




Dell EMC OpenManage Enterprise–Tech Release

User's Guide

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。

© 2017 - 2018 Dell Inc. またはその子会社。無断転載を禁じます。Dell、EMC、およびその他の商標は、Dell Inc. またはその子会社の商標です。その他の商標は、それぞれの所有者の商標である場合があります。

OpenManage Enterprise–Tech Release について

OpenManage Enterprise–Tech Release は、Dell EMC サーバ、シャーシ、ネットワークスイッチ、エンタープライズネットワーク上のその他のデバイスの包括的なビューを提供するハードウェア管理および監視アプリケーションです。Dell EMC システムおよびその他の他社製デバイス用のウェブベースの1対多システム管理アプリケーションである OpenManage Enterprise–Tech Release では、次のことができます。

- ・ データセンター環境でのデバイスの検出および監視。
- ・ OpenManage Enterprise–Tech Release のユーザーおよびその権限の作成および管理。
- ・ デバイスのグループ化とデバイスの管理。
- ・ デバイスの正常性の監視。
- ・ デバイスファームウェアバージョンの管理、およびシステムアップデートとリモートタスクの実行。
- ・ デバイス設定テンプレートの作成と導入（サーバの場合のみ）。
- ・ システムアラートおよびアラートポリシーの表示と管理（サーバの場合のみ）。
- ・ ハードウェアインベントリおよびコンプライアンスレポートの表示
- ・ 保証とライセンスの監視および報告。

メモ: サポートされているブラウザの詳細については、『*OpenManage Enterprise–Tech Release Support Matrix*』（OpenManage Enterprise–Tech Release サポートマトリックス）を参照してください。

OpenManage Enterprise–Tech Release のセキュリティ機能の一部：

- ・ 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役割ベースのアクセス。
- ・ 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–Tech Release 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管理者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–Tech Release 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–Tech Release ユーザーが実行するタスクの一般的な順序

- ・ OpenManage Enterprise–Tech Release の導入と管理
- ・ テキストユーザーインターフェースの使用による OpenManage Enterprise–Tech Release の設定
- ・ 監視または管理のためのデバイスの検出
- ・ すべてのデバイスの管理
- ・ OpenManage Enterprise–Tech Release ダッシュボードを使用したデバイスの監視
- ・ デバイスのグループ化
- ・ デバイスファームウェアの管理
- ・ デバイスの表示と設定
- ・ デバイスのアラートの監視
- ・ アーカイブされたアラートの表示
- ・ デバイス保証情報の表示
- ・ デバイス設定テンプレートの管理
- ・ デバイス設定コンプライアンスベースラインの管理
- ・ コンプライアンステンプレートを使用したデバイスコンプライアンスの監視
- ・ 監査ログの管理
- ・ OpenManage Enterprise–Tech Release アプライアンス設定の管理
- ・ インベントリジョブを今すぐ実行する
- ・ デバイス保証の管理
- ・ レポート
- ・ MIB ファイルの管理

- ・ 役割ベースの OpenManage Enterprise–Tech Release ユーザー権限
- ・ OpenManage Enterprise–Tech Release でのディレクトリサービスの統合

トピック：

- ・ OpenManage Enterprise— サーバ設定管理ライセンス

OpenManage Enterprise— サーバ設定管理ライセンス

メモ: OpenManage Enterprise — サーバ設定管理ライセンスは OpenManage Enterprise–Tech Release のインストールと使用には必要ありません。OpenManage Enterprise — サーバ設定管理ライセンスがターゲットサーバにインストールされていることを必須とするのは、サーバ設定管理機能のみです。OpenManage Enterprise — サーバ設定管理および OpenManage Essentials ライセンスは、サーバ上でのデバイス設定導入、および設定コンプライアンスの検証にのみ必要です。このライセンスは、サーバからデバイス設定テンプレートを作成する場合には必要ありません。

OpenManage Enterprise — サーバ設定管理ライセンスにより、ライセンス付与されたサーバでのデバイス設定の導入、およびデバイス設定コンプライアンスの検証が可能になります。ライセンスは、サーバの寿命到達まで有効な永久ライセンスで、一度に1台のサーバのサービスタグにのみバインドすることができます。OpenManage Enterprise–Tech Release 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 の順にクリックします。実行 をクリックします。「レポートの実行」を参照してください。

メモ: OpenManage Enterprise–Tech Release 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 — サーバ設定管理ライセンスがターゲットサーバにインストールされていれば、そのサーバでサーバ設定管理機能を使用することができます。

ライセンス可能サーバ

OpenManage Enterprise — サーバ設定管理ライセンスは以下の PowerEdge サーバに導入できます。

- ・ ファームウェアのバージョンが iDRAC8 2.50.50.50 以上の第 13 世代 (13G) サーバ。13G iDRAC バージョンは、下位互換性があり、iDRAC7 バージョン (12G) もサポートします。
- ・ ファームウェアのバージョンが iDRAC9 3.10.10.10 以上の第 14 世代 (14G) サーバ。

ライセンスの購入

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

ライセンス情報の確認

OpenManage Enterprise–Tech Release にはビルトインレポートが備わっており、OpenManage Enterprise–Tech Release の監視対象デバイスのリスト、およびそのライ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」を参照してください。

OpenManage Enterprise — サーバ設定管理ライセンスがサーバにインストールされているかどうかは、以下の方法で確認できます。

- ・ OpenManage Enterprise–Tech Release 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–Tech Release 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–Tech Release でのライセンスベースの機能

最新バージョンのインストール済み OpenManage Enterprise–Tech Release アプライアンスを確認するには：

- ・ 一般的にすべての OpenManage Enterprise–Tech Release ページの右上隅に表示される **i** シンボルをクリックします。
- ・ アプリケーションの **設定** > **コンソールのアップデート** の順にクリックします。

i **メモ:** OpenManage Enterprise–Tech Release の新しいバージョンが使用可能かどうかを確認するには、「[OpenManage Enterprise–Tech Release バージョンの確認とアップデート](#)」を参照してください。また、サポートサイトで入手可能な『*OpenManage Enterprise–Tech Release Release Notes*』（OpenManage Enterprise–Tech Release リリースノート）を参照してください。

OpenManage Enterprise–Tech Release のセキュリティ機能

OpenManage Enterprise–Tech Release のセキュリティ機能の一部：

- ・ 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役割ベースのアクセス。
- ・ 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)。

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–Tech Release 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があります。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: AD および LDAP ディレクトリユーザーをインポートし、OpenManage Enterprise–Tech Release 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。コンソールにログインするまでの間に限り、シングルサインオン (SSO) 機能を使用できます。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。

OpenManage Enterprise–Tech Release は、割り当てられたグループに基づくユーザー権限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 > グループごとのユーザー権限 の順にをクリックします。実行 をクリックします。「レポートの実行」を参照してください。

関連情報

OpenManage Enterprise–Tech Release の導入と管理

トピック：

- ・ 役割ベースの OpenManage Enterprise–Tech Release ユーザー権限
- ・ OpenManage Enterprise–Tech Release ユーザーの役割タイプ

役割ベースの OpenManage Enterprise–Tech Release ユーザー権限

ユーザーは、コンソール設定およびデバイス管理機能へのアクセスのレベルを決定する役割を割り当てられます。この方式は、役割ベースのアクセスコントロール (RBAC) と呼ばれています。以下は、ユーザーの役割と OpenManage Enterprise–Tech Release の機能に基づいた、ユーザー向けの RBAC 共通リストです。ただし、個々のタスクレベルのユーザー RBAC リストについては、必要に応じて各セクションで参考として説明します。したがって、コンソールはアカウントごとに1つの役割を強制します。

OpenManage Enterprise–Tech Release でのユーザー管理の詳細については、「OpenManage Enterprise–Tech Release ユーザーの管理」を参照してください。

OpenManage Enterprise–Tech Release は、割り当てられたグループに基づくユーザー権限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 > グループごとのユーザー権限 の順にをクリックします。実行 をクリックします。「レポートの実行」を参照してください。

表 1. OpenManage Enterprise–Tech Release での役割ベースのユーザー権限

OpenManage Enterprise–Tech Release の機能	OpenManage Enterprise–Tech Release にアクセスするためのユーザーレベル		
	管理者	デバイス管理者	閲覧者

OpenManage Enterprise–Tech Release の機能	OpenManage Enterprise–Tech Release にアクセスするためのユーザーレベル		
OpenManage Enterprise–Tech Release アプリアランスの設定	Y	N	N
ベースラインの管理	Y	Y	N
デバイスの設定	Y	Y	N
デバイスの更新	Y	Y	N
検出の管理	Y	N	N
グループの管理	Y	N	N
インベントリの更新	Y	N	N
ジョブの管理	Y	Y	N
監視ポリシーの作成	Y	Y	N
OS の導入	Y	Y	N
電源の制御	Y	Y	N
レポートの管理	Y	Y	N
レポートの実行	Y	Y	Y
セキュリティの設定	Y	N	N
テンプレートの管理	Y	Y	N
トラップの管理	Y	N	N
表示	Y	Y	Y

関連タスク

[OpenManage Enterprise–Tech Release の導入と管理](#)

関連資料

[OpenManage Enterprise–Tech Release ユーザーの役割タイプ](#)

OpenManage Enterprise–Tech Release ユーザーの役割タイプ

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–Tech Release 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。コンソールにログインするまでの間に限り、シングルサインオン (SSO) 機能を使用できます。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。

OpenManage Enterprise–Tech Release は、割り当てられたグループに基づくユーザー権限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 > グループごとのユーザー権限** の順にをクリックします。**実行** をクリックします。「**レポートの実行**」を参照してください。

表 2. OpenManage Enterprise–Tech Release 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	<p>コンソール上で実行できるタスクのすべてに対する完全アクセス権があります。</p> <ul style="list-style-type: none"> 完全アクセス (GUI および REST を使用) により、OpenManage Enterprise–Tech Release による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。

デバイス管理者 (DM)

メモ: DM は互いに作成したタスクとポリシーに対する許可を共有できます。この共有は、タスクまたはポリシーに含まれているデバイスグループと DM に割り当てられているデバイスグループが完全に重複することによって発生します。DM でタスクまたはポリシーに含まれているグループとの完全な重複が失われる場合、DM はこの重複が復元されない限り、実行または編集できなくなります。

- 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
- ユーザーパスワードの変更

- 管理者からデバイスグループの許可のみを取得します。その他のすべての許可は修正されます。
- 管理者によって割り当てられたグループのデバイス上のタスク、ポリシーおよびその他のアクションを実行します。
- どのグループも削除または変更することはできません。
- 複数の DM を同じ静的、動的、およびデバイスのシステムグループへのアクセスに割り当てることができます。
- 任意の数のグループを DM に割り当てることができます。

メモ: デバイスマネージャ (DM) 権限を持つユーザーには、グループを割り当てることができません。

閲覧者

- OpenManage Enterprise–Tech Release 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場合は、完全な管理者権限を持ちます。閲覧者が DM に変更される場合、デバイスグループが DM に割り当てられていない場合は、DM には閲覧者と同じ権限があります。

メモ: ユーザー役割の変更はログイン中のユーザーには影響しません。変更内容は、次のユーザーログイン後にのみ有効になります。

メモ: 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。

関連タスク

[OpenManage Enterprise–Tech Release の導入と管理](#)

関連情報

[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)

OpenManage Enterprise–Tech Release の導入と管理

Dell EMC OpenManage Enterprise–Tech Release はハイパーバイザの導入とリソースを管理してダウンタイムを最小化する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、アプリケーションウェブ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–Tech Release バージョンの確認とアップデート](#)」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: サポートされているブラウザの詳細については、サポートサイトで入手可能な『[OpenManage Enterprise–Tech Release Support Matrix](#)』 (OpenManage Enterprise–Tech Release サポートマトリックス) を参照してください。

関連資料

- [OpenManage Enterprise–Tech Release ユーザーの役割タイプ](#)
- [OpenManage Enterprise–Tech Release バージョンをチェックし、アップデートするためのプロセスマップ](#)
- [OpenManage Enterprise–Tech Release グラフィカルユーザーインターフェイスの概要](#)
- [OpenManage Enterprise–Tech Release のセキュリティ機能](#)

関連情報

[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)

トピック :

- [インストールの前提条件と最小要件](#)
- [VMware vSphere での OpenManage Enterprise–Tech Release の導入](#)
- [Hyper-V ホストへの OpenManage Enterprise–Tech Release の導入](#)
- [Deploying the Hyper-V appliance on Microsoft Server 2012](#)

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–Tech Release Support Matrix](#)』 (Dell EMC OpenManage Enterprise–Tech Release サポートマトリックス) を参照してください。

OpenManage Enterprise–Tech Release 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「[OpenManage 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

表 3. 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
デバイス数	最大 5,500	1000
RAM	16 GB	8 GB
プロセッサ	合計 8 コア	合計 4 コア
ハードドライブ	200 GB	20 GB

OpenManage Enterprise–Tech Release の導入のための最小システム要件

表 4. 最小要件

項目	最小要件
ハイパーバイザ	VMware vSphere、および HyperV
ネットワーク	OpenManage Enterprise–Tech Release から管理されるすべてのデバイスの管理ネットワークにアクセスできる使用可能な仮想 NIC。
ウェブブラウザ	<ul style="list-style-type: none">Internet Explorer (64 ビット) 11 以降Mozilla Firefox 52 以降Google Chrome 58 以降
ユーザーインターフェース	HTML 5、JS ベース

メモ: OpenManage Enterprise–Tech Release 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り『*Dell EMC OpenManage Enterprise–Tech Release Support Matrix*』(Dell EMC OpenManage Enterprise–Tech Release の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–Tech Release の導入

メモ: OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。

- VMware vSphere Client でアクセス可能な場所に .zip ファイルを解凍します。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。
- 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。
- 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。
- 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。
- 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。
- 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。
- 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。
- 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。
- ディスクの形式** ページで、次のオプションのいずれかを選択します。
 - 必要に応じてストレージ容量を VM に割り当てるには、**シンプロビジョニング** をクリックします。
 - ドライブ作成時に物理ストレージ容量を VM に事前割り当てするには、**シックプロビジョニング** をクリックします。
- 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 ホストへの OpenManage Enterprise–Tech Release の導入

1. Windows Server 2008 R2 以降のバージョンで Hyper-V Manager を開きます。Windows 2012 ホストが Hyper-V マネージャの下に表示されます。
2. ホストを選択し、**アクション > 仮想マシンのインポート** の順に選択します。
3. スナップショット、仮想ドライブ、VM、インポートファイルを含む、OpenManage Enterprise–Tech Release 仮想アプライアンスが存在するフォルダを選択します。**次へ** をクリックします。
4. **仮想マシンの選択** ページで、インポートする仮想マシンを選択し (使用可能なオプションは1つだけ)、**次へ** をクリックします。
5. **インポートタイプの選択** ページで、**仮想マシンのコピー** を選択して **次へ** をクリックします。
6. **宛先の選択** ページで、デフォルト値を保持するか、VM、スナップショット、スマートページングの場所を選択します。
7. **次へ** をクリックします。
8. **ストレージフォルダの選択** ページで、デフォルト値を保持するか、**参照** をクリックして仮想ドライブの場所を選択し、**次へ** をクリックします。
9. **概要** 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 Hyper-V ホストに OpenManage Enterprise–Tech Release 仮想アプライアンスを導入します。
10. OpenManage Enterprise–Tech Release 仮想アプライアンスが導入されたら、OpenManage Enterprise–Tech Release 仮想アプライアンスを選択し、**アクション** の下の **開始** をクリックします。

 **メモ:** OpenManage Enterprise–Tech Release アプライアンスファイルは、互換性のある KVM 環境を使用しても導入できます。

Deploying the Hyper-V appliance on Microsoft Server 2012

1. Extract the `openmanage_enterprise_vhd_format.zip` file, and then move or copy the enclosed VHD file into the appropriate location on your system where you want to store the OpenManage Enterprise (OME) virtual drive.
2. Start Hyper-V Manager.
3. Click **Action > New > Virtual Machine**.
4. On the **Specify Name and Location** page, select the VM name and a storage location appropriately for your environment.
5. Navigate to the **Specify Generation** page and select **Generation 1**. OpenManage Enterprise–Tech Release does not support Generation 2.

 **NOTE:** Ensure that 8192 MB is assigned as the memory. Dynamic memory can be turned on, but for best performance, it is recommended to leave the option 'disabled'.

6. On the **Networking Configuration** page, ensure that the network adapter is connected to the network. If set to 'Not Connected', OME–Tech Release will not function properly during the first reboot, and requires redeployment if this situation recurs.
7. On the **Connect Virtual Hard Disk** page, select **Use an existing virtual disk drive**, and then go to the VHD file you copied in step 1 earlier.
8. Complete the on-screen instructions.
9. Open the settings of the newly created VM.

OpenManage Enterprise–Tech Release - はじめに

トピック：

- ・ [OpenManage Enterprise–Tech Release へのログイン](#)
- ・ [OpenManage Enterprise–Tech Release の設定](#)
- ・ [OpenManage Enterprise–Tech Release でサポートされるプロトコルおよびポート](#)

OpenManage Enterprise–Tech Release へのログイン

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。初めて OpenManage Enterprise–Tech Release にログインする場合、テキストユーザーインターフェイス (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–Tech Release の設定](#)」を参照してください。

1. サポートされているブラウザを起動します。
2. アドレスボックスに OpenManage Enterprise–Tech Release アプライアンスの IP アドレスを入力します。
3. ログインページで、ログイン資格情報を入力し、**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–Tech Release 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–Tech Release の設定](#)」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: 誤った **OpenManage Enterprise–Tech Release** ログイン資格情報が入力された場合は、**OpenManage Enterprise–Tech Release** のアカウントがロックされ、ロックダウンの期間を完了するまでログインすることはできません。

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

テキストユーザーインターフェイス (TUI) ツールでは、管理者パスワードを変更し、アプライアンスステータスおよびネットワーク設定を表示し、ネットワークパラメータを設定し、フィールドサービスのデバッグ要求を有効にするテキストインターフェイスが利用できます。

メモ: TUI インターフェイスで移動するには、矢印キーを使用するか、または **Tab** を押して進み、**Shift + Tab** を押して戻り、オプション内を移動します。**Enter** を押してオプションを選択します。スペースバーはチェックボックスのステータスを切り替えます。

1. TUI にログインする前に、プロンプトが表示されたら EULA に同意します。
 - a) **管理者パスワードの変更** 画面で、新しいパスワードを入力し、パスワードを確認します。

メモ: 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。

- b) 矢印キーを使用するか、または **Tab** を押して、**適用** を選択します。
- c) 確認画面で **はい** を選択し、**Enter** を押します。

これで OpenManage Enterprise–Tech Release を TUI で設定できるようになります。

TUI の画面では、次のオプションを表示できます。

- ・ **管理者パスワードの変更**
- ・ **現在のアプライアンスステータスを表示する**
- ・ **現在のネットワーク設定を表示する**

- ・ ネットワークパラメータを設定する
 - ・ フィールドサービスデバッグ (FSD) モードを有効にする
 - ・ アプライアンスを再起動する
2. 現在のアプライアンス Administrator パスワードを確認するには、**管理者パスワードの変更** を選択してから、パスワードを入力します。**Tab** を押して、**続行** を選択します。
 3. TUI 画面での操作：
 - a) アプライアンスのステータス、IPv4 および IPv6 のステータスおよびアドレスを表示するには、**現在のアプライアンスステータス** を選択します。
 - b) ネットワークインタフェースを設定するには、**ネットワークパラメータを設定する** を選択します。
 ネットワークインタフェースを設定する 画面で、IPv4、または IPv6、あるいは両方を有効にするには、**Enter** を押し、**適用** を選択します。
メモ: TUI で書き込み操作を実行するには、**Administrator** パスワードを入力してから、**IPv4** または **IPv6** を設定します。
 - メモ:** IPv6 を設定するには、それがすでに vCenter サーバで設定されていることを確認します。
 - c) コンソールのデバッグを有効にするには、**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。「**フィールドサービスデバッグのワークフロー**」を参照してください。
 - d) OpenManage Enterprise–Tech Release を再起動するには、**アプライアンス再起動** を選択します。

OpenManage Enterprise–Tech Release の設定

OpenManage Enterprise–Tech Release 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。基本的な設定を行うには、**初期設定** をクリックし、ダイアログボックスで次のデータを入力または選択します。

