vSphere Client を使用した OpenManage Integration for VMware vCenter
ユーザーズガイドバージョン 2.0

メモ、注意、警告

メモ: コンピュータを使いやすくするための重要な情報を説明しています。

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

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

2013

Rev. A00

目次

1

概要

OpenManage Integration for VMware vCenter

VMware vCenter は、IT 管理者が VMware vSphere ESX/ESXi ホストを管理および監視するために使用するプライマリコンソールです。標準の仮想化環境では、システム管理者に対して個別のコンソールを起動してハードウェア問題を解決するよう指示するために、VMware アラートと監視が使用されます。現在、OpenManage Integration for VMware vCenter を使用して、管理者が仮想化環境内で Dell ハードウェアを管理および監視する次のような新しい機能を利用できます。

- アラート通知と環境の監視
- 単一サーバー監視と報告
- ファームウェアアップデート
- 拡張された展開オプション

主な機能

デルのお客様は OpenManage Integration for VMware vCenter を使用して次の機能を実行することができます。

インベントリ	主要資産のインベントリを実行、設定タスクを実行、Dell プラットフォームのクラスタビューとデータセンタビューを提供。
監視とアラートの実施	主要なハードウェア障害を検知し、仮想化を認識した動作（たとえば、作業負荷の移行、あるいはホストをメンテナンスモードに設定）を実行。
ファームウェアアップデート	Dell ハードウェアを最新バージョンの BIOS とファームウェアにアップデート。
展開とプロビジョニング	ハードウェアプロファイル、ハイパーバイザプロファイルを作成し、vCenter を使用して、リモートかつ PXE 無しでベアメタル Dell PowerEdge サーバーにこの 2 つの任意の組み合わせを展開。
サーバー情報	Dell からオンラインで保証情報を取得。

vCenter 管理における OpenManage Integration for VMware vCenter の役割

OpenManage Integration for VMware vCenter は、現在の vCenter 管理機能を補完する追加の仮想化機能を提供します。

- タスクを要約し、ファームウェアアップデートやベアメタル展開などの管理プロセスを vCenter Server 管理コンソールに追加します。
- 起動前実行環境（PXE）を必要とすることなく、複数のベアメタルサーバーの展開を準備します。
- サーバー問題を診断するための追加の情報（インベントリ、イベント、警告）を提供します。

- 標準の vCenter 認証、規則、権限と一体化します。

OpenManage Integration for VMware vCenter の機能

以下は、OpenManage Integration for VMware vCenter の高度な機能です。

- 標準の vCenter イベントとアラームサブシステムを使用した Dell プラットフォームの監視
- 高度なハードウェア管理と設定の実施
- PXE を使用せずにベアメタルシステム上で VMware ESX / ESXi ハイパーバイザーのゼロタッチ展開を実行
- ハードウェアと VMware ESX / ESXi ハイパーバイザーのプロファイルを構築
- ファームウェアアップデートの実行
- インフラストラクチャ問題のトラブルシューティング
- データセンターとクラスタビューでの報告 — CSV ファイルへのエクスポート
- OpenManage Integration for VMware vCenter の機能を標準の vCenter の役割および許可と統合

2

OpenManage Integration for VMware vCenter の設定

次の項では、OpenManage Integration for VMware vCenter の初期設定の順を追った手順を説明します。アップグレード、アンインストール、およびセキュリティ役割についての情報も次の項に記載されています。

セキュリティの役割および許可

OpenManage Integration for VMware vCenter は、ユーザー資格情報を暗号化フォーマットで保管します。問題につながる可能性のある不適切な要求を避けるため、クライアントアプリケーションにはパスワードを一切提供しません。データベースのバックアップは、カスタムセキュリティフレーズで完全に暗号化されるため、データが誤使用されることはありません。
デフォルトで、管理者グループ内のユーザーはすべての特権を持ちます。管理者は、VMware vCenter 内の OpenManage Integration for VMware vCenter のすべての機能を使用することができます。管理者以外のユーザーが製品を管理する場合は、両方の Dell 役割を含む役割を作成して、インベ取り内のルート / トップノードに許可を割り当てて、必要に応じてユーザーへのアクセスを許可したい子ノードに許可を伝播します。例えば、ユーザーにクラスタ A のみを管理させたい場合は、クラスタ A の許可はそのままにして、他のクラスタからは許可を削除します。

データ整合性

OpenManage Integration for VMware vCenter 仮想アプライアンス、管理コンソール、および vCenter の間の通信は、SSL / HTTPS を使用して行われます。OpenManage Integration for VMware vCenter は、vCenter およびアプライアンスの間の信頼された通信のために SSL 証明書を生成します。また、通信と OpenManage Integration for VMware vCenter 登録の前に vCenter サーバーの証明書を検証して信頼します。OpenManage Integration for VMware vCenter コンソールタブ（VMware vCenter）は、管理コンソールおよびバックエンドサービスとの間でキーをやり取りする間、セキュリティプロシージャを使用して不適切な要求を回避します。このタイプのセキュリティではクロスサイトリクエストフォージェリは成り立ちません。
セキュア管理コンソールセッションには 5 分間のアイドルタイムアウトがあり、セッションは現行のブラウザウィンドウおよび / またはタブでのみ有効です。ユーザーが新しいウィンドウまたはタブでセッションを開こうとすると、有効なセッションを求めるセキュリティエラーが作成されます。この処置は、管理コンソールセッションを攻撃する可能性のある悪意のある URL をユーザーがクリックすることを防ぎます。

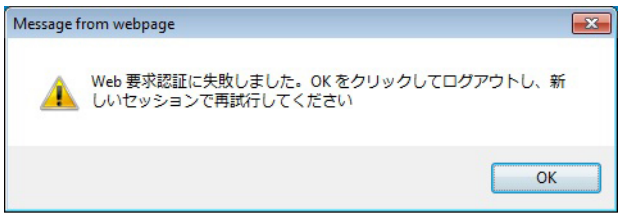

図 1. Error Message（エラーメッセージ）

アクセス制御認証、許可、および役割

OpenManage Integration for VMware vCenter は、仮想アプライアンスが vCenter 操作を実行するように、vSphere クライアントの現行のユーザーセッションと保存された管理資格情報を使用します。OpenManage Integration

for VMware vCenter は、vCenter サーバーのビルトイン役割と権限モデルを使い、仮想アプライアンスおよび vCenter の管理下オブジェクト（ホストおよびクラスタ）に対するユーザー処置を許可します。

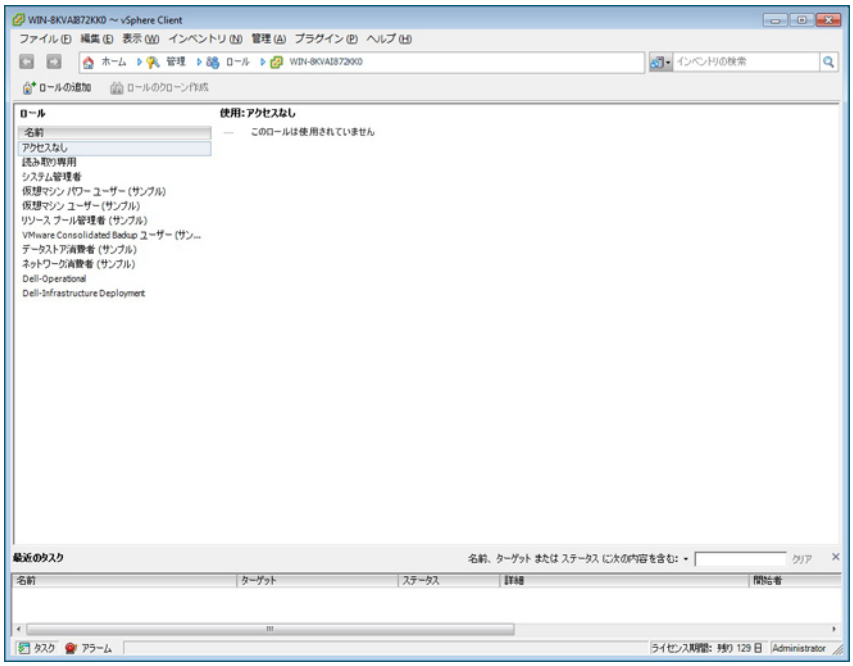

図 2. vCenter vSphere クライアントの役割と権限

Dell 操作の役割

ファームウェアアップデート、ハードウェアインベントリ、ホストの再起動、ホストをメンテナンスモードに設定、vCenter Server タスクの作成を含む、アプライアンスおよび vCenter サーバーのタスクを実行する権限 / グループが含まれます。

この役割には次の権限グループが含まれます。

権限グループ - Dell.Configuration	権限 - ホスト関連タスクの実行、vCenter 関連タスクの実行、SelLog の設定、ConnectionProfile の設定、ClearLed の設定、ファームウェアアップデート
権限グループ - Dell.Inventory	権限 - インベントリの設定、保証取得の設定、読み取り専用の設定
権限グループ - Dell.Monitoring	権限 - 監視の設定、監視
権限グループ - Dell.Reporting (使用されていません)	権限 - レポートの作成、レポートの実行

Dell インフラストラクチャ展開の役割

この役割には、ハイパーバイザー展開機能に特化した権限が含まれます。

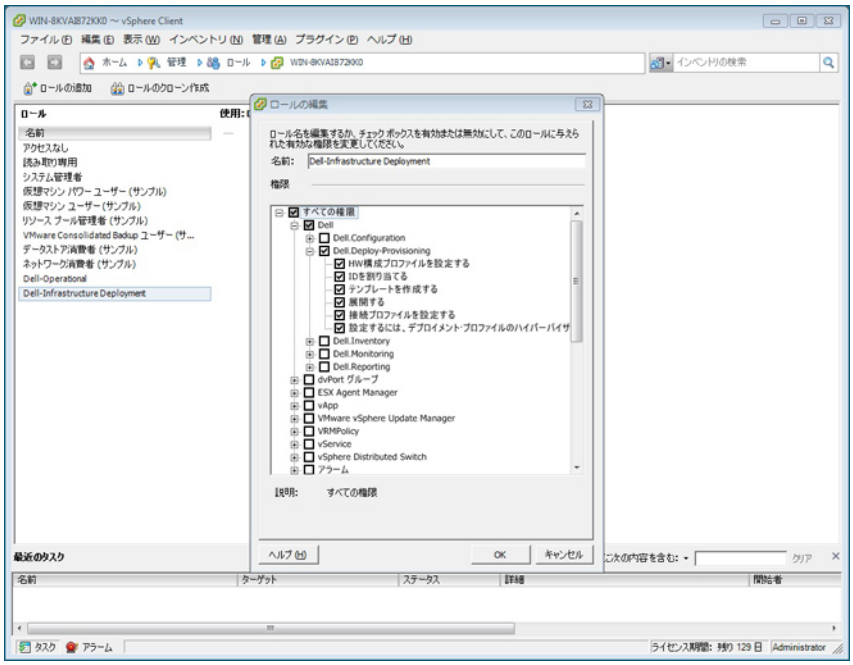

図 3. Dell インフラストラクチャ展開の役割

この役割の権限は、テンプレートの作成、HW 設定プロファイルの設定、ハイパーバイザー展開プロファイルの設定、接続プロファイルの設定、ID の割り当て、および展開です。

Dell.展開 — プロビジョニング	テンプレートの作成、HW 設定プロファイルの設定、ハイパーバイザー展開プロファイルの設定、接続プロファイルの設定、ID の割り当て、展開

権限について

OpenManage Integration for VMware vCenter によって実行されるすべての処置は、権限に関連付けられています。次の項では、実行可能な処置と、それに関連付けられている権限をリストします。

- Dell.Configuration.Perform vCenter-Related Tasks
  - メンテナンスモードを終了および実行
  - 許可をクエリするために vCenter ユーザーグループを取得
  - 警告を登録および設定。たとえば、イベント設定ページでのアラートの有効化 / 無効化
  - vCenter にイベント / アラートを掲示
  - イベント設定ページでイベント設定を実行
  - イベント設定ページでデフォルトのアラートを復元
  - アラート / イベント設定を実行しながら、クラスタの DRS ステータスをチェック
  - アップデートまたはその他の設定処置を実行した後にホストを再起動
  - vCenter タスクのステータス / 進捗状態を監視
  - vCenter タスクを作成。たとえば、ファームウェアアップデートタスク、ホスト設定タスク、およびインベントリタスク
  - vCenter タスクのステータス / 進捗状態をアップデート
  - ホストプロファイルを取得
  - データセンターにホストを追加

- クラスタにホストを追加
- ホストにプロファイルを適用
- CIM 資格情報を取得
- コンプライアンスのためにホストを設定
- コンプライアンスタスクのステータスを取得

- Dell.Inventory.Configure ReadOnly
  - 接続プロファイルの設定中に、すべての vCenter ホストを取得して vCenter ツリーを構築
  - タブが選択されてるときにホストが Dell サーバーかどうかをチェック
  - vCenter のアドレス / IP を取得
  - ホストの IP / アドレスを取得
  - vSphere クライアントセッション ID に基づいて現在の vCenter セッションユーザーを取得
  - vCenter インベントリツリーを取得して、vCenter インベントリをツリー構造で表示

- Dell.Monitoring.Monitor
  - イベントを掲示するためのホスト名を取得
  - イベントログ操作を実行。たとえば、イベント数の取得、またはイベントログ設定の変更
  - イベント / アラートを登録、登録解除、および設定 – SNMP トラップの受信とイベントの受信

- Dell.Configuration.Firmware Update
  - ファームウェアアップデートを実行
  - ファームウェアアップデートウィザードページにファームウェアリポジトリと DUP ファイル情報をロード
  - ファームウェアインベントリをクエリ
  - ファームウェアリポジトリ設定を実行
  - ステージングフォルダを設定、およびステージング機能を使用したアップデートを実行
  - ネットワークとリポジトリ接続をテスト

- Dell.Deploy-Provisioning.Create Template
  - 展開テンプレートの作成、表示、削除、および編集

- Dell.Configuration.Perform Host-Related Tasks
  - Dell Server Management（Dell サーバー管理）タブから LED を点滅、LED をクリア、OMSA URL を設定
  - OMSA コンソールを起動
  - iDRAC コンソールを起動
  - SEL ログを表示およびクリア

- Dell.Inventory.Configure Inventory
  - Dell Server Management（Dell サーバー管理）タブでシステムインベントリを表示
  - ストレージ詳細を取得
  - 電源監視詳細を取得
  - 接続プロファイルページで接続プロファイルを作成、表示、編集、削除、およびテスト
  - インベントリスケジュールを計画、アップデート、および削除
  - ホストでインベントリを実行

3

OpenManage Integration for VMware vCenter の設定または編集方法の理解

OpenManage Integration for VMware vCenter の基本的なインストールが完了したら、2 つのうちいずれかの方法でアプライアンスを設定します。設定ウィザードの使用が一般的な方法ですが、Dell Management Center でアプライアンスの設定ページを通して行うこともできます。

両方共、ユーザーインタフェースは似通っていますが、ウィザードでは *保存して続行*をクリックするのに対し、設定オプションでは *適用*をクリックします。

設定ウィザード使用の設定タスク

設定ウィザードを使って OpenManage Integration for VMware vCenter を設定する際は、これらのタスクを使用します。

1. 設定ウィザードようこそページ
2. 新しい接続プロファイルの作成
3. イベントおよびアラームの設定
4. プロキシサーバーの設定
5. インベントリジョブのスケジューリング
6. 保証取得ジョブの実行
7. 展開資格情報の設定
8. デフォルトファームウェアアップデートリポジトリの設定
9. OMSA リンクの有効化

設定オプションを使用した設定タスク

これらのタスクを使って OpenManage Integration for VMware vCenter 設定タスクを設定または編集します。

- 新しい接続プロファイルの作成
- イベントおよびアラームの設定
- プロキシサーバーの設定
- インベントリジョブスケジュールの変更
- 保証の取得
- 展開資格情報の表示または編集
- ファームウェアリポジトリおよび資格情報の設定
- OMSA リンクの有効化

OpenManage Integration for VMware vCenter ホームページ

OpenManage Integration for VMware vCenter ホームページにログインすると、ナビゲーションボタンが左ペインに、便利なリンクや情報が右ペインに提供されます。このデザインは、最も頻度が高いタスクへの主要リンクを提供します。これらのタスクはすべて左ペインのナビゲーションにありますが、使いやすいようにホームページでも見ることができます。このページで提供されるタスクは、次のカテゴリに属します。

- ホストおよびサーバーの展開
  この項は、ホストおよびサーバー展開に関してさらなる情報を提供します。

- vSphere ホストおよびベアメタルサーバーの対応性
  この項では、さらなる情報が提供され、非対応ホストまたはベアメタルサーバーの詳細を表示したり、またはウィザードを実行して解決することができます。
- インベントリスケジュール
  この項では、インベントリスケジュールについてより多く学ぶことができます。
- 保証データ検索スケジュール
  この項では、保証スケジュールについて学び、または表示 / 変更ができます。
- ライセンス
  この項では、ライセンスについて説明されています。リンクを使用してライセンスタスクに移動します。
- イベントおよびアラームの設定
  イベントおよびアラームについてさらに学び、あるいはリンクを使って設定を行うことができます。
- ホスト接続ライセンス
  ここでは、リアルタイムでホスト接続ライセンスを表示することができます。また、今すぐ購入リンクを使用して、複数ホストを管理できる完全版のライセンスを購入することができます。今すぐ購入リンクは、デモライセンスを使用している場合にのみ表示されます。

設定ウィザードようこそページ

OpenManage Integration for VMware vCenter をインストールした後、設定を行う必要があります。

1. **vSphere Client** の **管理** で、**Dell Management Center** アイコンをクリックします。
2. 初めて **Dell Management Center** アイコンを実行する場合、**設定ウィザード** が開きます。このウィザードには、 **Dell Management Center** → **設定** ページでアクセスすることもできます。
3. **ようこそタブ** で、これから実行する手順を確認し、**次へ** をクリックします。

新規接続プロファイルの作成ウィザード

接続プロファイルは、仮想アプライアンスが Dell サーバーと通信するのに使用する資格情報を保存します。各 Dell サーバーは、OpenManage Integration for VMware vCenter によって管理される接続プロファイルに関連付けらている必要があります。複数のサーバーを 1 つの接続プロファイルに割り当てることができます。接続プロファイルの作成方法は、設定ウィザードと Dell Management Center、設定オプションではほぼ同様です。

メモ: 第 12 世代サーバー使用のホストでのインストールでは、OMSA エージェントのインストールは必要ありません。第 11 世代サーバーへのインストールでは、OMSA エージェントは展開プロセス中に自動的にインストールされるようになりました。

メモ: 追加されたホスト数がライセンス制限を超過した場合、接続プロファイルを作成できます。

接続プロファイルで Active Directory 資格情報を使用する前に、Active Directory に Active Directory ユーザーアカウントが存在し、このアカウントが iDRAC で既に有効化されている必要があります。このウィザードは、Active Directory アカウントの作成、または iDRAC における Active Directory の有効化用ではありません。

ウィザードを使用する新規接続プロファイルの作成には、以下を行います。

1. **接続プロファイル** タブで、**新規作成** をクリックします。
2. **プロファイル名と説明** ページで、カスタム接続プロファイルの管理に役立つ **接続プロファイル名** とオプションの **接続プロファイルの説明** を入力します。
3. **関連ホスト** ページで、接続プロファイルのホストを選択し、**次へ** をクリックします。
4. **資格情報** ページで、情報を読んでから **次へ** をクリックします。
5. iDRAC ページの資格情報で、次のいずれかを実行します。

メモ: iDRAC アカウントには、ファームウェアのアップデート、ハードウェアプロファイルの適用、およびハイパーバイザの展開に管理者権限が必要です。

– 使用する Active Directory 用に iDRAC の設定および有効化が Active Directory ですでに行われている場合は、**Active Directory を使用する** チェックボックスを選択します。それ以外は、iDRAC 資格情報の設定に進みます。

  * **Active Directory ユーザー名** テキストボックスに、ユーザー名を入力します。ユーザー名は、ドメイン\ユーザー名、ドメイン/ユーザー名、またはユーザー名@ドメインのいずれかの形式で入力してください。ユーザー名は 256 文字に制限されています。ユーザー名の制限については、Microsoft Active Directory マニュアルを参照してください。
  * **Active Directory パスワード** テキストボックスにパスワードを入力します。パスワードは 127 文字に制限されています。
  * **パスワードの確認** テキストボックスにパスワードを再度入力します。
  * 証明書チェックのドロップダウンリストから、次のいずれかを選択します。
    - 今後すべての接続の際に iDRAC 証明書をダウンロードおよび保存して、証明書の検証を行うには、**有効** を選択します。
    - 証明書のチェックを行わず、保存しない場合は、**無効** を選択します。

– Active Directory なしで iDRAC 資格情報を設定するには、次のいずれかを行います。

  * **ユーザー名** テキストボックスにユーザー名を入力します。ユーザー名は 16 文字に制限されています。お使いのバージョンの iDRAC におけるユーザー名の制限についての情報は、iDRAC マニュアルを参照してください。

    メモ: ローカル iDRAC アカウントには、ファームウェアのアップデート、ハードウェアプロファイルの適用、およびハイパーバイザの展開に管理者権限が必要です。
  * **パスワード** テキストボックスにパスワードを入力します。パスワードは 20 文字に制限されています。
  * **パスワードの確認** テキストボックスにパスワードを再度入力します。
  * 証明書チェックのドロップダウンリストから、次のいずれかを選択します。
    - 今後すべての接続の際に iDRAC 証明書をダウンロードおよび保存して、証明書の検証を行うには、**有効** を選択します。
    - iDRAC 証明書のチェックを行わず、保存しない場合は、**無効** を選択します。

6. **次へ** をクリックします。
7. ホスト資格情報ページの資格情報で、次のいずれかを実行します。

– 使用する Active Directory 用にホストの設定および有効化が Active Directory ですでに行われている場合は、**Active Directory を使用する** チェックボックスを選択します。それ以外は、iDRAC 資格情報の設定に進みます。

  * **Active Directory ユーザー名** テキストボックスに、ユーザー名を入力します。ユーザー名は、ドメイン\ユーザー名、ドメイン/ユーザー名、またはユーザー名@ドメインのいずれかの形式で入力してください。ユーザー名は 256 文字に制限されています。ユーザー名の制限については、Microsoft Active Directory マニュアルを参照してください。
  * **Active Directory パスワード** テキストボックスにパスワードを入力します。パスワードは 127 文字に制限されています。
  * **パスワードの確認** テキストボックスにパスワードを再度入力します。

* 証明書チェックのドロップダウンリストから、次のいずれかを選択します。
  - 今後すべての接続の際にホスト証明書をダウンロードおよび保存して、証明書の検証を行うには、**有効** を選択します。
  - ホスト証明書のチェックを行わず、保存しない場合は、**無効** を選択します。

– Active Directory なしでホスト資格情報を設定するには、次のいずれかを行います。

* **ユーザー名** テキストボックスに、ユーザー名を入力します。ユーザー名はデフォルトで root で、ここは読み取り専用フィールドです。**Active Directory を使用する** を選択している場合、別のユーザー名を入力することができます。
* **パスワード** テキストボックスにパスワードを入力します。パスワードは 127 文字に制限されています。

  メモ: OMSA 資格情報は、ESX および ESXi ホストに使われたものと同じです。

* **パスワードの確認** テキストボックスにパスワードを再度入力します。
* 証明書チェックのドロップダウンリストから、次のいずれかを選択します。
  - 今後すべての接続の際にホスト証明書をダウンロードおよび保存して、証明書の検証を行うには、**有効** を選択します。
  - ホスト証明書のチェックを行わず、保存しない場合は、**無効** を選択します。

8. **次へ** をクリックします。
9. 接続プロファイルのテストページで、次のいずれかを行います。
   – テストを開始するには、**選択したテスト** をクリックします。その他のオプションはアクティブになっていません。
   – テストを中止するには、**すべてのテストを中止** をクリックします。

   メモ: iDRAC Express または Enterprise カードがないサーバーでは、iDRAC テスト接続結果は、このシステムには該当しませんが表示されます。
10. プロファイルを完了するには、**保存** をクリックします。
11. イベントとアラームの設定を続けるには、**保存して続行** をクリックします。

イベントおよびアラームの設定ウィザード

設定ウィザードを使用して、または Dell Management Center、イベントおよびアラームの設定オプション からイベントおよびアラームの設定を行います。

メモ: Dell PowerEdge 第 12 世代サーバ以前のホストでは、この機能を使用するには、ホストのイベントを vCenter に表示させるために、OMSA で仮想アプライアンスがトラップ送信先として設定されている必要があります。第 12 世代サーバでは、iDRAC の SNMP トラップの送信先を OpenManage Integration for VMware vCenter のアドレスに設定する必要があります。

イベントおよびアラームを設定するには、以下を行います。

1. **設定ウィザード** の **イベント掲載レベル** で、 以下のいずれかを選択します。
   – すべてのイベントを掲載をしない - ハードウェアイベントはブロックされます。
   – すべてのイベントを掲載する - すべてのハードウェアイベントが掲載されます。
   – 重要および警告イベントのみを掲載する - 重要または警告レベルのハードウェアイベントのみが掲載されます。

– 仮想化関連の重要および警告イベントのみを掲載する - 仮想化関連の重要および警告イベントのみが掲載されます。これはデフォルトのイベント掲載レベルです。

2. すべてのハードウェアアラームとイベントを有効化するには、**Dell ホストのアラームを有効にする** チェックボックスを選択します。

   メモ: アラームが有効化されている Dell ホストは、重要イベントに対応して保守モードに入ります。

3. 表示されるダイアログボックスで **続行** をクリックしてこの変更を確定するか、または **キャンセル** をクリックします。

   メモ: この手順は、**Dell ホストのアラームを有効にする** が選択されている場合にのみ表示されます。

4. すべての管理されている Dell サーバーで、デフォルトの vCenter アラーム設定を復元するには、**デフォルトのアラームの復元** をクリックします。

   変更が有効になるには、最大 1 分間かかることがあります。

5. ウィザードを続けるには、**保存して続行** をクリックします。

プロキシサーバーの設定ウィザード

設定ウィザードまたは後に Dell Management Center の **設定 → プロキシ** ページでプロキシサーバーを設定します。

プロキシサーバーを設定するには、以下を行います。

1. **HTTP プロキシの設定ウィンドウ** で以下のいずれかを行います。
   – プロキシサーバーを使用しない場合は、**保存して続行** をクリックします。
   – プロキシサーバーを使用する場合は、**設定** で **プロキシサーバーのアドレス** を入力します。
2. **プロキシポート番号** を入力します。
3. 必要に応じて、**資格情報が必須です** チェックボックスを選択します。
4. **資格情報が必須です** を選択した場合は、以下を行います。
   a) **プロキシユーザー名** テキストボックスにプロキシユーザー名を入力します。
   b) **プロキシパスワード** テキストボックスにプロキシパスワードを入力します。
   c) **パスワードの確認** テキストボックスにプロキシパスワードを再入力します。
5. **プロキシ** で **プロキシを使用する** チェックボックスを選択します。
6. これらのオプションを保存して継続するには **保存して続行** をクリックします。

インベントリジョブのスケジュールウィザード

インベントリスケジュール設定は、設定ウィザードと Dell Management Center の設定オプション間でほぼ同じです。唯一の違いは、ウィザードではインベントリをただちに実行するオプションを選択できることです。

メモ: OpenManage Integration for VMware vCenter で今後もアップデートされた情報を確実に表示するようにするため、定期的なインベントリジョブをスケジュールすることをお勧めします。インベントリジョブは最小限のリソースのみを消費し、ホストのパフォーマンスを劣化させることはありません。

