスカテゴリ	デバイスリスト
ストレージ	• SC シリーズ • MD シリーズ • ME シリーズ
FX2、VRTX、および M1000e シャーシ内のネットワーク デバイス	• F10 スイッチ

表 34. ファームウェア/ドライバー コンプライアンス ベースライン レポート — 「false」準拠デバイス（続き）

デバイスカテゴリ	デバイスリスト
	• IOA（入力/出力アグリゲーター） • IOM（入力/出力モジュール）
ハイパーコンバージド アプライアンス（HCI）	• VXRail • XC シリーズ
各デバイスの Dell Update Package（DUP）を用いてアップデート可能なデバイスだが Dell カタログでは直接サポートされていない	• MX9116n ファブリック エンジン • MX5108n Ethernet スイッチ • PowerEdge MX5000s
Dell カタログまたは個別の DUP を用いてアップデートできないデバイス **メモ:** これらのデバイスのファームウェア/ドライバーのアップデートについては、各デバイスのインストール ガイドを参照してください。	• MX7116n ファブリック エクスパンダー モジュール • PowerEdge MX 25GbE PTM

メモ: SC、MD、ME、XC シリーズのデバイスの完全なリストについては、次を参照： https://topics-cdn.dell.com/pdf/dell-openmanage-enterprise_compatibility-matrix2_en-us.pdf

Dell EMC PowerEdge サーバーの汎用命名規則

一連のサーバー モデルに対応するため、PowerEdge サーバーは世代ではなく汎用命名規則を使用して参照されるようになりました。

このトピックでは、汎用命名規則を使用して参照された PowerEdge サーバーの世代を識別する方法について説明します。

例：

R740 サーバー モデルは、インテル プロセッサー搭載第 14 世代サーバーの中の、ラック型、プロセッサー 2 基搭載のシステムです。この文書では、R740 を参照するために、汎用命名規則 **YX4X** サーバーが使用されています。ここで、

- 文字 **Y**（アルファベット）は、次のサーバー フォーム ファクターを示すために使用されます。
  - **C** = クラウド - ハイパースケール環境用モジュラー型サーバー ノード
  - **F** = フレキシブル - ラックベース FX2/FX2s エンクロージャ用のハイブリッド ラックベース スレッド
  - **M** または **MX*** = モジュラー - モジュラー型エンクロージャ MX7000、M1000e および/または VRTX 用のブレード サーバー
  - **R** = ラックマウント型サーバー
  - **T** = タワー サーバー
- 文字 **X**（数字）は、サーバーのクラス（プロセッサー数）を示します。
- 数字 **4** は、サーバーの世代を示します。
- 文字 **X**（数字）は、プロセッサーのモデルを示します。

表 35. PowerEdge サーバーの命名規則と例

YX3X サーバー	YX4X システム
PowerEdge M630	PowerEdge M640
PowerEdge M830	PowerEdge R440
PowerEdge T130	PowerEdge R540