1. **タイムゾーン** ドロップダウンメニューからタイムゾーンを選択します。選択したタイムゾーンを保存するには、**適用** をクリックします。そのタイムゾーンをデフォルト値に設定するには、**破棄** をクリックしてください。タイムゾーンを更新した後、すべてのアクティブなユーザーが OpenManage Enterprise–Tech Release からログアウトされます。
 2. 時刻同期に NTP サーバを使用するには、**NTP サーバの使用** チェックボックスを選択します。
メモ: NTP サーバの設定が更新されると、現在ログインしているユーザーは、**OpenManage Enterprise–Tech Release** セッションから自動的にログアウトされます。
 3. 時刻を同期させるには、**プライマリ NTP サーバのアドレス** と **セカンダリ NTP サーバのアドレス** (オプション) に IP アドレスまたはホスト名を入力します。
 4. 外部通信用にプロキシサーバを設定する場合は、**HTTP プロキシ設定の使用** チェックボックスを選択します。
 5. **サーバ IP アドレス** ボックスに、プロキシサーバの IP アドレスまたはホスト名を入力します。
 6. **ポート** ボックスに、プロキシサーバのポート番号を入力します。
 7. プロキシサーバがログインするための資格情報を要求する場合は、**プロキシの資格情報を使用する** 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。
 8. **終了** をクリックします。
- メモ:** サポートされているブラウザの詳細については、サポートサイトで入手可能な『**OpenManage Enterprise–Tech Release Support Matrix**』 (OpenManage Enterprise–Tech Release サポートマトリックス) を参照してください。

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

- ・ 「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」を参照してください。
- ・ 「管理ステーションでサポートされるプロトコルおよびポート」を参照してください。

管理ステーションでサポートされるプロトコルおよびポート

表 5. OpenManage Enterprise–Tech Release 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	方向	使用状況
21	FTP	TCP	256 ビット	入力 / 出力	dell.com にアクセスします

ポート番号	プロトコル	ポートタイプ	最大暗号化レベル	方向	使用状況
22	SSH	TCP	256 ビット	入力 / 出力	FSD が使用されている場合にのみ受信に必要です。OpenManage Enterprise-Tech Release 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	出力	オプションの電子メールアラート処置
53	DNS	UDP/TCP	なし	出力	ネットワークの設定
68/546 (IPv6)	DHCP	UDP/TCP	なし	出力	ネットワークの設定
111	NFS	TCP	なし	入力 / 出力	その他の管理機能
123	NTP	TCP	なし	出力	時間の同期化 (有効にされている場合)
137、138	CIFS	UDP/TCP	なし	入力 / 出力	その他の管理機能
139、445	CIFS	TCP	なし	入力 / 出力	その他の管理機能
162	snmp	UDP	なし	入力 / 出力	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	入力 / 出力	Web GUI。dell.com からアップデートします。ウェブ GUI の HTTPS を使用して、OpenManage Enterprise-Tech Release と通信する際は 256 ビットの暗号化が許可されます。
514	Syslog	TCP	なし	出力	シスログポリシーアクション

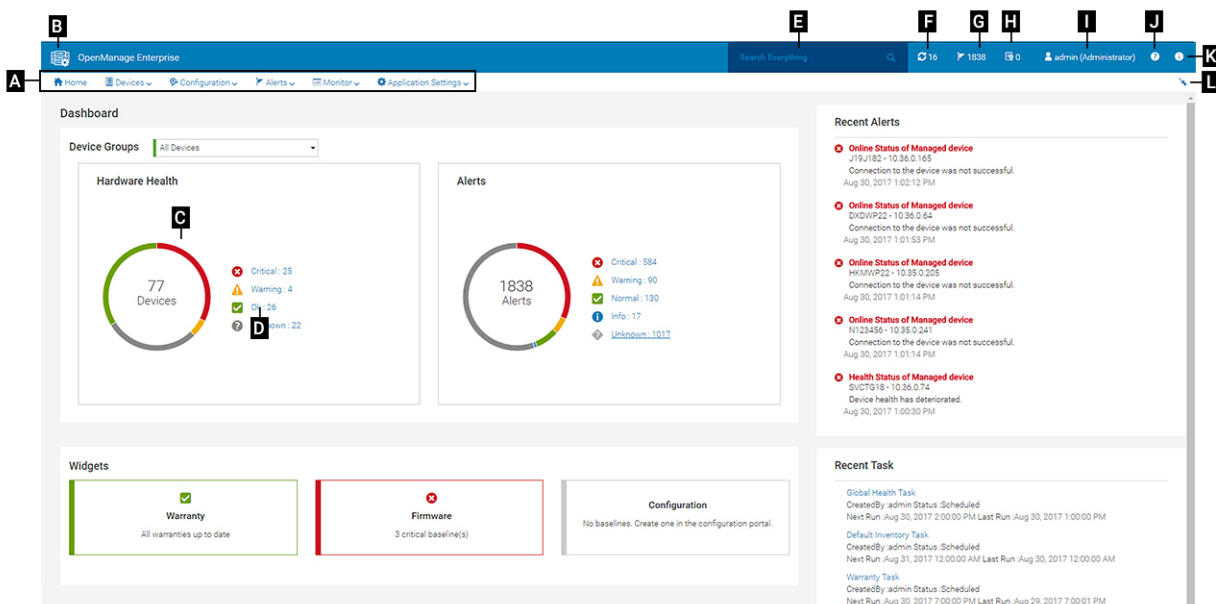
管理下ノードでサポートされるプロトコルおよびポート

表 6. OpenManage Enterprise-Tech Release でサポートされる管理ノード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	方向	使用状況
22	SSH	TCP	256 ビット	入力 / 出力	Linux OS 検出専用
80	HTTP	TCP	なし	入力 / 出力	コンテキストアプリケーションの起動 — Networking コンソール。
161	snmp	UDP	なし	入力 / 出力	SNMP クエリ管理。
162	snmp	UDP	なし	入力 / 出力	管理ステーション用トラップ
443	専用 / WS-Man/Redfish	TCP	256 ビット	入力 / 出力	iDRAC7 およびそれ以降のバージョンの検出とインベントリ、および CMC 管理用。
623	RMCP	UDP	なし	入力 / 出力	LAN を使用した IPMI アクセス。

OpenManage Enterprise–Tech Release グラフィカルユーザーインタフェースの概要

OpenManage Enterprise–Tech Release 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–Tech Release の設定、システムアラート、およびファームウェア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–Tech Release 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–Tech Release 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–Tech Release 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記号をクリックして、メニュー項目がすべての OpenManage Enterprise–Tech Release 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–Tech Release 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–Tech Release が監視した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。「[デバイスの表示と設定](#)」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](#)」を参照してください。
- E — **すべてを検索** ボックスには、OpenManage Enterprise–Tech Release によって監視および表示される内容について入力して、デバイス IP、ジョブ名、グループ名、ファームウェアベースライン、保証データなどの結果を確認します。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。
 - 検索条件に入力したテキストは、大文字と小文字が区別されます。
 - 次のワイルドカード文字、#、@、%、-、:、=、&、\$、+、|、/、.、_、(、および) はサポートされていません。

- ・ F— 現在、キューに入っている OpenManage Enterprise–Tech Release のジョブ数。検出、インベントリ、保証、ファームウェア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](#)」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。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](#)」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- 保証ステータスが重要で、ただちに注意を払う必要があるデバイスの数。クリックすると、各カテゴリのシステムアラートを表示します。この機能を有効にするには、保証設定を有効にします。「[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。役割に基づいたユーザーの詳細については、「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」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、状況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–Tech Release 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–Tech Release 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–Tech Release 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](#)」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。フィルタ条件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–Tech Release 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、「[Dell EMC OpenManage Enterprise–Tech Release Support Matrix](#)」(Dell EMC OpenManage Enterprise–Tech Release 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、ファームウェアベースライン、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–Tech Release のアップデートバージョンがある場合は、[今すぐアップデート](#) をクリックしてただちにバージョンを更新することを警告されます。すべての OpenManage Enterprise–Tech Release 権限 (Administrator、デバイスマネージャ、およびビューア) を持つユーザーは、メッセージを表示し、バージョンをアップデートできますが、管理者のみが、メッセージを後で通知するか、または無視するのを選択できます。OpenManage Enterprise–Tech Release 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–Tech Release バージョンの確認とアップデート](#)」を参照してください。

OpenManage Enterprise–Tech Release 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、画面の左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](#)」を参照してください。

関連情報

[OpenManage Enterprise–Tech Release の導入と管理](#)

OpenManage Enterprise–Tech Release のホームポータル

OpenManage Enterprise > ホーム をクリックして、OpenManage Enterprise–Tech Release 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、ライセンスの保証期限が切れた、または期限が切れる寸前のデバイス、およびベースラインおよびコンプライアンスから逸脱しているデバイスのファームウェアバージョンがリストされます。ウィジェットで利用可能な機能についての詳細は、「[OpenManage Enterprise–Tech Release ダッシュボードを使用したデバイスの監視](#)」を参照してください。右ペインには、OpenManage Enterprise–Tech Release 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。「[デバイスのアラートの監視](#)」および「[デバイスコントロール用ジョブの使い方](#)」を参照してください。
- ・ OpenManage Enterprise–Tech Release のアップデートバージョンがある場合は、**今すぐアップデート** をクリックしてただちにバージョンを更新することを警告されます。OpenManage Enterprise–Tech Release 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–Tech Release バージョンの確認とアップデート](#)」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–Tech Release 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](#)」を参照してください。

トピック：

- ・ [OpenManage Enterprise–Tech Release ダッシュボードを使用したデバイスの監視](#)
- ・ [デバイスのグループ化](#)
- ・ [ドーナツグラフ](#)
- ・ [デバイスの正常性状態](#)

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

① **メモ:** OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。

初回ログインを別にすれば、ダッシュボードは、OpenManage Enterprise–Tech Release へのその後のすべてのログインの後に表示される最初のページです。OpenManage Enterprise–Tech Release 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、リアルタイムの監視データを使用して、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–Tech Release 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–Tech Release 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–Tech Release 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、「[デバイスのグループ化](#)」および「[監視または管理のためのデバイスの検出](#)」を参照してください。

- ・ [デバイスファームウェアの管理](#)
- ・ [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–Tech Release アプライアンス設定の管理](#)

ハードウェアの正常性 セクションは、デフォルトで、OpenManage Enterprise–Tech Release 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。「[デバイスのアラートの監視](#)」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。「[デバイスの表示と設定](#)」を参照してください。

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。Excel、CSV、HTML、または PDF 形式にデータ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](#)」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](#)」および「[デバイスの正常性状態](#)」を参照してください。OpenManage Enterprise–Tech Release 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。

i **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。「[デバイスの表示と設定](#)」を参照してください。

ウィジェット セクションには、OpenManage Enterprise–Tech Release 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。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。「[OpenManage Enterprise–Tech Release ダッシュボードを使用したデバイス保証の管理](#)」を参照してください。デバイスの保証の管理については、「[デバイス保証の管理](#)」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:** OpenManage Enterprise–Tech Release で作成されたファームウェアコンプライアンスベースラインのロールアップ状態が表示されます。使用可能な場合は、**重要** および **警告** ファームウェアベースラインが本項に一覧表示されます。
 - ・ 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『*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。
 - ・ クリックすると、**ファームウェア** ダイアログボックスの詳細が表示されます。
 - ・ 「[OpenManage Enterprise–Tech Release ダッシュボードを使用したファームウェアベースラインの管理](#)」を参照してください。
 - ・ 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、「[デバイスファームウェアの管理](#)」を参照してください。
- ・ **設定:** OpenManage Enterprise–Tech Release 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をを使用したデバイスコンプライアンスの監視](#)」を参照してください。

OpenManage Enterprise–Tech Release ダッシュボードを使用したファームウェアベースラインの管理

OpenManage Enterprise–Tech Release ダッシュボードページで、**ウィジェット** セクションの **ファームウェア** セクションに重要な正常性状態の 1 つまたは複数のデバイスを持つファームウェアベースラインの数が表示されます。「[デバイスの正常性状態](#)」を参照してください。ファームウェア管理の詳細については、「[デバイスファームウェアの管理](#)」を参照してください。

ベースラインのリストを表示するには、**ファームウェア** をクリックします。ファームウェア ダイアログボックス内の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](#)」を参照してください。

OpenManage Enterprise–Tech Release ダッシュボードを使用したデバイス保証の管理

OpenManage Enterprise–Tech Release ダッシュボードページの **ウィジェット** セクションでは、**保証** セクションに有効期限の終了が近いかすでに終了しているデバイスの数が表示されます。デバイスの保証の管理の詳細については、「[デバイス保証の管理](#)」を参照してください。

有効期限の終了が近い保証のリストを表示するには、**保証** をクリックします。**保証** ダイアログボックスで、サービスタグと共に、次の情報が表示されます。

- ・ デバイスのサービスタグ、モデル名、およびモデルタイプ。

- ・ **保証タイプ** :
 - ・ 初期 : OpenManage Enterprise–Tech Release を最初に購入した際に提供される保証を使用することにより、保証は引き続き有効です。
 - ・ 延長 : OpenManage Enterprise–Tech Release を最初に購入した際に提供される保証期間が期限切れのため、保証が延長されます。
- ・ **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契約 (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](#)」を参照してください。

OpenManage Enterprise–Tech Release ダッシュボードを使用したデバイスコンプライアンスベースラインの管理

OpenManage Enterprise–Tech Release ダッシュボードページの **ウィジェット** セクションでは、**設定** セクションに、比較するテンプレートのプロパティに準拠しない設定コンプライアンスベースラインの数が表示されます。

テンプレートのプロパティから離れた設定コンプライアンスベースラインのリストを表示するには、**設定** をクリックします。**設定** ダイアログボックス :

- ・ **コンプライアンス** 設定コンプライアンスベースラインが離れているレベルを示します。
- ・ **テンプレート名** ベースラインが比較対象となるコンプライアンスベースラインテンプレートを示します。

「[デバイス設定コンプライアンスベースラインの管理](#)」を参照してください。導入用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ベースラインテンプレートを作成できます。「[コンプライアンスベースラインテンプレートの管理](#)」を参照してください。

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。「[デバイスの表示と設定](#)」を参照してください。

OpenManage Enterprise–Tech Release は、OpenManage Enterprise–Tech Release 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](#)」を参照してください。

i **メモ**: OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」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。

i **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『**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。

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りません。デフォルトでは、OpenManage Enterprise–Tech Release 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–Tech Release 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および非表示に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 シリーズデバイスなど)
- ・ **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 VRTX シャーシ
- ・ **ネットワークデバイス** : Dell Force10 ネットワークスイッチとファイバチャネルスイッチ
- ・ **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 EMC Compellent 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。現在、OpenManage Enterprise-Tech Release では、検出された 5,500 台のデバイスを監視できます。「[監視または管理のためのデバイスの検出](#)」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：ユーザー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：

- ・ 併用はできません。
- ・ 複数の親グループは持ってません。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。

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-Tech Release 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-Tech Release 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は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または編集](#)」および「[クエリデバイスグループの作成](#)」を参照してください。

メモ：OpenManage Enterprise-Tech Release 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。「[役割ベースの OpenManage Enterprise-Tech Release ユーザー権限](#)」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更新されます。

関連タスク

[OpenManage Enterprise-Tech Release からのデバイスの削除](#)

[デバイスインベントリを更新する](#)

[デバイスステータスの更新](#)




ドーナツグラフ

OpenManage Enterprise-Tech Release 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-Tech Release 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-Tech Release 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](#)」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-Tech Release 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。「[デバイスのアラートの監視](#)」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、「[デバイスファームウェアの管理](#)」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ベースラインの管理](#)」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、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 7. OpenManage Enterprise–Tech Release 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。

- メモ:** ダッシュボードに表示されるデータは、OpenManage Enterprise–Tech Release 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。

すべてのデバイスの管理

OpenManage Enterprise > **デバイス** > **すべてのデバイス** をクリックして、OpenManage Enterprise–Tech Release が管理するデバイスとデバイスグループを表示できます。システムグループは、出荷時に OpenManage Enterprise–Tech Release によって作成されるデフォルトグループであり、カスタムグループは管理者やデバイス管理者などのユーザーによって作成されます。これらの2つの親グループの下に子グループを作成できます。親 - 子の規則の詳細については、「[デバイスグループ](#)」を参照してください。作業中のペインに、左側のペインで選択したグループ内のデバイスの正常性および数がドーナツグラフに表示されます。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。

ドーナツグラフに続く表には、左ペインで選択したデバイスのプロパティが一覧表示されます。デバイスのプロパティを表示したり設定を編集したりするには、リストのデバイス名または IP アドレスをクリックします。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。

- ① **メモ:** デバイス リストで、デバイス名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。デバイス (iDRAC など) にインストールされている管理アプリケーションにログインするには、IP アドレスをクリックします。「[デバイスの表示と設定](#)」を参照してください。
- ① **メモ:** 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、インベントリの更新、ステータスの更新、サーバ制御など) は、デバイス <デバイス名> ページでも実行できます。
- ① **メモ:** OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。

次のデバイス関連タスクを実行できます。 :

- ・ 新しいグループを作成し、デバイスを追加。「[新規グループへのデバイスの追加](#)」および「[既存のグループへのデバイスの追加](#)」を参照。
- ・ OpenManage Enterprise–Tech Release からデバイスを削除。「[OpenManage Enterprise–Tech Release からのデバイスの削除](#)」を参照してください。
- ・ OpenManage Enterprise–Tech Release による監視からデバイスを除外。「[OpenManage Enterprise–Tech Release からのデバイスの除外](#)」を参照してください。
- ・ デバイスのファームウェアバージョンのアップデート。「[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。
- ・ 選択したデバイスのハードウェアおよびソフトウェアのインベントリをアップデート。「[デバイスインベントリの更新](#)」を参照。
- ・ 選択したデバイス (複数可) の最新の稼働状態を収集。
- ・ デバイスをオンボーディング。「[デバイスのオンボーディング](#)」を参照。
- ・ デバイスグループのリストにあるアイテムを PDF、HTML、CSV 形式でエクスポート。「[デバイスグループインベントリのエクスポート](#)」を参照。
- ・ 追加アクション タブから選択した、またはすべてのデバイスに関するデータをエクスポート。「[データのエクスポート](#)」を参照。
- ・ 完全な情報を表示し、デバイスを管理します。「[デバイスの表示と設定](#)」を参照してください。
- ・ Lifecycle Controller 管理アプリケーションで iDRAC を起動。「[管理アプリケーション \(iDRAC\) の起動](#)」を参照。
- ・ 仮想コンソールを起動します。「[仮想コンソールの起動](#)」を参照してください。

デバイスグループ関連のタスクについては、「[デバイスのグループ化](#)」を参照してください。

右上隅の **クイックリンク** セクションで、OpenManage Enterprise–Tech Release の以下の機能へのクイックリンクを使用します。

- ・ [デバイスの検出](#)
- ・ [インベントリスケジュールジョブを今すぐ実行](#)
- ・ [検出結果からデバイスをグローバルに除外する](#)

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。選択をクリアするには、**選択のクリア** をクリックします。

- ① **メモ:** GUI に表示されるまたは情報目的でログに保存される特定のイベントとエラーの詳細については、サポートサイトの最新の『[Event and Error Message Reference Guide for Dell EMC PowerEdge Servers](#)』 (Dell EMC PowerEdge Server 用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。

トピック：

- ・ デバイスのグループ化
- ・ デバイスの表示と設定
- ・ デバイスの管理アプリケーション iDRAC の開始
- ・ 仮想コンソールの起動

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。「[デバイスの表示と設定](#)」を参照してください。

OpenManage Enterprise-Tech Release は、OpenManage Enterprise-Tech Release 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](#)」を参照してください。

メモ: OpenManage Enterprise-Tech Release 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。「[役割ベースの OpenManage Enterprise-Tech Release ユーザー権限](#)」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『**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。

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-Tech Release 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-Tech Release 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および非表示に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 シリーズデバイスなど)
- ・ **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 VRTX シャーシ
- ・ **ネットワークデバイス:** Dell Force10 ネットワークスイッチとファイバチャネルスイッチ
- ・ **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 EMC Compellent 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。現在、OpenManage Enterprise-Tech Release では、検出された 5,500 台のデバイスを監視できます。「[監視または管理のためのデバイスの検出](#)」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: ユーザー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：

- ・ 併用はできません。

- 複数の親グループは持ってません。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。

① 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-Tech Release 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-Tech Release 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または編集」および「クエリデバイスグループの作成」を参照してください。

① メモ: OpenManage Enterprise-Tech Release 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。「役割ベースの OpenManage Enterprise-Tech Release ユーザー権限」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更新されます。

関連タスク

[OpenManage Enterprise-Tech Release からのデバイスの削除](#)

[デバイスインベントリを更新する](#)

[デバイスステータスの更新](#)