インベントリジョブのスケジュールには、以下を行います。

1. **設定ウィザード** の **インベントリのスケジュール** ウィンドウで、以下の中から 1 つを行います。
   – インベントリスケジュールを実行するには、**選択した曜日** をクリックします。
   – インベントリスケジュールを実行しない場合は、**Dell ホストではインベントリを実行しない** を選択します。
2. **選択した曜日** を選択した場合は、以下を行います。
   a) インベントリを実行したい各曜日の横にあるチェックボックスを選択します。

b) テキストボックスに、時刻を HH:MM フォーマットで入力します。

入力時刻は現地時刻です。インベントリの収集を適切な時刻に実行するよう、時間差を計算します。

c) ウィザードの完了後、インベントリタスクを自動的に実行するには、**ウィザードの最後にインベントリを実行します（推奨）**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、選択した曜日のチェックボックスが選択された場合にのみ表示されます。

3. 変更を適用して継続するには、**保存して続行** をクリックします。

保証取得ジョブウィザードの実行

保証取得ジョブの設定は、ウィザードと Dell Management Center の設定オプションからの間でほぼ同じです。また、ジョブキューから保証取得ジョブを今すぐ実行することができます。

保証取得ジョブを実行するには以下を行います。

1. **設定ウィザード**の**保証のスケジュール**ウィンドウで、以下のいずれかを行います。
   - 保証スケジュールを実行するには、**選択した曜日**をクリックします。
   - 保証スケジュールを実行しないようにするには、**保証情報を取得しない**を選択します。
2. **選択した曜日** を選択した場合は、以下を行います。
   a) 保証ジョブを実行したい各曜日の横にあるテキストボックスを選択します。
   b) テキストボックスに、時刻を HH:MM フォーマットで入力します。

   入力した時刻は入力地の現地時刻です。保証ジョブを実行する必要のある正しい時刻について時差を計算してください。
3. 変更を適用して継続するには、**保存して続行** をクリックします。

展開資格情報の設定ウィザード

展開資格情報は、最初の検出から展開プロセスの終了まで、iDRAC を使ってベアメタルシステムとセキュアな通信を行うために使用されます。展開が完了すると、資格情報は展開ウィザードから接続プロファイルでベアメタルシステムに一致するものに変更されます。展開資格情報が変更されると、その時点以降に新たに検出されるシステムは新しい資格情報でプロビジョニングが行われます。ただし、変更前に検出されたサーバーの資格情報には影響を及ぼしません。

展開資格情報の設定には、以下を行います。

1. **展開資格情報** ウィンドウで、資格情報を表示または変更できます。ベアメタルサーバーは、これらの資格情報から接続プロファイルで指定されたものに切り替えます。
2. これらの資格情報を変更するには、**ベアメタルサーバー展開用の資格情報** 下で以下を行います。
   a) **ユーザー名** テキストボックスでユーザー名を編集します。
   b) **パスワード** テキストボックスでパスワードを編集します。
   c) **パスワードの確認** テキストボックスでパスワードを確認します。
3. 特定した資格情報を保存して設定ウィザードを続けるには、**保存して続行** をクリックします。

デフォルトのファームウェアアップデートリポジトリの設定ウィザード

ファームウェアリポジトリ設定には、展開済みサーバーのアップデートに使用されるファームウェアカタログの場所が含まれます。ファームウェアリポジトリの設定は最初にこのウィザードで設定するか、後で Dell Management Center の設定オプションで設定できます。さらに、ファームウェアアップデートも後で OpenManage Integration タブから実行できます。

デフォルトのファームウェアアップデートリポジトリを設定するには、以下を行います。

1. **設定ウィザード** の **ファームウェアリポジトリ** で、ファームウェアアップデートのためにデフォルトリポジトリを選択するには、以下のいずれか 1 つを選択します。

   – Dell Online

   ステージングフォルダのある、デフォルトのファームウェアリポジトリ（ftp.dell.com）です。OpenManage Integration for VMware vCenter は選択されたファームウェアのアップデートをダウンロードし、それらをステージングフォルダに保存して、後に必要に応じて適用します。

   – ローカル / 共有リポジトリ

   これは Dell Repository Manager アプリケーションで作成されます。このローカルリポジトリは、Windows ベースのファイル共有で見つけることができます。

2. **ローカル / 共有リポジトリ** を選択した場合、以下を行います。
   a) 次のフォーマットを使って、**カタログファイルの場所** を入力します。

      * xml ファイル用の NFS 共有: host:/share/filename.xml
      * gz ファイル用の CIFS 共有: \\host\share\filename.gz
      * xml ファイル用の CIFS 共有: \\host\share\filename.xml
      * gz ファイル用の CIFS 共有: \\host\share\filename.gz

   b) CIFS 共有を使用する場合、**ユーザー名**、**パスワード**、**パスワードの確認** を入力します。両パスワードは一致する必要があります。これらの欄は CIFS 共有を入力する場合にのみアクティブになります。

      メモ: 共有ネットワークフォルダのユーザー名 / パスワードには、@ 文字は使用できません。

   c) 入力情報を確認するには、**テストの開始** をクリックします。
3. この選択を保存して **設定ウィザード** を継続するには、**保存して続行** をクリックします。

OMSA リンクの有効化ウィザード

OpenManage Integration for VMware vCenter 仮想アプライアンス内で OpenManage Server Administator（OMSA）を起動するには、OMSA Web Server のインストールと設定が必要です。Web Server のインストールおよび設定の手順に関しては、『*OpenManage Server Administrator Installation Guide*』（OpenManage Server Administrator インストールガイド）を参照してください。

メモ: OMSA は Dell PowerEdge 第 12 世代サーバーより前の Dell サーバーにのみ必要です。

OMSA を使用して、以下を行うことができます。

- vCenter エレメント（詳細センサ / コンポーネントレベルの正常性情報）の管理。
- コマンドログおよびシステムイベントログ（SEL）の消去。
- NIC 統計情報の取得。
- OpenManage Integration for VMware vCenter が、選択したホストからイベントをキャプチャしていることを確認します。

1. **設定ウィザード** の **OpenManage Server Admin** ページで **OMSA Web Server URL** テキストボックスを使って OMSA URL を入力します。HTTPS およびポート番号を含む完全な URL を入力する必要があります。（例 : https:\\<OMSA_サーバー IP またはホスト名>:1311）
2. この URL を保存して設定ウィザードを終了するには、**終了** をクリックします。

NFS 共有の設定

OpenManage Integration for VMware vCenter で、バックアップと復元操作用、ファームウェアアップデート用、およびステージングフォルダとして NFS 共有を使用するには、完了する必要がある特定の設定があります。CIFS 共有には追加設定を行う必要はありません。

NFS 共有の設定には、以下を行います。

1. NFS 共有をホストしているマシンで、**/etc/exports** を編集して **/share/path <appliance IP> (rw) *(ro)** を追加します。
   これにより、仮想アプライアンスは完全に共有の読み書きができるようになりますが、他のユーザーは読み取り専用となります。
2. nfs サービスの開始：
   ```
   service portmap start service nfs start service nfslock status
   ```
   メモ: 上記の手順は、使用している Linux ディストリビューションによって異なる場合があります。
3. すでにいずれかのサービスが実行されている場合は、以下を行います。
   ```
   exportfs -ra
   ```

設定の概要

OpenManage Integration for VMware vCenter 設定セクション:

- OpenManage Integration for VMware vCenter 設定を表示します。
- 最初に VMware vCenter でサーバーを管理、展開するのに必要な OpenManage Integration for VMware vCenter 機能を手順ごとに説明する、設定ウィザードを起動します。
- vCenter 登録、仮想アプライアンス管理、アラート管理、および OpenManage Integration for VMware vCenter データベースのバックアップ/復元を行うことができる OpenManage Integration for VMware vCenter 管理コンソールを起動します。

関連タスク:

- 一般: vCenter の Dell ホストタブに表示される OMSA URL を設定します。また、保証期限通知を有効化または無効化することもできます。
- イベントとアラーム: すべてのハードウェアアラームを有効化または無効化します（現在のアラートステータスはアラームタブに表示されます）。また、受信するイベントおよびアラートのフィルタリングも設定します。
- プロキシ: インターネットサイトとの通信中のプロキシの使用を有効化または無効化します。
- インベントリのスケジュール: vCenter ホストインベントリスケジュールを設定します。
- 保証のスケジュール: Dell Online から Dell ホストへの保証情報の検索スケジュールを設定します。
- 展開資格情報: 初期検出時に Dell サーバーと通信する際、およびベアメタルサーバー展開で使用される資格情報を設定します。
- ファームウェアリポジトリ: ファームウェアアップデートを保存するロケーションの編集を可能にします。
- セキュリティ: 展開できるサーバーを制限するサーバーホワイトリストを提供します。

一般設定の概要

一般設定は、以下を行うために使われます。

- OpenManage Server Administrator（OMSA）URL の定義。
- 保証期限通知の有効化または無効化。

OMSA ソフトウェアは以下のために使用できます。

- vCenter エレメントの管理（詳細センサー、コンポーネントレベルの正常性情報）。
- コマンドログおよびシステムイベントログ（SEL）の消去。
- NIC 統計情報の取得。
- OpenManage Integration for VMware vCenter が選択したホストからイベントをキャプチャしていることを確認します。

メモ: OMSA ソフトウェアは Dell PowerEdge 第 12 世代サーバーより前の Dell サーバーにのみ必要です。

保証期限通知は、以下のために使用できます。

- 保証期限の監視。
- 最低保証残余期間基準の警告または重要アラートの発生以降の設定。アラートは、ホストの OpenManage Integration タブにアイコンとして表示されます。

関連タスク:

- OMSA リンクの有効化
- 保証期限通知の有効化または無効化

設定ウィザード外での OMSA リンクの有効化

OpenManage Integration for VMware vCenter 仮想アプライアンス内で OpenManage Server Administator（OMSA）を起動するには、OMSA Web Server のインストールと設定が必要です。Web Server のインストールおよび設定の手順に関しては、お使いの OMSA バージョン向け『*Dell OpenManage Server Administrator Installation Guide*』（Dell OpenManage Server Administrator インストールガイド）を参照してください。

メモ: OMSA は Dell PowerEdge 第 12 世代サーバーより前の Dell サーバーにのみ必要です。

OMSA リンクを有効化するには、以下を行います。

1. OMSA 起動ツール下の **Dell Management Center 設定** → **一般** で、**編集** をクリックします。
2. **OMSA Web Server URL** テキストボックスを使用して、OMSA の URL を入力します。HTTPS およびポート番号 1311 を含む完全な URL を入力する必要があります。
3. この URL を保存するには、**適用** をクリックします。
   OMSA トラップ先を設定することに関する情報は、「OMSA トラップ先の設定」を参照してください。

サーバー保証期限通知の有効化または無効化

保証設定は、保証スケジュールを有効化または無効化し、最小日数しきい値アラートを設定することで、Dell オンラインからサーバー保証情報を検索する時期を管理することができます。このページを使用してホストとクラスタのサーバー保証期限通知を有効化または無効化します。この機能は、Dell Management Center の設定、一般ページで設定または編集できます。
サーバー保証期限通知の有効化または無効化には、以下を行います。

1. **Dell Management Center** で、 **設定** → **一般** をクリックします。
2. **一般**ページで、通知を有効化するには **保証状態の通知を有効にする**チェックボックスを選択します。
3. **最小日数しきい値アラート**を設定するには、以下を行います。
   a) 警告を設定するには、**警告**ドロップダウンリストでサーバー警告ステータスに関する日数を選択します。
   b) 重要ライセンスステータスを設定するには、**重要**ドロップダウンリストで重要サーバー保証ステータスに日数を設定します。
4. 変更を適用するには、**適用**をクリックします。

新しい接続プロファイルの作成

接続プロファイルは Dell サーバーと通信するために仮想サーバーが使用する資格情報を保存します。各 Dell サーバーは OpenManage Integration for VMware vCenter が管理する 1 つだけの接続プロファイルに関連付けられている必要があります。1 つの接続プロファイルに複数のサーバーを割り当てることができます。 接続プロファイルの作成方法は、接続ウィザードからであっても、**Dell Management Center → 設定** であってもほぼ同じです。設定ウィザードは初めて Dell Management Console にアクセスしたとき、またはその後、設定ウィンドウから実行することもできます。

メモ: 本リリース、および第 12 世代サーバー以降のホストでのインストールでは、OMSA エージェントのインストールは必要ありません。Dell PowerEdge 第 11 世代サーバーへのインストールでは、現在、OMSA エージェントは展開プロセス中に自動的にインストールされます。

メモ: ライセンスの詳細については、「OpenManage Integration for VMware vCenter ライセンスについて」を参照してください。

メモ: 追加されたホスト数がライセンス制限を超過した場合、接続プロファイルを作成できます。

新しい接続プロファイルを作成するには、次の手順を実行します。

1. **Dell Management Center** の左ペインで、**接続プロファイル** をクリックします。
2. **プロファイル名と説明** ページで、カスタム接続プロファイルの管理に役立つ **接続プロファイル名** とオプションの **接続プロファイルの説明** を入力します。
3. **関連ホスト** ページで、接続プロファイルのホストを選択し、**次へ** をクリックします。
4. **資格情報** ページで、情報を読んでから **次へ** をクリックします。
5. iDRAC ページの資格情報で、次のいずれかを実行します。

   メモ: iDRAC アカウントには、ファームウェアのアップデート、ハードウェアプロファイルの適用、およびハイパーバイザの展開に管理者権限が必要です。

   – 使用する Active Directory 用に iDRAC の設定および有効化が Active Directory ですでに行われている場合は、**Active Directory を使用する** チェックボックスを選択します。それ以外は、iDRAC 資格情報の設定に進みます。

     * **Active Directory ユーザー名** テキストボックスに、ユーザー名を入力します。ユーザー名は、ドメイン\ユーザー名、ドメイン/ユーザー名、またはユーザー名@ドメインのいずれかの形式で入力してください。ユーザー名は 256 文字に制限されています。ユーザー名の制限については、Microsoft Active Directory マニュアルを参照してください。
     * **Active Directory パスワード** テキストボックスにパスワードを入力します。パスワードは 127 文字に制限されています。
     * **パスワードの確認** テキストボックスにパスワードを再度入力します。
     * 証明書チェックのドロップダウンリストから、次のいずれかを選択します。
       - 今後すべての接続の際に iDRAC 証明書をダウンロードおよび保存して、証明書の検証を行うには、**有効** を選択します。
       - 証明書のチェックを行わず、保存しない場合は、**無効** を選択します。

   – Active Directory なしで iDRAC 資格情報を設定するには、次のいずれかを行います。

     * **ユーザー名** テキストボックスにユーザー名を入力します。ユーザー名は 16 文字に制限されています。お使いのバージョンの iDRAC におけるユーザー名の制限についての情報は、iDRAC マニュアルを参照してください。

メモ: ローカル iDRAC アカウントには、ファームウェアのアップデート、ハードウェアプロファイルの適用、およびハイパーバイザの展開に管理者権限が必要です。

* **パスワード** テキストボックスにパスワードを入力します。パスワードは 20 文字に制限されています。
* **パスワードの確認** テキストボックスにパスワードを再度入力します。
* 証明書チェックのドロップダウンリストから、次のいずれかを選択します。
  - 今後すべての接続の際に iDRAC 証明書をダウンロードおよび保存して、証明書の検証を行うには、**有効** を選択します。
  - iDRAC 証明書のチェックを行わず、保存しない場合は、**無効** を選択します。

6. **次へ** をクリックします。
7. ホスト資格情報ページの資格情報で、次のいずれかを実行します。

– 使用する Active Directory 用にホストの設定および有効化が Active Directory ですでに行われている場合は、**Active Directory を使用する** チェックボックスを選択します。それ以外は、iDRAC 資格情報の設定に進みます。

* **Active Directory ユーザー名** テキストボックスに、ユーザー名を入力します。ユーザー名は、ドメイン\ユーザー名、ドメイン/ユーザー名、またはユーザー名@ドメインのいずれかの形式で入力してください。ユーザー名は 256 文字に制限されています。ユーザー名の制限については、Microsoft Active Directory マニュアルを参照してください。
* **Active Directory パスワード** テキストボックスにパスワードを入力します。パスワードは 127 文字に制限されています。
* **パスワードの確認** テキストボックスにパスワードを再度入力します。
* 証明書チェックのドロップダウンリストから、次のいずれかを選択します。
  - 今後すべての接続の際にホスト証明書をダウンロードおよび保存して、証明書の検証を行うには、**有効** を選択します。
  - ホスト証明書のチェックを行わず、保存しない場合は、**無効** を選択します。

– Active Directory なしでホスト資格情報を設定するには、次のいずれかを行います。

* **ユーザー名** テキストボックスにユーザー名を入力します。読み取り専用のデフォルトのユーザー名は root です。 **Active Directory を使用** を選択した場合、ユーザー名は root と異なることがあります。
* **パスワード** テキストボックスにパスワードを入力します。パスワードは 127 文字に制限されています。

  メモ: OMSA 資格情報は、ESX および ESXi ホストに使われたものと同じです。
* **パスワードの確認** テキストボックスにパスワードを再度入力します。
* 証明書チェックのドロップダウンリストから、次のいずれかを選択します。
  - 今後すべての接続の際にホスト証明書をダウンロードおよび保存して、証明書の検証を行うには、**有効** を選択します。
  - ホスト証明書のチェックを行わず、保存しない場合は、**無効** を選択します。

8. **次へ** をクリックします。
9. **接続性のテスト** ウィンドウで、選択されたサーバー用に入力された iDRAC およびホストルートの資格情報がテストされます。次のいずれかを行います。

– テストを開始するには、**選択したテスト** をクリックします。その他のオプションはアクティブになっていません。

– テストを中止するには、**テストの中止** をクリックします。

メモ: iDRAC Express または Enterprise カードがないサーバーでは、iDRAC テスト接続結果は、このシステムには該当しませんが表示されます。

10. プロファイルを完了するには、**保存** をクリックします。
    接続プロファイルを管理するには、「接続プロファイルの管理」を参照してください。

イベントおよびアラームの設定

Dell Management Center イベントおよびアラームページでは、すべてのハードウェアアラームを有効または無効にできます。現在のアラートステータスは vCenter アラームタブに表示されます。重要イベントは実際のまたは切迫したデータ喪失あるいはシステム異常を示します。警告イベントは必ずしも重大ではないが、将来の潜在的な問題を示す可能性があります。 イベントおよびアラームは VMware Alarm Manager を使用して有効化することもできます。イベントは、ホストとクラスタビューの vCenter タスクとイベントタブに表示されます。

メモ: Dell PowerEdge 第 12 世代サーバーより前のホストでは、vCenter でホストイベントを表示するため、OMSA で仮想アプライアンスがトラップ宛先に設定されている必要があります。OMSA の詳細については、「OMSA トラップ宛先の設定」を参照してください。

イベントおよびアラームは、Dell Management Center のイベントとアラームの設定オプションで設定できます。
イベントおよびアラームを設定するには、以下を行います。

1. **Dell Management Center** の **設定 → イベントとアラーム** で **編集** をクリックします。
2. **イベント掲載レベル** で以下のいずれかを選択します。
   – すべてのイベントを掲載をしない - ハードウェアイベントはブロックされます。
   – すべてのイベントを掲載する - すべてのハードウェアイベントが掲載されます。
   – 重要および警告イベントのみを掲載する - 重要または警告レベルのハードウェアイベントのみが掲載されます。
   – 仮想化関連の重要および警告イベントのみを掲載する - 仮想化関連の重要および警告イベントのみが掲載されます。これはデフォルトのイベント掲載レベルです。
3. すべてのハードウェアアラームとイベントを有効化するには、**Dell ホストのアラームを有効にする** チェックボックスを選択します。

   メモ: アラームが有効化されている Dell ホストは、重要イベントに対応して保守モードに入ります。
4. 表示されるダイアログボックスで **続行** をクリックしてこの変更を確定するか、または **キャンセル** をクリックします。
5. すべての管理されている Dell サーバーで、デフォルトの vCenter アラーム設定を復元するには、**デフォルトのアラームの復元** をクリックします。
   変更が有効になるには、最大 1 分間かかることがあります。
6. 保存するには、**保存** をクリックします。

プロキシの設定について

プロキシ設定は、HTTP プロキシおよびウェブ（Dell オンラインからを含む）から情報を検索するために使用される、必要な資格情報を定義します。それには以下が含まれます。

- プロキシサーバーの有効化または無効化
- 必要なプロキシサーバーとポート番号の入力
- 必要な資格情報（ユーザー名およびパスワード）の定義

メモ: プロキシパスワードは、31 文字を超えることはできません。

関連タスク:

- プロキシサーバーの設定
- ウェブベースデータを検索するための HTTP プロキシの使用
- 管理コンソールを使用した HTTP プロキシの設定

プロキシサーバーの設定

設定ウィザードを使用してプロキシサーバーを設定するか、後ほど設定オプション、プロキシを使って設定します。

メモ: プロキシパスワードは、31 文字を超えることはできません。

プロキシサーバーを設定するには、以下を行います。

1. Dell Management Center で **設定** → **プロキシ** を選択して、**編集** をクリックします。
2. **HTTP プロキシ** ウィンドウで以下のいずれかを行います。
   - プロキシサーバーを使用しない場合は、**保存して続行** をクリックします。
   - プロキシサーバーを使用する場合は、**設定** で **プロキシサーバーのアドレス** を入力します。
3. **プロキシポート番号** を入力します。
4. 必要に応じて、**資格情報が必須です** チェックボックスを選択します。
5. **資格情報が必須です** を選択した場合は、以下を行います。
   a) **プロキシユーザー名** テキストボックスにプロキシユーザー名を入力します。
   b) **プロキシパスワード** テキストボックスにプロキシパスワードを入力します。
   c) **パスワードの確認** テキストボックスに、今入力したばかりのプロキシパスワードを再入力します。
6. **プロキシ** で **プロキシを使用する** チェックボックスを選択します。
7. これらのオプションを保存するには、**保存** をクリックします。

ウェブベースデータを検索するための HTTP プロキシの使用

HTTP プロキシを使用してウェブベースのデータを検索するには、以下を行います。

1. **Dell Management Center** で **設定 HTTP プロキシ**を選択して、**編集**をクリックします。
2. **プロキシを使用する**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。
4. 設定を確認するには、**接続性のテスト**をクリックします。

インベントリジョブの実行

インベントリジョブを実行するには：

1. **設定ウィザード**が完了したら、**ジョブキュー** → **インベントリ** → **今すぐ実行** をクリックしてインベントリジョブをただちに実行します。
2. インベントリジョブのステータスを見るには、**更新**をクリックします。
3. **ホストおよびクラスタ** ビューに進み、いずれかの **Dell ホスト** をクリックして **OpenManage Integration** タブをクリックします。次の情報が表示されます。
   - 概要ページ
   - システムイベントログ
   - ハードウェアインベントリ

– ストレージ
– ファームウェア
– 電源監視
– 保証ステータス

メモ: ライセンス制限を超過するホストのインベントリジョブはスキップされて 失敗 とマークされます。

次のホストコマンドは、OpenManage Integration タブ内で機能します:

– インジケータライトの点滅
– ファームウェアアップデートウィザードを実行
– リモートアクセスの起動
– OMSA の起動
– CMC の起動
– 保証の更新

保証取得ジョブの実行

保証取得ジョブの設定手順はウィザードと **Dell Management Center → 設定** オプション間でほぼ同じです。ウィザードの実行後、**Dell Management Center → 設定 → 保証スケジュール** ページを使用して後でいつでも編集できます。保証取得ジョブは現在、**ジョブのキュー → 保証履歴**ページから実行することができます。

保証の取得ジョブのスケジューリングには、以下を行います。

1. **Dell Management Center** で **設定 → 保証のスケジュール** を選択します。
2. **保証のスケジュール**ウィンドウで **編集**をクリックします。
3. スケジュールを設定するには、次のいずれかを行います。
   a) 保証スケジュールを実行するには、**選択した曜日**をクリックします。
   b) 保証スケジュールを実行しない場合は、**Dell ホストではインベントリを実行しない**を選択します。
4. **選択した曜日** を選択した場合は、以下を行います。
   a) 保証ジョブを実行したい曜日の横にあるチェックボックスを選択します。
   b) テキストボックスに、時刻を HH:MM フォーマットで入力します。
      入力した時刻は入力地の現地時刻です。保証ジョブを実行する必要のある正しい時刻について時差を計算してください。
5. 保証ジョブを今すぐ実行するには、**ジョブキュー → 保証履歴** へ移動し、**今すぐ実行**をクリックします。

展開資格情報の表示または編集

Dell Management Center で展開資格情報を編集することができます。展開資格情報は、最初の検出から展開プロセスの最後まで、iDRAC を使用するベアメタルシステムとセキュアな通信を行うために使われます。展開が完了すると、資格情報は展開ウィザードからベアメタルシステムの接続プロファイルと一致するものに変更されます。展開資格情報が変更されると、その時点以降新たに検出されるすべてのシステムは、新しい資格情報でプロビジョニングが行われます。資格情報の変更前に検出されたサーバーの資格情報はこの変更での影響は受けません。ユーザー名は、16 文字以下（ASCII 印刷可能文字）である必要があります。パスワードは 20 文字以下（ASCII 印刷可能文字）である必要があります。

展開資格情報を表示または編集するには、以下を行います。

1. **Dell Management Center → 設定 → 展開用資格情報** で、**編集**をクリックします。
2. **ベアメタルサーバー展開用の資格情報**の **資格情報**で以下を行います。
   – **ユーザー名**テキストボックスにユーザー名を入力します。

ユーザー名は、16 文字以下（ASCII 印刷可能文字のみ）である必要があります。

– **パスワード**テキストボックスにパスワードを入力します。
パスワードは、20 文字以下（ASCII 印刷可能文字のみ）である必要があります。

– **パスワードの確認** テキストボックスにパスワードを再度入力します。
両パスワードは一致する必要があります。

3. **適用** をクリックします。

ファームウェアリポジトリの設定

ファームウェアリポジトリおよび資格情報を設定するには、以下を行います。

1. **Dell Management Center** で、**設定 → ファームウェアリポジトリ** を選択し、**編集**をクリックします。
2. **ファームウェアリポジトリ**ページでファームウェアのアップデートのためのデフォルトリポジトリを選択するには、以下のいずれかを選択します。

   – Dell Online
   これは、Dell Online（ftp.dell.com）のデフォルトファームウェアアップデートリポジトリを使用するもので、中継フォルダが必要です。OpenManage Integration for VMware vCenter は選択されたファームウェアアップデートをダウンロードし、中継フォルダに保存します。そこから必要に応じて適用されます。

   – ローカル / 共有リポジトリ
   これは Dell Repository Manager アプリケーションで作成されます。このローカルリポジトリは、Windows ベースのファイル共有で見つけることができます。

3. **ローカル / 共有リポジトリ** を選択した場合、以下を行います。
   a) 次のフォーマットを使って、**カタログファイルの場所** を入力します。
      * xml ファイル用の NFS 共有: host:/share/filename.xml
      * gz ファイル用の NFS 共有: host: /share/filename.gz
      * xml ファイル用の CIFS 共有: \\host\share\filename.xml
      * gz ファイル用の CIFS 共有: \\host\share\filename.gz
   b) CIFS 共有を使用する場合、**ユーザー名**、**パスワード**、**パスワードの確認** を入力します。両パスワードは一致する必要があります。これらの欄は CIFS 共有を入力する場合にのみアクティブになります。

      メモ: 共有ネットワークフォルダのユーザー名 / パスワードには、@ 文字は使用できません。

   c) 入力情報を確認するには、**テストの開始** をクリックします。
4. **適用** をクリックします。

展開のためのサーバーセキュリティの設定

ホワイトリストを使用して展開可能サーバーセットを制限します。サーバーがホワイトリストにある場合、自動検出時およびハンドシェークプロセス中に認証情報が提供され、展開に使用されるサーバーリストに表示されます。ホワイトリストは、サーバーサービスタグの追加、サービスタグの削除、または CSV ファイルからサービスタグリストをインポートすることにより、手動で保守されます。

メモ: サーバーをインポートするには、CSV の区切り付きファイルを使用します。これには別々の行の複数のレコードが含まれ、各レコードには 1 つまたはカンマで区切られた複数のサービスタグが含まれます。