静的デバイスグループの作成または編集

すべてのデバイス ページで、親の静的グループの下の子グループを作成または編集することができます。これらのタスクを実行するには、適切なユーザー権限が必要です。「役割ベースの OpenManage Enterprise-Tech Release ユーザー権限」を参照してください。

1. 静的グループ を右クリックし、静的グループの新規作成 をクリックします。
2. 静的グループ作成ウィザード ダイアログボックスで、グループ名を入力し、新しい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。グループが作成され、左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。

① メモ: 静的グループの下にデバイスを直接追加することはできません。子の静的グループを作成し、その後、子グループの下にデバイスを追加する必要があります。

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更新されます。

クエリデバイスグループの作成

① メモ: OpenManage Enterprise-Tech Release 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。「役割ベースの OpenManage Enterprise-Tech Release ユーザー権限」を参照してください。

1. クエリグループ を右クリックして、クエリグループの新規作成 をクリックします。静的グループまたはクエリ (動的) グループに関する定義については、「デバイスのグループ化」を参照してください。
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、グループ名を入力します。
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」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、左側ペインに親グループの行にリストされます。

① メモ: クエリグループの下にデバイスを直接追加できません。子クエリグループを作成し、次に子グループの下にデバイスを追加する必要があります。

クエリグループを編集するには、次の手順を実行します。

- a. 左ペインで、子クエリグループを右クリックし、編集 をクリックします。

- b. または、左ペインで、子クエリグループをクリックします。グループ内のデバイスのリストが作業ペインに一覧表示されます。デバイスリストの先頭にある灰色の帯域内で **編集** リンクをクリックします。クエリグループの作成ウィザード ダイアログボックスが表示されます。
- c. **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、このセクションの前半に記載されているデータを入力するか、選択します。

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](#)」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](#)」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–Tech Release 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。すべての既存のクエリに事前定義されているフィルタの数は、クエリのタイプによって異なります。たとえば、**ハイパーバイザのシステム**のクエリには、6つの事前定義されたフィルタがありますが、**ネットワークスイッチ**のクエリは、3つのみです。クエリの定義中に最大20件の条件（フィルタ）を定義できます。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–Tech Release 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：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を持つ組み込みクエリ条件です：Task Enabled=Yes
2. **Query1** のフィルタプロパティをコピーし、**Query2** を作成してから、別のフィルタ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。「[監査ログの管理](#)」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編集](#)

[設定コンプライアンスベースラインの削除](#)

静的子グループのデバイスの追加または編集

静的子グループを使用して、その用途、設定、使用分野、お客様などに基づいてサーバを分類することができます。子グループにデバイスを追加または削除し、編集、削除およびそのようなグループのクローンを作成することができます。

メモ：OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。

1. 静的子グループを右クリックして、**デバイスを追加** をクリックします。静的グループに関する定義については、「[デバイスのグループ化](#)」を参照してください。
2. **グループ <名前> へのデバイスの追加** ダイアログボックスで、グループに追加する必要があるデバイスのチェックボックスを選択します。選択したデバイスが、**選択されたすべてのデバイス** タブに表示されます。
3. **終了** をクリックします。
デバイスは、選択した静的子グループに追加され、右ペインに表示されます。

静的子グループのプロパティを編集するか、または静的子グループからデバイスを削除するには、次の手順を実行します。

1. 静的グループを右クリックして、**編集** をクリックします。
2. **グループ <名前>** への**デバイスの編集** ダイアログボックスで、グループのプロパティを編集し、**次へ** をクリックします。
3. **グループメンバーの選択** ダイアログボックスで、グループに追加するかまたはグループから削除する必要のあるデバイスのチェックボックスを選択するかまたはクリアします。選択したデバイスが、**選択されたすべてのデバイス** タブに表示されます。
4. **終了** をクリックします。デバイスが選択した静的子グループに追加されるか、またはデバイスが選択した静的子グループから削除されます。

メモ: この手順は、グループのデバイスプロパティを編集する場合にのみ適用されます。OpenManage Enterprise–Tech Release からデバイス削除するか、またはデバイスをグローバルに除外するには、「OpenManage Enterprise–Tech Release からのデバイスの削除」および「デバイスをグローバルに除外する」を参照してください。

静的またはクエリ動的グループの子グループの名前の変更

1. 静的グループまたはクエリグループを右クリックし、**名前の変更** をクリックします。静的グループまたはクエリ（動的）グループに関する定義については、「[デバイスのグループ化](#)」を参照してください。
2. **グループの名前変更** ダイアログボックスで、グループ名を入力し、**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。

静的またはクエリグループのクローニング

静的グループまたはクエリグループを使用して、その用途、設定、使用分野、お客様などに基づいてサーバを分類することができます。静的グループおよびクエリグループにデバイスを追加、編集、削除およびそのようなグループのクローンを作成することができます。静的グループまたはクエリグループのクローンを作成するには：

1. 静的グループまたはクエリグループを右クリックして、**クローン** をクリックします。
 2. **クローングループ** ダイアログボックスに、グループ名を入力し、クローン化された静的グループまたはクエリグループが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。
- メモ:** カスタムグループのみをクローン化することができます。「**編集**」および「**表示**」権限を持っている必要があります。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。

メモ: クローン化された静的グループまたはクエリグループの下に直接デバイスを追加できます。

新しいグループへのデバイスの追加

1. 作業中のペインで対象デバイスに対応するチェックボックスを選択し、**グループに追加**、**新規グループに追加** の順にクリックします。
 - a. **デバイスを新規グループに追加** 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。
 - 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。そうでない場合、手順5に進みます。
 2. **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。「[デバイスリスト](#)」を参照してください。
 3. **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デバイスをグループに追加する際には、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

メモ: OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」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。

2. 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。「[デバイスの表示と設定](#)」を参照してください。
3. 作業中のペインで、対象のデバイスに対応するチェックボックスを選択し、**グループに追加**、**既存グループに追加**の順にクリックします。
 - a. **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。
 - 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 5 に進みます。
4. **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。「[デバイスリスト](#)」を参照。
5. **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。

OpenManage Enterprise–Tech Release からのデバイスの削除

1. 左ペインで、デバイスを選択します。
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、**削除** をクリックします。
3. デバイスがグローバルに除外されてい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。
このデバイスは削除され、OpenManage Enterprise–Tech Release による監視の対象外になります。

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–Tech Release が削除されたリモートデバイスのトラップ送信先として設定されている場合、リモートデバイスから、OpenManage Enterprise–Tech Release を削除できます。

- 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。

関連情報

[デバイスのグループ化](#)

OpenManage Enterprise–Tech Release からのデバイスの除外

- メモ:** OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。

ファームウェアアップデート、検出、インベントリの生成など、繰り返されるタスクを効率的に処理するために、デバイスをグループ化します。ただし、OpenManage Enterprise–Tech Release によって監視されていないために、除外されたデバイスがこれらのアクティビティのいずれかに参加しないようにデバイスを除外することができます。このタスクは、グローバル除外と同様です。「[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。

1. 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。
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、**除外する** をクリックします。
3. 選択したデバイスを除外するかどうか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。
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–Tech Release によって監視されません。
4. グローバル除外を削除して OpenManage Enterprise–Tech Release でデバイスを再度監視するためには、デバイスをグローバル除外範囲から削除して、再検出します。

ファームウェアベースラインを使用したデバイスファームウェアのアップグレードまたはダウングレード

① メモ: OpenManage Enterprise-Tech Release 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。「役割ベースの OpenManage Enterprise-Tech Release ユーザー権限」を参照してください。

次の場所から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またはダウングレードすることができます。

- すべてのデバイス ページ：複数のデバイスのファームウェアをアップデートする際に推奨されます。デバイス メニューから、**デバイス** を選択します。デバイスを選択して、**追加アクション > ファームウェアのアップデート** をクリックします。
- すべてのデバイス ページ：単一のデバイスのファームウェアをアップデートする際に推奨されます。デバイス メニューから、**デバイス** を選択します。デバイスを選択して、**詳細の表示 > ファームウェア** をクリックします。
- ファームウェアの設定 ページ：**設定** メニューから **ファームウェア** を選択します。デバイスを選択し、**コンプライアンスの確認 > レポートの表示** をクリックします。

① メモ: デバイスを接続したときにファームウェアのバージョンがベースラインのバージョンより古いと、バージョンは自動的に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. 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。「**デバイスリスト**」を参照。

① 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ます。
3. **追加アクション > ファームウェアのアップデート** をクリックします。
4. **ファームウェアのアップデート** ダイアログボックスで、次のように実行します。
 - a. **ソースの選択** セクションで、次の手順を実行します。
 - ベースライン ドロップダウンメニューから、デバイスのファームウェアの比較とアップグレードまたはロールバックに使用すべき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。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。ただし、**詳細の表示** ページで個々のデバイスのコンプライアンスを確認すると、ファームウェアのバージョンをアップグレードまたはロールバックできます。「**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**」を参照してください。
 - 1. 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。
 - 2. **次へ** をクリックします。
 - b. **前提条件** セクションに、デバイスの前提条件が表示されます（ある場合）。**次へ** をクリックします。
 - c. **スケジュール** セクションで、次のように選択します。
 - 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。この後でこのジョブを実行することができます。
5. **終了** をクリックします。ジョブリストにファームウェアアップデート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**」を参照してください。

① メモ: 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。

① メモ: 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。

ファームウェアソースの選択

ファームウェアソースの**選択** タブでは、ファームウェアをアップデートするために必要なベースラインまたは個々のアップデートパッケージを選択できます。

ベースライン	アップデートするファームウェアのベースラインバージョンをアップデートするには、このオプションを選択します。ドロップダウンから必要なベースラインバージョンを選択します。
コンプライアンス	ファームウェアバージョンがカタログファイルで定義されているベースラインに準拠しているかどうかを示します。
モデル	デバイスのモデルを表示します。
サービスタグ	ファームウェアをアップデートするデバイスのサービスタグを表示します。
デバイス名/コンポーネント	デバイスまたはコンポーネントの名前を表示します。
再起動必須	ファームウェアがインストールされた後にシステムの再起動が必要かどうかを示します。
現在のバージョン	インストールされているファームウェアのバージョンを表示します。
ベースラインバージョン	ファームウェアのベースラインを表示します。
個々のパッケージ	カタログからファームウェアをアップデートするには、このオプションを選択します。 参照 をクリックして、カタログファイルがある場所に移動します。

処置

次へ	前提条件 タブを表示します。
キャンセル	変更を保存せずにウィザードを閉じます。

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。「[デバイスの表示と設定](#)」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。

- i **メモ:** 個々のデバイスのアップデート機能を使用してアップグレードされたファームウェアのみをロールバックすることができます。
- i **メモ:** 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 を使用して更新された任意のデバイスファームウェアはここにリストされず、更新できません。ベースラインの作成については、「[ファームウェアのベースラインの作成](#)」を参照してください。

- 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。
- <デバイス名> ページで、**ファームウェア** をクリックします。
- 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、「[デバイスファームウェアのコンプライアンスレポートの表示](#)」を参照してください。
- ↓ 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に関して、対応するそのチェックボックスをオンにします。
- ファームウェアのロールバック** をクリックします。
- 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。
- 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。

- i **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。

デバイスインベントリを更新する

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は、24時間ごと（つまり毎日 AM 12:00 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、デバイスまたはグループのインベントリレポートを収集できます。

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、デバイスリストに表示されます。
2. デバイスに対応するチェックボックスを選択し、**インベントリの更新** 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、ジョブステータス行に **新規** と示されます。
選択したデバイス（複数可）のインベントリが収集され、今後の検索および分析のために保存されます。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、「**デバイスの表示と設定**」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つのデバイスインベントリのエクスポート**」を参照してください。

関連情報

[デバイスのグループ化](#)

デバイスステータスの更新

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、**ステータスの更新** 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–Tech Release 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つのデバイスインベントリのエクスポート**」を参照してください。

関連情報

[デバイスのグループ化](#)


1つのデバイス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のは1つのデバイスのみで、エクスポート形式は MS Excel 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:** MS-Excel 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。

デバイスリスト

デバイスリストには、IP アドレスおよびサービスタグなどのデバイスプロパティが表示されます。

-  **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** は、デバイスの動作状態を示します。正常性状態（OK、重要、警告）は、色記号によって識別されます。「**デバイスの正常性状態**」を参照してください。
- ・ **電源状態** は、デバイスのオン/オフを示します。
- ・ **接続状態** は、デバイスが OpenManage Enterprise–Tech Release へ接続されているかどうかを示します。
- ・ **タイプ** は、デバイスのタイプ（サーバ、シャーシ、Dell ストレージ、ネットワークスイッチ）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。
- ・ **管理状態** 列は、デバイスがオンボードしているかどうかを示します。「**デバイスのオンボーディング**」を参照してください。

表のデータをフィルタするには、**詳細フィルタ** または **フィルタアイコン** 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。「**デバイスの表示と設定**」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、デバイスリスト、保証情報、Support Assist などに関連。
- ・ 次のファイル形式にエクスポートされます：HTML、CSV、PDF、および MS-Excel。

メモ: ただし、単一のデバイスのインベントリは、**MS Excel 形式** にのみエクスポートできます。「**1つのデバイスインベントリのエクスポート**」を参照してください。

メモ: 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**」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。

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 > すべてのデバイス > 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、次の操作を実行できます。

- ・ 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–Tech Release は、OpenManage Enterprise–Tech Release の監視対象デバイス上で使用される NIC、BIOS、HDD、および VD 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** 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。「**デバイスファームウェアの管理**」を参照してください。
- ・ 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**」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ベースラインの管理**」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。詳しくは、idracmanual.com で入手可能な『iDRAC User's Guide』(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。管理 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。
 - ・ **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](#)」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、バッテリーなど、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。
- ① メモ**: **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](#)」を参照してください。
 - ・ iDRAC をリセットします。
 - ・ SupportAssist レポートを解凍およびダウンロードします。「[SupportAssist レポートの解凍とダウンロード](#)」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](#)」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](#)」を参照してください。

OpenManage Enterprise–Tech Release は、OpenManage Enterprise–Tech Release 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](#)」を参照してください。

デバイスのハードウェア情報

OpenManage Enterprise–Tech Release 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](#)」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。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『[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。
- ・ **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–Tech Release は、監視対象デバイスで使用可能な HDD または仮想ドライブに関して、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](#)」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–Tech Release は、監視対象デバイスに設置されたフィールド交換可能装置 (FRU) に関して、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**」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–Tech Release 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 ID 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

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**: http://en.community.dell.com/techcenter/extras/m/white_papers/20438187 でテクニカルホワイトペーパー『*Remotely Running Automated Diagnostics Using WS-Man and RACADM Commands*』(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**」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て、**<サービスタグ>.<時刻>.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。

SupportAssist レポートの解凍とダウンロード

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**」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

- ・ [<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、「[監査ログの管理](#)」を参照してください。
- ・ 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

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。
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。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。
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](#)」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。

メモ: 次の RACADM コマンドを実行しないでください。

- `chassislog view -n all`
- `chassislog view -n`
- `gettraclog`

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](#)」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、第 14 世代サーバの iDRAC Enterprise ライセンスで機能します。第 12 世代および第 13 世代サーバでは、このリンクは 2.50.50 以降のバージョンの OME Enterprise の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バージョンが ActiveX 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を向上させるために、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表示されます。「[仮想コンソールプラグインタイプの変更](#)」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。




デバイスファームウェアの管理

OpenManage Enterprise > 設定 をクリックして、以下を選択します。

- ・ **ファームウェア**：ファームウェアベースラインを使用して、デバイスのファームウェアを管理します。
- ・ **導入**：テンプレートを作成して設定コンプライアンスベースラインを定義し、そのテンプレートを管理します。
- ・ **コンプライアンス**：デバイスまたは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を作成してデバイス設定を管理します。関連するテンプレートのベースラインの概要を確認するには、「[OpenManage Enterprise–Tech Release ダッシュボードを使用したデバイスコンプライアンスベースラインの管理](#)」を参照してください。

メモ：デバイスを接続したときにファームウェアのバージョンがベースラインのバージョンより古いと、バージョンは自動的に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。

メモ：OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。これらの設定を管理するには、OpenManage Enterprise–Tech Release 管理者レベルの資格情報が必要です。

- ・ ファームウェア機能を使用すると、次の操作を実行できます。
 - ・ Dell.com、またはネットワークパスにあるカタログを使用して、ファームウェアカタログを作成。[Dell.com 使用によるファームウェアカタログの作成](#)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。デバイス上のファームウェアのバージョンをカタログのバージョンと迅速に比較するためのローカルベンチマークとして機能するファームウェアベースラインを作成するには、カスタマイズしたファームウェアカタログを使用します。
 - ・ 使用可能なファームウェアのカタログを使用して、ファームウェアのベースラインを作成します。「[ファームウェアのベースラインの作成](#)」を参照。ダッシュボード上にもファームウェアベースラインレポートを表示できます。「[OpenManage Enterprise–Tech Release ダッシュボードを使用したファームウェアベースラインの管理](#)」を参照してください。
 - ・ 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が、ベースラインのバージョンに適合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のバージョンがファームウェアのベースラインと同じである場合は、白いチェックマークが付いた緑色のボックス .
 - ・ **アップグレード** — ターゲットデバイスにファームウェアベースラインより前のバージョンが1つ以上ある場合は、内側に白い乗算記号が入った赤い円 。「[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。
 - ・ **ダウングレード** - デバイスファームウェアがベースラインバージョンよりも後である場合は、青い下向き矢印 .
 - ・ 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。
 - ・ ファームウェアのベースラインを使用して、デバイスのファームウェアバージョンをアップデートします。「[ファームウェアベースラインを使用したデバイスファームウェアのアップグレードまたはダウングレード](#)」を参照してください。

メモ：すべての使用可能なベースラインにあるデバイスのコンプライアンスレベルは、ドーナツグラフで示されます。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、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、多くのデバイスのコンプライアンスレベルがOKおよびダウングレードでも、グループ内の1台のデバイスのコンプライアンスレベルがアップグレードの場合、その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して示されます。

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。「[デバイスの表示と設定](#)」を参照してください。

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。

関連タスク

ファームウェアのベースラインの削除

トピック：

- ・ [ファームウェアカタログの管理](#)
- ・ [ファームウェアカタログの編集](#)
- ・ [ファームウェアのベースラインの作成](#)
- ・ [ファームウェアのベースラインの削除](#)
- ・ [ベースラインとデバイスファームウェアの照合の確認](#)
- ・ [ファームウェアのベースラインの編集](#)
- ・ [ファームウェアのベースラインの削除](#)

ファームウェアカタログの管理

カタログは、デバイスタイプに基づいてファームウェアにバンドルされています。使用可能なすべてのカタログ（アップデートパッケージ）は検証されて Dell.com に掲載されます。そこから、要件に基づいてカタログをダウンロードし、お使いのデバイスのためのローカルリポジトリとして機能するファームウェアのベースラインを作成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は、Dell.com へ頻繁にアクセスする必要がなくなり、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。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](#)」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。

- ・ **Dell.com にある最新コンポーネントファームウェアバージョン**：最新のデバイスのファームウェアバージョンがリストされます。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**：Dell.com または Dell Repository Manager (DRM) から展開（ローカルダウンロード）後に、カタログおよびオプションとして関連付けられたアップデート情報が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。
 - ① **メモ**：ローカルシステムに保存されている単一のデバイスアップデートパッケージを、ローカルネットワークのカタログの一部として使用できます。

Dell.com 使用によるファームウェアカタログの作成

① **メモ**：OpenManage Enterprise-Tech Release 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。「[役割ベースの OpenManage Enterprise-Tech Release ユーザー権限](#)」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. **ファームウェアカタログの追加** ダイアログボックスで、次の手順を実行します。
 - a) ファームウェアカタログの名前を入力し、**Dell.com にある最新コンポーネントファームウェアバージョン** を選択します。
 - b) **終了** をクリックします。

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** 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。

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

1. **カタログ管理** ページで、**追加** をクリックします。
2. **ファームウェアカタログの追加** ダイアログボックスで、次の手順を実行します。
 - a) ファームウェアカタログの名前を入力して、**ネットワークパス** 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。
 - b) 次のいずれか1つを選択します。
 - ・ NFS
 1. **共有アドレス** ボックスに、ファームウェアカタログがネットワーク上に保存されている、システムの IP アドレスを入力します。
 2. **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完全なファイルパスを入力します。
 3. **終了** をクリックします。

・ CIFS

1. **共有アドレス** ボックスに、ファームウェアカタログがネットワーク上に保存されている、システムの IP アドレスを入力します。
2. **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完全なファイルパスを入力します。
3. **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。
4. **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。
5. **パスワード** ボックスに、デバイスのパスワードを入力して共有にアクセスします。

・ HTTP

1. **共有アドレス** ボックスに、ファームウェアカタログがネットワーク上に保存されている、システムの IP アドレスを入力します。
2. **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完全なファイルパスを入力します。

・ HTTPS

1. **共有アドレス** ボックスに、ファームウェアカタログがネットワーク上に保存されている、システムの IP アドレスを入力します。
2. **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完全なファイルパスを入力します。
3. **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。
4. **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。
5. **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。

3. **追加** をクリックします。

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** 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。

関連タスク

[ファームウェアカタログの削除](#)

SSL 証明書情報

ファームウェアアップデート用のカタログファイルは、デルサポートサイト、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。


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。

ファームウェアカタログの削除

1. **カタログ管理** ページで、対象のカタログ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。カタログファイルがリストから削除されます。
2. **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。

 **メモ:** ファームウェア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使用によるファームウェアカタログの作成](#)

ファームウェアカタログの編集

1. **カタログ管理** ページで、対象のカタログに対応するチェックボックスを選択します。
ファームウェアカタログの詳細が、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. **ファームウェアカタログの編集** ダイアログボックスで、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 使用によるファームウェアカタログの作成](#)」および「[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。
4. **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。

ファームウェアのベースラインの作成

- ① **メモ:** **OpenManage Enterprise-Tech Release** 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。「[役割ベースの OpenManage Enterprise-Tech Release ユーザー権限](#)」を参照してください。
- ① **メモ:** デバイスを接続したときにファームウェアのバージョンがベースラインのバージョンより古いと、バージョンは自動的に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。

ベースラインはカスタマイズされ、ファームウェアバージョン一式がローカルに保存されるので、簡単にアクセスして適用できます。ベースラインは次に基づいて適用できます：1つのベースライン対複数のデバイス、複数のベースライン対1台のデバイス、および複数のベースライン対複数のデバイス。たとえば、ある BIOS バージョン用に作成されたベースラインを、同じ BIOS を実行している複数のサーバに適用できます。同様に、1つはファームウェアバージョン用に、他方は BIOS 用という具合に、2つのベースラインを1つのデバイスに適用することもできます。ファームウェアのベースラインを作成するには、次の手順を実行します。

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. **ファームウェア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。
 1. **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。
 2. このリストにカタログを追加するには、**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。
 3. **ベースライン名** ボックスで、ベースラインの名前を入力してから説明を書き込みます。
 4. **次へ** をクリックします。
 - b) **デバイスの選択** セクションで、次の手順を実行します。
 - ・ ターゲットデバイスを選択する場合：
 1. **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。
 2. **デバイスの選択** ダイアログボックスには、OpenManage Enterprise-Tech Release、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。
 3. 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。
 4. 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：
 1. **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。
 2. **グループの選択** ダイアログボックスには、OpenManage Enterprise-Tech Release、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。
 3. 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。
 4. 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](#)」を参照してください。

ファームウェアのベースラインの削除

ファームウェアに、使用可能なファームウェアのベースラインのリストが表示されます。ベースラインに対応するチェックボックスを選択し、**削除**をクリックします。ファームウェアのベースラインが削除され、ベースラインのリストから削除されます。

ベースラインとデバイスファームウェアの照合の確認




- ① **メモ:** OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。
- ① **メモ:** デバイスを接続したときにファームウェアのバージョンがベースラインのバージョンより古いと、バージョンは自動的に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 **メモ:** ダッシュボードでもファームウェアベースラインレポートを確認できます。「[OpenManage Enterprise–Tech Release ダッシュボードを使用したファームウェアベースラインの管理](#)」を参照してください。

ファームウェアのベースラインを作成したら、カタログの使用によって定義されたベースラインバージョンと、デバイスのコンポーネントのファームウェアバージョンのコンプライアンスを定期的に照合することができます。デバイスのファームウェアバージョンのコンプライアンスを確認するには、次の手順を実行します。

- 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。ファームウェアベースラインコンプライアンスジョブが再実行されます。
 - ① **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](#)」を参照してください。
- ① **メモ:** Dell EMC M1000e および VRTX シャーシのファームウェアコンプライアンスベースラインレベルをチェックするとき、ファームウェアバージョンが同じでも、コンプライアンスレベルは **ダウングレード** と示されます。これは、**OpenManage Enterprise–Tech Release** と **FTP** の間でのファームウェアバージョンの命名規則に違いがあるためです。このようなステータスは**無視**し、ファームウェアのバージョンをダウングレードしないことを推奨します。
- コンプライアンスレポートを表示して、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またはダウン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。

デバイスファームウェアのコンプライアンスレポートの表示

すべての使用可能なベースラインにあるデバイスのコンプライアンスレベルは、ファームウェアページのドーナツグラフで示されます。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、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いて、多くのデバイスのコンプライアンスレベルがOK 、ダウングレード  になっていても、グループ内で1台のデバイスのコンプライアンスが**重要**  になっている場合は、ベースラインのコンプライアンスレベルは**重要**と示されます。

ただし、あるファームウェアベースラインに関連付けられている個々のデバイスのファームウェア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。デバイスファームウェア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。

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『*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。

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、「[デバイスファームウェアの管理](#)」を参照してください。

メモ: Dell EMC M1000e および VRTX シャーシのファームウェアコンプライアンスベースラインレベルをチェックするとき、ファームウェアバージョンが同じでも、コンプライアンスレベルはダウングレードと示されます。これは、OpenManage Enterprise-Tech Release と FTP の間でのファームウェアバージョンの命名規則に違いがあるためです。このようなステータスは無視し、ファームウェアのバージョンをダウングレードしないことを推奨します。

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ファームウェアベースラインに対するコンプライアンス状態が一覧表示されます。

2. ファームウェアのコンプライアンスステータスがクリティカルで、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選択します。

3. [ファームウェアのアップデート](#) をクリックします。「[デバイスのファームウェアバージョンのアップデート](#)」を参照。

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、「[デバイスの表示と設定](#)」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 **i**: 各デバイスコンポーネントに対応する記号は、サポートサイトページにリンクされており、そこからファームウェアを更新できます。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: ファームウェアのベースラインで使用可能なデバイスの対応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-Tech Release グラフィカルユーザーインターフェースの概要](#)」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バージョンのアップデート

メモ: OpenManage Enterprise-Tech Release 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。「[役割ベースの OpenManage Enterprise-Tech Release ユーザー権限](#)」を参照してください。

メモ: デバイスを接続したときにファームウェアのバージョンがベースラインのバージョンより古いと、バージョンは自動的に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。

After you run a firmware compliance report, if the firmware version on the device is earlier than the version on the catalog, the


Compliance Report page indicates the device firmware status as Upgrade 。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をアップデートするには:

1. 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、「[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。

2. ファームウェア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. **ファームウェアのアップデート** をクリックします。
4. **ファームウェアのアップデート** ダイアログボックスで、次のように選択します。
 - ・ **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。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。
5. **アップデート** をクリックします。

 **メモ:** デバイスをアップデートするには、デバイスとカタログを相互に関連付ける必要があります。

ファームウェアのベースラインの編集

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、右ペインで **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** 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。

ファームウェアのベースラインの削除

ベースライン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。ファームウェアのベースラインが削除され、更新された情報がベースラインのリストに表示されます。

関連情報

[デバイスファームウェアの管理](#)

デバイス設定テンプレートの管理

OpenManage Enterprise > **設定** > **導入** の順にクリックして、**導入** を選択すると、既定のテンプレートを使用して、ファームウェアのバージョン、ネットワークプロパティ、およびサーバ、シャーシ、ストレージデバイスの BIOS バージョンなどの設定プロパティを設定できます。テンプレートを使用すると、データセンターのリソース、内容領域専門家 (SME) 帯域幅を最適化し、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。テンプレートを利用すれば、ソフトウェア定義インフラストラクチャを使用するコンバイン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。

メモ: 標準ユーザーは、管理者が権限を付与したテンプレートに限り、表示および使用することができます。**OpenManage Enterprise-Tech Release** 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。「[役割ベースの OpenManage Enterprise-Tech Release ユーザー権限](#)」を参照してください。

トピック：

- ・ [テンプレート情報の表示](#)
- ・ [テンプレートの作成または編集](#)
- ・ [デバイステンプレートの導入](#)
- ・ [テンプレートのクローン作成](#)

テンプレート情報の表示

OpenManage Enterprise メニューで、**設定** > **導入** をクリックします。使用可能なテンプレートのリストが表示されます。

1. テンプレートのリストで、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 ページの **設定の詳細** セクションに、テンプレートの作成に使用された属性が表示されます。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。
3. 要素を展開して子コンポーネントを表示するには：
 - ・ テンプレートを導入するには、「[デバイステンプレートの導入](#)」を参照してください。
 - ・ テンプレートを編集するには、「[テンプレートの作成または編集](#)」を参照してください。
 - ・ テンプレートデータを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](#)」を参照してください。
 - ・ リストの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。

テンプレートの作成または編集

メモ: **OpenManage Enterprise-Tech Release** 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。「[役割ベースの OpenManage Enterprise-Tech Release ユーザー権限](#)」を参照してください。

参照デバイスを使用するか、既存のテンプレートからインポートすることによって、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. **作成** をクリックして **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) **テンプレート情報** セクションに、テンプレートの名前と説明を入力します。
 - b) 次の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。
 - c) **次へ** をクリックします。
 - d) **参照デバイス** 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。

- 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。サーバをデバイスとして使用してテンプレートを作成する場合は、iDRAC、BIOS、Lifecycle Controller、イベントフィルタなどのサーバ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。たとえば、iDRAC および RAID です。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。
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。正常に作成された後、ジョブがリストに表示されます。ジョブ ページにもジョブ情報が表示されます。

既存のテンプレートファイルからインポートして作成するには、「[テンプレートファイルをインポートしてテンプレートを作成する](#)」を参照してください。

- ・ 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、テンプレートのリストに表示されます。

テンプレートファイルをインポートしてテンプレートを作成する

1. **作成** をクリックして **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) 新しいテンプレート名を入力します。
 - 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) **サーバ** または **シャーシ** を選択して、テンプレートのタイプを示します。
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、新しいテンプレートが作成されます。
 - ・ 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。上のテンプレートの **詳細** ページで、テンプレートを展開および編集できます。「[デバイステンプレートの導入](#)」および「[テンプレートの作成または編集](#)」を参照してください。
 - ・ 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、テンプレートのリストに表示されます。

設定テンプレートの作成中のネットワークプロパティの編集

該当する NIC 属性を含む任意のテンプレートのネットワーク設定を編集できます。

1. 必要に応じて、次を編集します。
 - ・ **番号** : NIC 番号
 - ・ **NIC ID** : NIC の拡張完全修飾デバイスディスクリプタ
 - ・ **ポート** : ネットワークポート番号
 - ・ **パーティション** : ネットワークパーティション番号
 - ・ **最小帯域幅 (%)** : ネットワークの最小帯域幅
 - ・ **最大帯域幅 (%)** : ネットワークの最大帯域幅
2. **終了** をクリックします。更新されたネットワークプロパティが保存されます。

デバイス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設定テンプレートを導入すると、デバイスの設定を確実に統一できます。

メモ: OpenManage Enterprise-Tech Release 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。「[役割ベースの OpenManage Enterprise-Tech Release ユーザー権限](#)」を参照してください。

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テンプレートのクローニングが完了している。「[テンプレートの作成または編集](#)」を参照してください。
- ・ ターゲットデバイスは、[OpenManage Enterprise–Tech Release の導入のための最小システム要件](#) に指定されている要件を満たします。
- ・ OpenManage Enterprise ライセンスがすべてのターゲットデバイスにインストールされている。

△注意: 適切なデバイスのみが再利用およびベアメタルデバイスグループに追加されていることを確認します。再利用およびベアメタルデバイスに設定テンプレートを導入した後は、デバイスを元の設定に戻すことができない可能性があります。

1. テンプレートのリストで、テンプレートを導入する必要があるデバイスに対応するチェックボックスを選択します。
2. テンプレートの詳細 ページで、テンプレートの導入 をクリックします。
3. 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。
①メモ: OpenManage Enterprise–Tech Release は、選択されたデバイスに推奨するテンプレートのみを表示します。
 - b) **次へ** をクリックします。
4. ネットワーク ISO からの起動 セクションで：
 - 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。このチェックボックスは、ターゲットデバイスがサーバである場合にのみ表示されます。
 - b) CIFS または NFS のいずれかを選択し、フィールドに ISO イメージファイルのパスなどの情報を入力し、ISO イメージファイルが保存される場所を共有します。
 - c) **次へ** をクリックします。
5. 電源オプション セクションでは、導入後にデバイスを再起動する必要がある場合のみ、入力または選択します。各フィールドの説明を表示するには、その上にポインタを置きます。このセクションは、ターゲットデバイスがサーバである場合にのみ表示されます。
6. **次へ** をクリックします。
7. 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](#)」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](#)」を参照してください。

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)、**導入** をクリックします。利用可能な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。クローンのテンプレートが作成され、テンプレートのリストに表示されます。

デバイス設定コンプライアンスベースラインの管理

OpenManage Enterprise > 設定 > コンプライアンス をクリックして **コンプライアンス** を選択すると、ビルトインまたはユーザー作成のテンプレートを使用して設定ベースラインを作成できます。設定コンプライアンスベースラインテンプレートを作成するには、既存のビルトインテンプレートのクローンを作成する必要があります。この機能を使用するには、サーバに OpenManage Enterprise-Tech Release 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。シャーシ管理コントローラ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。「[役割ベースの OpenManage Enterprise-Tech Release ユーザー権限](#)」を参照してください。「[OpenManage Enterprise-Tech Release ダッシュボードを使用したデバイスコンプライアンスベースラインの管理](#)」も参照してください。

① メモ: 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、各ベースラインにコンプライアンスレベルの概要が表にリストされます。各デバイスに独自のステータスがあり、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『*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。

この機能を使用すると、次の操作を実行できます。

- ・ 設定コンプライアンスのベースラインを作成します。「[設定コンプライアンスベースラインの作成](#)」を参照してください。
- ・ 設定コンプライアンスのベースラインに対して、デバイスまたはデバイスグループのコンプライアンスをチェックします。
- ・ コンプライアンステンプレートを管理します。「[コンプライアンステンプレートを使用したデバイスコンプライアンスの監視](#)」を参照してください。

設定コンプライアンスのベースラインデータを使用して、ベースラインポリシーを逸脱した場合に警告するアラートポリシーを設定します。アラートは OpenManage Enterprise-Tech Release のダッシュボードページで表示できるコンプライアンスベースラインに基づいて生成されます。アラートポリシーの設定の詳細については、「[デバイスのアラートの監視](#)」を参照してください。

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**
- ・ **前回の実行時刻**：このベースラインのコンプライアンスレベルをチェックするために最後に設定インベントリレポートが実行された時刻。

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](#)」を参照してください。

OpenManage Enterprise-Tech Release 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 > テンプレートのコンプライアンスベースラインごとのデバイス数** 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](#)」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](#)

[設定コンプライアンスベースラインの編集](#)

[設定コンプライアンスベースラインの削除](#)

[コンプライアンスベースラインテンプレートの管理](#)

[クエリ条件の選択](#)

トピック：

- ・ [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の編集](#)

- ・ [設定コンプライアンスベースラインの削除](#)

設定コンプライアンスベースラインの作成

OpenManage Enterprise–Tech Release は、10 のベースラインを単一のデバイスに割り当て、一度に最大 500 デバイスのコンプライアンスレベルをチェックすることができます。ビルトインのベースラインを表示するには、**OpenManage Enterprise > 設定 > コンプライアンス** の順にクリックします。

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ベースラインの管理](#)」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コンプライアンスベースラインテンプレートを作成する](#)」を参照してください。
- ・ サポートデバイスからインポートされテンプレートを使用する。「[ファイルからインポートしてコンプライアンスベースラインを作成する](#)」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](#)」を参照してください。

△ 注意: ベースラインに使用するテンプレートがすでに別のベースラインに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とすで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が変更されます。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『[Error and Event Message Reference Guide](#)』（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 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. **ベースラインの作成** をクリックします。
2. **コンプライアンス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、ビルトインまたはユーザーが作成した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ベースラインの管理](#)」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](#)」を参照してください。

① 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、ベースライン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せん。
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ベースラインの管理](#)」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削除](#)

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ベースラインの管理](#)」を参照してください。

△ 注意: ベースラインに使用するテンプレートがすでに別のベースラインに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とすで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が変更されます。「[ベースラインコンプライアンステンプレートの編集](#)」を参照してください。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『*Error and Event Message Reference Guide*』（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. **OpenManage Enterprise** > **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、**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](#)」を参照してください。

関連タスク

[コンプライアンスベースラインテンプレートの管理](#)
[クエリ条件の選択](#)

関連情報

[デバイス設定コンプライアンス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削除](#)

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ベースラインの管理](#)」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–Tech Release** 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『*Error and Event Message Reference Guide*』（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. **OpenManage Enterprise** > **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](#)
[クエリ条件の選択](#)
[コンプライアンスベースラインテンプレートの管理](#)
[設定コンプライアンスベースラインの編集](#)

関連情報

[デバイス設定コンプライアンスベースラインの管理](#)

コンプライアンステンプレートをを使用したデバイスコンプライアンスの監視

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のベースラインを作成し、その後、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の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ベースラインの管理](#)」を参照してください。導入用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ベースラインテンプレートを作成できます。「[コンプライアンスベースラインテンプレートの管理](#)」を参照してください。

OpenManage Enterprise > **設定** > **コンプライアンス** の順にクリックすると、**全体的なコンプライアンスのサマリ** ページが表示され、**テンプレートの管理** タブで設定コンプライアンスベースラインの作成に使用したテンプレートを管理できます。

関連タスク

[コンプライアンスベースラインテンプレートの管理](#)

[コンプライアンスのベースラインテンプレートのクローン作成](#)

トピック：

- ・ [コンプライアンスベースラインテンプレートの管理](#)

コンプライアンスベースラインテンプレートの管理

導入用テンプレート、リファレンスデバイスを使用するか、またはファイルからインポートしてベースラインテンプレートを作成できます。

OpenManage Enterprise > **設定** > **コンプライアンス** > **テンプレートの管理** の順にクリックして、コンプライアンステンプレートのリストを表示できます。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コンプライアンスベースラインテンプレートを作成する](#)」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コンプライアンスベースラインテンプレートを作成する](#)」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。「[ファイルからインポートしてコンプライアンスベースラインを作成する](#)」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。「[ベースラインコンプライアンステンプレートの編集](#)」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。「[コンプライアンスのベースラインテンプレートのクローン作成](#)」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](#)」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。

関連情報

[デバイス設定コンプライアンス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編集](#)

[設定コンプライアンスベースラインの削除](#)

[コンプライアンステンプレートを使用したデバイスコンプライアンスの監視](#)

[導入テンプレートからコンプライアンスベースラインテンプレートを作成する](#)

[ベースラインコンプライアンステンプレートの編集](#)

導入テンプレートからコンプライアンスベースラインテンプレートを作成する

1. **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での **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ベースラインとして使用する必要があるテンプレートを選択します。
3. ベースライン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。
コンプライアンステンプレートが作成され、設定コンプライアンスベースラインのリストに一覧表示されます。

関連タスク

[コンプライアンスベースラインテンプレートの管理](#)

[コンプライアンスのベースラインテンプレートのクローン作成](#)

リファレンスデバイスからコンプライアンスベースラインテンプレートを作成する

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](#)」を参照してください。

1. **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、ベースライン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のいずれかのプロパティをクローンすることによって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、テンプレートを作成するためにマスター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](#)」を参照してください。
 - a) マスターとして「サーバ」を選択した場合は、クローニングする必要のあるサーバ設定のプロパティも選択します。
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ベースラインテンプレートは、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。

ファイルからインポートしてコンプライアンスベースラインを作成する

1. **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、ベースライン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ザして選択します。
4. **終了** をクリックします。
設定コンプライアンス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ベースラインテンプレートのクローン作成

1. **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

[コンプライアンステンプレートを使用したデバイスコンプライアンスの監視](#)
[導入テンプレートからコンプライアンスベースラインテンプレートを作成する](#)
[ベースラインコンプライアンステンプレートの編集](#)

ベースラインコンプライアンステンプレートの編集

設定ベースラインのプロパティを編集する場合、それにリンクされているテンプレートのプロパティを編集することができます。

△ 注意: ベースラインに使用されている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『*Error and Event Message Reference Guide*』（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. **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. **終了** をクリックします。
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

[コンプライアンスベースラインテンプレートの管理](#)
[コンプライアンスのベースラインテンプレートのクローン作成](#)