ホワイトリストを設定し、管理するには、以下から選択してください。

- サーバーホワイトリストの有効化

- ホワイトリストへのサーバーの追加
- ホワイトリストからのサーバーの削除

展開可能サーバーホワイトリストの有効化

展開可能サーバーのセキュリティ設定に関する情報については、「展開のためのサーバーセキュリティ設定」を参照してください。
サーバーホワイトリストを有効化するには、以下を行います。

1. **Dell Management Center** の左ペインで **設定**を選択します。
2. 右ペインで、**セキュリティ**を選択します。
3. **セキュリティ**ウィンドウで、**編集**をクリックします。
4. サーバーの展開を制限するためにホワイトリストを使用するには、**サーバーホワイトリストを強制する**チェックボックスを選択します。
5. **適用**をクリックすると、サーバーホワイト設定が有効に変わります。

ホワイトリストへの展開可能サーバーの追加

展開可能サーバーに対するセキュリティ設定に関する情報については、「展開のためのサーバーセキュリティ設定」を参照してください。実施した場合、サーバーホワイトリストに記載されている Dell サーバーのみが OpenManage Integration for VMware vCenter を使用して展開可能となります。 ホワイトリストに展開可能サーバーを追加するには、手動で、またはリストを使ってインポートすることができます。
展開可能サーバーをホワイトリストに追加するには、以下を行います。

1. **Dell Management Center** の左ペインで **設定 → セキュリティ** を選択します。
2. **サーバーホワイトリスト** ウィンドウで、**編集** をクリックして、以下のいずれかを行います。
   - サーバーをホワイトリストに手動で追加するには、**サーバーの追加** をクリックします。
     * **サービスタグの追加** ダイアログで、サービスタグを入力します。
     * タグを追加するには、**続行** をクリックします。
   - サービスタグのリストをインポートするには、**ホワイトリストのインポート** をクリックします。
     * **アップロードファイルの選択** ダイアログボックスが表示されたら、該当の CSV ファイルを参照し、**開く** をクリックします。
       ホワイトリストの例は次のとおりです。
       ASDFG12
       SDCNRD0
       TESCVD3
       AS243AS, ASWERF3, DFGVCSD9
     * **ファイルでこれらのサービスタグを検出しました** ダイアログが表示されたら、**適用** をクリックします。

   サービスタグが、サービスタグリストに表示されます。

ホワイトリストからの展開可能サーバーの削除

展開可能サーバーのセキュリティ設定に関する情報については、「展開のためのサーバーセキュリティ設定」を参照してください。

展開可能サーバーをホワイトリストから削除するには、以下を行います。

1. **Dell Management Center** の左ペインで、**設定**を選択します。
2. 右ペインで、**セキュリティ**を選択します。
3. **セキュリティ**ウィンドウで**編集**をクリックします。
4. 次の手順のいずれか 1 つを実行します。
   - 個別サーバーを削除するには、**サービスタグ**チェックボックスをクリックして、次に **選択項目の削除**をクリックします。
   - 全サーバーを削除するには、**サービスタグ**チェックボックスをクリックして、次に **選択項目の削除**をクリックします。
5. **選択したサービスタグを削除してよろしいですか** ダイアログが表示されたら、**適用**をクリックするか、または **キャンセル**をクリックして取り消します。
6. 変更が完了したら、**適用**をクリックします。

ホスト、ベアメタルおよび iDRAC 対応問題について

ホスト、ベアメタルサーバー、および iDRAC を OpenManage Integration for VMware vCenter で管理するには、それぞれが一定の最低基準を満たさなければなりません。対応していない場合、OpenManage Integration for VMware vCenter で正しく管理できません。非対応のホスト、ベアメタルサーバー、および iDRAC 対応リンクを使って、どのホスト / ベアメタルサーバー / iDRAC が非対応となっているか確認し、修正します。このウィザードは次の状態にあるホスト / ベアメタルサーバー / iDRAC を表示します。

- ホストが接続プロファイルに割り当てられていない。
  接続プロファイルがホストに割り当てられない場合、接続プロファイル画面に移動するためのダイアログボックスが表示されます。この設定はこのウィザードの範囲外です。後でこのウィザードの実行に戻ってください。
- 再起動時にシステムインベントリを収集（CSIOR）が無効化されている、または実行されたことがないので手動の再起動が必要。
- OMSA エージェント（ホストルート資格情報）がインストールされていない、古い、または正しく設定されていない。
- ベアメタルサーバーの Integrated Dell Remote Access Controller (iDRAC) ファームウェア、Lifecycle Controller (LC) ファームウェア、または BIOS バージョンが古い。

注意: ロックダウンモードのホストは、非対応であっても対応確認に表示されません。表示されないのは対応ステータスが確認できないからです。これらのシステムの対応状況は手動で確認してください。確認が必要な場合は警告が表示されます。

それぞれの場合、以下のいずれかを実行して対応問題を解決する必要があります。

- vSphere ホスト対応問題を解決するには、「非対応の vSphere ホスト解決ウィザードの実行」を参照してください。
- 対応問題のあるベアメタルサーバーを解決するには、「非対応のベアメタルサーバー解決ウィザードの実行」を参照してください。
- iDRAC 対応問題を解決するには、「iDRAC ライセンス対応」を参照してください。

関連情報

- ベアメタルサーバー対応性の再確認
- 手動ファームウェアアップデートのための ISO のダウンロード

非準拠 vSphere ホストの修正ウィザードの実行

非準拠 vSphere ホストの修正ウィザードを実行して、非準拠ホストを修正します。コンプライアンスについては、「ホストおよびベアメタルのコンプライアンス問題について」を参照してください。一部の非準拠 ESXi

ホストでは再起動が必要です。OpenManage Server Administrator（OMSA）をインストールまたはアップデートする必要がある場合は、ESXi ホストの再起動が必要です。さらに、CSIOR を実行したことがないホストでも再起動が必要です。ESXi ホストを自動的に再起動するように選択した場合は、次の動作が行われます。

- CSIOR ステータス修正:
  ホストで CSIOR が実行されたことがない場合、CSIOR はホストで*オン*と設定され、ホストはメンテナンスモードに入り、再起動されます。
- OMSA ステータス修正：
  a. OMSA がホストにインストールされます。
  b. ホストは、メンテナンスモードに入り、再起動されます。
  c. 再起動が完了すると、変更が有効になるように OMSA が設定されます。
  d. ホストはメンテナンスモードを終了します。
  e. インベントリが実行され、データが更新されます。

非準拠 vSphere ホストの修正ウィザードを実行するには、以下を行います。

1. **Dell Management Center** の左ペインで **コンプライアンス → vSphere ホスト** をクリックします。
2. **vSphere ホストコンプライアンス** ウィンドウで、非準拠ホストを表示し、次に **非準拠 vSphere ホストの修正** をクリックします。
3. **非準拠 vSphere ホストの修正** ウィザードで、修正するホストのチェックボックスを選択します。
4. **次へ** をクリックします。
5. 接続プロファイルのないサーバーがある場合は、ウィザードを終了してそれらのシステムを **接続プロファイル** ページで修正するか、このウィザードを継続するかのオプションが示されます。「新規接続プロファイルの作成」を参照してください。完了したらこのウィザードに戻ります。
6. **CSIOR をオンにする** ウィンドウで、選択されたホストの **CSIOR** を起動するチェックボックスを選択します。
7. **次へ** をクリックします。
8. **OMSA の修正** ウィンドウで、選択されたホストの **OMSA** を修正するチェックボックスを選択します。
9. **次へ** をクリックします。
10. **ホストの再起動** ウィンドウで、再起動する必要のある ESXi ホストを表示します。OpenManage Server Administrator（OMSA）をインストールまたはアップデートする必要がある場合は、ESXi ホストの再起動が必要です。さらに、CSIOR を実行したことがないホストでも再起動が必要です。以下のいずれかを行います。
    - 自動的にホストを保守モードにして、必要なときに再起動するには、**ホストを自動的にメンテナンスモードに切り替えて、必要に応じて再起動する** チェックボックスを選択します。
    - 手動で再起動したい場合、以下を行う必要があります。
        1. ホストで *OMSA のインストール*タスクが完了したら、ホストを再起動します。
        2. ホストが立ち上がったら、OMSA が設定されていない場合は、OMSA を手動で設定するか、コンプライアンスウィザードを使用します。
        3. インベントリを再実行します。「インベントリジョブの実行」を参照してください。
11. **次へ** をクリックします。
12. **概要** ウィンドウで、非準拠ホストで行われるアクションを確認します。これらが適用されるには、手動再起動が必要です。
13. **終了** をクリックします。

非ベアメタルサーバーの解決ウィザードの実行

非対応ベアメタルサーバーの解決ウィザードを実行して、非対応ベアメタルサーバーを解決します。対応に関する情報は、「ホストおよびベアメタルの対応問題について」を参照してください。

非対応ベアメタルサーバーの解決ウィザードを実行するには、以下を行います。

1. **Dell Management Center** の左ペインで、**対応 → ベアメタルサーバー**をクリックします。
2. **ベアメタルサーバー**ウィンドウで非対応ホストを表示し、**非対応ベアメタルサーバーの修正**をクリックします。
3. **ベアメタルサーバーの修正**ウィザードで、解決したいホストのチェックボックスを選択します。
4. **次へ** をクリックします。
5. **概要**ウィンドウで、非対応ベアメタルサーバーで行われる操作を確認します。
6. **終了** をクリックします。

ベアメタルサーバー対応性の再確認

OpenManage Integration for VMware vCenter 外で解決したサーバーについては、この手動でのサーバー対応性再確認を実行する必要があります。これは Dell Management Center、対応、ベアメタルサーバーページで見つけることができます。
ベアメタルサーバー対応性を再確認するには、以下を行います。

1. **Dell Management Center → 対応 → ベアメタルサーバー** ページで、**対応の再チェック**をクリックします。
2. **非対応サーバー**ウィンドウで、リストを更新するには、**更新**をクリックします。
3. 再確認を実行するには、**対応のチェック**をクリックします。
4. 再確認を中止するには、**すべてのテストを中止**をクリックします。
5. システムが正しく解決された場合、リストは更新されシステムがリストから取り外されます。そうでない場合は、非対応システムはリストに残ります。
6. 終了したら、**完了**をクリックします。

手動ファームウェアアップデートのための ISO のダウンロード

OpenManage Integration for VMware vCenter は、コンプライアンス問題の大部分を自動的に修正します。場合によっては、手動の ISO インストールが必要となります。必要な ISO をダウンロードし、次の手順でコンプライアンス問題を手動で修正することができます。

1. **Dell Management Center → 対応 → ベアメタルサーバー** ページで、ISO をダウンロードするには、**ISO のダウンロード**をクリックします。
2. **ISO のダウンロード**ダイアログボックスで、ISO のロケーションを見つけるには、**ダウンロード**をクリックします。

   メモ: 外部ブラウザウィンドウがこのアプリケーションウィンドウの背後で開く可能性があります。
3. 対応させる必要があるベアメタルサーバーの ISO ファイルに移動します。
4. ISO を書き込み、この ISO からホストを起動し、ファームウェアのコンポーネントを必要なレベルにアップデートします。

iDRAC ライセンスの対応

iDRAC ライセンス対応のページを選択すると、対応テストが実行されます。このテストには数分かかります。このページに記載されている vSphere ホストおよびベアメタルサーバーは互換性のある iDRAC ライセンスがないため非対応です。テーブルには、iDRAC ライセンスのステータスが表示されます。このページには、ライセンスの残余期間が示されるので、必要に応じてアップデートします。*インベントリジョブの実行*リンクが無効になっている場合、それは、iDRAC ライセンスのために非対応となっている vSphere ホストがないことを示しています。*ベアメタルサーバー対応の再チェック*リンクが無効になっている場合、それは iDRAC ライセンスのために非対応となっているベアメタルサーバーがないことを示しています。

1. **Dell Management Center** の左ペインで、**対応**をクリックします。
2. **対応**を展開して **iDRAC ライセンス**をクリックします。

このページに到着すると、対応テストが実行されます。これは **更新**をクリックしたときに実行されるものと同じテストです。

3. ライセンスが古い場合、**iDRAC ライセンスの購入 / 更新**をクリックします。
4. **Dell ライセンス管理**ページにログインし、新しい iDRAC ライセンスにアップデートまたは購入します。このページの情報を使って、iDRAC を識別およびアップデートします。
5. iDRAC ライセンスのインストール後、vSphere ホスト用にインベントリジョブを実行し、インベントリジョブ完了後このページに戻ります。ベアメタルサーバーに関しては、ライセンスされたベアメタルサーバーの対応性を再確認します。

Upgrading OpenManage Integration for VMware vCenter

The following is the upgrade scenario for the OpenManage Integration for VMware vCenter:

- Upgrading From Trial Version To Full Product Version

NOTE: Perform an appliance backup before you begin the upgrade. See Performing An Immediate Backup.

試用バージョンから完全製品バージョンへのアップグレード

試用バージョンから完全製品バージョンにアップグレードするには、次の手順を実行します。

1. **Dell ウェブサイト** へ移動し、完全製品バージョンを購入します。
   また、**ライセンス** ウィンドウ内の管理ポータルにあるリンクと同様に、**今すぐ購入** リンクを使用して、OpenManage Integration for VMware vCenter の Dell ウェブサイトにアクセスすることもできます。これは、評価用ライセンスを使用している場合にのみ適用されます。
2. ダウンロードには、新しい完全バージョンの製品と新しいライセンスファイルが含まれています。
3. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示される設定したい仮想マシンの **管理コンソール URL** を入力、または **Dell Management Console → 設定** ページからのリンクを使用します。URL は次のフォーマット **https://<ApplianceIPAddress>** を使用し、大文字小文字は区別されません。
4. **管理コンソールログインウィンドウ** で、パスワードを入力し、**ログイン** をクリックします。
5. ライセンスファイルをアップロードするには、**アップロード** をクリックします。
6. **ライセンスのアップロード** ウィンドウで **参照** をクリックし、ライセンスファイルを参照します。
7. ライセンスファイルを選択して、**アップロード** をクリックします。

OpenManage Integration for VMware vCenter ライセンスについて

OpenManage Integration for VMware vCenter には 2 タイプのライセンスがあります。

評価用ライセンス	試用版には、OpenManage Integration for VMware vCenter が管理している 5 つのホスト（サーバー）の評価用ライセンスが含まれます。これは、11G 以降のバージョンにのみ当てはまります。これはデフォルトのライセンスであり、90 日間の試用期間のみ使用できます。
標準ライセンス	完全製品バージョンには、最高 10 の vCenters 標準ライセンスが含まれ、OpenManage Integration for VMware vCenter が管理するホスト接続をいくつでも購入できます。

標準ライセンスから完全な標準ライセンスにアップグレードすると、新しいライセンスの XML ファイルが電子メールで送信されます。ファイルをローカルシステムに保存し、管理コンソールを使って新しいライセンスをアップロードします。ライセンスは、次の情報を示します。

- vCenter 接続ライセンスの最大数 - 最大 10 の登録済みおよび使用中の vCenter 接続が許容されます。
- ホスト接続ライセンスの最大数 - 購入されたホスト接続の数です。
- 使用中 - 使用中の vCenter 接続またはホスト接続ライセンスの数です。ホスト接続では、この数は検出およびインベントリされたホスト（またはサーバー）の数を示します。
- 使用可能 - 将来使用できる vCenter 接続またはホスト接続ライセンスの数です。
- ライセンスのないホスト - ライセンス数を超えたホスト接続の数です。OpenManage Integration for VMware vCenter は引き続き正常に動作しますが、この警告を解決するには、新しいライセンスを購入してインストールする必要があります。

4

エンドツーエンドのハードウェア管理

エンドツーエンドのハードウェア管理の目的は、管理者が Dell Management Center または vCenter を離れずに、重大なハードウェア事象に対応するために必要な、システム正常性ステータスや最新のインフラストラクチャ情報を入手できるようにすることです。OpenManage Integration for VMware vCenter によるエンドツーエンドハードウェア管理は、4 つの部分に分かれています。

- 監視
- インベントリ
- アドバンスホスト管理
- 保証検索

データセンターおよびホストシステムの監視

データセンターおよびホストシステム監視では、vCenter の タスクとイベント タブにハードウェア（サーバーおよびストレージ）と仮想化関連イベントを表示することにより、管理者はインフラストラクチャの正常性を監視することができます。さらに、重要なハードウェアアラームが OpenManage Integration for VMware vCenter をトリガして、ホストシステムをメンテナンスモードにし、場合によっては仮想マシンを他のホストシステムに移行するようにもできます。第 12 世代より前のホストの場合、OpenManage Integration for VMware vCenter は OMSA アラームを転送して、特定イベントのために新しいアラームを生成します。これらのアラームを使用して、再起動、メンテナンスモード、または移行などの vCenter が許容するアクションをトリガすることができます。例えば、デュアル電源装置が故障してアラームが生成されたら、その結果としてそのマシンの仮想マシンを新しいマシンに移行するという結果にすることができます。

監視を実施するには以下を行います。

1. **イベントとアラーム** を設定します。
2. **SNMP OMSA トラップの送信先**を設定します（必要な場合）。
3. vCenter で **タスクとイベント** タブを使用して、イベント情報を確認します。

イベントとアラームの理解

イベントとアラームは、OpenManage Integration for VMware vCenter の **管理 → 設定** タブで編集できます。 ここから、イベント掲載レベルの選択、Dell Hosts に対するアラームの有効化、またはデフォルトアラームの復元を行うことができます。各 vCenter に対してイベントとアラームを設定することも、すべての登録済み vCenters に対して一括で設定することもできます。

メモ: Dell イベントを受信するには、アラームとイベントの両方を有効にする必要があります。

4 つのイベント掲載レベルがあります。

表 1. イベント掲載レベルの説明

イベント	説明
イベントは掲載しない	OpenManage Integration for VMware vCenter がイベントやアラートを関連する vCenters に転送しないようにします。

全イベントを掲載	OpenManage Integration for VMware vCenter が関連する vCenters に管理下の Dell ホストから受信する非公式イベントも含め、すべてのイベントを掲載します。
重要および警告イベントのみ掲載	重要または警告イベントのみを関連 vCenter に掲載します。
仮想化関連の重要および警告イベントのみを掲載	ホストから受信する仮想化関連イベントのみを、関連 vCenter に掲載します。仮想化関連イベントとは、仮想マシンを実行しているホストにとって最も重要であるとデルが選定したものです。

イベントとアラームを設定する際に、それらを有効にすることができます。有効化されると、重要なハードウェアアラームによって OpenManage Integration for VMware vCenter はホストシステムを保守モードにし、場合によって仮想マシンを別のホストシステムに移行します。OpenManage Integration for VMware vCenter は管理下 Dell ホストから受信したイベントを転送し、該当イベントに対するアラームを出します。このアラームを使い、vCenter に対し、再起動、保守モードまたは移行などの措置を起動できます。例えば、デュアル電源が故障しアラームが出された場合、対応措置はそのマシン上の仮想マシンを別のホストに移行します。

ホストはリクエストされた場合のみ、保守モードを起動または終了します。保守モードを起動するホストがクラスタの一部の場合、停止した仮想マシンを退避するオプションを選択できます。このオプションを選択した場合、停止した仮想マシンは、同一クラスタ内に当該仮想マシンとの互換性のあるホストがない場合を除き、それぞれ別のホストに移行されます。保守モードにある限り、ホストは仮想マシンの使用または*起動*を行いません。保守モードとなるホストで実行されている仮想マシンは、手動または VMware Distributed Resource Scheduling (DRS) により自動的に、別のホストに移行するかシャットダウンする必要があります。

クラスタ外のホスト、または VMware Distributed Resource Scheduling (DRS) が起動されていないクラスタにあるホストでは、重要イベントのために仮想マシンはシャットダウンされる可能性があります。DRS は全リソースプールの使用率を連続的に監視し、使用可能なリソースをビジネスニーズにしたがって各仮想マシンに知的に割り当てます。DRS と Dell Alarms が設定されたクラスタを使って、重要なハードウェアイベントの際に仮想マシンが自動的に移行されるようにしてください。画面上のメッセージの詳細に記載されているのは、この vCenter インスタンスにある、影響を受ける可能性のあるクラスタです。イベントと警報を有効化する前に、クラスタが影響を受けるかどうか確認してください。

デフォルトアラーム設定を復元する必要がある場合は、デフォルトアラームにリセットボタンで行います。このボタンは、製品のアンインストールと再インストールを行わずにデフォルトのアラーム設定を行うことができるので便利です。インストール以降に Dell アラーム設定が変更された場合、このボタンで元に戻すことができます。

メモ: OpenManage Integration for VMware vCenter は、ホストが仮想マシンを実行するのに不可欠な仮想化関連イベントを予め選択します。Dell ホストアラームはデフォルトで無効化されています。Dell アラームを有効化する場合、クラスタは VMware Distributed Resource Scheduler を使って、重要イベントが送られる仮想マシンの移行を自動的に行うようにしなければなりません。

Dell PowerEdge 第 11 世代ホスト用 OMSA についての理解

Dell PowerEdge 第 12 世代より前のサーバーでは、OpenManage Integration for VMware vCenter との連動のため、OMSA のインストールが必須です。OMSA は展開中に第 11 世代 Dell PowerEdge ホストに自動でインストールされますが、手動でインストールしたい場合は、それも可能です。

メモ: OMSA エージェントを OpenManage Integration for VMware vCenter を使用して展開すると、httpClient サービスが開始してポート 8080 が有効になり、ESXi 5.0 より後のリリースで OMSA VIB をダウンロードしてインストールします。OMSA のインストールが完了すると、サービスは自動的に停止してポートが閉じます。

OMSA を Dell PowerEdge 第 11 世代サーバーで設定する方法は、次のいずれかを選択します。

- OMSA エージェントを ESXi システムに展開

- OMSA エージェントを ESX システムに展開
- OMSA トラップ先の設定

OMSA エージェントの ESX システムへの展開

OMSA tar.gz を ESX システムにインストールし、システムからインベントリと警告情報を収集します。

メモ: 第 12 世代より前の Dell PowerEdge サーバーの Dell ホストには、OpenManage エージェントが必要です。OpenManage Integration for VMware vCenter を使用して OMSA をインストールするか、OpenManage Integration for VMware vCenter をインストールするより先に手動でホストにインストールします。エージェントの手動インストールの詳細については、**http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx** を参照してください。

OMSA エージェント tar.gz を必要なリモート有効化設定（-c）オプションで ESX システムに展開するには、次の手順を実行します。

1. OMSA エージェントインストレーションスクリプトを実行します。
   ```
   sh srvadmin-install.sh -x
   ```
2. OMSA サービスを起動します。
   ```
   srvadmin-services.sh start
   ```
3. OMSA エージェントがすでにインストールされている場合、リモート有効化設定（-c）オプションが行われているか確認してください。設定されていない場合は、OpenManage Integration for VMware vCenter のインストレーションは正しく完了しません。-c オプションで再インストールしてサービスを再起動します。
   ```
   srvadmin-install.sh -c srvadmin-services.sh restart
   ```

OMSA エージェントの ESXi システムへの展開

OMSA VIB を ESXi システムにインストールし、システムのインベントリおよび警告情報を収集します。

メモ: 第 12 世代より前の Dell PowerEdge サーバーの Dell ホストには、OpenManage エージェントが必要です。OpenManage Integration for VMware vCenter を使用して OMSA をインストールするか、OpenManage Integration for VMware vCenter をインストールするより先に手動でホストにインストールします。エージェントの手動インストールの詳細については、**http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx** を参照してください。

1. まだインストールされていない場合は、vSphere コマンドラインツール（vSphere CLI）を **http://www.vmware.com** からインストールします。
2. 次のコマンドを入力します。
   ```
   Vihostupdate.pl -server <IP Address of ESXi host> -i -b OM-SrvAdmin-Dell-Web-6.3.0-2075.VIB-ESX41i_A00.8.zip
   ```
   メモ: OMSA のインストールには数分かかることがあります。このコマンドの完了後、ホストを再起動する必要があります。

OMSA トラップ先の設定

すべての第 11 世代 のホストには OMSA が設定されている必要があります。

メモ: OMSA は Dell PowerEdge 第 12 世代サーバーより前の Dell サーバーにのみ必要です。

OMSA トラップ先を設定するには、以下を行います。

1. **設定 → 一般** にある OMSA ユーザーインタフェースへのリンクを使用するか、またはウェブブラウザ（**https://<HostIP>:1311/**）から OMSA エージェントに移動します。
2. インタフェースにログインして、**アラート管理** タブを選択します。

3. **アラート処置** を選択し、監視対象イベントに **ブロードキャストメッセージ** オプションが設定されており、イベントが送出されることを確認します。
4. タブの上部にある、**プラットフォームイベント** オプションを選択します。
5. グレーの **宛先の設定** ボタンをクリックし、次に **宛先** リンクをクリックします。
6. **トラップ先を有効にする** チェックボックスを選択します。
7. OpenManage Integration for VMware vCenter アプライアンスの IP アドレスを **送信先 IP アドレス** フィールドに入力します。
8. **変更の適用** をクリックします。
9. さらなるイベントの設定には、手順 1～8 を繰り返します。

イベントの表示

イベントを表示するには、以下のいずれかを行います。

- 仮想マシンへ移動し、右クリックして **vCenter → vCenter のタスクとイベント** タブを表示し、**イベント** をクリックして選択したイベントレベルを表示します。
- ホストまたは vCenter のルートフォルダの親ノード（クラスタまたはデータセンター）をクリックします。

イベントは、vSphere ツリーのノードのみに表示されます。

vSphere クライアントホストの概要

この概要では、個別コンポーネントの正常性、識別、ハイパーバイザー、およびファームウェア情報などの主なホストサーバー属性に関する情報が提供されます。

ハードウェアコンポーネントの正常性

コンポーネントの正常性は、システムシャーシ、電源装置、温度、ファン、電圧、プロセッサ、バッテリ、イントルージョン、ハードウェアログ、電力管理およびメモリなど、すべての主要ホストサーバーコンポーネントに関するグラフ表示です。表示可能なステータスには以下があります。

- 正常（緑色のチェックマーク） - コンポーネントは通常通りに動作中
- 警告（黄色の三角に感嘆符） - コンポーネントには重大でない不具合があります
- 重要（赤い X 印） - コンポーネントには重大な障害があります
- 不明（疑問符） - コンポーネントステータスは不明

グローバルの正常性ステータスはヘッダーバーの右上に表示されます。

サーバー情報

サーバー情報では、以下のような識別、ハイパーバイザー、およびファームウェア情報が提供されます。

- ホスト名、電源状態、iDRAC IP、管理 IP、使用中の接続プロファイル、モデル、サービスタグおよび資産タグ番号、保証残り期間、最後のインベントリスキャン実行日。
- ハイパーバイザー、BIOS ファームウェア、および iDRAC ファームウェアバージョン。
- 10 個の最新システムイベントログ項目。詳細をクリックして、さらなるログ詳細を表示するシステムイベントログウィンドウを起動します。

ホスト情報

ホスト概要の左ペインに、以下のようなホスト情報へのリンクが提供されます。

- システムイベントログ
  ハードウェアシステムイベントログ情報を表示します。「システムイベントログの理解」を参照してください。
- ハードウェアインベントリ

以下のハードウェアデバイスについて情報を表示します。

- DIMM、システムプラナー、電源装置、バックプレーン、コントローラカードなどのフィールド交換可能装置（FRU）
- メモリ - 使用可能および使用中のスロット数、最大容量および使用中のメモリ量、および個別 DIMM の詳細。
- ネットワークインタフェースカード（NIC） - インストールされているカード数および個別 NIC の詳細。
- PCI スロット - 全スロット数および使用スロット数ならびに個別スロットに関する詳細。
- 電源装置 - 総数および個別 PSU の詳細。
- プロセッサ - 総数および個別 CPU の詳細。
- リモートアクセスカード - IP アドレス情報と RAC タイプ、およびウェブインタフェース URL。