デバイスのアラートの監視

OpenManage Enterprise メニューをクリックして **アラート** にある項目を選択すると、次のことが実行できます。

- アラートの管理方法：
 - アラートの確認
 - アラートの無視
 - アーカイブされたアラートの表示 および アーカイブされたアラートのダウンロード
- アラートポリシーの作成と管理。「アラートポリシー」を参照してください。
- アラート定義の表示。「アラートの定義」を参照してください。
- すべてまたは選択したアラートデータをエクスポートします。「データのエクスポート」を参照してください。

i **メモ:** これらの設定を管理するには、**OpenManage Enterprise–Tech Release** 管理者レベルの資格情報が必要です。「**役割ベースの OpenManage Enterprise–Tech Release ユーザー権限**」を参照してください。

OpenManage Enterprise–Tech Release にはビルトインレポートが備わっており、OpenManage Enterprise–Tech Release 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。「**レポートの実行**」を参照してください。

関連概念

[アラートログの表示](#)

関連タスク

[アラートの削除](#)

トピック：

- アラートログの表示
- アラートの確認
- アラートの未確認
- アラートの無視
- アラートの削除
- アーカイブされたアラートの表示
- アーカイブされたアラートのダウンロード
- アラートポリシー
- アラートの定義

アラートログの表示

OpenManage Enterprise > 設定 > アラート > アラートログの順にクリックします。アラートのリストが表示されます。アラートの重要度、生成時刻、アラートを生成したソースデバイス、アラートカテゴリ、およびアラートメッセージが表示されます。

- 重要度は、アラートの重要度を示します。
- 確認は、アラートが表示され、確認されると、チェックマークを表示します。生成されたアラートの合計数も OpenManage Enterprise–Tech Release のヘッダーに表示されます。「**OpenManage Enterprise–Tech Release グラフィカルユーザーインターフェースの概要**」を参照してください。
- ソース名 の下のハイパーリンクされているデバイス名をクリックして、アラートを生成したデバイスのプロパティを表示して、設定します。「**デバイスの表示と設定**」を参照してください。
- カテゴリ は、アラートのカテゴリを示します。たとえば、システムの正常性や監査などです。

アラートが表示および確認されると、アラートに対応する **確認** 列にチェックマークが表示されます。

このページで実行できるのは、アラートデータの確認、未確認、無視、エクスポート、削除、およびアーカイブです。アーカイブされたアラートの詳細については、「**アーカイブされたアラートの表示**」を参照してください。

関連タスク

[アラートの削除](#)

関連情報

[デバイスのアラートの監視](#)

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。これを確認するには、対象のアラートに対応するチェックボックスを選択し、**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。

アラートの未確認

不正なアラートまたは繰り返し表示されるアラートを未確認の状態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、**確認の解除** をクリックします。**確認** 行で、そのアラートに対応するチェックマークが削除されます。それ以外の場合は、チェックマークをクリックして、すでに確認されたアラートメッセージを未確認の状態にできます。

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-Tech Release 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。OpenManage Enterprise-Tech Release で今後発生するこのアラートが表示されないようにするには、アラートを無視します。「[アラートの無視](#)」を参照してください。

1. 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。
2. **はい** をクリックします。
アラートが削除されます。

OpenManage Enterprise-Tech Release 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。

関連概念

[アラートログの表示](#)

関連情報

[デバイスのアラートの監視](#)

アーカイブされたアラートの表示

OpenManage Enterprise-Tech Release を使用して、一度に最大 50,000 件のアラートを生成し、閲覧できます。上限の 50,000 件の 95% (47,500 件) に達すると、OpenManage Enterprise-Tech Release 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-Tech Release はアーカイブされたアラートの 10% (5,000 件) を自動的にページすることを通知します。次の表では、アラートのページに関連するさまざまなシナリオを示します。

表 8. アラートのページ

ワークフロー	説明	結果
ページタスク	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、ページアーカイブにチェックを入れて生成します。

ワークフロー	説明	結果
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 」を参照してください。

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、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表示されます。
 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。
- i** **メモ**：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。「[役割ベースの OpenManage Enterprise-Tech Release ユーザー権限](#)」を参照してください。

アラートポリシー

OpenManage Enterprise > **アラート** > **アラートポリシー** の順にクリックすると、以下を実行できます。

- ・ 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。
- ・ 定義済みカテゴリのアラートが生成されると、アラートを電子メールアドレス、電話、SNMPトラップに送信したり、デバイスの電源のオン/オフを切り替えるなどのデバイス電源制御アクションを実行したりできます。
- ・ アラートポリシーの作成、編集、有効化、無効化、削除を行います。

チェックマークが付いているアラートポリシーは、そのアラートポリシーが有効になっていることを示しています。ポリシーの基準を満たすアラートを受信した場合、電子メールメッセージの送信やSNMPトラップ転送の有効化などのアクションを実行するためのポリシーを設定することができます。前述の設定をすることによって、次の操作を行うことができます。

- ・ 電子メールメッセージを送信する場合、次の操作を行います。
 1. アラートポリシーに対応する **電子メール** セルをクリックします。
 2. **アラート処置**：電子メール ダイアログボックスで、送信するメッセージに関する情報を入力します。テキストボックスに示されているサンプルメッセージパターンを使用します。
 3. **終了** をクリックします。チェックマークがセルに表示されます。設定されたポリシー基準を満たすアラートを受信すると、電子メールメッセージが送信されます。
- ・ SNMPトラップを転送する場合、次の操作を行います。
 1. アラートポリシーに対応する **SNMPトラップ** セルをクリックします。
 2. プロンプトが表示されたら、**はい** をクリックします。
 3. アラートの下で、**SNMP設定** を展開します。
 4. 「**SMTP、SNMP、およびシスログアラートの設定**」のタスクを完了します。チェックマークがセルに表示されます。設定されたポリシー基準を満たすアラートを受信すると、SNMPトラップが作動します。
- ・ アラートポリシーを無視する場合、次の操作を行います。
 1. アラートポリシーに対応する **無視** セルをクリックします。
 2. ポリシーに関連付けられているすべてのアクションが削除されること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。チェックマークがセルに表示されます。ポリシー基準を満たすアラートを受信しても無視されます。
- ・ 通知をモバイルデバイスに送信します。プッシュ通知を送信するには OpenManage Enterprise-Tech Release と携帯電話を設定する必要があります。「[OpenManage Mobile 設定](#)」を参照してください。

- アラートポリシーに対応する **モバイル** セルをクリックします。有効にした場合、ポリシーは無効にされ、チェックマークが消えます。無効にした場合は、逆になります。
- SMS メッセージを送信する場合、次の操作を行います。
 - アラートポリシーに対応する **SMS** セルをクリックします。
 - アラート処置：SMS** ダイアログボックスに電話番号を入力します。
 - 終了** をクリックします。チェックマークがセルに表示されます。設定されたポリシー基準を満たすアラートを受信すると、SMS メッセージが送信されます。
 - デバイスで電源制御操作を実行する場合、次の操作を行います。
 - アラートポリシーに対応する **電源制御** セルをクリックします。
 - アラート処置：電源制御** ダイアログボックスで、デバイスの電源サイクルのオン/オフを選択します。
 - 終了** をクリックします。チェックマークがセルに表示されます。設定されたポリシー基準を満たすアラートを受信すると、SMS メッセージが送信されます。
 - リモートスクリプトを実行する場合、次の操作を行います。
 - アラートポリシーに対応する **リモートスクリプトの実行** セルをクリックします。
 - プロンプトが表示されたら、**はい** をクリックします。
 - スクリプトの実行** タブの **リモートコマンドの設定** で、「**デバイスの管理用リモートコマンドジョブの作成**」にあるタスクを完了します。チェックマークがセルに表示されます。設定されたポリシー基準を満たすアラートを受信すると、指定したコマンドを実行します。

関連タスク

- [アラートポリシーの削除](#)
- [アラートポリシーを無効にする](#)
- [アラートポリシーを有効にする](#)
- [アラートポリシーの編集](#)
- [アラートポリシーの作成](#)

アラートポリシーの作成

メモ: OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。

- アラートポリシー > **作成** の順をクリックします。
- アラートポリシーの作成** ダイアログボックスで、**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。
 - デフォルトでアラートポリシーを有効にするには、**ポリシーの有効化** チェックボックスを選択します。
 - 次へ** をクリックします。
- カテゴリ** セクションで、**すべて** チェックボックスを選択してそのアラートポリシーをすべての使用可能なカテゴリに適用します。デフォルトで、次のカテゴリが表示されますが、適用はされていません。各カテゴリの下にサブカテゴリを表示するには、カテゴリを展開します。
 - 次へ** をクリックします。
- ターゲット** セクションでグループまたはデバイスを追加します。「[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。
 - 次へ** をクリックします。
- 日付と時刻** セクションの **日付範囲** 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。
 - 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。
 - 次へ** をクリックします。
- 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。
 - 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。
 - 次へ** をクリックします。
- アクション** セクションで、ポリシー実行時に開始される以下のアクションのチェックボックスを1つ、または複数選択します
 - 電子メール** チェックボックスを選択して電子メールを宛先の受信者に送信し、フィールドでデータを指定します。
 - SNMP アラートを設定する場合は、**SNMP トラップ転送** チェックボックスの横にある **有効** をクリックします。**SNMP 設定** ダイアログボックスで、データを入力または選択します。「[SMTP、SNMP、およびシスログアラートの設定](#)」を参照してください。

- ・ シスログプロパティを設定します。
 - ・ 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。
 - ・ SMS を電話番号に送信する場合は、**宛先** に電話番号を入力します。
 - ・ デバイスの電源を制御する場合は、対象のデバイスで電源サイクリングまたは電源のオン/オフを実行します。電源制御処置を実行する前に OS をシャットダウンするには、**最初に OS をシャットダウンする** チェックボックスを選択します。
 - ・ リモートコマンドを実行する場合は、**リモートスクリプトの実行** の横にある **有効** をクリックします。
 - ・ **リモートコマンドの設定** ダイアログボックスに、実行するリモートコマンドを設定する情報を入力するか、または選択します。「[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。
 - ・ 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。「[OpenManage Enterprise–Tech Release アプライアンス設定の管理](#)」で説明されているリモートコマンドの実行も設定できます。
 - ・ **モバイル**：このバージョンの OpenManage Enterprise–Tech Release に登録されている携帯電話に通知を送信します。「[OpenManage Mobile 設定](#)」を参照してください。
8. **次へ** をクリックします。
 9. **概要** セクションには、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。

関連情報

[アラートポリシー](#)

SMTP、SNMP、およびシスログアラートの設定

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電子メール (SMTP) アドレス、SNMP 送信先、シスログの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–Tech Release 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–Tech Release 間の電子メールの通信を管理する SMTP サーバを設定し認証するには、次の手順を実行します。

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 サーバを認証するには、**認証を有効にする** チェックボックスを選択し、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. **適用** をクリックします。
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。

SNMP トラップの転送を設定するには、次の手順を実行します。

1. **SNMP 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。
4. **SNMP バージョン** ドロップダウンメニューから SNMP バージョンのタイプを選択します。現在サポートされているのは、SNMP1 バージョンと SNMP2 バージョンのみです。
5. **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。
6. SNMP トラップのデフォルトのポート番号は 162 です。必要に応じて編集します。「[OpenManage Enterprise–Tech Release でサポートされるプロトコルおよびポート](#)」を参照してください。
7. 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。
8. **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。

シスログメッセージを設定するには、次の手順を実行します。

1. **シスログ設定** を展開します。
2. **サーバ** 行の各サーバのチェックボックスを選択して、シスログ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、シスログ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–Tech Release でサポートされるプロトコルおよびポート](#)」を参照してください。
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き、OpenManage Enterprise–Tech Release のスクリプトを実行してアラート管理用の他社製チケットシステムのチケットを開くためのポリシーを設定することができます。すぐに実行する、または後で実行するためのリモートコマンドは4つ作成して保存することができます。

1. **リモートコマンドの設定** ダイアログボックスで、次の手順を実行します。
 - a) 後で実行する際に適切なスクリプトを選択して実行するために役立つよう、スクリプト名を入力します。
 - b) コマンドを実行する OpenManage Enterprise–Tech Release サーバの IP アドレスを入力します。
 - c) 資格情報を入力して、OpenManage Enterprise–Tech Release サーバにログインします。
 - d) チケットを開くために OpenManage Enterprise–Tech Release サーバで実行する必要のあるコマンドを入力します。たとえば、`./RCE.sh $IP $MODEL $DATE $ASSETTAG $SERVICETAG`

2. **保存** をクリックします。

コマンドが保存されます。これらのコマンドは、アラートポリシーを設定中にも設定して実行できます。「[アラートポリシーの作成](#)」を参照してください。


メモ:


- 一度に実行できるのは、1つの実行可能ファイルまたはスクリプトのみです。
- 実行可能ファイルまたはスクリプトは、必ずしも **OpenManage Enterprise–Tech Release** によって検出または管理されないサーバに保存できます。
- スクリプトは、最大 **1024** 文字を入力できます。
- **OpenManage Enterprise–Tech Release** は、スクリプトまたはチケットシステムに役立つトークン代替をサポートします。サポートされるトークン：**\$IP**、**\$MSG**、**\$HOSTNAME**、**\$SERVICETAG**、**\$ASSETTAG**、**\$DATE**、**\$TIME**、**\$MODEL**

アラートポリシーを有効にする

アラートポリシーを有効にできるのは、アラートポリシーが無効の場合だけです。**名前と説明** セクションで **ポリシーの有効化** チェックボックスを選択すると、アラートポリシー作成中にそのアラートポリシーを有効にできます。「[アラートポリシーの作成](#)」を参照してください。

アラートポリシーを有効にするには、対象のアラートポリシー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。アラートポリシーが有効化され、アラートポリシーが有効であることを示すチェックマーク (**有効** 列) が表示されます。

 **メモ:** 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有効にすることができます。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。

 **メモ:** 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。

関連情報

[アラートポリシー](#)

アラートポリシーの編集

1. アラートポリシー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. **アラートポリシーの作成** ダイアログボックスで、アラートポリシーのプロパティを編集します。ダイアログボックス内の別のセクションを移動するには、「[アラートポリシーの作成](#)」を参照してください。

関連情報

[アラートポリシー](#)

アラートポリシーを無効にする

アラートポリシーが有効になっている場合に限り、それを無効にすることができます。アラートポリシー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、そのポリシーが無効になります。「[アラートポリシーの作成](#)」を参照してください。

アラートポリシーを無効にする場合は、対象のアラートポリシーに対応するチェックボックスを選択し、**無効** をクリックします。アラートポリシーが無効になり、アラートポリシーが有効であることを示すチェックマーク (**有効** 行) が削除されます。

メモ: 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無効にできます。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。ただし、アラートポリシーには、少なくとも1つ関連付けられたアクションが必要です。

メモ: すでに無効になっているアラートポリシーの **無効** ボタンは、グレー表示されます。

関連情報

アラートポリシー

アラートポリシーの削除

アラートポリシーを削除する場合は、対象のアラートポリシー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。対象のアラートポリシーが削除され、アラートポリシーの表から削除されます。

メモ: 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。

関連情報

アラートポリシー

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ーフェイス (GUI) と、RACADM および WS-Man のコマンドラインインターフェイス (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。

監査ログの管理

監査ログは、OpenManage Enterprise–Tech Release で監視されているデバイスで実行されたアクションをリストします。ログデータは、ユーザーおよび Dell EMC サポートチームによるトラブルシューティングと分析に役立ちます。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](#)」を参照してください。

メモ: OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。

OpenManage Enterprise メニューをクリックして **監視** にある項目を選択すると、次のことが実行できます。

- ・ デバイスの電源およびデバイス LED のステータスを制御するジョブを作成します。「[デバイス制御のためのジョブの使用](#)」を参照。
- ・ デバイスの検出と管理。「[デバイスの検出](#)」を参照。
- ・ デバイスインベントリを生成するジョブの計画。「[デバイスインベントリの管理](#)」を参照してください。
- ・ デバイスの保証に関するアラートの作成と受信。「[デバイス保証の管理](#)」を参照してください。
- ・ デバイスコンポーネントに関するレポートの作成。「[デバイスのパフォーマンスのレポート](#)」を参照。
- ・ MIB の管理。「[MIB の管理](#)」を参照。

メモ: 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 > **監視** > **監査ログ** の順にクリックすると、OpenManage Enterprise–Tech Release を使用して実行されるタスクに関して、OpenManage Enterprise–Tech Release が保存および表示する監査ログを管理できます。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。

1. OpenManage Enterprise メニューの **モニター** の下で、**監査ログ** を選択します。

a) 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。

モニター ページの **監査ログ** の下に、実行された各種アクティビティのリストが表示され、重要度、時刻、ユーザー名、メッセージ ID、システム IP、カテゴリ、およびアクティビティの説明などの情報が示されます。

2. 監査ログに関する情報を素早く検索するには、**詳細フィルタ** 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。

3. 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。
- ・ **開始時刻** および **終了時刻**：タスクが実行されるおおよその開始時刻と終了時刻を選択します。
- ・ **ユーザー**：タスクを実行するシステムのユーザー名を入力します。
- ・ **ソースアドレス**：タスクを実行するシステムの IP アドレスを入力します。
- ・ **カテゴリ**：タスクが属しているカテゴリを選択します。そのカテゴリ内のすべてのメッセージが表示されます。
- ・ **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。検索条件に一致すると、リスト内のすべてのアイテムが削除され、目的のメッセージ ID のみが表示されます。

4. フィルタを削除する場合は、**詳細フィルタ** をクリックします。

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。

監査ログデータをエクスポートするには、「[すべてまたは選択したデータのエクスポート](#)」を参照してください。

デバイスコントロール用ジョブの使い方

① **メモ:** OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。

① **メモ:** 各ジョブは次に説明するデバイスに制限されます。

- ・ ユーザーがアクセス権を与えられている。
- ・ 必要なアクションを完了する機能がある。

このルールは、デバイス選択タスクを伴う点滅、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のベースラインの管理などのすべてのタスクに適用できます。

OpenManage Enterprise > 監視 > ジョブ の順にクリックすると、以下を実行できます。

- ・ 現在実行中、失敗、および正常に完了した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](#)」、「[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。「[デバイスの表示と設定](#)」を参照してください。
- ・ ジョブに対応するチェックボックスを選択して **今すぐ実行** をクリックし、ジョブを実行します。
- ・ 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、ジョブを停止します。
- ・ ジョブに対応するチェックボックスを選択して **有効** をクリックし、ジョブを有効にします。
- ・ ジョブ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、ジョブを無効にします。
- ・ 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、ジョブを削除します。

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](#)
- ・ [個々のジョブ情報の表示](#)
- ・ [デバイスの LED を点滅させるジョブの作成](#)
- ・ [電源管理のためのジョブの作成](#)
- ・ [デバイスの管理用リモートコマンドジョブの作成](#)
- ・ [仮想コンソールプラグインタイプの変更](#)
- ・ [ターゲットデバイスおよびデバイスグループの選択](#)

ジョブリストの表示

OpenManage Enterprise > 監視 > ジョブ の順にクリックして、既存ジョブのリストを表示します。ジョブのステータス、ジョブのタイプ、日時などの情報が表示されます。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](#)」を参照してください。ジョブのステータスは次のとおりです。

- ・ **新規:** ジョブは作成されていますが、まだ実行されていません。ジョブを実行するには、対応するチェックボックスを選択して **今すぐ実行** をクリックします。ジョブが開始され、ジョブのステータス 列にステータスは **実行中** と表示されます。
- ・ **実行中**
- ・ **スケジュール済み**
- ・ **完了**
- ・ **エラーで終了**
- ・ **失敗**
- ・ **停止**

ジョブは、次のいずれかのタイプに属します。

- ・ **正常性:** デバイスの正常性状態を取得します。「[デバイスの正常性状態](#)」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](#)」を参照してください。

- ・ デバイスの設定：デバイスの設定コンプライアンススペ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スペースラインの管理](#)」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](#)」を参照してください。
- ・ 保証：デバイスの保証状態についてのデータを生成します。「[デバイス保証の管理](#)」を参照してください。
- ・ オンボーディングタスク：「[デバイスのオンボーディング](#)」を参照してください。
- ・ 検出：OpenManage Enterprise–Tech Release で管理するデバイスの検出。「[監視または管理のためのデバイスの検出](#)」を参照してください。

OpenManage Enterprise–Tech Release 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](#)」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。

メモ：デフォルトでは、新しいジョブを作成するための作成タブだけが有効になっています。ただし、リストからジョブを選択した場合は、ジョブの実行、削除、有効化、停止、無効化タブが有効になります。

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。

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](#)」を参照してください。

デバイスの LED を点滅させるジョブの作成

1. **作成** をクリックして **デバイスの点滅** を選択します。
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。
 1. **ジョブ名** ボックスにジョブ名を入力します。
 2. **LED の点滅期間** ドロップダウンメニューで、LED を設定した期間または無限に点滅させるか、オフにするオプションを選択します。
 3. **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](#)」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](#)」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で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](#)」を参照してください。

電源管理のためのジョブの作成

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。
 1. ジョブ名 にジョブ名を入力します。
 2. 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
 3. 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」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」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で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」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

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) インタフェース ドロップダウンメニューから、IPMI、または RACADM のいずれかのコマンドラインインタフェース (CLI) を選択します。
 - c) 引数 ボックスにコマンドを入力し、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。

メモ: raclog コマンドラインジョブウィザード ダイアログボックスで、raclog RACADM コマンドを実行しないでください。ハードウェアログ タブの下のデバイスハードウェアのログデータを確認します。
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」を参照してください。
4. 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」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. このジョブが後の時点で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」を参照してください。

仮想コンソールプラグインタイプの変更

お使いのサーバで使用されているプラグインがHTML5 以前のバージョンの場合は、プラグインタイプのアップデートを求めるメッセージが表示されます。アップデートするには、HTML5 に変更 をクリックし、次の操作を行います。

1. 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。
2. 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。
3. 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」を参照してください。
 - a) 次へ をクリックします。
4. 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」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. 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](#)」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。

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–Tech Release 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](#)」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](#)」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。

監視または管理のためのデバイスの検出

① **メモ:** OpenManage Enterprise-Tech Release 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。「[役割ベースの OpenManage Enterprise-Tech Release ユーザー権限](#)」を参照してください。

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。

① **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。

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。「[デバイスをグローバルに除外する](#)」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](#)

[デバイス検出ジョブの詳細の表示](#)

[デバイス検出ジョブの停止](#)

[デバイス検出ジョブの実行](#)

[サーバ検出ジョブを作成するための検出モード指定](#)

[サーバ用の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](#)

[デル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](#)

[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編集](#)

トピック：

- ・ [デバイス検出ジョブの詳細の表示](#)
- ・ [デバイス検出ジョブの削除](#)
- ・ [デバイス検出ジョブの停止](#)
- ・ [デバイス検出ジョブの実行](#)
- ・ [デバイス検出ジョブの作成](#)
- ・ [.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する](#)
- ・ [デバイスをグローバルに除外する](#)
- ・ [サーバ用の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](#)
- ・ [デル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](#)
- ・ [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編集](#)
- ・ [Windows または Hyper-V サーバを検出するために WS-Man in HTTPS モードを有効にする](#)

デバイス検出ジョブの詳細の表示

1. 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。
2. 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](#)」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

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

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

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

デバイス検出ジョブの作成

メモ: OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。

デバイスを検出するには、次の手順を実行します。

1. **検出 > 作成** の順にクリックします。

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。これを変更するには、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、次のフィールドがもう1セット表示されます：タイプ、IP/ホスト名/範囲、設定。
 - ・ .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する](#)」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 **ネットワークスイッチ** を選択します。「[ストレージ、デルストレージ、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](#)」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。
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](#)」を参照してください。
8. **検出されたサーバからのトラップ受信の有効化** を選択し、OpenManage Enterprise–Tech Release が検出されたサーバから着信トラップを受信するのを有効にします。
9. **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、およびシスログアラートの設定](#)」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。
10. **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](#)」を参照してください。

i **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、OpenManage Enterprise–Tech Release がシャーシではなく、すべてのサーバでトラップの送信先として設定されます。

SMTP、SNMP、およびシスログアラートの設定

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電子メール (SMTP) アドレス、SNMP 送信先、シスログの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–Tech Release 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–Tech Release 間の電子メールの通信を管理する SMTP サーバを設定し認証するには、次の手順を実行します。

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 サーバを認証するには、**認証を有効にする** チェックボックスを選択し、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. **適用** をクリックします。
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。

SNMP トラップの転送を設定するには、次の手順を実行します。

1. **SNMP 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。
4. **SNMP バージョン** ドロップダウンメニューから SNMP バージョンのタイプを選択します。現在サポートされているのは、SNMP1 バージョンと SNMP2 バージョンのみです。
5. **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。
6. SNMP トラップのデフォルトのポート番号は 162 です。必要に応じて編集します。「[OpenManage Enterprise–Tech Release でサポートされるプロトコルおよびポート](#)」を参照してください。
7. 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。
8. **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。

シスログメッセージを設定するには、次の手順を実行します。

1. **シスログ設定** を展開します。
2. サーバ 行の各サーバのチェックボックスを選択して、シスログ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、シスログ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–Tech Release でサポートされるプロトコルおよびポート](#)」を参照してください。
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。

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。

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。

- ① **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。
- ① **メモ:** OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」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–Tech Release 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。
 - ・ アラートの管理対象: デバイスは正常にオンボードされ、OpenManage Enterprise–Tech Release コンソールがアラートレシーバーとしてデバイスに登録されます。
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、**その他の操作 > オンボード** の順にクリックします。このとき、オンボードをサポートしているデバイスタイプのみ選択されていることを確認します。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。
 - ① **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ません。iDRAC のみがサポートされます。したがって、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. **詳細設定** を展開します。
 - 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。
 - 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。

- ① **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。

.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する

1. **デバイスの検出** ダイアログボックスで、**検出ジョブ名** に検出ジョブの名前を入力します。デフォルトでは、検出ジョブの名前が入力されます。
2. **インポート** をクリックします。

① **メモ:** .csv ファイルに無効な範囲が含まれてい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。
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。

① **メモ:** 必要に応じて、サンプルの .csv ファイルをダウンロードします。

デバイスをグローバルに除外する

- ① **メモ:** OpenManage Enterprise-Tech Release 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。「[役割ベースの OpenManage Enterprise-Tech Release ユーザー権限](#)」を参照してください。
- ① **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。

すべての使用可能なデバイスからデバイスを検出する場合は、次の手順を実行して OpenManage Enterprise-Tech Release による監視から特定のデバイスを除外することができます。

1. **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](#)」を参照してください。
2. **追加** をクリックします。
3. 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-Tech Release 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。

① **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。

次の順にクリックしてグローバルに除外されたデバイスのリストを表示できます。

- ・ **デバイス > すべてのデバイス > グローバルに除外**。 **グローバル除外範囲** ダイアログボックスに除外されたデバイスのリストが表示されます。
- ・ **モニタ > 検出 > 作成 > グローバル除外**。 **グローバル除外範囲** ダイアログボックスに除外されたデバイスのリストが表示されます。
- ・ **モニタ > 検出 > グローバル除外リスト**。 **グローバル除外範囲** ダイアログボックスに除外されたデバイスのリストが表示されます。

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 OpenManage Enterprise-Tech Release によって監視されています。OpenManage Enterprise-Tech Release 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。

- ① **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-Tech Release** から削除されます。

- メモ:** 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 Hyper-V、Windows、または Linux オペレーティングシステムを使用して検出します。
 - ・ **デル以外のサーバ (帯域外経由)** : IPMI を使用してサードパーティのサーバを検出します。
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。「[サーバおよびシャーシ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](#)」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](#)

サーバ用の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

検出ウィザード ダイアログボックスで、次の手順を実行します。

1. **WSMAN の有効化** チェックボックスを選択し、WS-Man コマンドを使用してサーバを検出できるようにします。
2. 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。
3. **詳細設定** を展開します。
 - 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-Tech Release でサポートされるプロトコルおよびポート](#)」を参照してください。
 - ・ **信頼できるキーの生成** : デフォルトでは無効です。選択して、デバイスと通信するために信頼できるデバイスを生成します。

メモ: 最初、ユーザーは REST API を使用して、信頼キーを生成する必要があり、その後でのみこのオプションを使用できます。このキーはデバイスごとに生成され、管理下デバイスとの信頼関係を有効にします。
 - d) デバイスの共通名が OpenManage Enterprise-Tech Release 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. 次のチェックボックスのいずれかを選択して、それらのプロトコルを使用して検出を有効にします。対応するデバイスの資格情報を入力します。
 - ・ **SNMP を有効にする** : SNMP 互換デバイスの検出用。
 - ・ **RedFish を有効にする** : サーバの検出用。
 - ・ **IPMI を有効にする** : サーバの検出用。
 - ・ **SSH を有効にする** : Linux サーバの検出用。
 - ・ **VMware を有効にする** : ESXi ホストの検出用。

5. **終了** をクリックします。
6. 「[デバイス検出ジョブの作成](#)」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](#)

シャーシ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、**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作成する場合は、**追加の設定** をクリックします。「[サーバおよびシャーシ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。

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。

デル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

1. **タイプ** ドロップダウンメニューで **DELL ストレージ** または **ネットワークスイッチ** 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、検出するデバイスの SNMP バージョンを入力します。
4. **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、ストレージやネットワークなどの SNMP 向けにカスタマイズした検出テンプレートを作成する方法については、「[SNMP デバイス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。
6. 「[デバイス検出ジョブの作成](#)」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](#)

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 を有効にする** チェックボックスは、ストレージ、ネットワーク、または他の SNMP デバイスの検出を有効にするために選択されます。**検出ウィザード** ダイアログボックスで、次の手順を実行します。

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. 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。
3. **詳細設定** を展開します。
 - 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。
4. **終了** をクリックします。
5. 「[デバイス検出ジョブの作成](#)」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](#)

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、「[サーバ用の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](#)」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](#)

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. **デバイスの検出** 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](#)

Windows または Hyper-V サーバを検出するために WS-Man in HTTPS モードを有効にする

デフォルトでは、WS-Man サービスは Windows サーバ上で有効になりません。HTTPS モードでは、ターゲットサーバ上で WS-Man サービスを有効にする必要があります。

前提条件：


- ・ IIS と HTTPS 有効
- ・ WS-Man サービスと HTTPS 有効
- ・ PowerShell 4.0 が証明書を使用して WS-Man サービスを設定

自己署名証明書の作成

 **メモ:** 公開署名証明書がある場合は、簡単です。Set-WSManQuickConfig -UseSSL を使用できます。管理者としてログインすることにより **PowerShell** で次のコマンドを実行します。

```
$Cert = New-SelfSignedCertificate -CertstoreLocation Cert:\LocalMachine\My -DnsName "myHost"
```

-DnsName パラメータには、リモートで管理したいサーバの名前を入力することが重要です。サーバに DNS 名がある場合は、完全修飾ドメイン名 (FQDN) を使用する必要があります。

 **メモ:** \$Cert 変数には今後のコマンドで使用するためのサンプリントが保存されているため重要です。

ホストシステムでの PowerShell リモート処理の作成

Enable-PSRemoting も WS-Man リスナーを起動しますが、HTTP に対してのみです。

```
Enable-PSRemoting -SkipNetworkProfileCheck -Force
```

1. 他の人に HTTP を使用してサーバに接続されたくない場合は、コマンドを実行して、HTTP リスナーを削除できます。

```
Get-ChildItem WSMan:\localhost\listener | Where -Property Keys -eq "Transport=HTTP" | Remove-Item -Recurse
```

2. 新しい HTTPS リスナーを追加するには、すべての WS-Man リスナーを削除します。

```
Remove-Item -Path WSMAN:\localhost\listener\listener* -Recurse
```

3. WS-Man HTTPS リスナーを追加します。

```
New-Item -Path WSMAN:\localhost\Listener -Transport HTTPS -Address * -  
CertificateThumbPrint $Cert.Thumbprint -Force
```

i **メモ:** 先ほどサンプリントの読み取りのために定義した **\$Cert** 変数を使用します。この変数では、**New-Item cmdlet** が証明書ストアの証明書を検索することができます。

4. ファイアウォールルールを追加します。

```
New-NetFirewallRule -DisplayName "Windows Remote Management (HTTPS-In)" -Name "Windows  
Remote Management (HTTPS-In)" -Profile Any -LocalPort 5986 -Protocol TCP
```

5. 次を実行して設定を確認します。

```
C:\Windows\system32>winrm g winrm/config  
Config  
  MaxEnvelopeSizekb = 500  
  MaxTimeoutms = 60000  
  MaxBatchItems = 32000  
  MaxProviderRequests = 4294967295  
  Client  
    NetworkDelays = 5000  
    URLPrefix = wsman  
    AllowUnencrypted = false  
    Auth  
      Basic = true  
      Digest = true  
      Kerberos = true  
      Negotiate = true  
      Certificate = true  
      CredSSP = false  
    DefaultPorts  
      HTTP = 5985  
      HTTPS = 5986  
    TrustedHosts  
  Service  
    RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)  
    MaxConcurrentOperations = 4294967295  
    MaxConcurrentOperationsPerUser = 1500  
    EnumerationTimeoutms = 240000  
    MaxConnections = 300  
    MaxPacketRetrievalTimeSeconds = 120  
    AllowUnencrypted = false  
    Auth  
      Basic = true  
      Kerberos = true  
      Negotiate = true  
      Certificate = false  
      CredSSP = false  
      CbtHardeningLevel = Relaxed  
    DefaultPorts  
      HTTP = 5985  
      HTTPS = 5986  
    IPv4Filter = *  
    IPv6Filter = *  
    EnableCompatibilityHttpListener = false  
    EnableCompatibilityHttpsListener = true  
    CertificateThumbprint = 02554D694FD06BB3C765E5868EFB59B7D786ED67  
    AllowRemoteAccess = true  
  Winrs  
    AllowRemoteShellAccess = true  
    IdleTimeout = 7200000  
    MaxConcurrentUsers = 2147483647  
    MaxShellRunTime = 2147483647  
    MaxProcessesPerShell = 2147483647
```

```
MaxMemoryPerShellMB = 2147483647
MaxShellsPerUser = 2147483647
```

メモ: `service-basic-authentication` が `false` の場合は、次のコマンドを実行します。

```
winrm set winrm/config/service/auth @{Basic="true"}
```

メモ: WinRM 設定では、コマンドを実行して HTTPS を有効にします。

```
winrm set winrm/config/service @{EnableCompatibilityHttpsListener="true"}
```

- IIS を有効にして 443 で HTTPS を許可する - リモートシステムから Hyper-V サーバで次のコマンドを実行して、設定が動作することを確認します。

```
winrm e wmi/root/virtualization/v2/Msvm_SummaryInformation -r:https://<hyper-v server ip>:443/wsman -u:UserName -p:password -skipCNcheck -skipCAcheck -skipRevocationcheck -a:Basic
```

- IIS マネージャを開始します。
- デフォルトの Web サイト経由でサイトをバインディング ダイアログボックスで、HTTPS ポート番号として 443 を入力します。
- Administrator としてログインして、PowerShell で作成する SSL 証明書を選択します。

デバイスインベントリの管理

メモ: OpenManage Enterprise–Tech Release 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。「役割ベースの OpenManage Enterprise–Tech Release ユーザー権限」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–Tech Release 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**」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
- インベントリジョブの停止
- インベントリジョブの削除
- インベントリジョブの作成

トピック:

- ・ インベントリジョブの作成
- ・ インベントリジョブを今すぐ実行する
- ・ インベントリジョブの停止
- ・ インベントリジョブの削除
- ・ インベントリスケジュールジョブの編集

インベントリジョブの作成

メモ: OpenManage Enterprise–Tech Release 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。「役割ベースの OpenManage Enterprise–Tech Release ユーザー権限」を参照してください。

1. **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。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**」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**」を参照してください。

5. 設定コンプライアンスベースラインのインベントリを生成するには、**設定インベントリの追加の実行** チェックボックスを選択します。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ベースラインの管理](#)」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が指定されます。「[インベントリジョブを今すぐ実行する](#)」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](#)

インベントリジョブを今すぐ実行する

i **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](#)

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](#)

インベントリジョブの削除

i **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](#)

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](#)」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。

デバイス保証の管理

メモ: OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」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–Tech Release によって監視されているデバイスの保証ステータスを表示できます。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ができます。右ペインで、**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、保証を管理できます。保証 ページで、保証の状態とサービスタグと共に、次の情報が表示されます。

- ・ デバイスのサービスタグ、モデル名、およびモデルタイプ。
- ・ **保証タイプ** :
 - ・ 初期 : OpenManage Enterprise–Tech Release を最初に購入した際に提供される保証を使用することにより、保証は引き続き有効です。
 - ・ 延長 : OpenManage Enterprise–Tech Release を最初に購入した際に提供される保証期間が期限切れのため、保証が延長されます。
- ・ **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契約 (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](#)」を参照してください。

OpenManage Enterprise–Tech Release は、次の 30 日で期限切れす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](#)」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–Tech Release グラフィカルユーザーインターフェースの概要](#)」を参照してください。表内のデータを更新するには、右上隅にある **保証の更新** をクリックします。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](#)」を参照してください。

関連タスク

[デバイス保証情報の表示](#)

トピック :

- ・ [デバイス保証情報の表示](#)

デバイス保証情報の表示

OpenManage Enterprise > 監視 > 保証 の順にクリックします。デバイスおよび、それらのサービスタグ、モデル、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。有効期限の終了が近い保証ステータスのデバイスを簡単に確認するには、「[OpenManage Enterprise–Tech Release ダッシュボードを使用したデバイス保証の管理](#)」を参照してください。

- ・ フィールドの説明については、「[デバイス保証の管理](#)」を参照してください。
- ・ デバイスの保証情報を表示するには、デバイスに対応するチェックボックスを選択します。デバイスの保証情報が、右ペインに表示されます。他の情報とともに、サービスレベルコード、サービスプロバイダ、保証の開始日および終了日が表示されます。
- ・ 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、デバイス保証を管理できます。
- ・ 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。
- ・ 右上隅で、**保証の更新** ボタンをクリックすると、保証の一覧に表示されるデータが更新されます。
- ・ デバイスを検索するには **詳細フィルタ** オプションを使用します。

関連情報

[デバイス保証の管理](#)

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。

メモ: OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。

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–Tech Release 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。

メモ: レポートに表示されるデータは、OpenManage Enterprise–Tech Release の権限によって異なります。たとえば、レポートを生成するときに、特定のデバイスグループを表示する権限がない場合、そのグループに関するデータは表示されません。

表 9. OpenManage Enterprise–Tech Release のレポートを管理するための役割に基づいたアクセス権限

ユーザー役割...	許可されているレポートタスク...
管理者とデバイス管理者	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

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：アセット、FRU、ファームウェア、ファームウェア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](#)

[レポートの実行と電子メールの送信](#)

[レポートの編集](#)

[レポートの削除](#)

トピック：

- ・ [レポートの実行](#)
- ・ [レポートの実行と電子メールの送信](#)
- ・ [レポートの編集](#)
- ・ [レポートのコピー](#)
- ・ [レポートの削除](#)
- ・ [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

- メモ:** OpenManage Enterprise-Tech Release 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。「[役割ベースの OpenManage Enterprise-Tech Release ユーザー権限](#)」を参照してください。

レポートを実行すると、デフォルトでは、最大 1,000 行が表示されます。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](#)」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。役割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](#)」を参照してください。

- メモ:** 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。

- メモ:** レポートのカテゴリが「デバイス」の場合は、レポートの最初の列は、デバイスの名、デバイスモデル、およびデバイスのサービスタグになります。

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](#)」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](#)

レポートの実行と電子メールの送信

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** フィールドに、受信者の電子メールアドレスを入力します。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。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](#)」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](#)

レポートの編集

カスタマイズされたレポートのみを編集できます。

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](#)

レポートのコピー

カスタマイズされたレポートのみをコピーできます。

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

カスタマイズされたレポートのみを削除できます。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](#)

レポートの作成

メモ: **OpenManage Enterprise–Tech Release** 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。**「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。

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 10. OpenManage Enterprise–Tech Release のレポートを生成するための役割に基づいたアクセス権限

ユーザー役割...	許可されているレポートタスク...
管理者とデバイス管理者	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](#)」を参照してください。
 - b) **列** メニューを展開し、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。これらの列のデータは、定義したフィルタ条件を使用して入力されます。
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](#)」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。

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](#)」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](#)」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–Tech Release 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。すべての既存のクエリに事前定義されているフィルタの数は、クエリのタイプによって異なります。たとえば、**ハイパーバイザのシステム**のクエリには、6つの事前定義されたフィルタがありますが、**ネットワークスイッチ**のクエリは、3つのみです。クエリの定義中に最大20件の条件(フィルタ)を定義できます。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–Tech Release 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。

① 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を持つ組み込みクエリ条件です：**Task Enabled=Yes**
2. **Query1** のフィルタプロパティをコピーし、**Query2** を作成してから、別のフィルタ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。「[監査ログの管理](#)」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編集](#)

[設定コンプライアンスベースラインの削除](#)