「インベントリジョブについて」を参照してください。

- ストレージ
  ホストシステムストレージは、ホストベースのストレージコントローラに接続されている、物理および論理ストレージの容量およびタイプのグラフおよび詳細表示を提供しています。それには以下が含まれます。
  - ホストシステムの合計ストレージ容量、設定済み、未設定、グローバルおよび専用ホットスペア両方のディスク容量
  - 当該コンポーネントに関する詳細情報を含む、システムコンポーネントデータテーブルに存在している各ストレージコンポーネント数のリスト
- ファームウェア
  ファームウェアアップデートウィザードを実行、またはファームウェアステータスを表示します。「ファームウェアのアップデート」を参照してください。
- 電源監視
  ホストシステム電源監視は、一般的な電源情報、エネルギー統計情報、および予備電源情報を提供します。これには以下が含まれます。
  - 現在の電力バジェット、プロファイル、警告および故障のしきい値
  - エネルギー消費量、システムピーク電力およびアンペア数統計情報
  - 予備電源およびピーク予備容量

    メモ: すべての電源装置はこの機能を備えておらず、ブレードエンクロージャの電源装置には対応していません。
- 保証
  保証の取得は、Dell サーバーについて以下の情報を提供します。
  - アップデートされたサービス保証情報、ただしホストサービスタグのみを送信
  - 定期的にアップデートされた保証情報
  - プロキシサーバーおよび資格情報を使ったセキュアな送信
  - 検証されたセキュアな接続による情報

「保証の取得」を参照してください。

ホストアクション

ホストアクションは、以下のような現在のホストサーバーに実行されたコマンドです。

- インジケータライトを点滅を使用して、LCD 前面インジケータを点滅させます。「物理サーバー前面インジケータライトの設定」を参照してください。
- ファームウェアアップデートウィザードの実行を使用して、ファームウェアアップデートウィザードを表示し、ホストサーバーファームウェアをアップデートします。「ファームウェアアップデートウィザードの実行」を参照してください。

- iDRAC リセットを使用して、アプライアンスを再起動することなく iDRAC をリセットします。「iDRAC のリセット」を参照してください。

管理コンソール

管理コンソールを使って以下のような外部システム管理コンソールを起動します。

- リモートアクセスコンソールをクリックして、Integrated Dell Remote Access Controller（iDRAC）ウェブユーザーインタフェースを起動します。
- 設定されている場合、OMSA コンソールをクリックして、OpenManage Server Administrator（OMSA）ユーザーインタフェースを起動します。 OMSA リンクの有効化を参照してください。
- ブレードシャーシコンソールをクリックして、Chassis Management Controller（CMC）ウェブユーザーインタフェースを起動します。

Dell オンラインサービス

Dell オンラインサービスは、ホストシステムの保証を更新するためのアクセスを提供します。

- 保証の更新をクリックして、ホストシステムの保証を更新するために使用されるポータルを起動します。サーバー情報で残存保証期間の確認ステータスを確認し、保証の更新が必要か判断します。保証期限が近くなると警告または重大アイコンが表示されます。「ホスト保証の更新」を参照してください。

iDRAC のリセット

iDRAC は時折要求に応答しなくなることがあり、その結果 OpenManage Integration for VMware vCenter 内で予期しない動作が生じます。この状態から回復する唯一の方法は iDRAC をリセットすることです。iDRAC リセットは iDRAC の正常再起動を行います。この再起動ではホストは再起動されません。リセット実行後は、iDRAC が使用可能状態に戻るまで 1～2 分かかります。

iDRAC の再起動中、次の状況が生じる場合があります。

- OpenManage Integration for VMware vCenter が正常性ステータスを取得する間に遅延または通信エラーが発生する。
- iDRAC とのオープンセッションがすべて閉じられる。
- iDRAC 用の DHCP アドレスが変更される。iDRAC が IP アドレスに DHCP を使用する場合、IP アドレスが変更される可能性があります。これが発生した場合、ホストインベントリジョブを再実行して、インベントリデータ内の新規 iDRAC IP を取得します。

メモ: iDRAC のソフトリセットでは iDRAC を元の再利用可能な状態に戻せない場合があります。ハードリセットが必要な場合があります。ハードリセットを実行するには、サーバーでサーバーの電源を切り、電源ケーブルを取り外し、2 分待ってからケーブルを接続してみてください。iDRAC のリセットの詳細に関しては、お使いのバージョンの iDRAC ユーザーズガイドを参照してください。

メモ: Dell では、iDRAC をリセットする前にホストをメンテナンスモードにすることを推奨します。

1. **インベントリ** の見出しの下の **vSphere クライアント** で、**ホストとクラスタ** を選択します。
2. **ホストとクラスタ** からツリービューのホストシステムを選択し、**OpenManage Integration** タブを選択します。
3. **ホストアクション** で、**iDRAC リセット** を選択します。
4. iDRAC リセットダイアログボックスで、**iDRAC リセットを続行** を選択し、**OK** をクリックします。

インベントリスケジュールについて

インベントリスケジュールは、以下のようにインベントリジョブを実行する時刻 / 日付を設定します。

- 毎週の特定の時刻と曜日
- 一定の期間ごと

OpenManage Integration for VMware vCenter 機能のほとんどでは、必要データを収集するためにまずインベントリを完了する必要があります。この情報を表示するには、全ホストシステムのイベントリが収集される必要があります。ホストシステムでインベントリを行うには、通信および認証情報を提供する接続プロファイルを作成してください。インベントリが完了したら、データセンター全体、または個々のホストシステムのためのインベントリ結果を表示することができます。

メモ: インベントリに最新情報が含まれていることを確実にするため、インベントリジョブは最低 1 週間に 1 度行われるようスケジュールしてください。インベントリジョブは最低限のリソースしか消費せず、ホスト性能が劣化することはありません。

関連タスク:

- インベントリジョブの実行
- インベントリジョブスケジュールの変更
- シングルホストシステムのインベントリの表示
- データセンターハードウェア設定およびステータスの表示

インベントリジョブスケジュールの変更

インベントリスケジュールは、次のようにインベントリジョブを実行する日付と時刻を設定します。

- 毎週特定の曜日の特定の時刻などが設定できます。
- OpenManage Integration for VMware vCenter 機能の大部分で必要とされるデータを収集するため、一定間隔でインベントリを実施する必要があります。

メモ: インベントリに最新情報が含まれるようにするためには、最低 1 週間に 1 度はインベントリジョブを実行するようにします。インベントリジョブは最小限のリソースしか消費しないので、ホストパフォーマンスを低下させません。

インベントリジョブスケジュールを変更するには、以下を行います。

1. Dell Management Center で **設定 → インベントリのスケジュール**を選択します。
2. 現在のスケジュールを変更するには、**編集**をクリックします。
3. **選択した曜日**オプションボタンを選択し、次に曜日のチェックボックスを選択して、時刻を入力します。入力情報を消去するには、**クリア**をクリックします。
4. インベントリスケジュールを変更するには、**適用**をクリックします。あるいは、インベントリスケジュールを取り消すには、**キャンセル**をクリックします。
5. ジョブを今すぐ実行するには、管理センターで **ジョブキュー**と **インベントリ履歴**タブを選択します。
6. **今すぐ実行**をクリックします。
7. **前回のインベントリジョブの詳細**をアップデートするには、**更新**をクリックします。

vCenter におけるシングルホストシステムのインベントリ表示

シングルホストシステムのインベントリを表示するには、以下を行います。

1. **vSphere クライアント** から、**インベントリ**の見出しの下で **ホストとクラスタ**を選択します。
2. **ホストとクラスタ** から、左ペインでホストシステムを選択し、次に **OpenManage Integration** タブを選択します。
3. 選択されたホストの概要が表示されます。
   概要には、個別コンポーネントの正常性、識別情報、ハイパーバイザー、およびファームウェア情報を含む、主なホストサーバー属性が提供されます。

– ハードウェアコンポーネントの正常性は、すべての主なホストサーバーコンポーネントのステータスのグラフ表示です。それには、システムシャーシ、電源装置、温度、ファン、電圧、プロセッサ、バッテリ、イントルージョン、ハードウェアログ、電源管理、およびメモリが含まれます。以下のような利用可能なステータスがあります。

  * 正常（緑色のチェックマーク） - コンポーネントは通常通りに動作中
  * 警告（黄色の三角に感嘆符） - コンポーネントには重大でない不具合があります
  * 重要（赤い X 印） - コンポーネントには重大な障害があります
  * 不明（疑問符） - コンポーネントステータスは不明

  グローバルの正常性ステータスはヘッダーバーの右上に表示されます。

– サーバー情報は、次のような識別情報、ハイパーバイザー、およびファームウェア情報を提供します。

  * ホスト名、電源状況、iDRAC IP アドレス、管理 IP アドレス、使用中の接続プロファイル、モデル、サービスタグと資産タグ番号、保証残余期間、最後のインベントリスキャン実行日。
  * ハイパーバイザー、BIOS ファームウェア、および iDRAC ファームウェアバージョン
  * 耐障害性メモリ（FRM）：これは BIOS 属性で、サーバーの初回セットアップ中に BIOS で有効にされ、サーバーのメモリ操作モードを表示します。メモリ操作モード値を変更する際はシステムを再起動する必要があります。これは、R620、R720、T620、M620 サーバーの ESXi 5.5 バージョン以降に当てはまります。次の 4 つの値があります:

    • 有効かつ保護状態：この値は、システムがサポートされており、オペレーティングシステムのバージョンが ESXi 5.5 以降であり、BIOS のメモリ操作モードが FRM に設定されていることを示します。

    • 有効かつ非保護状態：この値は、メモリ動作モードが BIOS で FRM に設定されているものの、オペレーティングシステムはこの機能に対応していないことを示します。

    • 無効：この値はどのオペレーティングシステムのバージョンのシステムでもサポートし、ここでは BIOS のメモリ操作モードは FRM に設定されていないことを示します。

    • ブランク：BIOS のメモリ操作モードがサポートされていない場合、FRM 属性が表示されません。

– 最新システムログには、最新 10 個のシステムイベントログ項目が提供されます。**システムイベントログ**ウィンドウを起動して、さらなるログ詳細を表示するには、**詳細**をクリックします。

4. **ホスト情報**で、**ハードウェアインベントリ**をクリックして、次のようなホストシステムにインストールされているすべてのコンポーネントのリストと、さらなる詳細を表示します。

   – フィールド交換可能装置（FRU） - DIMMS、システムプラナー、電源装置、バックプレーン、コントローラカード等。
   – メモリ - 使用可能および使用中のスロット数、最大容量および使用中のメモリ量、および個別 DIMM の詳細。
   – ネットワークインタフェースカード（NIC） - インストールされているカード数および個別 NIC の詳細。
   – PCI スロット - 使用可能および使用中のスロット数、および個別スロットの詳細。
   – 電源装置 - 総数および個別 PSU の詳細。
   – プロセッサ - 総数および個別 CPU の詳細。
   – リモートアクセスカード - IP アドレス情報、RAC タイプ、およびウェブインタフェース URL。

5. **ホスト情報**で **ストレージ**をクリックして、次のような物理および仮想ストレージの容量とタイプのグラフおよび詳細ビューを表示します。

   – ホストシステムの合計ストレージ容量、設定済み、未設定およびグローバルホットスペアのディスク容量。
   – システムにインストールされている各ストレージコンポーネント数のリスト。
   – 当該コンポーネントに関する詳細情報を含むコンポーネントデータテーブル。

6. **ホスト情報**で、**ファームウェア**をクリックして、以下を含むすべての Dell Lifecycle Controller ファームウェア情報を表示します。
   - アップデート名 - BIOS、Dell Lifecycle Controller、電源装置等。
   - アップデートタイプ - BIOS、ファームウェアまたはアプリケーション。
   - 個別アップデート詳細 - アップデートが進行中の場合、バージョン、インストール時刻、またはアップデートステータスおよびアップデートバージョン。アップデートステータスとバージョンには、アップデートがスケジュールされている場合にのみデータが含まれ、アップデートバージョンは、システムが今後アップデートされるファームウェアバージョンです。
7. **ホスト情報**で、**電源監視**をクリックし、次のような一般電源情報、エネルギー統計情報、および予備電源情報を表示します。
   - 現在の電力バジェット、プロファイル、警告および障害しきい値。
   - エネルギー消費量、システムピーク電力、およびアンペア数統計情報。
   - 予備電源およびピーク予備容量。
8. **ホスト情報**で **保証**をクリックして、次のようなシステム保証情報を表示します。
   - 保証プロバイダ名および保証の説明。
   - 保証の開始および終了日ならびに残余期間。
   - 保証ステータス（有効、無効）および最新保証情報アップデート日。

インベントリおよびライセンス

サーバーデータの検索と表示ができない場合、いくつかの原因が考えられます。

- サーバーが接続プロファイルによって関連付けられておらず、インベントリタスクが完了できませんでした。
- データを収集するインベントリタスクがサーバーで実行されなかったので、表示できるデータがありません。
- ホストライセンス数が超過しており、インベントリタスクを完了するにはさらなるライセンスが必要です。
- このサーバーには、第 12 世代サーバーに必要な正しい iDRAC ライセンスがないので、正しい iDRAC ライセンスを購入する必要があります。

今すぐ購入 のリンクは、初めて製品を購入するためのものであり、アップグレードのためではなりません。今すぐ購入 のリンクは評価用ライセンスを使用している場合にのみ表示されます。

関連タスク:

- 既存接続プロファイルの表示および編集
- インベントリジョブスケジュールの変更

OpenManage Integration for VMware vCenter には 2 タイプのライセンスがあります。

- 評価用ライセンス: OpenManage Integration for VMware vCenter が管理している 5 つのホスト（サーバー）の評価用ライセンスが含まれます。
- 標準ライセンス: 完全な製品バージョンには、OpenManage Integration for VMware vCenter によって管理される 10 の vCenter および購入したホスト接続数のライセンスが含まれます。

関連タスク:

- OpenManage Integration for VMware vCenter ライセンスについて
- OpenManage Integration for VMware vCenter ライセンスを管理コンソールにアップロードする

メモ: 標準ライセンス期間は 3 年間のみであり、追加したライセンスは既存ライセンスに付加され、上書きはされません。

ストレージインベントリの表示

ホストシステムストレージは、ホストベースのストレージコントローラに接続されている、物理および論理ストレージの容量およびタイプのグラフおよび詳細表示を提供しています。それには以下が含まれます。

- ホストシステムの合計ストレージ容量、設定済み、未設定、グローバルおよび専用ホットスペア両方のディスク容量
- システムにある各ストレージコンポーネント数のリスト
- 当該コンポーネントに関する詳細情報を含む、コンポーネントデータテーブル

ストレージデータの表示には以下を行います。

1. **vSphere クライアント**で、ホストを選択し、次に **OpenManage Integration タブ** を選択します。
2. **ホストの概要**ページの左ペインで、**ストレージ**をクリックします。
3. **ストレージ**ページでグラフ概要を表示するか、テーブルと **表示**および **フィルタ** ドロップダウンリストを使ってインベントリ情報を並べ替えます。

ホスト電源監視の表示

ホストシステム電源監視は、一般的な電源情報、エネルギー統計情報、および予備電源情報を提供します。これには以下が含まれます。

- 現在の電力バジェット、プロファイル、警告および故障のしきい値
- エネルギー消費量、システムピーク電力およびアンペア数統計情報
- 予備電源およびピーク予備容量

ホスト電源監視を表示するには、次を実行します。

1. **vSphere クライアント**でホストを選択し、次に **Dell Server Management** タブを選択します。
2. **ホスト情報**の左ペインで **電源監視**をクリックします。
3. **電源監視**ページで、このホスト用の電源を表示します。

全データセンターハードウェアの設定およびステータスの表示

全データセンターハードウェアの設定およびステータスを表示する前に、インベントリジョブを完了する必要があります。インベントリを実行したら、以下のいずれも表示することができます。

- ハードウェア: フィールド交換可能パーツ
- ハードウェア: プロセッサ
- ハードウェア: 電源装置
- ハードウェア: メモリ
- ハードウェア: NIC
- ハードウェア: PCI スロット
- ハードウェア: リモートアクセスカード
- ストレージ: 物理ディスク
- ストレージ: 仮想ディスク
- ファームウェア
- 電源監視

- 保証

全データセンターハードウェアの設定およびステータスを表示するには、以下を行います。

1. **vSphere クライアント** の **インベントリ** 下で **ホストとクラスタ** を選択します。
2. **ホストとクラスタ** でツリービューからデータセンターを選択し、**OpenManage Integration** タブを選択します。
3. データセンター内の全ホストの概要が表示されます。**表示** ドロップダウンリストを使用してインベントリカテゴリを表示します。
4. **フィルタ** テキストボックスを使ってインベントリデータのフィルタを入力します。
5. 表示されたインベントリを更新するには、**更新** をクリックします。
6. **ダウンロードの場所** ウィンドウでインベントリを保存するロケーションを参照し、**保存** をクリックします。

接続プロファイルの管理

接続プロファイルは、アクセスおよび導入資格情報を一連のホストシステムに関連付け、通常以下を含みます。

- プロファイル名および固有の説明（プロファイル管理を容易にするため）
- 接続プロファイルに関連付けられたホストのリスト
- iDRAC 資格情報
- ホストの資格情報
- 作成日
- 変更日

設定ウィザードの実行後、OpenManage Integration for VMware vCenter の **管理タブ → テンプレートとプロファイル** から、次の機能を使用して資格情報のプロファイルを管理します。

- 新しい接続プロファイルの作成
- 既存接続プロファイルの表示および編集
- 接続プロファイルの削除
- 接続プロファイルのテスト
- 接続プロファイルの更新

接続プロファイルの編集

接続プロファイルの設定後、プロファイル名、説明、関連ホスト、および資格情報を編集できます。

メモ: この手順中に表示される vCenter は、同じシングルサインオン（SSO）で認証されています。vCenter のホストが見えない場合、別の SSO にあるか、バージョン 5.1 以前の VMware vCenter を使用しているためと考えられます。

メモ: ライセンスによる制限に関係なく、接続プロファイルを編集することができます。

1. OpenManage Integration for VMware vCenter の **管理 → 接続プロファイル** タブで、接続プロファイルを選択します。
2. **編集** アイコンをクリックします。
3. ようこそ タブの接続プロファイルウィンドウで情報を読み、**次へ** をクリックします。
4. 名前と資格情報 タブで、次の手順を行います。
   a) プロファイルの下で **プロファイル名** とオプションで **説明** をタイプします。

b) vCenter の下で、この接続プロファイルの関連ホストを確認します。ここに表示されるホストが見える理由については、上記の注記を参照してください。

c) iDRAC 資格情報で、次の手順を行います。

* ユーザー名は root で、**Active Directory** を選択しない場合、このエントリは変更できません。**Active Directory** が設定されている場合は、root のみに限らずすべての Active Directory のユーザーを選択することができます。
* Domain\Username：ユーザー名を、ドメイン\ユーザー名、または ドメイン@ユーザー名、のいずれかの形式でタイプします。

  メモ: 次の文字、/（スラッシュ）、&、\（バックスラッシュ）、.（ピリオド）、"（引用符）、@、%（パーセント）を、ユーザー名に使用することができます（最大 127 文字）。

  ドメインには英数字および -（ダッシュ）、.（ピリオド）のみを使用できます（最大 254 文字）。ドメインの最初と最後の文字は必ず英数字にしてください。
* パスワード：自分のパスワードをタイプします。

  次の文字、/（スラッシュ）、&、\（バックスラッシュ）、.（ピリオド）、"（引用符）、は、パスワードに使用することはできません。
* パスワード確認： 自分のパスワードを再度タイプします。
* 証明書のチェックを有効にする：デフォルトで、チェックボックスにチェックは入っていません。iDRAC 証明書をダウンロードして保存し、将来のすべての接続中に検証するよう、**証明書のチェックを有効にする** を選択するか、**証明書のチェックを有効にする** チェックボックスをクリアして証明書のチェックを実行せず証明書を保存しないようにします。

  メモ: Active Directory を使用する場合は、**有効にする**を選択する必要があります。

d) ホストルートで、次の手順を実行します。

* **Active Directory を使用する** チェックボックスを選択して、アクティブディレクトリに関連付けられたすべてのコンソールにアクセスします。

  ユーザー名：デフォルトのユーザー名は **root** で、変更できません。Active Directory を使用する を選択している場合、任意の Actifve Directory ユーザー名を使用できます。
* パスワード：自分のパスワードをタイプします。

  次の文字、/（スラッシュ）、&、\（バックスラッシュ）、.（ピリオド）、"（引用符）、は、パスワードに使用することはできません。
* パスワード確認： 自分のパスワードを再度タイプします。
* 証明書のチェックを有効にする：デフォルトで、チェックボックスにチェックは入っていません。iDRAC 証明書をダウンロードして保存し、将来のすべての接続中に検証するよう、**証明書のチェックを有効にする** を選択するか、**証明書のチェックを有効にする** チェックボックスをクリアして証明書のチェックを実行せず証明書を保存しないようにします。

  メモ: Active Directory を使用する場合は、**有効にする**を選択する必要があります。

メモ: OMSA の資格情報は、ESX および ESXi ホストに使われる資格情報と同じです。

メモ: iDRAC Express または Enterprise カードがないサーバーでは、iDRAC テスト接続結果は、*このシステムには該当しません*が表示されます。

5. **次へ** をクリックします。
6. ホストの選択 ダイアログボックスで、この接続プロファイルのホストを選択します。
7. **OK** をクリックします。
8. 関連ホスト タブで、選択したサーバー上の iDRAC とホストの資格情報をテストできます。次の手順で行います。

– テストを開始するには、チェックを行うホストを選択し、**テスト接続** アイコンをクリックします。その他のオプションは非アクティブです。

テストが完了したら、**完了** をクリックします。

– テストを停止させるには **すべてのテストを中止** をクリックします。テストを中止 ダイアログボックスで **OK** をクリックし、**完了** をクリックします。

接続プロファイルの削除

1. OpenManage Integration for VMware vCenter の **管理 → 接続プロファイル** タブで、削除するプロファイルを選択します。
2. **削除** アイコンをクリックします。
3. 削除の確認 メッセージで、プロファイルを削除する場合は **はい**、削除処置をキャンセルする場合は **いいえ** をクリックします。

接続プロファイルのテスト

1. Dell Management Center の **管理 → 接続プロファイル** タブで、テストする接続プロファイルを選択します。
2. 接続プロファイルのテスト ダイアログで、テストするホストを選択し、**テスト接続** アイコンをクリックします。
3. 選択したすべてのテストを中止してテストをキャンセルするには、**テスト接続の中止** をクリックします。テストを中止 ダイアログボックスで **OK** をクリックします。
4. 終了するには、**キャンセル**をクリックします。

接続プロファイルの更新

OpenManage Integration for VMware vCenter の **管理 → 接続プロファイル** タブで、VMware vSphere Web Client 内のタイトルバー上の **更新** アイコンをクリックします。

メモ: ホストを vCenter から取り外した後、接続プロファイルのページに移動すると、ホストを接続プロファイルから削除するように指示されます。削除を確定すると、ホストが接続プロファイルから削除されます。

vSphere クライアントのホストビューにおけるシステムイベントログの理解

システムイベントログは、OpenManage Integration for VMware vCenter により検出されたハードウェアのステータス情報を提供します。

システムイベントログは、以下の基準に基づいて情報を提供します。

ステータス - 情報	いくつかのステータスアイコンがあります。情報（青色の感嘆符）、警告（黄色の三角に感嘆符）、エラー（赤色の X 印）。
時刻：サーバー時刻	イベント発生時の時刻と日付を示します
このページを検索	特定のメッセージ、サーバー名、設定、その他を表示します。

重要度は次のように定義されます。

情報：	OpenManage Integration for VMware vCenter 操作は正常に完了しました。
警告：	OpenManage Integration for VMware vCenter 操作の一部が正常に完了しておらず、部分的に成功したのみです。

エラー： OpenManage Integration for VMware vCenter 操作に失敗しました。

セキュリティ システムセキュリティに関する情報が含まれます。

ログは、外部 CSV ファイルとして保存できます。

関連情報

- 個別ホストに対するシステムイベントログの表示

Dell Management Center におけるログ表示

Dell Management Center ログには、検出されたハードウェアのステータス情報やユーザー操作履歴が含まれます。

Dell Management Center におけるログを表示するには、以下を行います。

1. **Dell Management Center** の左ペインで、**ログ**を選択します。
2. ログを最新データでアップデートするには、**更新**をクリックします。
3. ログデータのフィルタリングのために重要度カテゴリを選択するには、**すべてのカテゴリ**ドロップダウンリストで、すべてのカテゴリ、情報、警告、エラー、またはセキュリティの中から 1 つを選択します。
4. ログデータのフィルタとして日付範囲を選択するには、**先週**ドロップダウンリストをクリックして、先週、先月、昨年またはカスタム範囲から 1 つを選択します。
   カスタム範囲を選択した場合は、**開始日**および **終了日**のドロップダウンリストが表示されます。
5. カスタム日付範囲を選択した場合、以下を行います。
   a) **開始日**を入力するため、カレンダーをクリックします。
   b) **終了日**を入力するため、カレンダーをクリックします。
   c) 設定を保存するには、**適用**をクリックします。
6. ログの表示方法を制御するには、表示コントロールを使って、**画面ごとの記録**を設定し、必要な **ページ**に行き、前へおよび次へのページ制御を使います。
7. ログコンテンツをカンマで区切られた（CSV）ファイルにエクスポートするには、**エクスポート**をクリックします。
8. ダウンロードロケーションウィンドウで、ログを保存するロケーションを表示して、**保存**をクリックします。

個別ホストのイベントログの表示

システムハードウェアイベントログは、以下の基準に基づく情報を提供します。

- ステータス - 情報
  いくつかのステータスアイコンがあります。情報（青色の感嘆符）、警告（黄色の三角に感嘆符）、エラー（赤色の X 印）。
- 時刻：サーバー時刻
  イベント発生時の日時を表示します。
- このページを検索
  特定のメッセージ、サーバー名、設定、その他を表示します。

個別ホストのシステムイベントログを表示するには、以下を行います。

1. **vSphere クライアント**の、**インベントリ**の見出し下で **ホストとクラスタ**を選択します。
2. ツリービューで、ホストシステムを選択します。
3. **OpenManage Integration** タブを選択します。
4. **最近のシステムログ項目**で、**システムイベントログ**ウィンドウを起動するには、**詳細**をクリックします。

5. **システムイベントログ**をアップデートするには、**ログの更新**をクリックします。
6. イベントログ項目数を制限（フィルタ）するには、以下のいずれかを選択します。
   - 検索フィルタテキストボックスに、動的にログ項目をフィルタするテキスト文字列を入力します。
   - フィルタテキストボックスを消去するには、**X** をクリックするとすべてのイベントログ項目が表示されます。
7. すべてのイベントログ項目を消去するには、**ログのクリア**をクリックします。すべてのログ項目は消去後削除されるとのメッセージが表示されます。次のいずれかを選択します。
   - ログの消去に同意する場合は、**OK** をクリックします。
   - 取り消すには、**キャンセル**をクリックします。
8. イベントログを CSV ファイルにエクスポートするには、**エクスポート**をクリックします。
9. システムイベントログを保存するロケーションを表示して、**保存**をクリックします。

ファームウェアアップデートについて

サーバーがファームウェアアップデートを受けるロケーションは、Dell Management Center で使用できるグローバル設定です。ファームウェアリポジトリは Dell Management Center で設定できますが、アップデートは vSphere クライアントにおける特定の Dell ホストタブで実行されます。

ファームウェアリポジトリ設定には、展開されたサーバーをアップデートするのに使用される、ファームウェアカタログロケーションが含まれています。ロケーションタイプには 2 種類あります。

Dell（ftp.dell.com）	Dell（**ftp.dell.com**）のファームウェアアップデートリポジトリを使用します。OpenManage Integration for VMware vCenter が、選択されたファームウェアアップデートをデルからダウンロードします。
ローカル / 共有リポジトリ	Dell Repository Manager™ によって作成されます。これらのローカルリポジトリは、CIFS または NFS ファイル共有にあります。

メモ: リポジトリが作成されたら、登録されたホストがアクセスできるロケーションに保存します。リポジトリのパスワードは 31 文字を超えることはできません。パスワードには、@、&、%、'、"、,（カンマ）、<> の文字は使用できません。

ファームウェアアップデートウィザードは常に、iDRAC、BIOS、および Lifecycle Controller の最低ファームウェアレベルをチェックし、最低必須のバージョンにアップデートすることを試みます。iDRAC、Lifecycle、および BIOS ファームウェアバージョンが最低要件を満たすと、ファームウェアアップデートウィザードが、iDRAC、Lifecycle Controller、RAID、NIC/LOM、電源装置、BIOS などを含むすべてのファームウェアのアップデートを行います。

メモ: 第 9 および第 10 世代のサーバーにおいては、BIOS/BMC/DRAC ファームウェアバージョンは vCenter のクラスタビューレベル、または個別ホストビューの概要ページでのみ表示することができます。ファームウェアバージョン情報は、ファームウェア下の個別ホストビューでアクティブになっておらず、そのページはグレーアウト表示されます。リモートファームウェアアップデートは利用できません。

2010 年 10 月 14 日以降のファームウェアバージョン

2010 年 10 月 14 日以降にアップデートされたファームウェアについては、ファームウェアアップデートウィザードが実行されます。

2009 年 7 月 29 日以降で 10 月 14 日より前のファームウェアバージョン

ファームウェアが 2009 年 7 月 29 日以降、2010 年 10 月 14 日の前日までにアップデートされている場合、ファームウェアアップデートウィザードはまだ使用できませんが、ファームウェアをアップデートするための ISO バンドルが付属しています。このアップデート後、最新ファームウェアにならない可能性があります。バンドルの実行後に再度アップデートを実行することを推奨します。

2009 年 7 月 29 日より古いファームウェアバージョン

ファームウェアが 2009 年 7 月 29 日より古い場合、ISO ファイルをダウンロードして実行し、マシンのアップデートを行わなければならない可能性があります。ISO の実行後、ファームウェアアップデートウィザードを実行することを推奨します。

関連情報

- ファームウェアリポジトリおよび資格情報の設定
- ファームウェアアップデートウィザードの実行
- 古いファームウェアバージョンのアップデート
- クラスタおよびデータセンターのためのファームウェアアップデートウィザードの実行

ファームウェアアップデートウィザードの実行

この機能が使用できるのは、iDRAC Express または Enterprise カードが装備された第 11 および 12 世代の Dell サーバーのみです。お使いのファームウェアが 2010 年 10 月 14 日以降にインストールされた場合、ファームウェアアップデートウィザードを使用してファームウェアバージョンを自動的にアップデートすることができます。

メモ: ブラウザのタイムアウト問題を避けるため、デフォルトタイムアウトを 30 秒に変更します。デフォルトタイムアウト設定の変更についての情報は、『*User's Guide*』（ユーザーズガイド）の「How Come I see an Error Message Displayed After Clicking the Firmware Update Link」（ファームウェアアップデートリンクをクリックした後にエラーメッセージが表示される理由）の項を参照してください。

メモ: 試用/評価用ライセンスについて、ライセンスの有効期限が残っている限り、ファームウェアウィザードを使用できます。

ファームウェアアップデートウィザードを実行するには、次の手順を行います。

1. **vSphere クライアント → OpenManage Integration タブ → ホスト情報** で、**ファームウェア → ファームウェアアップデートの実行** とクリックします。
2. **ファイルから単一のファームウェアアップデートをロード** オプションを使用するには、次の手順を行います。
   a) 次の形式でファイルパスを入力します。
   ```
   CIFS: \\<host accessible share path>\<FileName>.exe or NFS: host:/share/filename.exe
   ```
   b) NFS がある場合、手順 7 に進んでください。それ以外の場合は **ユーザー名** および **パスワード** を、共有ドライブにアクセスできるドメイン形式で入力します。
   c) 手順 7 に進みます。

   このオプションのかわりに **リポジトリからアップデート** オプションを使用するには、次の手順を行います。
   a) **リポジトリからアップデート** を選択します。
   b) **ftp.dell.com** へのネットワーク接続があることを確認します。
   c) **次へ** をクリックします。
3. お使いのホスト向けのバンドルを選択し、**次へ** をクリックします。
4. 使用するファームウェアアップデートを選択し、**次へ** をクリックします。ダウングレード、すでに最新、または現在アップデート用にスケジュール済みのコンポーネントは選択不可になっています。**コンポーネントのダウングレードを許可** チェックボックスを選択する場合は、ダウングレードとしてリストされているオプションを選択します。このオプションの選択は、ファームウェアのダウングレードによる影響を理解している上級ユーザーのみにお勧めします。
5. 希望する再起動オプションを選択します。
   - **メンテナンスモードにしてアップデートを適用し、再起動する。**
     ホストがメンテナンスモードになります。ホストをメンテナンスモードにできない場合は、ホストは再起動されず、アップデートは次回の再起動で適用されます。アップデート後にメンテナンスモード

を終了するには、**ファームウェアアップデート完了後にメンテナンスモードを終了** チェックボックスを選択します。

- **次回の再起動でアップデートを適用する。**
  サービスの中断を避けるため、再起動前にホストをメンテナンスモードにすることが推奨されます。
- **メンテナンスモードにせずにアップデートを適用し、再起動を強制する。**
  アップデートが適用され、ホストがメンテナンスモードでなくても再起動が行われます。この方法は推奨されません。

6. **終了** をクリックします。
7. アップデートが正常に行われたことを確認するには、Dell Management Center で **ジョブキュー → インベントリ履歴 → 今すぐ実行** と選択し、**Dell Management Center 概要** ページで新しいバージョンを確認します。

古いファームウェアバージョンのアップデート

ファームウェアアップデートウィザードを実行するには、ファームウェアは最低必須レベルでなければなりません。最低必須レベルになっていない場合、ファームウェアアップデートウィザードを実行する前にファームウェアをアップデートするオプションが提供されます。通常、2009 年 7 月 29 日より前にインストールされたファームウェアでは、ISO ファイルをダウンロードして実行する必要があります。「ファームウェアのアップデート」を参照してください。2009 年 7 月 29 日 から 2010 年 10 月 14 日の間にインストールされたファームウェアでは、OpenManage Integration for VMware vCenter から自動的にインストールされる ISO バンドルが提案されます。2010 年 10 月 14 日以降インストールされたファームウェアの場合は、ファームウェアアップデートウィザードを実行できます。ファームウェアのアップデートはホストの OpenManage Integration タブの vSphere クライアントで実行できます。リポジトリを設定するには 「ファームウェアリポジトリの設定」を参照してください。

古いファームウェアバージョンをアップデートするには、以下を行います。

1. **ホスト処置**にある **OpenManage Integration** タブの **vSphere クライアント**で、**ファームウェアアップデートウィザードの実行** をクリックします。
   ホストのファームウェアがウィザードを実行するには低過ぎるバージョンの場合、アップデートが必要ダイアログが表示されます。ISO ファイルをダウンロードして実行するか、アップデートのバンドルを実行するよう指示されます。
2. **アップデートが必要**ダイアログボックスで、次のいずれかを行います。
   - ファームウェアのアップデート後に自動的に保守モードを終了するには、**ファームウェアアップデートの完了後にメンテナンスモードを終了**チェックボックスを選択します。
   - マシンをクラスタに戻す前に検査またはテストするため、保守モードに入る場合は、このチェックボックスをマークしないでください。
3. **アップデート**をクリックします。
4. **成功**ダイアログボックスがアップデート実行中であることを示します。
   ファームウェアアップデートの完了後にメンテナンスモードを終了チェックボックスを選択していた場合、ファームウェアアップデートはホストを保守モードにして、自動的に再起動されます。そうでない場合は、保守モードにとどまります。
5. アップデートの進捗を見るには、vSphere クライアントの **最近のタスク**エリアを参照してください。
   この手順の後、ファームウェアアップデートウィザードを再度実行し、ファームウェアを完全にアップデートします。

クラスタおよびデータセンターのためのファームウェアアップデートウィザードの実行

この機能は、iDRAC Express または Enterprise カードのいずれかを装備した第 11 および 12 世代の Dell サーバーにのみ使用できる機能です。お使いのファームウェアが 2010 年 10 月 14 日以降にインストールされた場合

は、ファームウェアアップデートウィザードを使用してファームウェアバージョンを自動でアップデートできます。このウィザードは、接続プロファイルの一部であり、ファームウェア、CSIOR ステータス、ハイパーバイザ、および OMSA ステータス（第 11 世代サーバーのみ）に関して適合するホストのみをアップデートします。お使いのホストがリストされていない場合は、OpenManage Integration for VMware vCenter から vSphere ホスト向け対応ウィザードを実行するか、ホストとクラスタビューからリストされていないホストを選択してファームウェアアップデートウィザードを使用します。各ホストのファームウェアコンポーネントのアップデートは通常 30 分から 60 分かかります。クラスタで DRS を有効化して、ファームウェアアップデートプロセス中にホストがメンテナンスモードに入る / 終了するときに仮想マシンを移行できるようにします。ファームウェアアップデートタスクは、一度に 1 つしかスケジュールまたは実行できません。

ウィザードからエクスポートする場合は、CSV へのエクスポートボタンを使用します。特定のクラスタ、データセンター、ホスト、またはデータグリッドからの任意のトピックアイテム（適用日を除く）を探すため、検索を使用できます。

メモ: ファームウェアは常に、リポジトリバンドル（BIOS、iDRAC、および Lifecycle Controller）の一部として一緒にアップデートするようにしてください。

メモ: デフォルトタイムアウト設定の変更についての情報は、『*User's Guide*』（ユーザーズガイド）の「How Come I see an Error Message Displayed After Clicking the ファームウェア アップデート Link」（ファームウェアアップデートリンクをクリックした後にエラーメッセージが表示される理由）の項を参照してください。

ファームウェアアップデートジョブは、ジョブキューページからステータスの表示および管理を行うことができます。「クラスタおよびデータセンターのためのファームウェアアップデートステータスの表示」を参照してください。

1. **インベントリ** 見出しの **vSphere クライアント** で **ホストとクラスタ** を選択します。
2. **ホストとクラスタ** のツリービューで、データセンターまたはクラスタを選択し、次に **OpenManage Integration** タブを選択します。
3. **ファームウェアのアップデート** をクリックします。

   このリンクが有効ではない、またはオプションをクリックするとポップアップメッセージが表示される場合は、進行中またはスケジュール済みのファームウェアアップデートジョブが存在します。ダイアログは無視してください。待機してから後ほど再試行します。ジョブキューのファームウェアアップデートジョブタブで、すべてのジョブのステータスを表示します。
4. ウィザードに進む前に、ようこそページでアップデートについての情報を確認します。
5. **次へ** をクリックします。
6. ファームウェアインベントリ ページで、既にシステムにインストール済みのコポーネントを確認します。
7. **次へ** をクリックします。
8. アップデートされたバンドルの選択ページで、チェックボックスを使ってアップデートバンドルを選択します。
9. **次へ** をクリックします。
10. アップデートするシステム / コンポーネントの選択ページで、チェックボックスを使用してアップグレードまたはダウングレードするコンポーネントを選択します。ダウングレードする場合は、**コンポーネントのダウングレードを許可する** チェックボックスを選択します。

    メモ: すべてのコンポーネントを選択しても一部が未選択のままである場合は、これらのコンポーネントにアップグレードがないことを意味します。これらのコンポーネントはダウングレードのために選択することができます。
11. **次へ** をクリックします。
12. ファームウェアアップデート情報ページで、アップグレードまたはダウングレード用に選択したコンポーネントを確認します。
13. **次へ** をクリックします。
14. ファームウェアアップデートのスケジュールページにあるジョブ名で、次を行います。

a) ファームウェアアップデートジョブ名テキストボックスに **ファームウェアアップデートジョブ名** を入力します。

これは必須フィールドです。入力されなかった場合は、アップグレードがブロックされます。すでに使用されている名前は使わないでください。この名前をパージすれば、再度使用することができます。

b) ファームウェアアップデート説明に **説明** を入力します。

15. ジョブスケジュールで、次のいずれかを行います。

メモ: オプションの選択は必須です。何も選択されていないと、アップグレードがブロックされます。

- 今すぐアップデートジョブを実行する場合は、**今すぐアップデート** をクリックして **終了** をクリックします。
- アップデートジョブを後で実行する場合は、**アップデートのスケジュール** をクリックして、次を行います。

1. カレンダーボックスで **月と日** を選択します。
2. 時刻テキストボックスに HH:MM 形式で **時刻** を入力し、**終了** をクリックします。

メモ: この時刻は、お使いのクライアントが物理的に存在している場所のローカルタイムゾーンです。無効な時刻値はアップデートがブロックされる原因になります。

Viewing Firmware Update Status for Clusters and Datacenters

このページで情報を表示するには、クラスタまたはデータセンターのためのファームウェアアップデートを実行します。このページに表示されるのは、クラスタおよびデータセンターのためのファームウェアアップデートについての情報のみです。「クラスタおよびデータセンターのためのファームウェアアップデートウィザードの実行 を参照してください。

このページでは、ファームウェアアップデートジョブを更新、パージ、または中止することができます。

1. Dell Management Center で **ジョブキュー → ファームウェアアップデートジョブ** を選択します。
2. 最近の情報を表示するには、**更新** をクリックします。
3. データグリッドのステータスを確認します。このグリッドは、ファームウェアアップデートジョブに関する次の情報を提供します。

- 状態
- スケジュールされた時刻
- 名前
- 説明
- コレクションサイズ

  コレクションサイズとは、このファームウェアインベントリジョブにおけるサーバーの台数です。
- 進捗状況サマリ

  進捗状況サマリは、このファームウェアアップデートの進捗状況詳細をリストします。

4. 特定ジョブについてのよりくわしい詳細を表示するには、特定ジョブのデータグリッドで **詳細** をクリックします。

ここでは、次の詳細を確認できます。

- サービスタグ
- iDRAC IP
- 状態
- 警告

– ファームウェアアップデートジョブ詳細
– 開始時刻
– 終了時刻

5. 実行中ではないスケジュール済みファームウェアアップデートを中止するには、中止するジョブと同じ行で **中止** をクリックします。
6. スケジュール済みファームウェアアップデートをパージするには、**ジョブキューのパージ** をクリックします。
   パージできるのは、完了した、またはスケジュールされたジョブのみです。
7. **日付とジョブステータスより古い** を選択して、**適用** をクリックします。選択したジョブがキューからクリアされます。

vCenter を使用した高度なホスト管理

高度なホスト管理タスクは、管理者がデータセンター環境における物理サーバーの識別、サーバーベースの管理ツールの開始、サーバー保証情報の表示を行うことを可能にする、ホストシステムベースの作業です。これら作業のすべては、vCenter の OpenManage Integration タブから、または個別ホストシステムに対する *ホストとクラスタ*ビューでホストを右クリックすることで開始できます。

物理サーバー前面インジケータライトの設定

大規模なデータセンター環境で物理サーバーを見つけやすくするため、一定期間で前面インジケータライトを点滅させるよう設定できます。
物理サーバーの前面インジケータライトを設定するには、以下を行います。

1. **インベントリ** の見出しの下の **vSphere クライアント**で、**ホストとクラスタ** を選択します。
2. **ホストとクラスタ** からツリービューのホストシステムを選択し、**OpenManage Integration** タブを選択します。
3. **ホスト処理** で、**インジケータライトの点滅** を選択します。
4. 次のいずれかを選択します。
   – 点滅を開始し、期間を設定するには **インジケータライト** ダイアログボックスで **点滅オン** をクリックし、タイムアウトドロップダウンリストでタイムアウト間隔を選択して **OK** をクリックします。
   – 点滅を終了するには、**インジケータライト** ダイアログボックスで **点滅オフ** をクリックし、**OK** をクリックします。

サーバーベース管理ツール

vSphere クライアント → OpenManage Integration タブから起動できるサーバーベース管理ツールには、iDRAC および OMSA の 2 つがあります。左ペインの管理コンソールリンクで、次にアクセスできます。

- リモートアクセスの起動。
  このオプションを使って iDRAC ユーザーインタフェースを起動します
- OMSA の起動
  このオプションを使って、OpenManage Server Administrator ユーザーインタフェース URL を起動します。これは、最初の設定ウィザード中に、または **設定 → 一般** を使用して、管理センターにこの URL を入力することで行います。Windows ベースの管理ステーション上のサーバー管理者ウェブサーバー用にこの URL をインストールする必要があります。
- ブレードシステムを使っている場合、CMC を起動してシャーシ管理コントローラユーザーインタフェースを起動します。ブレードシステムでない場合、これは表示されません。

保証の取得

保証の取得は、Dell サーバーについて以下の情報を提供します。

- アップデートされたサービス保証情報、ただしホストサービスタグのみを送信
- 定期的にアップデートされた保証情報
- プロキシサーバーおよび資格情報を使ったセキュアな送信

メモ: デルは、送信されたサービスタグ情報は保存しません。

関連タスク:

- ホスト保証の更新
- 保証取得ジョブの実行
- シングルホストのサービス保証情報の表示
- 全データセンターの保証情報の表示

ホスト保証の更新

サーバーの保証ステータスを表示し、保証ページで保証を更新することができます。

1. **vSphere クライアント → OpenManage Integration タブ → ホスト情報**で、**保証**をクリックします。
2. 保証を更新して、システム保証を管理するデルのウェブページに移動するには、**保証の更新**をクリックします。
3. Dell ウェブページで **保証の更新 / アップグレード**をクリックします。

全データセンターのサーバー保証情報の表示

保証ジョブが完了したら、データセンタービューページで vSphere クライアントのサーバー保証情報を表示することができます。
全データセンターのサーバー保証情報を表示するには、以下を行います。

1. **インベントリ**の見出しの vSphere クライアントから **ホストとクラスタ**を選択します。
2. **ホストとクラスタ** でツリービューからデータセンターを選択し、**OpenManage Integration** タブを選択します。
3. データセンターの全ホストの概要が表示されます。表示ドロップダウンリストで **保証**を選択します。
4. **フィルタ**テキストボックスに保証データの検索語を入力します。
5. 表示されているインベントリを更新するには、**更新**をクリックします。
6. インベントリを CSV ファイルでエクスポートするには、**エクスポート**をクリックします。ダウンロードの場所ウィンドウで、インベントリを保存するロケーションを参照し、**保存**をクリックします。

シングルホストのサービス保証情報の表示

保証ジョブの完了後、ホストビューページの vSphere Client でシングルホストの保証情報を表示することができます。
シングルホストのサーバー保証情報を表示するには、以下を行います。

1. **インベントリ**の見出し下の vSphere クライアントで **ホストとクラスタ**を選択します。
2. **ホストとクラスタ** からツリービューのホストシステムを選択し、**OpenManage Integration** タブを選択します。
3. システム保証情報を表示するには、**保証**を選択します。保証ステータスページの情報には以下が含まれます。

- 保証プロバイダ名および保証の説明
- 開始日と終了日および保証残余期間
- 保証ステータス（有効または無効）および保証情報の最新更新日

5

ハードウェア管理

必要条件：

ハードウェアのプロビジョニングおよび展開を正しく行うためには、物理サーバーが展開ウィザードに表示される必要があります。すべての物理サーバーは次の必要条件を満たす必要があります。

- 具体的なハードウェアサポート情報については、『*OpenManage Integration for VMware vCenter リリースノート*』を参照してください。
- サーバーには、サポートされる最低必須バージョンの iDRAC ファームウェア、Lifecycle Controller および BIOS が必要です。具体的なハードウェアサポート情報については、『*OpenManage Integration for VMware vCenter Release Notes*』（VMware vCenter 用 Dell Management Plug-In リリースノート）を参照してください。

  メモ: ファームウェアバージョンが古い場合、2 段階のアップグレードプロセスが必要になる可能性があります。詳細なアップグレード手順については、ファームウェアのマニュアルを参照してください。
- OpenManage Integration for VMware vCenter は、組み込み / 統合 LOM を使ってのみ、展開をサポートします。展開後は手動で PCI スロットの NIC を設定できます。アドオン NIC を使用する場合、システムは、ホスト LOM を有効化していなければなりません。
- OpenManage Integration for VMware vCenter は、内蔵デュアル SD モジュール（ハイパーバイザーのみ）またはローカルハードディスクドライブへの展開を行います。ハイパーバイザーを内蔵デュアル SD モジュールにインストールするには、最大 1 または 2 GB のストレージが必要です。内蔵デュアル SD モジュールは、OpenManage Integration for VMware vCenter でハイパーバイザーを展開する前に BIOS で有効化しておく必要があります。管理 NIC は手動で変更し、システムを vCenter に追加することができます。
- iDRAC が専用モードになっている場合、その NIC は OpenManage Integration for VMware vCenter と通信ができるよう有効化されていなければなりません。
- CSIOR は有効化されている必要があります。また、自動検出を開始する前には、検索データが最新のものであることを確認し、システムの電源を完全に切断してから再投入（ハード再起動）してください。
- Dell サーバーは、自動検出とハンドシェークオプションを工場出荷時に事前設定して納入するよう発注することができます。サーバーがこのオプションで事前設定されていない場合、手動で OpenManage Integration for VMware vCenter IP アドレスを入力し、または、この情報を提供するようローカルネットワークを設定する必要があります。
- OpenManage Integration for VMware vCenter がハードウェア設定に使われない場合、ハイパーバイザーの起動前に以下の状態であることを確認してください。
  - BIOS における VT（仮想化テクノロジ）フラグが有効である。
  - オペレーティングシステムのインストールで、システム起動順を起動可能な仮想ディスク、または内蔵デュアル SD モジュールに設定する。
- ハードウェア設定に OpenManage Integration for VMware vCenter を使う場合は、BIOS 設定がハードウェアプロファイルの一部でなくても、VT の BIOS 設定は自動的に有効化されます。仮想ディスクがターゲットシステムにまだ存在していない場合は、Express/Clone RAID 設定が必要になります。
- サーバーが Dell PowerEdge 第 12 世代サーバーより前のバージョンからのものである場合、展開プロセスによって OpenManage Server Administrator パッケージがターゲットシステムにインストールされ、SNMP トラップ先が OpenManage Integration for VMware vCenter をポイントするように自動的に設定されます。
- 展開には、すべての Dell ドライバを含むカスタム ESXi イメージが必要です。正しいイメージは、Dell ドライバ & ダウンロードページに移動し、展開プロセス中アクセスすることができる場所にカスタムイメージを保存することによって、見つけることができます。本リリース向けの対応 ESXi バージョンの最新リストは、リリースノートを参照してください。

プロビジョニングの概要

データセンターの物理インベントリが完了すると、すべての自動検出ベアメタルシステムは OpenManage Integration for VMware vCenter のハードウェアのゼロタッチプロビジョニングとハイパーバイザー展開の対象となります。プロビジョニングと展開には、次を準備する必要があります。

ハードウェアプロファイルの作成	新しいサーバーの展開に使われる参照サーバーから収集したハードウェア設定が含まれます。「新規ハードウェアプロファイルの作成」を参照してください。
ハイパーバイザープロファイルの作成	ESX/ESXi 展開に必要なハイパーバイザーインストール情報が含まれます。「新規ハイパーバイザープロファイルの作成」を参照してください。
展開テンプレートの作成	オプションで、ハードウェアプロファイル、ハイパーバイザープロファイル、またはその両方が含まれます。これらのプロファイルは保存して、必要に応じてすべてのデータセンターサーバーで使用することができます。「展開テンプレートの構築」を参照してください。

展開テンプレートが作成できたら、展開ウィザードを使用してサーバーハードウェアのプロビジョニングと、新しいホストを vCenter に展開するようスケジュールされたジョブを作成するために必要な情報を収集します。展開ウィザードの実行に関する情報については、「展開ウィザードの実行」を参照してください。最後に、ジョブキューを使用して、ジョブステータスを表示し、未実行の展開ジョブを変更します。

メモ: 連続実行するようスケジュールできるのは、2 つの展開ジョブまでです。複数のジョブは、スケジュール機能を使って展開実行をずらすようにしてください。

展開ジョブ時間の理解

ベアメタルサーバーのプロビジョニングと展開には、特定の要素により、完了まで 30 分がら数時間かかる場合があります。展開ジョブを開始する場合は、提供されたガイドラインにしたがって、展開時間を計画することを推奨します。プロビジョニングと展開にかかる時間は展開タイプ、複雑性、同時に実行される展開ジョブ数などによって異なります。以下のテーブルは、展開ジョブにかかるおおよその時間のガイドラインを提供します。展開ジョブは、総合的な展開ジョブの時間を短縮するため、最大 5 台の並列サーバーによるバッチ処理で実行されます。並列ジョブの正確な数は使用可能リソースによって異なります。

表 2. おおよその展開時間シナリオ

展開タイプ	展開ごとのおおよその時間
ハイパーバイザーのみ	30 ～ 130 分
ハードウェアのみ	設定の複雑性、RAID、BIOS および起動オプションにより、最大 2 時間
ハイパーバイザーおよびハードウェアプロファイル	1 ～ 4 時間

展開シーケンス実行中のサーバー状態

インベントリジョブの実行時に、自動検出されたベアメタルシステムは、データセンターにとって新しいサーバーか、未完了の展開ジョブがスケジュールされているかなどを特定しやすくするため、いくつかの状態に分類されます。管理者はこれらの状態を使用してサーバーを展開ジョブに含めるべきかどうかを判断できます。状態には、以下があります。

未設定	サーバーは、OpenManage Integration for VMware vCenter と接触しており、設定を待機している状態です。「展開ジョブ時間の理解」を参照してください。

設定済み	サーバーには、正しいハイパーバイザー展開に必要なすべてのハードウェア情報が設定されています。

カスタム Dell ISO イメージのダウンロード

展開には、すべての Dell ドライバを含むカスタム ESXi イメージが必要です。Dell はカスタム ESX 4.1 イメージを作成できません。展開を行うには、すべてのドライバが VMware が生成する ISO にネイティブで存在する必要があります。本リリース向けの対応 ESXi バージョンの最新リストは、リリースノートを参照してください。

メモ: OpenManage Integration for VMware vCenter には、展開に必要な ESXi ISO イメージが含まれていません。これらのイメージは、展開中にアクセスできる場所にダウンロードしておくことが必要で、そうしない場合は展開が失敗する可能性があります。

1. **support.dell.com** にアクセスします。
2. 希望する言語の **ドライバおよびダウンロード** ページに行き、以下のいずれかを行います。
   - サービスタグまたはエクスプレスサービスコードを使ってドライバを選択するには、**はい** の下のテキストボックスにサービスタグまたはエクスプレスサービスコードを入力し、**送信** をクリックします。
   - 別のオプションでドライバを選択するには、**いいえ** の下で以下のいずれかを選択します。
     * 自動的にサービスタグを検出
     * 自分の製品およびサービスリストから選択
     * 全 Dell 製品リストから選択

     次に、**継続** をクリックして選択したオプションに対する指示に従います。
3. 選択されたサーバーに対するページで、**結果の絞込み** にスクロールダウンし、**オペレーティングシステム** でドロップダウンリストを使って、必要な ESX または ESXi システムを選択します。
4. **エンタープライズソリューション** をクリックします。
5. **エンタープライズソリューション** リストで、必要な ISO バージョンを選択し、**ファイルのダウンロード** をクリックします。

   メモ: 組み込み ISO は、ハイパーバイザーのデュアル内蔵 SD モジュールへのインストールに使用されます。インストール可能 ISO はハードディスクへのインストールに使用されます。
6. ダイアログボックスで、**ブラウザ経由でのシングルファイルダウンロード用** を選択し、**今すぐダウンロード** をクリックします。
7. ダイアログボックスで、展開用に ISO イメージを保存するロケーションを参照します。

ハードウェアプロファイルの設定方法の理解

サーバーハードウェア設定を行うには、ハードウェアプロファイルを作成する必要があります。ハードウェアプロファイルは、新たに検出されたインフラストラクチャコンポーネントに適用できる設定テンプレートで、以下の情報を必要とします。