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。

MIB ファイルの管理

メモ: OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」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–Tech Release ではこのような MIB の管理も可能になるため、Dell 以外の EMC MIB を OpenManage Enterprise–Tech Release 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–Tech Release は SM11 と SM12 をサポートします。OpenManage Enterprise–Tech Release 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 のみが、OpenManage Enterprise–Tech Release によって処理されます。

MIB の管理の仕方 :

- ・ MIB ファイルのインポート
- ・ MIB ファイルの削除
- ・ MIB タイプの解決

OpenManage Enterprise > 監視 > MIB を選択すると、OpenManage Enterprise–Tech Release 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 11. OpenManage Enterprise–Tech Release における MIB ファイルへの役割ベースのアクセス

OpenManage Enterprise–Tech Release の機能	MIB ファイルに対する役割ベースのアクセスコントロール		
	管理者	デバイス管理者	閲覧者
トラップまたは MIB の表示	有	有	有
MIB のインポートトラップの編集	有	無	無
MIB を削除	有	無	無
トラップの編集	有	無	無

OpenManage Enterprise–Tech Release 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

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 : ユーザーが **OpenManage Enterprise–Tech Release を MIB にアップロード** > **OpenManage Enterprise–Tech Release が MIB を解析** > **OpenManage Enterprise–Tech Release 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–Tech Release が MIB ファイルデータを表示**。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–Tech Release 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–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。

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**」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–Tech Release 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**」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–Tech Release 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**」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–Tech Release にインポートされたら、**最小** タブの下に表示されます。

① **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。

① **メモ:** すでに **OpenManage Enterprise–Tech Release** にインポートされたトラップはインポートできません。

① **メモ:** **OpenManage Enterprise–Tech Release** 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。

① **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–Tech Release 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–Tech Release 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。

① **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–Tech Release** 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

① **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」を参照してください。

① **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」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」を参照してください。

OpenManage Enterprise–Tech Release アプライアンス設定の管理

- ① **メモ:** OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。
- ① **メモ:** サポートされているブラウザの詳細については、サポートサイトで入手可能な『[OpenManage Enterprise–Tech Release Support Matrix](#)』（OpenManage Enterprise–Tech Release サポートマトリックス）を参照してください。

OpenManage Enterprise をクリックして、以下を実行できます。

- ・ IPv4、IPv6、時刻、およびプロキシ設定などの OpenManage Enterprise–Tech Release ネットワーク設定を行い、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。「[証明書署名要求の生成およびダウンロード](#)」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、およびシスログアラートの設定](#)」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–Tech Release のバージョンをアップデートします。「[OpenManage Enterprise–Tech Release バージョンの確認とアップデート](#)」を参照してください。
- ・ ユーザーの資格情報を設定し、RACADM、および 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 設定](#)」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

トピック：

- ・ [OpenManage Enterprise–Tech Release ネットワークの設定](#)
- ・ [OpenManage Enterprise–Tech Release ユーザーの管理](#)
- ・ [OpenManage Enterprise–Tech Release ユーザーの有効化](#)
- ・ [OpenManage Enterprise–Tech Release ユーザーの無効化](#)
- ・ [OpenManage Enterprise–Tech Release ユーザーの削除](#)
- ・ [ディレクトリサービスの削除](#)
- ・ [ユーザーセッションの終了](#)
- ・ [役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)
- ・ [OpenManage Enterprise–Tech Release ユーザーの追加と編集](#)
- ・ [OpenManage Enterprise–Tech Release ユーザーのプロパティの編集](#)
- ・ [Active Directory ユーザーのインポート](#)
- ・ [OpenManage Enterprise–Tech Release でのディレクトリサービスの統合](#)
- ・ [ログインセキュリティのプロパティの設定](#)
- ・ [セキュリティ証明書](#)
- ・ [コンソールプリファレンスの管理](#)
- ・ [SMTP、SNMP、およびシスログアラートの設定](#)

- ・ 着信アラートの管理
- ・ SNMP 資格情報の設定
- ・ 保証設定の管理
- ・ OpenManage Enterprise–Tech Release バージョンの確認とアップデート
- ・ リモートコマンドとスクリプトの実行
- ・ OpenManage Mobile 設定

OpenManage Enterprise–Tech Release ネットワークの設定

- ① **メモ:** OpenManage Enterprise–Tech Release 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。「役割ベースの OpenManage Enterprise–Tech Release ユーザー権限」を参照してください。
- ① **メモ:** vNIC を使用して OpenManage Enterprise–Tech Release 用の複数の IP がある場合は、REST API にアクセスするために現在の IP アドレス フィールド (アプリケーションの設定 > 現在の設定 の順にクリックします) に示される IPv4 アドレスのみを使用する必要があります。

現在の設定、時刻設定、および プロキシ設定 リンクを展開して OpenManage Enterprise–Tech Release ネットワークプロパティを表示または編集します。

- ・ OpenManage Enterprise–Tech Release の現在のネットワーク設定 (DNS ドメイン名、FQDN、IPv4 設定、IPv6 設定など) のみを表示するには、**現在の設定** を展開します。
- ・ タイムゾーン、日付、OpenManage Enterprise–Tech Release の NTP プロパティを設定するには、**時刻設定** を展開して次のように実行します。
 - a. フィールドでデータを選択するか入力します。
 - b. **適用** をクリックします。
 - c. 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。
- ・ OpenManage Enterprise–Tech Release プロキシ設定を設定するには、**プロキシ設定** を展開します。
 - a. **プロキシ認証の有効化** チェックボックスを選択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。
デフォルトでは、**HTTP プロキシ設定の有効化** チェックボックスはクリアされ、フィールドはグレー表示されています。これを選択して、データを編集します。デフォルトのプロキシアドレスは、10.116.2.243 です。ポート番号は 80 です。
 - b. **適用** をクリックします。
 - c. 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–Tech Release アプリケーション設定の管理」を参照してください。

OpenManage Enterprise–Tech Release ユーザーの管理

- ① **メモ:** OpenManage Enterprise–Tech Release 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。「役割ベースの OpenManage Enterprise–Tech Release ユーザー権限」を参照してください。
- ① **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–Tech Release 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。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 > 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–Tech Release ユーザーの表示、追加、有効化、編集、または削除。
 - ① **メモ:** 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。右のペインで **編集** をクリックして、パスワードを変更できます。
- ・ 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。
- ・ Active Directory からのユーザーのインポートと管理。

OpenManage Enterprise–Tech Release は、割り当てられたグループに基づくユーザー権限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 > グループごとのユーザー権限**の順にをクリックします。**実行**をクリックします。「**レポートの実行**」を参照してください。

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–Tech Release は次のようにデフォルトのユーザー役割を表示しますが、これは編集/削除できません：管理者、システム、ルートただし、デフォルトのユーザー名を選択し、**編集**をクリックすると、ログイン資格情報を編集できます。「[OpenManage Enterprise–Tech Release ユーザーの有効化](#)」を参照してください。
- ・ **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–Tech Release 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–Tech Release ユーザーの有効化](#)」および「[OpenManage Enterprise–Tech Release ユーザーの無効化](#)」を参照してください。
- ・ **役割**：OpenManage Enterprise–Tech Release 使用時のユーザー役割を示します。たとえば、OpenManage Enterprise–Tech Release の管理者とデバイスマネージャ。「[OpenManage Enterprise–Tech Release ユーザーの役割タイプ](#)」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](#)

[OpenManage Enterprise–Tech Release ユーザーの削除](#)

[ユーザーセッションの終了](#)

関連資料

[OpenManage Enterprise–Tech Release ユーザーの無効化](#)

[OpenManage Enterprise–Tech Release ユーザーの有効化](#)

OpenManage Enterprise–Tech Release ユーザーの有効化

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](#)

[OpenManage Enterprise–Tech Release ユーザーの削除](#)

[ユーザーセッションの終了](#)

関連情報

[OpenManage Enterprise–Tech Release ユーザーの管理](#)

OpenManage Enterprise–Tech Release ユーザーの無効化

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](#)

[OpenManage Enterprise–Tech Release ユーザーの削除](#)

[ユーザーセッションの終了](#)

関連情報

[OpenManage Enterprise–Tech Release ユーザーの管理](#)

OpenManage Enterprise–Tech Release ユーザーの削除

1. 対象の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。

関連資料

[OpenManage Enterprise–Tech Release ユーザーの無効化](#)

[OpenManage Enterprise–Tech Release ユーザーの有効化](#)

関連情報

[OpenManage Enterprise–Tech Release ユーザーの管理](#)

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。

関連資料

[OpenManage Enterprise–Tech Release ユーザーの無効化](#)

[OpenManage Enterprise–Tech Release ユーザーの有効化](#)

関連情報

[OpenManage Enterprise–Tech Release アプライアンス設定の管理](#)

[OpenManage Enterprise–Tech Release ユーザーの管理](#)

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て、**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。

関連資料

[OpenManage Enterprise–Tech Release ユーザーの無効化](#)

[OpenManage Enterprise–Tech Release ユーザーの有効化](#)

関連情報

[OpenManage Enterprise–Tech Release ユーザーの管理](#)

役割ベースの OpenManage Enterprise–Tech Release ユーザー権限

ユーザーは、コンソール設定およびデバイス管理機能へのアクセスのレベルを決定する役割を割り当てられます。この方式は、役割ベースのアクセスコントロール (RBAC) と呼ばれています。以下は、ユーザーの役割と OpenManage Enterprise–Tech Release の機能に基づいた、ユーザー向けの RBAC 共通リストです。ただし、個々のタスクレベルのユーザー RBAC リストについては、必要に応じて各セクションで参考として説明します。したがって、コンソールはアカウントごとに1つの役割を強制します。

OpenManage Enterprise–Tech Release でのユーザー管理の詳細については、「[OpenManage Enterprise–Tech Release ユーザーの管理](#)」を参照してください。

OpenManage Enterprise–Tech Release は、割り当てられたグループに基づくユーザー権限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 > グループごとのユーザー権限**の順にをクリックします。**実行**をクリックします。「**レポートの実行**」を参照してください。

表 12. OpenManage Enterprise–Tech Release での役割ベースのユーザー権限

OpenManage Enterprise–Tech Release の機能	OpenManage Enterprise–Tech Release にアクセスするためのユーザーレベル		
	管理者	デバイス管理者	閲覧者
OpenManage Enterprise–Tech Release アプリケーションの設定	Y	N	N
ベースラインの管理	Y	Y	N
デバイスの設定	Y	Y	N
デバイスの更新	Y	Y	N
検出の管理	Y	N	N
グループの管理	Y	N	N
インベントリの更新	Y	N	N
ジョブの管理	Y	Y	N
監視ポリシーの作成	Y	Y	N
OS の導入	Y	Y	N
電源の制御	Y	Y	N
レポートの管理	Y	Y	N
レポートの実行	Y	Y	Y
セキュリティの設定	Y	N	N
テンプレートの管理	Y	Y	N
トラップの管理	Y	N	N
表示	Y	Y	Y

関連タスク

[OpenManage Enterprise–Tech Release の導入と管理](#)

関連資料

[OpenManage Enterprise–Tech Release ユーザーの役割タイプ](#)

OpenManage Enterprise–Tech Release ユーザーの追加と編集

- ① **メモ:** OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。
- ① **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–Tech Release 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。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。

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では、すべてのユーザープロパティを編集できます。ただし、ディレクトリユーザーについては、役割とデバイスグループのみ（デバイスマネージャの場合）が編集できます。ディレクトリユーザーの追加については、「[ディレクトリサービスと使用するディレクトリの追加](#)」を参照してください。

1. ユーザー > 追加 の順にクリックします。

2. 新規ユーザーの追加

a) ユーザー資格情報を入力します。

パスワードは、少なくとも次の1文字が含まれている必要があります：大文字、小文字、数字、および特殊文字。

b) ユーザー役割

- ・ **管理者**：無制限のアクセス権があり、OpenManage Enterprise–Tech Release によって管理されているすべてのデバイスとデバイスグループの設定および管理を行います。デバイス管理者にデバイスグループを管理する権限を与えます。
- ・ **デバイスマネージャ**：OpenManage Enterprise–Tech Release、指定されたデバイス、およびグループを管理します。管理者は、デバイス管理者により管理することができるようになる前にグループを割り当てる必要があります。詳細については、「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。任意のグループの数をDMに割り当てることができます。これを選択すると、**グループの選択** リンクが表示されます。新しいユーザーが管理する必要があるデバイスグループを選択します。グループの選択の詳細については、「[デバイスグループの選択 \(グループ管理者向け\)](#)」を参照してください。
- ・ **閲覧者**：すべてのグループおよびデバイスに関する情報のみを表示できます。ただし、役割権限は、ユーザーがデバイスで実行するタスクを制限します。

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せん。

3. 終了

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。

デバイスグループの選択 (グループ管理者向け)

1. ユーザー役割

ドロップダウンメニューの **新規ユーザーの追加** ダイアログボックスで、**デバイス管理者** を選択します。**グループの選択** ボタンが表示されます。

2. デバイスグループの選択

ダイアログボックスの左側のペインで、ユーザーにアクセス権を与えるデバイスグループを選択します。または、左側のペインでグループを選択してから、ユーザーにアクセス権を与えるデバイスグループを選択します。

3. 終了

ユーザーには、選択したデバイスグループまたはデバイスへのアクセス権が与えられ、ジョブリストにジョブが作成されます。

OpenManage Enterprise–Tech Release 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–Tech Release ユーザーの追加と編集」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。

Active Directory ユーザーのインポート

メモ：管理者権限があるユーザーでも、Active Directory (AD) のユーザーを有効または無効にすることはできません。

1. ディレクトリユーザーのインポート

2. Active Directory のインポート

a) **ディレクトリソース** ドロップダウンメニューから、ユーザーを追加するためにインポートすべき Active Directory (AD) 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と使用するディレクトリの追加](#)」を参照してください。

b) 使用可能なグループを検索するために、グループ名を手動で入力します。

・ **手動** をクリックし、**グループ名の入力** ボックスに入力します。

・ **使用可能なグループ** をクリックします。プロンプトが表示されたら、ドメイン資格情報を入力し、ドメイングループを取得します。グループを手動で入力する場合の潜在的な失敗を回避するため、この方法を使用することをお勧めします。

- c) **グループ名の入力** ボックスに、検索するグループ名の検索文字列を入力します。文字列に一致するグループのすべてが表示されます。
- d) 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。
- e) **インポートするグループ** セクションで、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。役割ベースのアクセスの詳細については、「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。

メモ: デバイスマネージャ (DM) 役割に割り当てるグループの場合、その DM に対するグループの割り当ては、ローカルユーザーの編集およびデバイスマネージャに対するグループの割り当て手順を使用して、これらのタスクを完了した後で実行する必要があります。「[OpenManage Enterprise–Tech Release ユーザーの追加と編集](#)」を参照してください。

3. 必要に応じて、手順 2c~2e を繰り返します。
4. **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–Tech Release ヘログインします。

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。この場合、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。

OpenManage Enterprise–Tech Release でのディレクトリサービスの統合

ディレクトリサービスでは、コンソールで使用するために、AD または LDAP からディレクトリグループをインポートすることができます。ディレクトリ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と使用するディレクトリの追加](#)」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。「[Active Directory ユーザーのインポート](#)」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–Tech Release ユーザーの追加と編集](#)」を参照してください。

ディレクトリサービスと使用するディレクトリの追加

1. **ディレクトリサービス > 追加** の順にクリックします。
2. **ディレクトリサービス** に **接続** ダイアログボックスで、ディレクトリ名を入力し、FQDN または DNS サーバアドレスを入力します。
 - a) ディレクトリの接続タイプを選択します。
 - b) ディレクトリ接続の名前を入力します。
 - c) **DNS** または **マニュアル** を選択し、テキストボックスで要求される該当する IP アドレスを入力します。選択に基づいて、**詳細オプション** セクションの各フィールドは異なります。
3. **詳細オプション** では、必要に応じてデフォルトのデータを編集します。
4. サーバ認証証明書を確認する場合は、**証明書の検証** チェックボックスを選択し、証明書ファイルを参照して選択します。
5. 接続をテストするには、**テスト接続** をクリックしてください。
6. **終了** をクリックします。
ディレクトリがディレクトリサービスの下に追加および表示されます。

ログインセキュリティのプロパティの設定

- メモ:** OpenManage Enterprise–Tech Release 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」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–Tech Release** 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。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 > **アプリケーションの設定** > **セキュリティ** の順にクリックして、ログイン IP の範囲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、お使いの **OpenManage Enterprise–Tech Release** のセキュリティを守ることができます。

1. **ログイン IP 範囲** を展開します。
 - a. **OpenManage Enterprise–Tech Release** 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。
 - b. **IP 範囲のアドレス (CIDR)** ボックスで、カンマで区切った IP アドレスの範囲を入力します。
 - c. **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。
2. **ログインロックアウトポリシー** セクションで、次の手順を実行します。
 - a. 特定のユーザー名が **OpenManage Enterprise–Tech Release** 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。
 - b. 特定の IP アドレスが **OpenManage Enterprise–Tech Release** 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。
 - c. **ロックアウト失敗回数** ボックスには、**OpenManage Enterprise–Tech Release** 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。
 - d. **ロックアウト失敗時間枠** ボックスでは、**OpenManage Enterprise–Tech Release** 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。
 - e. **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。
 - f. **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。

関連資料

[セキュリティ証明書](#)

セキュリティ証明書

OpenManage Enterprise > **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 SLL 証明書についての情報を表示できます。

メモ: **OpenManage Enterprise–Tech Release** 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。「[役割ベースの OpenManage Enterprise–Tech Release ユーザー権限](#)」を参照してください。

証明書署名要求 (CSR) を生成するには、「[証明書署名要求の生成およびダウンロード](#)」を参照してください。

関連情報

[ログインセキュリティのプロパティの設定](#)

証明書署名要求の生成およびダウンロード

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。

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。

コンソールプリファレンスの管理

- メモ:** OpenManage Enterprise–Tech Release 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。「役割ベースの OpenManage Enterprise–Tech Release ユーザー権限」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–Tech Release 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。

- OpenManage Enterprise–Tech Release 上に表示できる行 (レポート) の最大数を設定するには：
 1. レポート設定 を展開します。
 2. レポートの行数の制限 ボックスに数字を入力します。許可される最大行数 = 1000。
 3. 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。
- OpenManage Enterprise–Tech Release 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更新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。
 1. デバイスの正常性 を展開します。
 2. 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。
 3. 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–Tech Release で今後は監視されなくなると、デバイスは OpenManage Enterprise–Tech Release に対して「不明」となります。
 4. 適用 をクリックします。
 5. 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。
- 検出する必要があるデバイスを使用してモードを設定するには：たとえば、DNS 名やホスト名などです。
 1. 検出設定 を展開します。
 2. デバイスの検出に DNS 設定を使用する場合は、**DNS を優先** チェックボックスを選択します。NetBIOS で **優先する NetBIOS** チェックボックスを選択します。
 3. デバイスの検出にシステムのホスト名を使用する場合は、**システムホスト名を優先** チェックボックスを選択します。
 4. iDRAC を介してシステムのホスト名を使用してデバイスを検出するには、**優先する iDRAC ホスト名** チェックボックスを選択します。
 5. 詳細設定 を展開します。
 - **無効なデバイスのホスト名** で、1つ、またはカンマで区切った複数の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。
 - **共通の MAC アドレス** で、カンマで区切った一般的な MAC アドレスを入力します。デフォルトでは、一般的な MAC アドレスのリストが設定されます。
 6. 適用 をクリックします。
 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。
- **すべてのデバイス** ビューに表示する必要があるデバイスを設定します。
 1. **すべてのデバイスのビュー設定** を展開します。
 2. **不明なデバイスの表示** ドロップダウンメニューから、次のものを選択します。
 - **False**：ダッシュボード ページで、すべてのデバイスおよびデバイスグループのリストに、不明なデバイスは表示されません。
 - **True**：リストに不明なデバイスが表示されます。
 3. 適用 をクリックします。
 4. 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。
- **SMB 設定** セクションで、ネットワーク通信用に使用する必要があるサーバメッセージブロック (SMB) バージョンを選択します。デフォルトでは、**Version2** (SMBv3) が有効になっています。

- メモ:** SMBv1 を有効にする、またはテンプレートの導入または診断レポートなどの機能を使用するには、Dell.com サイトからダウンロードします。

SMT、SNMP、およびシスログアラートの設定

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電子メール (SMTP) アドレス、SNMP 送信先、シスログの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-Tech Release 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-Tech Release 間の電子メールの通信を管理する SMTP サーバを設定し認証するには、次の手順を実行します。

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 サーバを認証するには、**認証を有効にする** チェックボックスを選択し、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. **適用** をクリックします。
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。