起動順序	起動順序は、起動デバイスシーケンスとハードドライブシーケンスで、起動モードが BIOS で設定されている場合にのみ編集できます。
BIOS 設定	BIOS 設定には、メモリ、プロセッサ、SATA、統合デバイス、シリアル通信、内蔵サーバー管理、電源管理、システムセキュリティ、およびその他の設定が含まれます。
iDRAC Settings（iDRAC 設定）	iDRAC 設定には、ネットワーク、ユーザーリスト、およびユーザー設定（IPMI / iDRAC 権限）が含まれます。

メモ: iDRAC Express を備えるシステムにおいては、iDRAC 構成は抽出できません。したがってサーバーは参照サーバーとして使用すべきではありません。ターゲットシステムとして使用される場合、参照サーバーからの iDRAC 設定は適用されません。

RAID 構成

RAID 構成は、ハードウェアプロファイルが抽出された時点における、RAID トポロジを、参照サーバーに表示します。

メモ: ハードウェアプロファイルで設定された RAID 構成オプションには 次の 2 種類があります : 1. *RAID1 を適用 + 専用ホットスペアの作成適用可能*。ターゲットサーバーにデフォルトの RAID 構成を適用したい場合は、このオプションを使用します。RAID 構成タスクは、デフォルトで RAID1 対応の内部コントローラ上の最初の 2 つのドライブを使用して RAID1 を構成します。さらに、専用ホットスペアの基準を満たす候補ドライブがある場合は、RAID1 アレイ用の専用ホットスペアが作成されます。 2. *次に示すように、RAID 構成を参照サーバーからクローン*。参照サーバーの設定をクローンしたい場合は、このオプションを使用します。「新規ハードウェアプロファイルの作成」を参照してください。

メモ: OpenManage Integration for VMware vCenter は、参照サーバーの設定にかかわらず、すべての展開サーバーにおける BIOS のプロセッサグループの特定の BIOS 設定を可能とします。新規ハードウェアプロファイルの作成に参照サーバーを使用する前に、再起動時にシステムインベントリを収集（CSIOR）設定を有効にして再起動し、正確なインベントリおよび構成情報を収集しておく必要があります。

ハードウェアプロファイルを作成するためのタスクには、以下が含まれます。

- 参照サーバーにおける CSIOR の有効化
- 新規ハードウェアプロファイルの作成
- 新規ハードウェアプロファイルのクローン
- ハードウェアプロファイル管理について

新規ハードウェアプロファイルの作成

新規ハードウェアプロファイルを作成するには、以下を実行します。

1. Dell Management Center で **展開** → **展開テンプレート** → **ハードウェアプロファイル** を選択します。
2. **新規作成** をクリックします。
3. **新規ハードウェアプロファイル** ページで、以下を行います。
   - **プロファイル名** テキストボックスに、プロファイル名を入力します。
   - **説明** テキストボックスに、オプションの説明を記入します。
4. **保存** をクリックします。
5. 続けるには、左ペインで **参照サーバー** をクリックします。
6. 参照サーバーウィンドウで、**編集** をクリックします。
7. vCenter で管理されている、OpenManage Integration for VMware vCenter で正しくインベントリが行われている対応参照サーバーを見つけるには、 **参照** をクリックします。
8. **サーバー** ダイアログボックスでリストを下にスクロールして、正しい参照サーバーを見つけ、**選択** をクリックします。
9. 参照サーバーの設定をデフォルトとしてカスタマイズするには、**参照サーバーからの設定をカスタマイズ** をクリックして、次に **保存** をクリックします。
10. 設定を抽出するのに数分かかります、というダイアログボックスが表示されます。設定を表示するには、**続行** をクリックします。選択されたサーバーの名前、iDRAC IP アドレス、およびサービスタグが **参照サーバーウィンドウ** に表示されます。

11. 左ペインで **起動順序** を選択します。プロファイルに再起動順の情報を含めるには、**このハードウェアプロファイルに起動順序を含める** チェックボックスを選択します。
12. 再起動順オプションを表示するには、**起動順序** を展開して、**編集** をクリックしてアップデートを行います。

    a. **ブートモード** ドロップダウンリストで BIOS または UEFI を選択します。
    b. **起動デバイスのシーケンス** 下の **表示 / 設定** ドロップダウンリストで、表示される再起動デバイス順を変更するには、デバイスを選択して **上へ移動** または **下へ移動** をクリックします。
    c. **起動順序の再試行** ドロップダウンリストで、**有効** を選択し、サーバーが自動的に再起動シーケンスのリトライを行うようにするか、**無効** を選択して、リトライをしないようにします。
    d. **保存** をクリックして変更を保存するか、**キャンセル** をクリックして変更を取り消します。

13. **BIOS 再起動モード** が選択された場合、**ハードドライブのシーケンス** を展開して、ハードドライブ順オプションを表示し、**編集** をクリックしてアップデートを行うことができます。

    – 表示されているハードドライブ順を変更するには、デバイスを選択して **上に移動** または **下に移動** をクリックします。
    – **保存** をクリックして変更を保存するか、**キャンセル** をクリックして変更を取り消します。

14. 左ペインで **BIOS 設定** を選択します。プロファイルに BIOS 設定情報を含めるには、**このハードウェアプロファイルに BIOS 設定を含める** チェックボックスを選択します。カテゴリを展開して設定オプションを表示し、**編集** をクリックして以下のいずれかのアップデートを行います。

    – メモリ設定
    – プロセッサ設定
    – SATA 設定
    – 内蔵デバイス
    – シリアル通信
    – 組み込みサーバー管理
    – 電源管理
    – システムセキュリティ
    – その他の設定

    カテゴリ内のすべてのアップデートが完了したら、**適用** をクリックして変更を保存するか、**キャンセル** をクリックして変更を取り消します。

    メモ: 設定オプションおよび説明を含む詳細 BIOS 情報については、選択したサーバーの『*Hardware Owner's Manual*』（ハードウェアオーナーズマニュアル）を参照してください。

15. 左ペインで **iDRAC 設定** を選択し、**ネットワーク** を選択します。
16. ネットワーク設定情報をプロファイルに含めるには、**このハードウェアプロファイルにネットワーク設定を含める** チェックボックスを選択します。カテゴリを展開して設定オプションを表示し、**編集** をクリックして、以下のいずれかのアップデートを行います。

    – ネットワーク
    – ネットワーク設定
    – 仮想メディア

    カテゴリ内のすべてのアップデートが完了したら、**適用** をクリックして変更を保存するか、**キャンセル** をクリックして変更を取り消します。

    メモ: 設定オプションおよび説明を含む詳細 iDRAC 情報については、選択したサーバーの『*iDRAC User's Guide*』（iDRAC ユーザーガイド）を参照してください。

17. 左ペインで、**iDRAC 設定 → ユーザーリスト** を選択します。プロファイルにユーザーリスト情報を含めるには、**このハードウェアプロファイルにユーザーリストを含める** チェックボックスを選択します。
iDRAC ローカルユーザーリストで以下のいずれかを行います。

a) **ユーザーの追加**: 手動で iDRAC ユーザーと必要情報を入力します。完了したら **保存** をクリックして変更を保存するか、**キャンセル** をクリックして取り消します。
b) **ユーザーの削除**: 選択したユーザーを削除します。当該ユーザーのチェックボックスを選択して **削除** をクリックするか、**キャンセル** をクリックして取り消します。
c) **ユーザーの編集**: 手動で iDRAC ユーザー情報を編集します。完了したら **保存** をクリックして変更を保存するか、**キャンセル** で取り消します。

メモ: 設定オプションおよび説明を含む詳細 iDRAC 情報については、選択したサーバーの『*iDRAC User's Guide*』（iDRAC ユーザーガイド）を参照してください。

18. 左ペインで、**RAID 設定** を選択します。プロファイルに RAID 設定情報を含めるには、**このハードウェアプロファイルに RAID 設定を含める** チェックボックスを選択します。次に、以下のいずれかを選択します。

- RAID1 を適用 + 専用ホットスペアの作成適用可能。
  ターゲットサーバーにデフォルトの RAID 構成を適用したい場合は、このオプションを使用します。RAID 構成タスクは、デフォルトで RAID1 対応の内部コントローラ上の最初の 2 つのドライブを使用して RAID1 を構成します。さらに、専用ホットスペアの基準を満たす候補ドライブがある場合は、RAID1 アレイ用の専用ホットスペアが作成されます。
- RAID 構成を参照サーバーからクローン。
  参照サーバーの設定をクローンしたい場合は、このオプションを使用します。

このプロファイルは自動的に保存され、**使用可能なプロファイル** 下の **ハードウェアプロファイル** に表示されます。

参照サーバーにおける CSIOR の有効化

参照サーバーを使ってハードウェアプロファイルを作成する前に、再起動時にシステムインベントリを収集（CSIOR）の設定を有効化し、サーバーを再起動して正確なインベントリおよび設定情報を収集します。CSIOR を有効化するには 2 つの方法があります。

ローカル	これは、Dell Lifecycle Controller United Server Configurator (USC) ユーザーインタフェースを使って、個別ホストを利用します。
リモート	これは、WS-Man スクリプトを使用します。この機能をスクリプトすることに関する詳細は、「*Dell Tech Center*」および「*DCIM Lifecycle Controller 管理プロファイル*」を参照してください。

参照サーバーでの CSIOR をローカルで有効化するには、以下を行います。

1. システムに電源を入れ、POST 中に **<F10>** を押して USC を起動します。
2. **ハードウェア設定 → 部品交換設定**を選択します。
3. **再起動時にシステムインベントリを収集**の設定を有効化し、USC を終了します。

ハードウェアプロファイルのクローン

新規ハードウェアプロファイルをクローンするには、以下を実行します。

1. Dell Management Center で **展開 → 展開テンプレート → ハードウェアプロファイル** を選択します。
2. **新規作成** をクリックします。
3. **新規ハードウェアプロファイル** ページで、以下を行います。
   - **プロファイル名** テキストボックスにプロファイル名を入力します。
   - **説明** テキストボックスに、オプションで説明を入力します。
4. **保存** をクリックします。

5. 左ペインで、**参照サーバー** をクリックします。
6. **参照サーバー** ウィンドウで **編集** をクリックします。
7. 参照サーバーからすべてのハードウェア設定を抽出するには、**参照サーバー設定のクローン** オプションボタンをクリックします。
8. **保存** をクリックします。
9. 設定の抽出には数分かかります、というダイアログボックスが表示されたら、**続行** をクリックします。設定が表示され、選択されたサーバー名、iDRAC IP アドレス、およびサービスタグが参照サーバーウィンドウに表示されます。
   プロファイルは保存され、**使用可能プロファイル** 下の **ハードウェアプロファイル** ウィンドウに表示されます。

ハードウェアプロファイル管理について

ハードウェアプロファイルは、参照サーバーを使ってサーバーのハードウェア設定を定義します。Dell Management Center では、以下を始め、既存のハードウェアプロファイルに対し多くの管理処理を実行することができます。

- ハードウェアプロファイルの表示または編集
- ハードウェアプロファイルの複製
- ハードウェアプロファイル名の変更
- ハードウェアプロファイルの削除
- ハードウェアプロファイルの更新

ハードウェアプロファイルの表示または編集

ハードウェアプロファイルを表示または編集するには、以下を実行します。

1. Dell Management Center で **展開** → **展開テンプレート** → **ハードウェアプロファイル** を選択します。
2. プロファイルを選択して、**表示 / 編集**をクリックします。
3. **ハードウェアプロファイル** ウィンドウで、変更するには、**編集** をクリックします。
4. 変更を適用するには、**保存** をクリックします。または **キャンセル** をクリックして変更を取り消します。

ハードウェアプロファイルの複製

ハードウェアプロファイルを複製するには、以下を行います。

1. Dell Management Center で **展開** → **展開テンプレート** → **ハードウェアプロファイル** を選択します。
2. **ハードウェアプロファイル** ページでプロファイルを選択して、**複製** をクリックします。
3. **複製** ダイアログボックスで、一意のハードウェアプロファイル名を入力します。
4. **適用** をクリックして新しい名前でプロファイルのコピーを作成するか、または **キャンセル** をクリックして取り消します。

ハードウェアプロファイル名の変更

ハードウェアプロファイル名を変更するには、以下を行います。

1. Dell Management Center で **展開** → **展開テンプレート** → **ハードウェアプロファイル** を選択します。
2. **ハードウェアプロファイル** ページでプロファイルを選択して **名前の変更** をクリックします。
3. **名前の変更** ダイアログボックスで一意のハードウェアプロファイル名を入力します。
4. 新しい名前を使用するには、**適用** をクリックします。または **キャンセル** をクリックして取り消します。

ハードウェアプロファイルの削除

ハードウェアプロファイルを削除するには、以下を行います。

メモ: 実行中の展開タスクの一部であるハードウェアプロファイルを削除すると、タスクが失敗する原因になります。

1. Dell Management Center で **展開** → **展開テンプレート** → **ハードウェアプロファイル** を選択します。
2. プロファイルを選択して、**削除** をクリックします。
3. プロファイルの削除メッセージダイアログボックスで、**削除** をクリックするか、または **キャンセル** をクリックして取り消します。

アップデートされたハードウェアプロファイルの更新

アップデートされたハードウェアプロファイルを更新するには、以下を行います。

1. Dell Management Center で **展開** → **展開テンプレート** → **ハードウェアプロファイル** を選択します。
2. **更新** をクリックします。
   アップデートされたハードウェアプロファイル情報が表示されます。

新しいハイパーバイザープロファイルの作成

ESX/ESXi をサーバーに展開して設定するには、ハイパーバイザープロファイルを作成する必要があります。ハイパーバイザープロファイルには、以下の情報が必要です。

- NFS または CIFS 共有上のスクリプト可能な参照 ISO ソフトウェアメディアロケーション
- 展開されたホストおよびオプションのホストプロファイルを管理する vCenter インスタンス
- OpenManage Integration for VMware vCenter が vCenter でサーバーを展開する宛先クラスタまたはデータセンター

メモ: 参照 ISO ファイル名には、次の命名法を使用します。

```
NFS format: host:/share/hypervisor_image.iso

CIFS format: \\host\share\hypervisor.iso
```

メモ: 正しい展開には、ESX ISO に正しいドライバが備わっていることが必要です。より新しい Dell システムでは、すべての必要な Dell ドライバが含まれる Dell カスタム ISO イメージが必要になる可能性があります。ESX 4.1 はより新しい Dell システムでは動作しない可能性があり、Dell から入手可能なカスタム ISO を備えていない可能性があります。

新しいハイパーバイザープロファイルを作成するには、次の手順を実行します。

1. Dell Management Center で **展開** → **展開テンプレート** → **ハイパーバイザープロファイル** を選択します。
2. **ハイパーバイザープロファイル** ページで、**新規作成** をクリックします。
3. **新規ハイパーバイザープロファイル** ページで以下を行います。
   - **プロファイル名** テキストボックスに、プロファイル名を入力します。
   - **説明** テキストボックスに、オプションで説明を入力します。
4. 左ペインで、**参照 ISO** をクリックし、次に **編集** をクリックし、**ハイパーバイザーのインストール元** ダイアログボックスで以下の情報を入力します。
   - **インストール元（ISO）** テキストボックスに、ハイパーバイザー共有ロケーションへのパスをタイプします。このハイパーバイザーイメージのコピーが変更され、スクリプトによるインストールが許容されます。参照 ISO ロケーションは、次のいずれかのフォーマットを使用する必要があります。

NFS フォーマット: host:/share/hypervisor_image.iso

CIFS フォーマット: ￥￥ host ￥ share ￥ hypervisor.iso

– **バージョンの選択** ドロップダウンリストで、ESX または ESXi バージョンを選択します。

このハイパーバイザープロファイルを使用して展開されたすべてのサーバーにはこのイメージが備わります。サーバーが Dell PowerEdge 第 12 世代サーバーより前のバージョンである場合、OpenManage Server Administrator の最新推奨バージョンがインストールされます。

5. CIFS 共有を使用する場合は、**ユーザー名**、**パスワード**、および **パスワードの確認** を入力します。両パスワードは一致している必要があります。
6. 設定をプロファイルに追加するには、**保存** をクリックします。
7. 左側のペインで、**vCenter 設定** をクリックして、必要な箇所を編集します。
   - **vCenter インスタンス**：展開後にホストを管理するサーバーインスタンスを表示します。
   - **vCenter バージョン**：現在のバージョンを表示します。
   - **vCenter 宛先コンテナ**：新しい物理サーバーをホストするデータセンターまたはクラスタです。**参照** をクリックして、vCenter の展開先を検索します。
   - **vCenter ホストプロファイル**：ホスト設定をカプセル化し、ホスト設定をしやすくするプロファイルを選択します。
8. 設定をプロファイルに追加するには、**保存** をクリックします。

ハイパーバイザープロファイルの管理に関する情報は、「ハイパーバイザープロファイルの管理」を参照してください。

ハイパーバイザープロファイルの管理

既存のハイパーバイザープロファイルについて実行できる管理処置には、以下が含まれます。

- VLAN サポートの理解
- ハイパーバイザープロファイルの表示または編集
- ハイパーバイザープロファイルの複製
- ハイパーバイザープロファイル名の変更
- ハイパーバイザープロファイルの削除
- ハイパーバイザープロファイルの更新

VLAN のサポート

OpenManage Integration for VMware vCenter は、ルータブル VLAN へのハイパーバイザー展開をサポートします。VLAN サポートは展開ウィザードで設定します。 展開ウィザードのこの部分では、VLAN の使用および VLAN ID を指定するオプションがあります。VLAN ID が提供されると、展開の際にハイパーバイザーの管理インタフェースに適用され、すべてのトラフィックがその VLAN ID でタグ付けされます。

展開の際に提供された VLAN が、仮想アプライアンスと vCenter サーバーの両方と通信できることを確認してください。 ハイパーバイザーを宛先のいずれかまたは両方と通信できない VLAN に展開すると、展開が失敗する原因となります。

1 つの展開ジョブで複数のベアメタルサーバーを選択し、同じ VLAN ID をすべてのサーバーに適用する場合、展開ウィザードのサーバー識別の箇所にあるデフォルト設定で、*選択したすべてのサーバーに設定を適用します*ボタンを使用します。これにより、同じ VLAN ID とともにその他のネットワーク設定を、その展開ジョブのすべてのサーバーに適用することができます。

メモ: OpenManage Integration for VMware vCenter はマルチホーム構成をサポートしません。 2 つ目のネットワークとの通信のための、アプライアンスへの 2 つ目のネットワークインタフェースの追加は、ハイパーバイザー展開、サーバーコンプライアンス、およびファームウェアアップデート操作が関わるワークフローに問題を生じます。

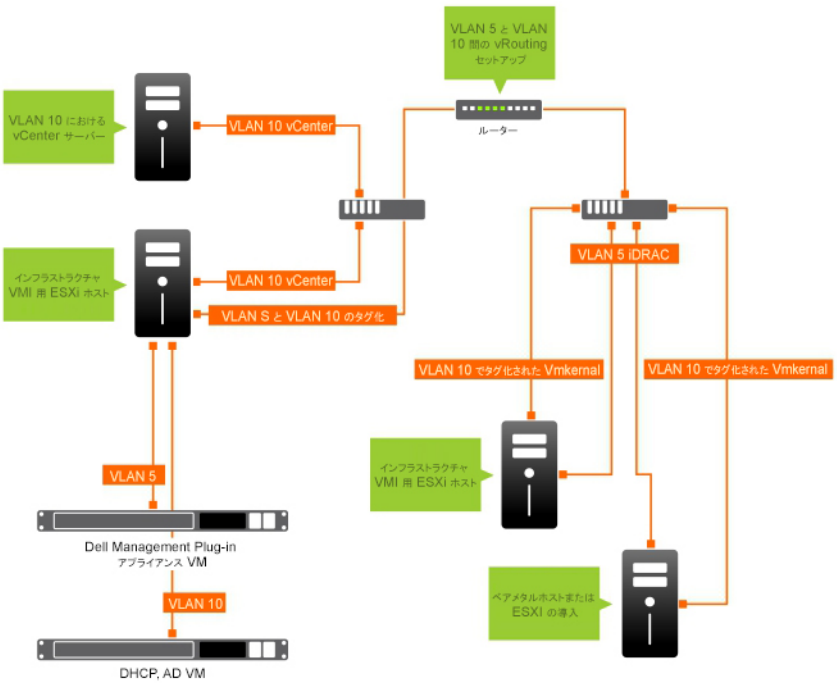

図 4. VLAN ネットワークの例。

このネットワークの例では、展開された vCenter と ESXi ホストの VMkernal は VLAN 10 にありますが、OpenManage Integration for VMware vCenter は VLAN 5 にあります。OpenManage Integration for VMware vCenter は VLAN のマルチホームをサポートしないため、すべてのシステムが互いに正しく通信するためには、VLAN 5 が VLAN 10 にルーティングされる必要があります。これらの VLAN でルーティングが有効でない場合、展開は失敗します。

ハイパーバイザープロファイルの表示または編集

ハイパーバイザープロファイルの表示または編集には以下を行います。

1. Dell Management Center で、**展開 → 展開テンプレート → ハイパーバイザープロファイル** ウィンドウを選択します。
2. プロファイルを選択して、**表示 / 編集**をクリックします。
3. **ハイパーバイザープロファイル : プロファイル名** ウィンドウで、表示または変更、および必要な変更を行うためのプロファイルセクションを選択します。
4. 変更を適用するには、**保存** をクリックします。または **キャンセル** をクリックして変更を取り消します。

ハイパーバイザープロファイルの複製

ハイパーバイザープロファイルの複製には、以下を行います。

1. Dell Management Center で **展開 → 展開テンプレート → ハイパーバイザープロファイル** を選択します。
2. **ハイパーバイザープロファイル** ページでプロファイルを選択して、**複製** をクリックします。
3. **複製** ダイアログボックスに、一意のハイパーバイザープロファイル名を入力します。
4. **適用** をクリックして新しい名前でプロファイルのコピーを作成するか、または **キャンセル** をクリックして取り消します。

ハイパーバイザープロファイル名の変更

ハイパーバイザー名を変更するには、以下を行います。

1. Dell Management Center で **展開 → 展開テンプレート → ハイパーバイザープロファイル** を選択します。
2. **ハイパーバイザープロファイル** ページで、プロファイルを選択して **名前の変更** をクリックします。
3. **名前の変更** ダイアログボックスで、一意のハイパーバイザープロファイル名を入力します。
4. 新しい名前を使用するには、**適用** をクリックします。または **キャンセル** をクリックして取り消します。

ハイパーバイザープロファイルの削除

ハイパーバイザープロファイルを削除するには、以下を行います。

メモ: 実行中の展開タスクの一部となっているハイパーバイザープロファイルを削除すると、展開タスクが失敗する可能性があります。

1. Dell Management Center で **展開 → 展開テンプレート → ハイパーバイザープロファイル** を選択します。
2. プロファイルを選択して、**削除** をクリックします。
3. メッセージダイアログボックスで、**削除** をクリックしてプロファイルを削除するか、**キャンセル** をクリックして取り消します。

ハイパーバイザープロファイルの更新

ハイパーバイザープロファイルを更新するには、以下を行います。

1. Dell Management Center で **展開 → 展開テンプレート → ハイパーバイザープロファイル** を選択します。
2. **更新** をクリックします。
   アップデートされたハイパーバイザープロファイル情報が表示されます。

新規の展開テンプレートの作成

展開テンプレートには、ハードウェアプロファイル、ハイパーバイザープロファイル、またはその両方が含まれます。展開ウィザードはこのテンプレートを使用してサーバーハードウェアのプロビジョニングを行い、ホストを vCenter 内に展開します。

新規展開テンプレートの作成には、以下を行います。

1. Dell Management Center で、**展開 → 展開テンプレート**を選択します。
2. **使用可能なプロファイル**で **新規作成**をクリックします。
3. **新規作成**ウィンドウで、テンプレート名を入力し、**保存**をクリックします。
4. テンプレートを完成するには、**編集**をクリックします。

5. 右ペインの **プロファイル**ドロップダウンリストで、プロファイルを選択して、以下のいずれかを行います。
   - 選択したプロファイルのハードウェア / ハイパーバイザープロファイル設定を表示するには、**表示**をクリックします。
   - 新規ハードウェア / ハイパーバイザープロファイルを作成するには、**新規作成**をクリックします。
6. 展開テンプレートについて、オプションでテンプレートの管理に役立つ **説明**を入力します。
7. プロファイルの選択を適用し、変更を保存するには、**保存**をクリックします。取り消すには、**キャンセル**をクリックします。

展開テンプレートの管理

Dell Management Center からは、既存の展開テンプレートに対して以下を始めとする管理作業を実施することができます。

- 展開テンプレートの作成
- 展開テンプレートのコピー
- 展開テンプレート名の変更
- 展開テンプレートの削除

展開テンプレートのコピー

展開テンプレートをコピーするには、以下を行います。

1. Dell Management Center で、**展開 → 展開テンプレート**を選択します。
2. 展開テンプレートページでテンプレートを選択し、**重複**をクリックします。
3. テンプレートの新しい名前を入力し、**適用**をクリックします。テンプレートの名前は一意である必要があります。

展開テンプレートの削除

展開テンプレートを削除するには、以下を行います。

1. Dell Management Center で、**展開 → 展開テンプレート**を選択します。
2. **展開テンプレート**ページでテンプレートを選択し、**削除**をクリックします。
3. メッセージボックスで **削除**をクリックして、テンプレートを削除するか、**キャンセル**をクリックして取り消します。

展開テンプレート名の変更

展開テンプレート名を変更するには、以下を行います。

1. Dell Management Center で、**展開 → 展開テンプレート**を選択します。
2. **展開テンプレート**ページでテンプレートを選択し、**名前の変更**をクリックします。
3. テンプレートの新しい名前を入力し、**適用**をクリックします。テンプレートの名前は一意である必要があります。
4. すべての展開テンプレートを表示するには、**Dell Management Center** で **展開 → 展開テンプレート** を選択して、**更新**をクリックします。

展開ウィザードの実行

展開ウィザードは、以下のベアメタルサーバー展開プロセスを順次ガイドします。

- 未展開サーバーの選択。

ハイパーバイザーを展開する場合、最低 1 GB を保存できる内蔵デュアル SD モジュールに展開することができます。内蔵デュアル SD モジュールは、ハイパーバイザーを OpenManage Integration for VMware vCenter で展開する前に、BIOS で有効化されている必要があります。

- 展開テンプレート（ハードウェアおよびハイパーバイザープロファイルの組み合わせ）の使用。
- グローバル設定のセットアップ。このページでは、ハイパーバイザーをハードディスクまたは内蔵デュアル SD モジュールのどちらに展開するか選択できます。
- 展開サーバーに対する識別情報の割り当て。
- 各サーバーへの希望する接続プロファイルの照合。
- サーバー展開ジョブ実行のスケジュール。
- 展開ジョブを管理できるジョブキューの表示。

メモ: ハードウェアプロファイルのみを展開する場合は、新規グローバル設定、サーバー識別情報、および接続プロファイルページを省略して、直接ジョブのスケジュールページへ進みます。

メモ: 試用/評価用ライセンスについて、ライセンスの有効期限が残っている限り、展開ウィザードを使用できます。

関連タスク:

- 展開ウィザード手順 1: サーバーの選択
- 展開ウィザード手順 2: 展開テンプレート
- 展開ウィザード手順 3: グローバル設定
- 導入ウィザード手順 4: サーバー識別情報
- 展開ウィザード手順 5: 接続プロファイル
- 展開ウィザード手順 6: ジョブのスケジュール

展開ウィザード - 手順 1: サーバーの選択

このページでは、サーバーの展開を説明しています。ハイパーバイザーを内蔵デュアル SD モジュールに展開したい場合、このページにそのオプションが使用可能かどうか表示されます。内蔵デュアル SD モジュールの詳細については、「展開ウィザードの実行」を参照してください。展開したいサーバーのリストに手順 2 が表示されない場合、サーバーを手動で追加し、この手順がリストに表示されるようにできます。「手動によるサーバーの追加」を参照してください。
サーバーを選択するには、以下を行います。

1. **Dell Management Center** で **展開** → **展開ウィザード**を選択します。
2. **サーバーの選択**ウィンドウで非展開サーバーをこの展開ジョブに割り当てるには、チェックボックスを使用して **サーバー**を選択します。
3. **次へ**をクリックします。

手順 2 のタスクへ進むには、展開ウィザード手順 2 をクリックします。

展開ウィザード手順 2: 展開テンプレート

ハードウェアプロファイルへの展開は、ハイパーバイザー展開とは異なります。ハードウェアプロファイルへの展開については、「展開ウィザード手順 6」を参照してください。

メモ: 正しい展開には、ESX ISO に正しいドライバが備わっていることが必要です。より新しい Dell システムでは、すべての必要な Dell ドライバが含まれる Dell カスタム ISO イメージが必要になる可能性があります。ESX 4.1 はより新しい Dell システムでは動作しない可能性があり、Dell から入手可能なカスタム ISO を備えていない可能性があります。

展開テンプレートを選択するには、以下を行います。

1. 展開テンプレートは、以下のように 1 つまたは多くの方法で展開テンプレートを選択 / 作成します。
   - **使用可能なテンプレート**で既存の展開テンプレートを選択します。選択したテンプレートに対する情報が右ペインに表示されます。
   - 既存の展開テンプレートを選択し、**編集**をクリックして 1 つまたは両方の関連プロファイルを変更します。
   - **新規作成**をクリックして、新しいテンプレートを定義します。
2. 次のいずれか 1 つを選択します。
   - ハードウェアプロファイルへの展開には、**次へ**をクリックし、展開ウィザード手順 6 に進みます。
   - ハイパーバイザープロファイルへの展開には、**次へ**をクリックし、展開ウィザード手順 3 に進みます。

展開ウィザード手順 3: グローバル設定

ハイパーバイザーをハードディスクドライブまたは内蔵デュアル SD モジュールのいずれかに展開できます。少なくとも選択されたサーバーの 1 台で内蔵デュアル SD モジュールが使用できる場合は、内蔵デュアル SD モジュールオプションボタンが有効となります。ドロップダウンリストは内蔵デュアル SD モジュールオプションボタンが選択されるまで無効となっています。オプションボタンは、ドロップダウンリストでの有効 / 無効を切り替えます。

1. グローバル設定ページで、ハイパーバイザーをインストールするには、以下の展開ターゲットの 1 つを選択します。
   - ハードディスク
     ハードディスクに展開する場合は、このオプションをクリックします。
   - 内蔵デュアル SD モジュール
     内蔵デュアル SD モジュールに展開する場合は、このオプションをクリックして **使用可能な内蔵デュアル SD モジュールのないサーバーの最初のハードディスクにハイパーザイザを展開します。**チェックボックスを選択します。これによって、ハイパーバイザーが当該システムの最初のディスクに展開されます。

     注意: ディスクドライブのすべてのデータは消去されます!

     選択されたサーバーのどれもが内蔵デュアル SD モジュールに対応していない場合、または内蔵デュアル SD モジュールが展開時にない場合、それらのサーバーへの展開は省略され、展開ジョブは次のサーバーに進みます。
2. **次へ**をクリックします。
   手順 4 のタスクに進むには、「展開ウィザード手順 4：サーバー識別情報」をクリックします。

導入ウィザード手順 4: サーバー識別情報

サーバー識別情報は、2 つの方法で提供することができます。

- ネットワーク情報を入力します（IP アドレス、サブネットマスクおよびゲートウェイ）。ホスト名の完全修飾ドメイン名は必須です。FQDN での *localhost* の使用はサポートされていません。FQDN はホストを vCenter に追加する場合に使用します。
- 動的ホスト構成プロトコル（DHCP）を使用して IP アドレス、サブネットマスク、ゲートウェイ IP、ホスト名および優先 / 代替え DNS サーバーを設定します。 ホストを vCenter に追加する場合、DHCP が割り当てる IP アドレスが使用されます。DHCP を使用する場合、選択された NIC MAC アドレスには IP 予約を使うことを強くお勧めします。

メモ: ホスト名には、 localhost ではなく完全修飾ドメイン名（FQDN）を使用します。ESXi 5.1 以降では、localhost という値は OpenManage Integration for VMware vCenter がホストから送信されるイベントを処理する際の障害となります。IP アドレスを FQDN に解決する DNS の記録を作成します。ESXi 5.1 からの SNMP アラートが正しく識別されるよう、DNS サーバーが逆引き要求に対応するように設定します。 導入ジョブのスケジュールが実行される前に、DHCP 予約および DNS ホスト名が設定されて検証されている必要があります。

この画面は VLAN ID を指定するオプションを提供します。VLAN ID が提供されると、導入の際にハイパーバイザーの管理インタフェースに適用され、すべてのトラフィックがその VLAN ID でタグ付けされます。

サーバーを識別するには、以下を行います。

1. サーバー ID は導入されたサーバーに新しい名前とネットワーク識別情報を割り当てます。ファームウェア、BIOS に関する最低要件を満たさない、またはその他の問題があるサーバーのリストを表示するには、**非対応サーバー** をクリックします。
2. 詳細情報については、**詳細**をクリックします。
3. システムがアップデートされたら、**対応のチェック**をクリックし、再テストを行い問題解決を検証します。このリストを更新するには、**更新**をクリックし、**すべてのテストを中止**をクリックしてテストを取り消します。
4. 個別サーバー情報を表示するには、 **^** をクリックして導入します。
5. **ホスト名と NIC** でサーバーの **完全修飾ホスト名**を入力します。
6. **NIC 管理タスク用** ドロップダウンリストで、サーバー管理に使用する NIC を選択します。
7. **IP アドレス**、**サブネットマスク**およびその他のネットワーク情報を入力するか、あるいは、**DHCP を使用して取得**チェックボックスを選択します。
8. VLAN ID を必要とするネットワークに導入する場合、VLAN のチェックボックスを選択してから VLAN ID を入力します。

   VLAN ID には、1～4094 の数字を使用します。VLAN ID 0 はフレームの優先順位タグ用に予約されています。
9. 導入するすべてのサーバーについてこれを繰り返すか、**選択したすべてのサーバーに設定を適用します** チェックボックスを選択します。
10. **次へ** をクリックします。

    手順 5 のタスクへ進むには、「導入ウィザード手順 5」をクリックします。

展開ウィザード手順 5: 接続プロファイル

接続プロファイルは、ホストの接続資格情報を iDRAC またはホストルートの資格情報と関連付けることにより、その接続資格情報を確立するために使われます。接続プロファイルウィンドウでは以下ができます。

- 現在の接続プロファイルの表示または編集
- 接続プロファイルの削除
- vCenter ホストの変更を反映するための接続プロファイルリストの更新

接続プロファイルを作成するには、以下を行います。

1. 接続プロファイルは展開ジョブが完了すると、自動的にサーバーを接続プロファイルに割り当てます。

   接続プロファイルを選択したら、 **次へ**をクリックします。
2. **すべてのサーバーを同じ接続プロファイルに割り当てる**オプションボタンを選択し、接続プロファイルをドロップダウンリストから選択し、すべてのサーバーを同じ既存プロファイルに割り当てます。
3. 新しいプロファイルを作成するには、**新規**をクリックします。選択したプロファイルの表示または編集を行うには、**表示 / 編集**をクリックします。
4. 選択された接続プロファイルを表示するには、**表示**をクリックします。
5. **各サーバーの接続プロファイルの選択**オプションボタンを選択し、ドロップダウンリストから各サーバーの接続プロファイルを選択します。

6. 接続プロファイルを選択したら、**次へ**をクリックします。
   手順 6 のタスクへ進むには、「展開ウィザード手順 6」をクリックします。

展開ウィザード手順 6: ジョブのスケジュール

スケジュールは、展開ジョブのスケジュールを設定します。展開ジョブの実行時期を設定するには、次のようなオプションがあります : ただちに実行、選択した日付と時刻に展開ジョブを実行するようスケジュール、展開ジョブを保留し手動で開始する
スケジュールを設定するには、以下を行います。

1. 日付と時刻を入力していつ展開ジョブを実行するか決定します。
   a) **サーバーの展開スケジュールの設定**をクリックします。
   b) カレンダーコントロールを使用して日付を選択します。
   c) 時刻を入力します。
      * ただちに: **今すぐサーバーを展開**をクリックします。
      * ジョブの延期: **展開ジョブの作成**をクリックします。
      * 保留: このオプションではスケジュールだけが変更でき、その他すべての展開ジョブオプションは変更できません。
2. **ジョブ名**と **ジョブの説明** を入力します。
3. **Finish（終了）**をクリックします。
4. これで展開ウィザードが終了したので、**ジョブキュー**を使って展開ジョブを管理することができます。
5. ウィザードを完了させるためにファームウェアアップデートが必要な、非対応サーバーのリストを表示するには、**非対応サーバー**をクリックします。

関連タスク:

- 展開ジョブキューを使用した展開ジョブの管理

ジョブキューの理解

ジョブキューは、サーバー展開およびインベントリ検索ジョブを管理します。それには以下が含まれます。

- 提出されたサーバー展開ジョブの表示。
- 展開ジョブまたはインベントリ / 保証履歴キューの更新
- 現在の vCenter にある Dell サーバー属性をアップデートするためのインベントリジョブのスケジュール。
- 展開ジョブキュー項目のパージ。
- クラスタおよびデータベースのためのファームウェアアップデートの管理。

メモ: インベントリ / 保証に最新情報が含まれていることを確認するため、最低 1 週間に 1 度は、インベントリ / 保証ジョブの実行をスケジュールします。インベントリ / 保証ジョブは最低限のリソースしか消費しないので、ホストパフォーマンスの低下はもたらしません。

このページのタスクには、以下が含まれます。

- 展開ジョブキューの使用による展開ジョブの管理
- インベントリジョブの実行
- インベントリジョブスケジュールの変更
- クラスタおよびデータセンターのためのファームウェアアップデートステータスの表示

展開ジョブキューの使用による展開ジョブの管理

展開ジョブキューを使用して展開ジョブを管理するには、以下を行います。

1. **Dell Management Center** で**ジョブキュー → 展開ジョブ**を選択します。
2. **展開ジョブの詳細**をアップデートするには、**更新**をクリックします。
3. 展開ジョブに含まれるサーバーの詳細情報を含む展開ジョブの詳細ダイアログを表示するには、**詳細**をクリックします。これにより、以下の詳細が表示されます。
   - サービスタグ
   - iDRAC の IP アドレス
   - サーバーステータス
   - 警告の発生状況
   - 展開ジョブの詳細
   - 開始および終了時刻

   ダイアログテーブルの各項目の完全な情報を表示するには、カーソルを項目に合わせるとさらにテキストポップアップが表示されます。
4. 選択されたジョブを保留し、またはアップデートされたスケジュールを入力するには、**変更**をクリックします。
5. 展開ジョブを中止するには、**中止**をクリックします。
6. メッセージが表示されたら、**ジョブを中止する** をクリックして中止するか、**ジョブを中止しない**をクリックして取り消します。

   メモ: 進行中の展開ジョブは中止できません。
7. 展開ジョブキューのパージウィンドウを表示するには、**パージジョブのキュー**をクリックします。**日付とジョブステータスより古い**を選択して、**適用**をクリックします。選択されたジョブはキューから消去されます。

手動によるサーバーの追加

検出プロセスで追加されなかったサーバーは、手動で追加することができます。サーバーは追加されると、展開ウィザードのサーバーリストに表示されます。

1. Dell Management Center **展開**で、**展開ウィザード**をクリックします。
2. **サーバーの選択**タブで、**サーバーの追加**をクリックします。
3. **サーバーの追加**ダイアログボックスで、以下を行います。
   a) **iDRAC IP アドレス**テキストボックスに iDRAC IP アドレスを入力します。
   b) **ユーザー名**テキストボックスにユーザー名を入力します。
   c) **Password**（パスワード）テキストボックスにパスワードを入力します。
4. **サーバーの追加**をクリックします。これには数分かかることがあります。

ベアメタルサーバーの取り外し

自動検出または手動で追加されたサーバーは、手動で取り外すことができます。

1. Dell Management Center **展開**で、**展開ウィザード**をクリックします。
2. **サーバーの選択** タブで、**サーバーの削除**をクリックします。
3. **サーバーの削除**ダイアログボックスで、取り外すサーバーのチェックボックスを選択します。
4. **選択したサーバーの削除**をクリックします。
5. **サーバーの選択**タブで、テーブルに記載されているサーバーを表示し、取り外されたことを確認します。

6

コンソール管理

OpenManage Integration for VMware vCenter とその仮想環境の管理は、2 つの追加管理ポータルを使って行います。

- ウェブベース管理コンソール
- 個別サーバーのコンソールビュー（アプライアンス仮想マシンコンソール）。

これら 2 つのポータルを使用して、vCenter 管理のためのグローバル設定、OpenManage Integration for VMware vCenter データベースのバックアップと復元、およびリセット / 再起動アクションを、すべての vCenter インスタンスにわたって入力、使用することができます。

ウェブベース管理コンソール

ウェブベース管理コンソールはいくつかの主要機能を提供します。それは、vCenter サーバーの登録および管理、仮想アプライアンスの管理、グローバル vCenter 警告の設定、および設定のバックアップと復元です。

vCenter サーバー接続の管理

管理コンソールの alertvCenter 登録ウィンドウで、vCenter サーバーを登録してライセンスをアップロードまたは購入することができます。デモライセンスを使用している場合、今すぐ購入リンクが表示され、複数ホストを管理するための完全バージョンのライセンスを購入することができます。この項では、サーバーの変更、アップデートおよび登録の取り消しを行うこともできます。

関連タスク:

- vCenter サーバーの登録
  - 管理者 vCenter ログインの変更
  - 登録 vCenter の SSL 証明のアップデート
  - vCenter から Dell OpenManage Integration for VMware vCenter のアンインストール
- 管理コンソールを使った OpenManage Integration for VMware vCenter ライセンスのアップロード

vCenter サーバーの登録

OpenManage Integration for VMware vCenter のインストール後、vCenter サーバーを OpenManage Integration for VMware vCenter に登録することができます。OpenManage Integration for VMware vCenter は、vCenter の動作に管理者ユーザーアカウントを使用します。OpenManage Integration for VMware vCenter はアプライアンスあたり 10 個の vCenter をサポートします。

1. OpenManage Integration for VMware vCenter の サマリ タブで、リンクを使って管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 新規サーバーを登録するには、左ペインで **VCENTER 登録**をクリックし、**新規 vCenter サーバーの登録**をクリックします。
4. **新規 vCenter の登録**ダイアログボックスの **vCenter 名**で次を行います。

a) **vCenter サーバー IP またはホスト名** テキストボックスに vCenter IP アドレスまたはホスト名を入力します。
b) **説明** テキストボックスに、オプションで説明を入力します。

5. **管理者ユーザーアカウント**で、次を行います。
a) **管理者ユーザー名**テキストボックスに管理者のユーザー名を入力します。
b) **Password**（パスワード）テキストボックスにパスワードを入力します。
c) **パスワードの確認** テキストボックスにパスワードを再度入力します。

6. **Register**（登録）をクリックします。

vCenter 管理者ログインの変更

1. OpenManage Integration for VMware vCenter の サマリ タブで、リンクを使って管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 左ペインで **VCENTER の登録**をクリックします。登録された vCenter が表に表示されます。**管理者アカウントの変更** ウィンドウを開くには、**資格情報**で、**変更**をクリックします。
4. vCenter 管理者の **ユーザー名**、**パスワード**および **パスワードの確認**を入力します。両パスワードは一致する必要があります。
5. パスワードを変更するには、**適用**をクリックします。または変更を取り消すには、**キャンセル**をクリックします。

登録された vCenter サーバーの SSL 証明書のアップデート

vCenter サーバーの SSL 証明書が変更された場合、OpenManage Integration for VMware vCenter に新しい証明書をインポートするため、次の手順を実行します。OpenManage Integration for VMware vCenter はこの証明書を使用して、通信相手の vCenter サーバーが正しい vCenter サーバーであって、偽装でないことを確認します。

OpenManage Integration for VMware vCenter は、2048 ビットキー長の RSA 暗号化標準を使って証明書署名要求（CSR）を作成するために openssl API を使用します。OpenManage Integration for VMware vCenter を使用して生成された CSR は、信頼された証明機関からデジタル署名付き証明書を取得するのに使用されます。
OpenManage Integration for VMware vCenter は、安全な通信のためにデジタル証明書を使って Web サーバー上で SSL を有効にします。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示された設定する仮想マシンの **管理コンソール URL** を入力、または **Dell Management Console → 設定ページ** からのリンクを使用します。URL は次のフォーマット **https://<ApplianceIPAddress>** を使用し、大文字小文字は区別されません。
2. 左ペインで **VCENTER の登録**をクリックします。登録された vCenter がテーブルに表示されます。証明書をアップデートするには、**アップデート**をクリックします。

VMware vCenter からの OpenManage Integration for VMware vCenter のアンインストール

OpenManage Integration for VMware vCenter を削除するには、管理コンソールを使って vCenter サーバーから登録解除する必要があります。

1. OpenManage Integration for VMware vCenter の サマリ タブで、リンクを使って管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. **vCenter 登録** ページの vCenter サーバー表の下で、**登録解除** をクリックして OpenManage Integration for VMware vCenter の登録を解除します。
vCenter が複数存在する場合があるので、正しい vCenter を選択するようにしてください。
4. 登録の取り消しを確認する **vCenter の登録解除** ダイアログボックスで **登録解除** をクリックします。

OpenManage Integration for VMware vCenter ライセンスを管理コンソールにアップロードする

1. OpenManage Integration for VMware vCenter の サマリ タブで、リンクを使って管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 左ペインで、**VCENTER の登録**をクリックします。登録された vCenters がテーブルに表示されます。アップロードライセンスダイアログボックスを表示するには、**ライセンスのアップロード**をクリックします。
4. ライセンスファイルに移動するには、**参照** ボタンをクリックし、ライセンスファイルに移動したら **アップロード** をクリックします。

メモ: ライセンスファイルを変更または編集すると、アプライアンスはこれを壊れたとみなし、ファイルが使用できなくなります。ホストの追加が必要な時はライセンスを追加することができます。上記プロセスに従ってライセンスを追加してください。

メモ: 正常にインベントリされた第 11 世代および第 12 世代のサーバーの数が、購入済みライセンスの数と同じ場合、新規または既存の接続プロファイルへの第 9、または 10 世代のサーバーの追加はブロックされるため、既存の接続プロファイルを編集して第 11 または 12 世代サーバーを削除し、代りに第 10 または 9 世代サーバーを追加します。削除した第 11、12 世代サーバーには新規接続プロファイルを作成してください。

仮想アプライアンス管理

仮想アプライアンス管理には、OpenManage Integration for VMware vCenter ネットワーク、バージョン、NTP、および HTTPS 情報が含まれ、管理者は次の操作を行うことができます。

- 仮想アプライアンスの再スタート
- 仮想アプライアンスのアップデート、およびアップデートリポジトリロケーションの設定
- アプライアンスログイン情報が含まれるトラブルシューティングバンドルの生成
- ネットワークタイムプロトコル（NTP）設定の入力
- HTTPS 証明のアップロードおよび管理

関連タスク:

- 仮想アプライアンスの再スタート
- リポジトリロケーションのアップデートおよびアプライアンスのアップデート
- トラブルシューティングバンドルのダウンロード
- NTP サーバーの設定

仮想アプライアンスの再スタート

仮想アプライアンスを再スタートするには、以下を行います。

メモ: 仮想アプライアンスを再スタートさせると、管理コンソールからログアウトされ、OpenManage Integration for VMware vCenter は、仮想アプライアンスとそのサービスがアクティブになるまで使用不可能となります。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示された設定する仮想マシンの **管理コンソール URL** を入力、または **Dell Management Console → 設定ページ** からのリンクを使用します。URL は次のフォーマット **https://<ApplianceIPAddress>** を使用し、大文字小文字は区別されません。
2. 左ペインで **アプライアンス管理** をクリックします。
3. OpenManage Integration for VMware vCenter を再スタートするには、**仮想アプライアンスの再スタート**をクリックします。

4. **仮想アプライアンスの再スタート**ダイアログボックスで、仮想アプライアンスを再スタートするには **適用**をクリックするか、または **キャンセル**をクリックして取り消します。

リポジトリの場所と仮想アプライアンスのアップデート

仮想アプライアンスのアップデート前にバックアップを実行し、すべてのデータを保護します。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示された設定する仮想マシンの **管理コンソール URL** を入力、または **Dell Management Console → 設定ページ** からのリンクを使用します。URL は次のフォーマット **https://<ApplianceIPAddress>** を使用し、大文字小文字は区別されません。
2. 左ペインで **アプライアンス管理** をクリックします。
3. アプライアンスのアップデートの横の **編集** をクリックします。
4. **アプライアンスアップデート** ウィンドウに **リポジトリの場所の URL** を入力し、**適用** をクリックします。

   メモ: アップデートロケーションが、Dell FTP サイトなどの外部ネットワークにある場合、HTTP プロキシエリアの下にプロキシを入力する必要があります。

仮想アプライアンスソフトウェアバージョンのアップデート

データの喪失を予防するため、ソフトウェアアップデートの開始前にアプライアンスのバックアップを実行します。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示された設定する仮想マシンの **管理コンソール URL** を入力、または **Dell Management Console → 設定** ページからのリンクを使用します。URL は次のフォーマットを使用し、大文字小文字が区別されます。

   https://<ApplianceIPAddress>
2. 左ペインで、 **アプライアンスメンテナンス** をクリックします。
3. 仮想アプライアンスを **アプライアンスアップデート** にリストされているソフトウェアバージョンにアップデートするには、**仮想アプライアンスのアップデート** をクリックします。
4. **アプライアンスのアップデート** ダイアログボックスには、現行で使用可能なバージョンがリストされています。アップデートを開始するには、**アップデート** をクリックします。
5. システムはロックダウンし、メンテナンスモードになります。アップデートが完了すると、アプライアンスページに新たにインストールされたバージョンが表示されます。

トラブルシューティングバンドルのダウンロード

この情報を使用してトラブルシューティング問題の参考にしたり、技術サポートへ送付します。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示された設定する仮想マシンの **管理コンソール URL** を入力、または **Dell Management Console → 設定** ページからのリンクを使用します。URL は次のフォーマットを使用し、大文字小文字は区別されません。

   https://<ApplianceIPAddress>
2. 左ペインで **アプライアンス管理** をクリックします。
3. トラブルシューティングバンドルのダイアログボックスを表示するには、**トラブルシューティングバンドルの作成**をクリックします。
4. 仮想アプライアンスログ情報を含む Zip ファイルを開くか保存するには、**トラブルシューティングバンドルのダウンロード**リンクをクリックします。
5. 終了するには、**閉じる**をクリックします。

HTTP プロキシの設定

HTTP プロキシ設定は、管理コンソールまたは Dell Management Console を使用して設定できます。

1. OpenManage Integration for VMware vCenter の サマリ タブで、リンクを使って管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 左ペインで **アプライアンス管理** をクリックします。
4. **アプライアンス管理**ページで **HTTP プロキシ設定**にスクロールし、**編集**をクリックします。
5. **編集**ページで以下を行います。
   a) HTTP プロキシ設定の使用を有効化するには、**HTTP プロキシ設定を使用**の横の **有効**を選択します。
   b) **プロキシサーバーのアドレス**テキストボックスにプロキシサーバーアドレスを入力します。
   c) **プロキシサーバーポート**テキストボックスにプロキシサーバーポートを入力します。
   d) プロキシ資格情報を使用するには、**プロキシ資格情報を使用する**の横で **はい**を選択します。
   e) 資格情報を使用している場合、**ユーザー名**テキストボックスにユーザー名を入力します。
   f) **パスワード**テキストボックスにパスワードをタイプします。
6. **適用** をクリックします。

NTP サーバーの設定

仮想アプライアンスクロックを NTP サーバーのそれと同期させるには、ネットワークタイムプロトコル（NTP）を使用します。

1. OpenManage Integration for VMware vCenter の サマリ タブで、このリンクを使って管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 左ペインで **アプライアンス管理** をクリックします。
4. **NTP 用の編集**をクリックします。
5. **有効**チェックボックスをクリックします。 **ホスト名**または **IP アドレス** を **プリファランス**または **セカンダリ NTP サーバー**に入力し、**適用**をクリックします。
6. 終了するには、**キャンセル**をクリックします。

証明書署名要求の生成

新規証明書署名要求を生成することは、以前作成された CSR で作成された証明書がアプライアンスにアップロードされることを防ぎます。

1. OpenManage Integration for VMware vCenter の サマリ タブで、このリンクを使って管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 左ペインで **アプライアンス管理** をクリックします。
4. **HTTPS 証明のための証明書署名要求の生成**をクリックします。新規の要求が生成されると、以前の CSR によって作成された証明書はアプライアンスにアップロードできなくなりますというメッセージが表示されます。要求を続けるには、**続行**をクリックします。または、 **キャンセル**をクリックして取り消します。
5. 要求の **コモンネーム**、**組織名**、**部署名**、**市区町村名**、**都道府県名**、**国名** および **E-メール** を入力します。**続行** をクリックします。
6. **ダウンロード** をクリックして、生成された HTTPS 証明書をアクセスできる場所に保存します。

HTTPS 証明書のアップロード

HTTPS 証明書は、仮想アプライアンスとホストシステム間のセキュアな通信に使用することができます。このタイプのセキュアな通信を設定するには、証明書署名要求を認証局に送り、その結果の証明書を管理コンソールを使用してアップロードする必要があります。また、自己署名によるデフォルト証明書もあり、セキュア通信に使用できます。この証明書は各インストール固有のものです。

メモ: 証明書のアップロードには、Microsoft Internet Explorer または Firefox を使用できます。

1. OpenManage Integration for VMware vCenter の サマリ タブで、このリンクを使って管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 左ペインで **アプライアンス管理** をクリックします。
4. **HTTPS 証明用の証明書のアップロード** をクリックします。
5. **証明書のアップロード**ダイアログボックスで、**OK** をクリックします。
6. アップロードする証明書を選択するには、**参照** をクリックして、**アップロード** をクリックします。
7. アップロードを中止するには、**キャンセル** をクリックします。

   メモ: 証明書は、PEM フォーマットを使用する必要があります。

デフォルト HTTPS 証明書の復元

1. OpenManage Integration for VMware vCenter の サマリ タブで、このリンクを使って管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 左ペインで **アプライアンス管理** をクリックします。
4. **HTTPS 証明用のデフォルト証明書の復元**をクリックします。
5. デフォルト証明書の復元ダイアログボックスで **適用** をクリックします。

グローバルアラートの設定

アラート管理によって、すべての vCenter インスタンスに対するアラートの保存方法のグローバル設定を入力できます。

1. OpenManage Integration for VMware vCenter の サマリ タブで、このリンクを使って管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 左ペインで **アラート管理** をクリックします。新規の vCenter アラート設定を入力するには、**編集** をクリックします。
4. 次の項目に対する数字の値を入力します。
   - 最大アラート数
   - アラートの保持日数
   - 重複アラートのタイムアウト時間（秒）
5. 設定を保存するには **適用** をクリックするか、**キャンセル** をクリックして取り消します。

バックアップおよび復元の管理

バックアップおよび復元の管理は、管理コンソールで行われます。このページのタスクには以下が含まれます。

- バックアップおよび復元の設定
- 自動バックアップのスケジュール
- 即時のバックアップの実行
- バックアップからのデータベースの復元

バックアップおよび復元の設定

バックアップおよび復元機能は、OpenManage Integration for VMware vCenter データベースをリモートロケーションにバックアップして、後日それに基づく復元を可能にします。このバックアップには、プロファイル、テンプレートおよびホスト情報が含まれます。データの喪失に備えるため、自動バックアップをスケジュールすることを推奨します。この手順のあと、バックアップスケジュールを設定する必要があります。