SNMP トラップの転送を設定するには、次の手順を実行します。

1. **SNMP 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。
4. **SNMP バージョン** ドロップダウンメニューから SNMP バージョンのタイプを選択します。現在サポートされているのは、SNMP1 バージョンと SNMP2 バージョンのみです。
5. **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。
6. SNMP トラップのデフォルトのポート番号は 162 です。必要に応じて編集します。「[OpenManage Enterprise-Tech Release でサポートされるプロトコルおよびポート](#)」を参照してください。
7. 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。
8. **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。

シスログメッセージを設定するには、次の手順を実行します。

1. **シスログ設定** を展開します。
2. サーバ行の各サーバのチェックボックスを選択して、シスログ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、シスログ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-Tech Release でサポートされるプロトコルおよびポート](#)」を参照してください。
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-Tech Release 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。「[役割ベースの OpenManage Enterprise-Tech Release ユーザー権限](#)」を参照してください。

OpenManage Enterprise > アプリケーションの設定 > 着信アラートの順をクリックすると、SNMP v3 プロトコルを使用して着信を受信するユーザーのプロパティを定義できます。また、TrapForward のプロパティを設定することもできます。

・ 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-Tech Release 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) **認証パスワード** ボックスに、選択した内容に基づいて SHA または MD_5 に関連するパスワードを入力します。
 - 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) **プライバシーパスワード** ボックスに、プライバシータイプに基づいてパスワードを入力します。
 - 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 161 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。

・ TrapForward 設定を適用するには、次の手順を実行します。

1. **TrapForward 設定** を展開します。
 - ・ トラップを転送するには、**AS_IS** を選択します。
 - ・ 正規化されたトラップを転送するには、**正規化** を選択します。
2. **適用** をクリックします。
3. 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 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-Tech Release 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) **認証パスワード** ボックスに、選択した内容に基づいて SHA または MD_5 に関連するパスワードを入力します。
 - 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) **プライバシーパスワード** ボックスに、プライバシータイプに基づいてパスワードを入力します。
3. **保存** をクリックします。

保証設定の管理

OpenManage Enterprise > **アプリケーションの設定** > **保証設定** の順にクリックし、次を実行して、OpenManage Enterprise-Tech Release ヘッダーに存在する保証スコアボード通知を有効にすることができます。このページ上のすべてのパラメータまたは設定は、保証スコアボードのカウントのロジックを決定します。デフォルトでは、ユーザーは保証期限の 90 日前に警告されます。日数を編集するには、次の手順を実行します。

1. **保証スコアボード通知の有効化** チェックボックスを選択します。
2. この値を編集するには、**有効期限が次より少ない場合** ボックスを入力します。OpenManage Enterprise-Tech Release ダッシュボードの **保証の有効期限が次より少ない** フィールドには、この基準に一致する保証が表示されます。
3. 保証期限が切れた後にメッセージを送信するためには、**保証が切れたとき** チェックボックスを選択します。選択すると、OpenManage Enterprise-Tech Release ダッシュボード (ウィジェット) に、有効期限が切れた保証の数が表示されます。
4. **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。

OpenManage Enterprise-Tech Release は、次の 30 日で期限切れす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**」を参照してください。

OpenManage Enterprise-Tech Release バージョンの確認とアップデート

OpenManage Enterprise > **アプリケーションの設定** > **コンソールアップデート** の順にクリックし、お使いの OpenManage Enterprise-Tech Release の現在のバージョンを表示して、利用可能なアップデートバージョンがある場合はそれを確認し、OpenManage Enterprise-Tech Release のバージョンをアップデートします。タスクのアップデート前およびアップデート後に利用できるチェックリストは、「**OpenManage Enterprise-Tech Release バージョンをチェックし、アップデートするためのプロセスマップ**」を参照してください。

- ・ 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。アップデートを低速のネットワーク接続を使用してダウンロードする必要がある場合は追加の時間を割り当てます。
- ・ デバイス構成タスクや導入タスクが実行されていないこと、または計画ダウンタイム中に実行がスケジュールされていないことを確認します。
- ・ 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。
- ・ 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。(必要な場合、これに対して追加のダウンタイムを割り当てます。)
- ・ 次のアップデートソースを選択します。
 - ・ Dell.com からの直接アップデート：コンソールが Dell.com および目的のアップデートにアクセスできることを確認します。コンソールアップデート ページで、**オンライン** をクリックし、**今すぐ確認** をクリックします。使用可能なすべてのアップデートの想定されるターゲットバージョンと説明を確認します。

① **メモ:** ユーザーは、ホーム ポータルで新しいアップデートパッケージまたは保証情報の利用可能性について自動的に警告されます。

- 内部 NFS からのアップデート：該当するファイルをダウンロードし、コンソールからアクセス可能なネットワーク共有上に保存します。コンソールアップデート ページで、オフライン をクリックし、今すぐ確認 をクリックします。使用可能なすべてのアップデートの想定されるターゲットバージョンと説明を確認します。

① **メモ:** Dell.com に自動的に接続されません。ローカル共有をセットアップし、アップデートパッケージを手動でダウンロードする必要があります。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。

① **メモ:** 自動 を選択し、利用可能な更新されたバージョンについての情報を表示します。アップデートは毎週末ごとに自動的に確認されます。この頻度は変更できません。

- 今すぐアップデート 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、製品が予想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についての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。

① **メモ:** OpenManage Enterprise–Tech Release バージョンが正常にアップデートされると、ジョブの詳細 ページの関連するジョブのステータスが 停止 と表示されます。ただし、これは実際のジョブのステータスは 完了 であることを示します。

① **メモ:** OpenManage Enterprise–Tech Release のバージョンアップデートプロセスが正常に終了したかどうかにかかわらず、現在、監査ログは作成されません。

表 13. OpenManage Enterprise–Tech Release のバージョンを更新するための役割に基づいたアクセス権限

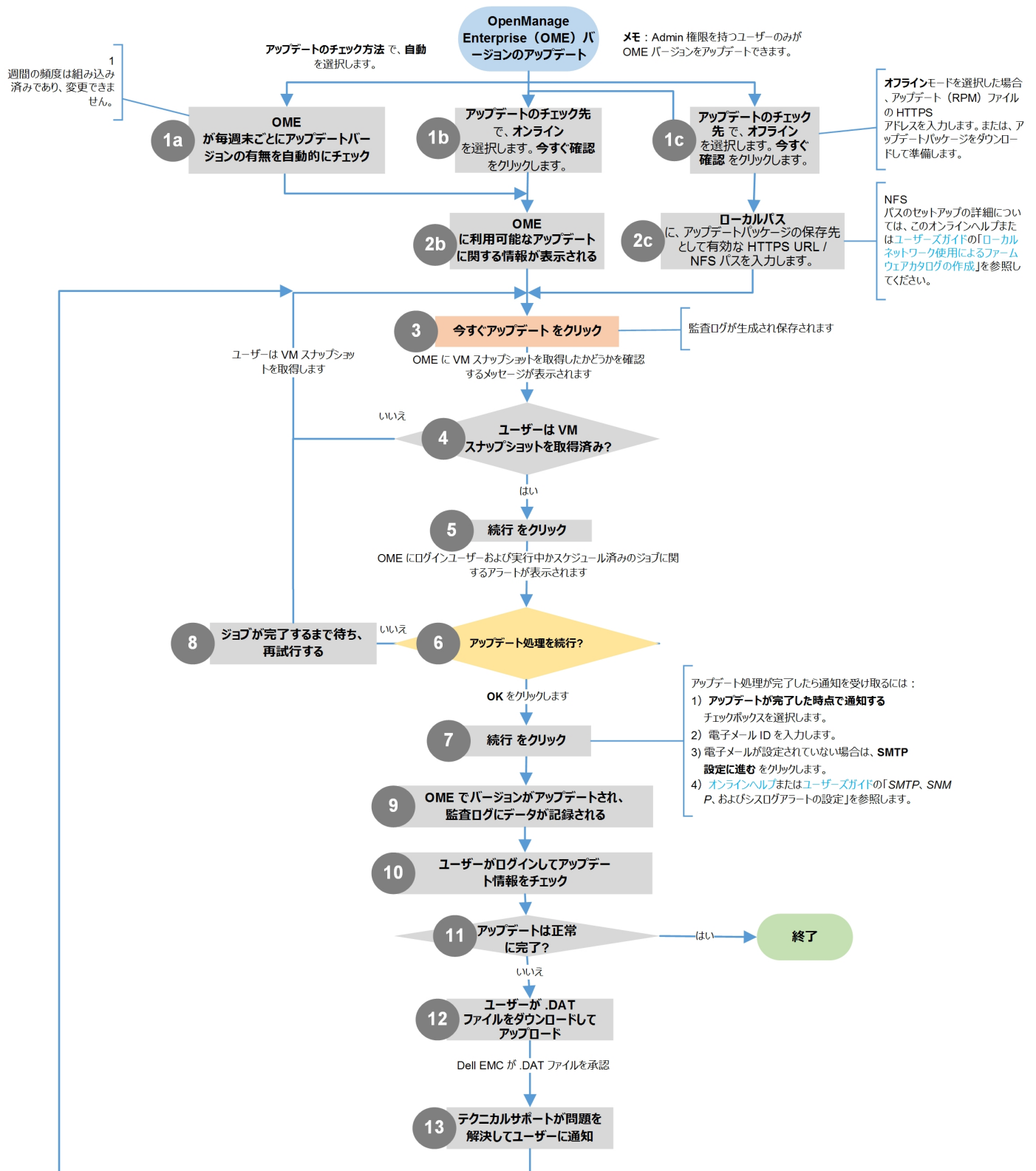
この役割を持つユーザー ...	次のことを行えます ...
システム管理者	現在の OpenManage Enterprise–Tech Release バージョンの表示とバージョンのアップデート
デバイス管理者と閲覧者	現在の OpenManage Enterprise–Tech Release バージョンの表示のみ

① **メモ:** OpenManage Enterprise–Tech Release のアップデートバージョンが利用可能な場合、メッセージがダッシュボードに表示されます。すべての権限 (Administrator、デバイスマネージャ、およびビューア) を持つユーザーは、メッセージを表示できますが、管理者のみが、メッセージを後で通知するのか、または無視するのかを選択できます。

OpenManage Enterprise–Tech Release VM のアップデートの確認

「OpenManage Enterprise–Tech Release バージョンの確認とアップデート」を参照してください。

OpenManage Enterprise–Tech Release バージョンをチェックし、アップデートするためのプロセスマップ



関連情報

OpenManage Enterprise–Tech Release の導入と管理

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き、OpenManage Enterprise–Tech Release のスクリプトを実行してアラート管理用の他社製チケットシステムのチケットを開くためのポリシーを設定することができます。すぐに実行する、または後で実行するためのリモートコマンドは4つ作成して保存することができます。

1. **リモートコマンドの設定** ダイアログボックスで、次の手順を実行します。

- 後で実行する際に適切なスクリプトを選択して実行するために役立つよう、スクリプト名を入力します。
- コマンドを実行する OpenManage Enterprise–Tech Release サーバの IP アドレスを入力します。
- 資格情報を入力して、OpenManage Enterprise–Tech Release サーバにログインします。
- チケットを開くために OpenManage Enterprise–Tech Release サーバで実行する必要があるコマンドを入力します。たとえば、`./RCE.sh $IP $MODEL $DATE $ASSETTAG $SERVICETAG`

2. **保存** をクリックします。

コマンドが保存されます。これらのコマンドは、アラートポリシーを設定中にも設定して実行できます。「[アラートポリシーの作成](#)」を参照してください。

メモ:

- 一度に実行できるのは、1つの実行可能ファイルまたはスクリプトのみです。
- 実行可能ファイルまたはスクリプトは、必ずしも **OpenManage Enterprise–Tech Release** によって検出または管理されないサーバに保存できます。
- スクリプトは、最大 **1024** 文字を入力できます。
- OpenManage Enterprise–Tech Release** は、スクリプトまたはチケットシステムに役立つトークン代替をサポートします。サポートされるトークン：`$IP`、`$MSG`、`$HOSTNAME`、`$SERVICETAG`、`$ASSETTAG`、`$DATE`、`$TIME`、`$MODEL`

OpenManage Mobile 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–Tech Release コンソールおよび/または integrated Dell Remote Access Controller (iDRAC) におけるデータセンター監視のサブセットおよび修正タスクをセキュアに実行することを可能にするシステム管理アプリケーションです。OpenManage Mobile を使用して以下を実行することができます。

- OpenManage Enterprise–Tech Release 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。

本章には、OpenManage Enterprise–Tech Release を介して設定できる OpenManage Mobile 設定についての情報が記載されています。また、OpenManage Mobile のトラブルシューティングに必要な情報も説明されています。

メモ: OpenManage Mobile のインストールと使用についての情報は、dell.com/OpenManageManuals 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](#)
- [OpenManage Mobile サブスクリイパーの有効化または無効化](#)
- [OpenManage Mobile サブスクリイパーの削除](#)
- [アラート通知サービスステータスの表示](#)
- [OpenManage Mobile のトラブルシューティング](#)

関連情報

- [OpenManage Mobile 用アラート通知の有効化または無効化](#)
- [OpenManage Mobile サブスクリイパーの有効化または無効化](#)
- [OpenManage Mobile のトラブルシューティング](#)

OpenManage Mobile 用アラート通知の有効化または無効化

OpenManage Enterprise–Tech Release 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–Tech Release から警告通知が送信されるのは、OpenManage Mobile ユーザーが OpenManage Enterprise–Tech Release 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 用の警告通知の有効化または無効化には、**omeAdministrator** 権限が必要です。

メモ: OpenManage Enterprise–Tech Release による OpenManage Mobile への警告通知の送信のため、OpenManage Enterprise–Tech Release 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–Tech Release から OMM に警告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 設定** 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 設定](#)

関連情報

[OpenManage Mobile 設定](#)

[OpenManage Mobile サブスクライバーの削除](#)

OpenManage Mobile サブスクライバーの有効化または無効化

Mobile サブスクライバー リスト内の **有効** 列にあるチェックボックスを使用して、OpenManage Mobile サブスクライバーに対するアラート通知の送信を有効化または無効化することができます。

メモ: OpenManage Mobile サブスクライバーの有効化または無効化には **omeAdministrator** ユーザー権限が必要です。

メモ: OpenManage Mobile サブスクライバーは、デバイスが恒久的に到達不可能であることをサブスクライバーのモバイルサービスプロバイダのプッシュ通知サービスが示す場合、OpenManage Enterprise–Tech Release によって自動的に無効化される場合があります。

メモ: OpenManage Mobile サブスクライバーが **Mobile** サブスクライバー リストで有効化されていたとしても、サブスクライバーは OpenManage Mobile アプリケーション設定でアラート通知の受信を無効化することができます。

OpenManage Mobile サブスクライバーに対するアラート通知を有効化または無効化するには、次の手順を実行します。

1. **OpenManage Enterprise > アプリケーションの設定 > Mobile 設定** 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 設定](#)


関連情報

[OpenManage Mobile 設定](#)

[OpenManage Mobile サブスクライバーの削除](#)

OpenManage Mobile サブスクライバーの削除

OpenManage Mobile サブスクライバーを削除すると、**モバイルサブスクライバー** リストからユーザーが削除され、ユーザーによる OpenManage Enterprise–Tech Release 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 サブスライバーの削除には **omeAdministrator** 権限が必要です。

OpenManage Mobile サブス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 設定** の順にクリックします。
2. 対象のサブス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](#)
[OpenManage Mobile サブスライバーの有効化または無効化](#)
[OpenManage Mobile サブスライバーの削除](#)
[アラート通知サービスステータスの表示](#)

関連情報

[OpenManage Mobile 設定](#)
[OpenManage Mobile サブスライバーの削除](#)

アラート通知サービスステータスの表示

OpenManage Enterprise–Tech Release は、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 OpenManage Mobile サブスライバーにアラート通知を転送します。OpenManage Mobile サブス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 設定** 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](#)





関連情報

[OpenManage Mobile 設定](#)
[OpenManage Mobile サブスライバーの削除](#)
[アラート通知サービスステータスの表示](#)

通知サービスステータス

次の表では、**アプリケーションの設定** > **Mobile 設定** ページに表示される **通知サービスステータス** についての情報を説明しています。

表 14. 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。サブスライバーのデバイスがインターネットまたはセルラーデータサービスに接続されていない場合、接続が回復されるまで通知は配信されません。
	サービスで、一時的な可能性のあるメッセージの配信エラーが発生しました。問題が解決されない場合は、トラブルシューティング手順に従うか、テクニカルサポートにお問い合わせください。
	サービスでメッセージの配信エラーが発生しました。トラブルシューティング手順に従うか、必要に応じてテクニカルサポートにお問い合わせください。

OpenManage Mobile サブスクライバー情報の表示

OpenManage Mobile ユーザーが OpenManage Enterprise–Tech Release を正常に追加すると、そのユーザーは OpenManage Enterprise–Tech Release の **Mobile サブスクライバー** 表に追加されます。**Mobile サブスクライバー** 表は、各 OpenManage Mobile サブスクライバーについての情報を提供します。

Mobile サブスクライバー情報を表示するには、OpenManage Enterprise–Tech Release で、**アプリケーション設定 > Mobile 設定** をクリックします。

Mobile サブスクライバー情報

次の表では、**アプリケーションの設定 > Mobile 設定** ページに表示される **Mobile サブスクライバ** の表についての情報が記載されています。

表 15. 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–Tech Release が Alert Forwarding Service に対して正常にアラート通知を送信できるかどうかを示す、サブスクライバーのステータスを表示します。
状態メッセージ	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的識別子です。
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–Tech Release 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–Tech Release にアクセスした日付と時間。
登録	ユーザーが OpenManage Mobile に OpenManage Enterprise–Tech Release を追加した日付と時間。
削除	クリックして、Mobile サブスクライバリストからサブスクライバを削除します。

OpenManage Mobile のトラブルシューティング

OpenManage Enterprise–Tech Release 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 16. OpenManage Mobile のトラブルシューティング

問題	理由	映像度
OpenManage Enterprise–Tech Release が Dell Message Forwarding Service に接続できない。[コード 1001/1002]	アウトバウンドインターネット (HTTPS) 接続が失われています。	ウェブブラウザを使用して、アウトバウンドインターネット接続が使用可能かどうかを確認します。

問題	理由	解像度
		<p>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。</p> <ul style="list-style-type: none"> 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。	<p>デバイスに OpenManage Mobile を再インストールするか、『OpenManage Mobile User's Guide』（OpenManage Mobile ユーザーズガイド）で説明されている OpenManage Mobile トラブルシューティング手順に従って、デバイスを OpenManage Enterprise–Tech Release に再接続します。</p> <p>デバイスが OpenManage Enterprise–Tech Release に接続されていない場合は、サブスクリバを削除します。</p>
OpenManage Enterprise–Tech Release 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–Tech Release が使用されています。	新しいバージョンの OpenManage Enterprise–Tech Release にアップグレードしてください。

関連タスク

[OpenManage Mobile 設定](#)

関連情報

[OpenManage Mobile 設定](#)

その他の参照情報およびフィールドの説明

OpenManage Enterprise–Tech Release グラフィカルユーザーインターフェース (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](#)
- ・ [ファームウェアのベースラインフィールドの定義](#)
- ・ [スケジュールジョブフィールドの定義](#)
- ・ [フィールドサービスデバッグのワークフロー](#)
- ・ [FSD 機能のブロック解除](#)
- ・ [署名済み FSD DAT.ini ファイルのインストールまたは許可](#)
- ・ [FSD を呼び出す](#)
- ・ [FSD の無効化](#)
- ・ [カタログの管理フィールドの定義](#)

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、「[ファームウェアのベースラインの作成](#)」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の管理](#)」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。「[ベースラインとデバイスファームウェアの照会の確認](#)」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。**毎時**、**毎日**、または **毎週** を選択してから、頻度を適切に選択します。

- ① **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。

フィールドサービスデバッグのワークフロー

OpenManage Enterprise–Tech Release 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](#)」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](#)」を参照してください。
3. FSD の呼び出し。「[FSD を呼び出す](#)」を参照してください。
4. FSD の無効化。「[FSD の無効化](#)」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 を呼び出す

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–Tech Release にアップロードされていることを確認します。

1. デバッグ機能呼び出すには、FSD 機能画面で、**FSD 機能呼び出す** を選択します。
2. **要求されたデバッグ機能呼び出す** 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。

① | 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–Tech Release 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–Tech Release に添付できます。

FSD の無効化

コンソールでデバッグ機能呼び出した後で、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。

リリース日: カタログファイルの使用をリリースする日付。