バックアップおよび復元を設定するには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示された設定する仮想マシンの **管理コンソール URL** を入力、または **Dell Management Console → 設定** ページからのリンクを使用します。URL は次のフォーマットを使用し、大文字小文字は区別されません。

   https://<ApplianceIPAddress>
2. 左ペインで、**バックアップと復元**をクリックします。
3. 現在のバックアップと復元設定を編集するには、**編集**をクリックします。
4. **設定と詳細**ページで、以下を行います。
   a) **バックアップの場所**テキストボックスにバックアップファイルへのパスをタイプします。
   b) **ユーザー名**テキストボックスにユーザー名をタイプします。
   c) **パスワード**テキストボックスにパスワードをタイプします。
   d) **バックアップを暗号化するために使用するパスワード**の下のテキストボックスに、暗号化パスワードをタイプします。
   暗号化パスワードには、英数字および次の特殊文字を使用できます：!@#$%*。長さの制限はありません。
   e) **パスワードの確認**テキストボックスに暗号化パスワードを再度入力します。
5. これらの設定を保存するには、**適用**をクリックします。
6. バックアップスケジュールを設定します。詳細は、「自動バックアップのスケジュール」を参照してください。

自動バックアップのスケジュール

これはバックアップおよび復元の第 2 部です。バックアップロケーションと資格情報に関する詳細は、「バックアップおよび復元の設定」を参照してください。

自動バックアップのスケジュールには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示された設定する仮想マシンの **管理コンソール URL** を入力、または **Dell Management Console → 設定** ページからのリンクを使用します。URL は次のフォーマットを使用し、大文字小文字は区別されません。

   https://<appliance IP address>
2. 左ペインで、**バックアップと復元**をクリックします。
3. バックアップおよび復元の設定を編集するには、**編集自動バックアップスケジュール** をクリックします（これによってフィールドがアクティブになります）。
4. バックアップを有効化するには、 **有効**をクリックします。
5. バックアップを実行したい曜日のチェックボックスを選択します。
6. **バックアップ時刻（24 時間フォーマット、HH:mm）** テキストボックスに時刻を HH:mm フォーマットで入力します。
   次のバックアップに次にスケジュールされたバックアップの日付と時刻が表示されます。

7. **適用** をクリックします。

即時のバックアップの実行

即時のバックアップを実行するには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示された設定する仮想マシンの **管理コンソール URL** を入力、または **Dell Management Console → 設定** ページからのリンクを使用します。URL は次のフォーマットを使用し、大文字小文字は区別されません。

   https://<ApplianceIPAddress>
2. 左ペインで、**バックアップと復元**をクリックします。
3. **今すぐバックアップ**をクリックします。
4. バックアップ設定からロケーションと暗号化パスワードを使用するには、**今すぐバックアップ**ダイアログボックスでそのチェックボックスを選択します。
5. **バックアップの場所**、**ユーザー名**、**パスワード**、および**暗号化パスワード**を入力します。

   暗号化パスワードには、英数字および次の特殊文字を使用できます：**!@#$%***。長さの制限はありません。
6. **バックアップ**をクリックします。

バックアップからのデータベースの復元

メモ: 復元の操作では、作業完了後、仮想アプライアンスを再起動させます。

バックアップからデータベースを復元するには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示された設定する仮想マシンの **管理コンソール URL** を入力、または **Dell Management Console → 設定** ページからのリンクを使用します。URL は次のフォーマットを使用し、大文字小文字は区別されません。

   https://<ApplianceIPAddress>
2. 左ペインで、**バックアップおよび復元**をクリックすると、現在のバックアップおよび復元設定が表示されます。
3. **今すぐ復元**をクリックします。
4. 今すぐ復元ダイアログボックスで、**ファイルロケーション（CIFS / NFS フォーマット）**を入力します。
5. バックアップファイルの **ユーザー名**、**パスワード**および**暗号化パスワード**を入力します。

   暗号化パスワードには、英数字および次の特殊文字を使用できます：**!@#$%***。長さの制限はありません。
6. 変更を保存するには、**適用** をクリックします。

   適用をクリックすると、アプライアンスは再起動または再スタートします。

vSphere ウェブクライアントコンソールの理解

コンソールは、仮想マシンの vSphere ウェブクライアント内にあります。このコンソールは管理コンソールと連動します。このコンソールには、次の機能があります。

- ネットワークの設定構成
- 仮想アプライアンスパスワードの変更
- ローカルタイムゾーンの設定
- 仮想アプライアンスの再起動
- 仮想アプライアンスの工場出荷時設定へのリセット

- コンソールの更新

矢印キーを使用して上下に移動します。希望のオプションを選択して **<ENTER>** を押します。コンソール画面にアクセスすると、カーソルは VMware vSphere Client に制御されます。カーソルの制御をエスケープするには、**<CTRL> + <ALT>** を押してください。

ネットワークの設定

ネットワークの設定変更は、vSphere クライアントのコンソールタブで行います。

ネットワークの設定には、以下を行います。

1. **vSphere クライアント**で、OpenManage Integration for VMware vCenter を選択して**コンソール** タブをクリックします。
2. **コンソール**ウィンドウで、**ネットワークの設定**を選択し、**<ENTER>** を押します。
3. **デバイスの編集**または **DNS の編集** 構成下で望ましいネットワーク設定を入力し、**保存して終了**をクリックします。変更を中止するには、**終了**をクリックします。

仮想アプライアンスパスワードの変更

仮想アプライアンスパスワードは、vSphere クライアントでコンソールタブを使用して変更します。

仮想アプライアンスパスワードを変更するには、以下を行います。

1. vSphere クライアントで、OpenManage Integration for VMware vCenter 仮想マシンを選択して**コンソール**タブをクリックします。
2. コンソールタブで、矢印キーを使って **管理パスワードの変更**を選択して、 **<ENTER>** を押します。
3. **現在の管理パスワード**を入力し、**<ENTER>** を押します。
   管理パスワードには、1 つの特殊文字、1 つの数字、1 つの大文字、1 つの小文字を含み、少なくとも 8 文字である必要があります。
4. **新規管理パスワードの入力**で新パスワードを入力し、**<ENTER>** を押します。
5. 新規パスワードを **管理パスワードを確認してください**テキストボックスに再度タイプし、**<ENTER>** を押します。これで管理パスワードは変更されました。

ローカルタイムゾーンの設定

ローカルタイムゾーンを設定するには、以下を行います。

メモ: 編集できるのはタイムゾーンだけで、現在の時刻と日付は編集できません。

1. **vSphere クライアント**で、OpenManage Integration for VMware vCenter 仮想マシンを選択して**コンソール** タブをクリックします。
2. **タイムゾーンの設定** を選択して **<ENTER>** を押します。
3. **タイムゾーンの選択** ウィンドウで、望ましいタイムゾーンを選択して、**OK** をクリックします。変更を取り消すには、**キャンセル** をクリックします。これでタイムゾーンがアップデートされました。

仮想アプライアンスの再起動

仮想アプライアンスを再起動するには、以下を行います。

1. **vSphere クライアント**で、OpenManage Integration for VMware vCenter 仮想マシンを選択して**コンソール**タブをクリックします。
2. **この仮想マシンを再起動**を選択し、 **<ENTER>** を押します。

3. 次のメッセージが表示されます。

   ```
   If there are any processes running on this appliance they will be
   terminated by this action. Are you sure you wish to do this?
   ```

4. 再起動するには、**y** を、取り消すには、**n** を入力します。これでアプライアンスは再起動されました。

仮想アプライアンスの工場出荷時設定へのリセット

仮想アプライアンスを工場出荷時設定へリセットするには、以下を行います。

1. **vSphere クライアント** で、OpenManage Integration for VMware vCenter 仮想マシンを選択してから **コンソール** タブをクリックします。
2. **この仮想アプライアンスを工場出荷時設定にリセット**を選択して、**<ENTER>** を押します。
3. 次の通知が表示されます。

   ```
   This operation is completely Irreversible if you continue you will
   completely reset *this* appliance to its original settings. All changes you
   have made to this appliance will be Lost. Are you sure you wish to Reset
   this Appliance to Factory Settings?
   ```

4. リセットするには、**y** を入力します。または **n** で取り消します。アプライアンスは当初の工場出荷時設定にリセットされます。

   メモ: 仮想アプライアンスが工場出荷時設定にリセットされる場合、ネットワーク設定に加えられたアップデートは維持されます。この設定はリセットされません。

コンソールビューの更新

コンソールビューを更新するには、**更新**を選択して、**<ENTER>** を押します。

読み取り専用ユーザー役割

読み取り専用と呼ばれる、診断目的のシェルアクセス権を持つ、非特権ユーザー役割があります。読み取り専用ユーザーにはマウントを実行するための限定的な特権があり、読み取り専用ユーザーのパスワードは管理者と同じものに設定されます。

1.6/1.7 から 2.0 に移行するための移行パス

OpenManage Integration for VMware vCenter バージョン 2.0 は OVF リリースのみとなっています。旧バージョンからこのバージョンへの RPM アップデートパスはありません。旧バージョン（1.6 または 1.7）は、バックアップと復元パスを使用してバージョン 2.0 リリースに移行させることができます。また、移行パスはバージョン 1.6 と 1.7 のみでサポートされます。1.6 より前のバージョンをお持ちの場合は、OpenManage Integration for VMware vCenter バージョン 2.0 に移行する前に、お使いのアプライアンスを対応バージョンにアップグレードする必要があります。

旧バージョンから OpenManage Integration for VMware vCenter 2.0 バージョンに移行するには、次の手順を実行します。

1. 以前のリリースのデータベースのバックアップを行います。詳細に関しては、本ガイドの「**Managing Backup and Restore (**バックアップと復元の管理**)**」の項を参照してください。
2. vCenter から旧アプライアンスの電源を切ります。

   メモ:

   プラグインの登録は vCenter から解除しないでください。プラグインを vCenter から登録解除すると、プラグインによって vCenter に登録されたアラームのすべてが削除され、vCenter でアラームに対して行われたアクションなどのカスタマイズのすべてが削除されます。バックアップ後にすでにプラグインを登

録解除した場合の詳細については、本ガイドの「**バックアップ後に旧プラグインを登録解除した場合のリカバリ方法**」の項を参照してください。

3. OpenManage Integration バージョン 2.0 OVF を展開します。OVF の展開についての詳細は、本ガイドの「**vSphere Client を使用した OpenManage Integration for VMware vCenter OVF の展開**」の項を参照してください。
4. OpenManage Integration バージョン 2.0 アプライアンスに電源を入れます。
5. アプライアンスでネットワーク、タイムゾーンなどをセットアップします。新しい OpenManage Integration バージョン 2.0 アプライアンスの IP アドレスは、旧アプライアンスのものと同じにすることをお勧めします。ネットワーク詳細をセットアップするには、本ガイドの「**OpenManage Integration for VMware vCenter の登録とライセンスファイルのインポート**」の項を参照してください。
6. データベースを新規アプライアンスに復元します。詳細に関しては、本ガイドの「**バックアップからのデータベースの復元**」の項を参照してください。
7. 新しいライセンスファイルをアップロードします。詳細に関しては、『**OpenManage Integration Version 2.0 Quick Install Guide**』（OpenManage Integration バージョン 2.0 のクイックインストールガイド）にある「**Registering OpenManage Integration for VMware vCenter And Importing The License File**」（OpenManage Integration for VMware vCenter の登録とライセンスファイルのインポート）の項を参照してください。
8. アプライアンスを検証します。データベース移行が正常に行われたことを確認するための詳細については、本ガイドの「**インストールの検証**」を参照してください。
9. 登録された vCenter すべてでインベントリを実行します。

メモ:

アップグレード後は、プラグインによって管理されているホストのすべてで再度インベントリを実行することが推奨されます。オンデマンドでインベントリを実行するための手順に関する詳細は、「**インベントリジョブの実行**」を参照してください。

新しい OpenManage Integration バージョン 2.0 アプライアンスの IP アドレスが旧アプライアンスの IP アドレスから変更された場合、新しいアプライアンスをポイントするように SNMP トラップのトラップ送信先を設定する必要があります。第 12 世代サーバーでは、これはホスト上でインベントリを実行することによって修正されます。旧仕様に準拠する第 11 世代以前のホストでは、この IP 変更が非準拠として表示され、OMSA の設定が必要になります。ホストの準拠性を修正するための詳細に関しては、本ガイドの「**非準拠 vSphere ホストの修正ウィザードの実行**」を参照してください。

バックアップ後に旧プラグインを登録解除した場合のリカバリ方法

旧バージョンのデータベースのバックアップ取得後にプラグインの登録を解除した場合は、移行に進む前に次の手順を実行してください。

メモ: プラグインの登録解除により、プラグインによって登録済みアラームに行われたカスタマイズのすべてが削除されています。次の手順では、カスタマイズを復元することはできませんが、アラームをデフォルト状態で再登録します。

1. 本章の「**1.6/1.7 から 2.0 への移行のための移行パス**」の項の手順 3～5 を実行します。
2. 旧プラグインで以前登録したものと同じ vCenter にプラグインを登録します。
3. 本章の「**1.6/1.7 から 2.0 への移行のための移行パス**」の項の手順 6～9 に進み、移行を完了させます。詳細に関しては、『**OpenManage Integration Version 2.0 Quick Install Guide**』（OpenManage Integration バージョン 2.0 クイックインストールガイド）にある「**Migration Path to migrate from 1.6/1.7 to 2.0**」（1.6/1.7 から 2.0 への移行のための移行パス）の項を参照してください。

7

Troubleshooting

本項を使用してトラブルシューティングの問題解決を行ってください。本項は次の内容で構成されています。

よくあるお問い合わせ (FAQ)

本項には一般的な質問と解決策を記載しています。

OpenManage Integration for VMware vCenter を使用した、ファームウェアバージョン 13.5.2 の Intel ネットワークカードのアップデートはサポートされていません。

Dell PowerEdge 第 12 世代サーバーとファームウェアバージョン 13.5.2 の一部の Intel ネットワークカードには、既知の問題があります。このバージョンのファームウェアを搭載した Intel ネットワークカードの一部のモデルのアップデートは、このファームウェアのアップデートを Lifecycle Controller を使用して適用すると失敗します。このバージョンのファームウェアを使用しているユーザーは、オペレーティングシステムでネットワークドライバのソフトウェアをアップデートしてください。 Intel ネットワークカードのファームウェアのバージョンが 13.5.2 以外であれば、OpenManage Integration for VMware vCenter を使用してアップデートすることができます。詳細に関しては、http://en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx を参照してください。

メモ: メモ：1 対多のファームウェアアップデートを使用する場合、バージョン 13.5.2 の Intel ネットワークアダプタを選択しないでください。アップデートに失敗して、残りのサーバーからのアップデートによるアップデートタスクが停止します。

無効な DUP でファームウェアのアップデートを行おうとすると、ジョブのステータス LC に "FAILED" と表示されるのに何時間も vCenter コンソールが失敗もタイムアウトもしません。なぜこれが起こっていますか？

ファームウェアのアップデートに無効な DUP を選択すると、vCenter コンソールウィンドウに表示されるタスクのステータスは「In Progress」（進行中）のままですが、表示されるメッセージは失敗の理由に変わります。これは既知の VMware の欠陥で、今後のリリースの VMware vCenter で解決される予定です。

対応処置： このタスクを手動でキャンセルする必要があります。

対象バージョン：すべて

管理ポータルに、到達不能なアップデートリポジトリの場所が表示されたままになっています。

ユーザーが到達不能なアップデートリポジトリパスを提供している場合、エラーメッセージ、"Failed: Error while connecting to the URL …. " がアプライアンスのアップデートビューの上部に表示されますが、アップデートリポジトリパスがアップデート以前の値にクリアされていません。

対応処置： このページから別のページに移動して、ページが更新されることを確認します。

対象バージョン：すべて

アプライアンスの IP に DHCP を使用し、DNS 設定が上書きされると、なぜ、アプライアンスの再起動後に DNS 構成設定が元の設定に戻るのですか?

静的に割り当てられた DNS 設定が DHCP からの値に置き換えられる、既知の不具合です。これは、IP 設定の取得のために DHCP を使用して、DNS の値が静的に割り当てられた場合に発生します。DHCP のリースを更新するかアプライアンスを再起動すると、静的に割り当てられた DNS 設定は削除されます。対応処置として、DNS サーバーの設定が DHCP と異なる場合は、IP 設定を静的に割り当てます。

対象バージョン：すべて

1 対多のファームウェアアップデートを実行したときに、システムがメンテナンスモードに入らなかったのはなぜですか?

一部のファームウェアアップデートにはホストの再起動は必要ありません。 このような場合、ファームウェアのアップデートは、ホストをメンテナンスモードにすることなく実行されます。

PERC S300 ブートコントローラのあるサーバーで、ESX / ESXi の展開に失敗するのはなぜですか?

PERC S300 ブートコントローラを搭載した Dell PowerEdge サーバー上で異なる ESX/ESXi バージョンを使用して OpenManage Integration for VMware vCenter を展開すると、失敗します。カスタマイズされた Dell の ESX/ESXi オペレーティングシステムには PERC S300 ブートコントローラ用のドライバを搭載していないため、オペレーティングシステムのインストール中にブートコントローラ / HDD が認識されません。PERC S300 ブートコントローラを搭載したサーバーは、OpenManage Integration for VMware vCenter の展開をサポートしていません。

ファームウェアのリンクをクリックした後、なぜ通信エラーメッセージが表示されるのですか。

ネットワーク通信速度が低速（9600 bps）の場合、通信エラーメッセージが表示されます。このエラーメッセージは、OpenManage Integration for VMware vCenter の vSphere Client でファームウェアのリンクをクリックした時に表示されることがあります。これは、ソフトウェアインベントリリストの取得の試行中に接続がタイムアウトすると表示されます。このタイムアウトは Microsoft Internet Explorer によって開始されます。
Microsoft Internet Explorer のバージョン 9/10 では、デフォルトの「受信タイムアウト」値は 10 秒に設定されています。次のステップでこの問題を修正してください。

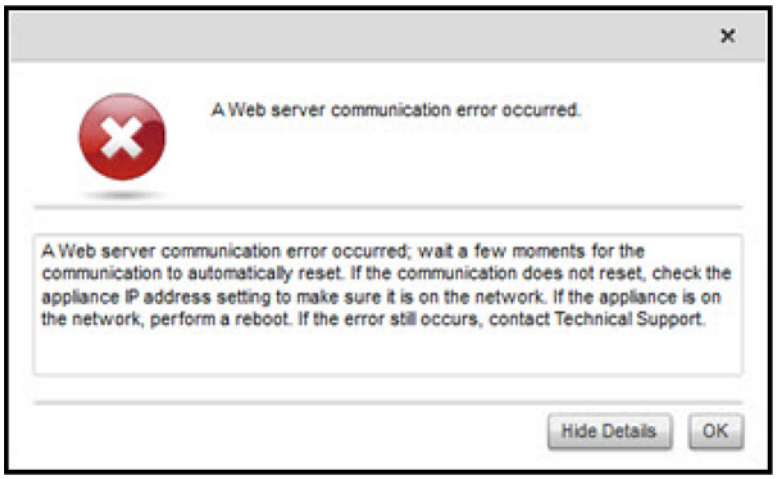

図 5. ファームウェアリンク通信エラー

1. Microsoft レジストリエディタ（Regedit）を開きます。
2. 次の場所に移動します。
   KHEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
3. 受信タイムアウトの DWORD 値を追加します。
4. 値を 30 秒（30000）に設定します（お使いの環境ではこれより大きい値にする必要のある場合もあります）。
5. Regedit を終了します。
6. Internet Explorer を再起動します。

   メモ: Internet Explorer ウィンドウを開くだけでは不十分です。Internet Explorer のブラウザを再スタートしてください。

OpenManage Integration for VMware vCenter で設定し SNMP トラップをサポートしているのは、どの世代の Dell サーバーですか?

OpenManage Integration for VMware vCenter は、第 12 世代より前の世代のサーバーで OMSA SNMP トラップをサポートし、第 12 世代のサーバーで iDRAC トラップをサポートしています。

OpenManage Integration for VMware vCenter は、リンクモードでの 4 つ以上の vCenter をどのようにサポートしていますか?

各仮想アプライアンスは、リンクモードで最大 3 つの vCenter をサポートします。10 より多い vCenter がある場合、vCenter 10 個ごとに、対応するライセンスを持つアプライアンスの新規インスタンスが必要です。

OpenManage Integration for VMware vCenter は、リンクモードの vCenter をサポートしていますか?

はい、OpenManage Integration for VMware vCenter は最大 10 個のリンクモードの vCenter をサポートしています。OpenManage Integration for VMware vCenter のリンクモードでの動作の詳細に関しては、www.Dell.com にあるホワイトペーパー、「*Dell Management Plug-in for VMware vCenter：リンクモードでの動作*」を参照してください。

OpenManage Integration for VMware vCenter ではどのようなポート設定が要求されますか?

メモ: Dell Management Center の準拠ウィンドウから利用できる*非準拠 vSphere ホストの修正*リンクを使用して OMSA エージェントを導入する場合、ESXi 5.0 以降のリリースで OpenManage Integration for VMware vCenter は httpClient サービスを開始してポート 8080 を有効にし、OMSA VIB をダウンロードおよびインストールします。OMSA のインストールが完了すると、サービスは自動的に停止し、ポートは閉じられます。

これらのポート設定は、OpenManage Integration for VMware vCenter 用です。

表 3. 仮想アプライアンスポート

ポート番号	プロトコル	ポートタイプ	最高暗号化レベル	方向	使用状況	設定可能
21	FTP	TCP	なし	出力	FTP コマンドクライアント	いいえ
53	DNS	TCP	なし	出力	DNS クライアント	いいえ
80	HTTP	TCP	なし	出力	Dell オンラインデータアクセス	いいえ
80	HTTP	TCP	なし	入力	管理コンソール	いいえ
162	SNMP エージェント	UDP	なし	入力	SNMP エージェント（サーバー）	いいえ
11620	SNMP エージェント	UDP	なし	入力	SNMP エージェント（サーバー）	いいえ
443	HTTPS	TCP	128 ビット	入力	HTTPS サーバー	いいえ
443	WSMAN	TCP	128 ビット	入力 / 出力	iDRAC/OMSA 通信	いいえ
4433	HTTPS	TCP	128 ビット	入力	自動検出	いいえ
2049	NFS	UDP	なし	すべて	パブリック共有	いいえ
4001～4004	NFS	UDP	なし	すべて	パブリック共有	いいえ
11620	SNMP エージェント	UDP	なし	0m	SNMP エージェント（サーバー）	いいえ

表 4. 管理下ノード

ポート番号	プロトコル	ポートタイプ	最高暗号化レベル	方向	使用状況	設定可能
162、11620	snmp	UDP	なし	出力	ハードウェアイベント	いいえ
443	WSMAN	TCP	128 ビット	入力	iDRAC/OMSA 通信	いいえ
4433	HTTPS	TCP	128 ビット	出力	自動検出	いいえ
2049	NFS	UDP	なし	すべて	パブリック共有	いいえ
4001～4004	NFS	UDP	なし	すべて	パブリック共有	いいえ
443	HTTPS	TCP	128 ビット	入力	HTTPS サーバー	いいえ
8080	HTTP	TCP		入力	HTTP サーバー；OMSA VIB をダウンロードし、非準拠 vSphere ホストを修正	いいえ
50	RMCP	UDP/TCP	128 ビット	出力	リモートメールチェックプロトコル	いいえ
51	IMP	UDP/TCP	該当なし	該当なし	IMP 論理アドレスメンテナンス	いいえ
5353	mDNS	UDP/TCP		すべて	マルチキャスト DNS	いいえ
631	IPP	UDP/TCP	なし	出力	インターネットプリンティングプロトコル（IPP）	いいえ
69	TFTP	UDP	128 ビット	すべて	トリビアルファイル転送	いいえ
111	NFS	UDP/TCP	128 ビット	入力	SUN リモートプロシージャコール（ポートマップ）	いいえ
68	BOOTP	UDP	なし	出力	ブートストラッププロトコルクライアント	いいえ

仮想アプライアンスの正常なインストールと操作のために最低限必要な要件は何ですか?

以下の設定は、最低限のアプライアンス要件の概要です。

- 物理 RAM： 3 GB
- 予約メモリ： 1 GB

メモ: 最適なパフォーマンスを得るため、Dell では 3 GB をお勧めします。

- ディスク： 32.5 GB
- CPU： 2 つの仮想 CPU

保証を更新するための翻訳はどのようにして見つければいいですか?

保証の更新ボタンをクリックすると、ウェブページには英語、またはサーバーが実際に設置されている地域のローカル言語が表示される場合があります。 以下の表は予期される翻訳を示しています。

表 5. 見込まれる翻訳

	クライアントの場所	サービスタグの場所	OpenManage Integration for VMware vCenter はクライアント環境をサポートしていますか？	OpenManage Integration for VMware vCenter のページをクライアント環境の言語で表示することができますか？	OpenManage Integration for VMware vCenter はデフォルトの英語でページを表示します。
1	場所 A	場所 A	はい	はい	いいえ
2	場所 A	場所 B	いいえ	いいえ	はい
3	場所 A	場所 B	はい	いいえ	はい
4	場所 A	場所 B	はい	いいえ	はい
5	場所 A	場所 A	いいえ	いいえ	はい

以下の例を参照してください。

表 6. 例

	クライアントの場所	サービスタグの場所	OpenManage Integration for VMware vCenter はクライアント環境をサポートしていますか？	OpenManage Integration for VMware vCenter のページをクライアント環境の言語で表示することができますか？	OpenManage Integration for VMware vCenter はデフォルトの英語でページを表示します。
1	フランス	フランス	はい	はい	いいえ
2	ブラジル	中国	いいえ	いいえ	はい
3	ドイツ	中国	はい	いいえ	はい
4	中国	ブラジル	はい	いいえ	はい
5	インド	インド	いいえ	いいえ	はい

新しい iDRAC バージョンの詳細が、vCenter ホストとクラスタ のページに表示されないのはなぜですか?

vSphere Web クライアントの最近のタスクペインでファームウェアアップデートのタスクが正常に終了した後、ファームウェアアップデートのページを更新して、ファームウェアのバージョンを確認します。そのページに古いバージョンが表示される場合は、Dell Management Center のホストの準拠ページへ移動し、そのホストの CISOR ステータスをチェックします。CISOR が有効化されていない場合は、CISOR を有効化してホストを再起動してください。CISOR がすでに有効化されている場合は、iDRAC コンソールにログインし、iDRAC をリセットして数分待ち、その後 vSphere Web クライアントのファームウェアアップデートのページを更新します。

OMSA を使用してハードウェア温度の異常をシミュレートすることによってイベント設定をテストする方法は?

イベントが正しく機能していることを確認するには、次の手順を行います。

1. OMSA ユーザーインタフェースで、**アラート管理 → プラットフォームイベント** と移動します。
2. **Enable Platform Event Filter Alerts（プラットフォームイベントフィルタアラートの有効化）**チェックボックスを選択します。
3. 一番下までスクロールして、**Apply Changes（変更の適用）**をクリックします。
4. 温度の警告など特定のイベントが有効になっていることを確認するには、左側のツリーで、**メインシステムシャーシ** を選択します。
5. **メインシステムシャーシ** の下で、**温度** を選択します。
6. **Alert Management（アラート管理）**タブを選択して、**Temperature Probe Warning（温度プローブ警告）**を選択します。
7. **Broadcast a Message（メッセージのブロードキャスト）**チェックボックスを選択して、**Apply Changes（変更の適用）**を選択します。
8. 温度警告イベントを作動させるには左側のツリービューから、**メインシステムシャーシ** を選択します。
9. **Main System Chassis（メインシステムシャーシ）**で **Temperatures（温度）**を選択します。
10. **System Board Ambient Temp（システム基板環境温度）**リンクを選択して、**Set to Values（値に設定）**オプションボタンを選択します。
11. **Maximum Warning Threshold（最大警告しきい値）**を現在リストされている読み取り値未満に設定します。たとえば、現在の読み取り値が 27 の場合は、しきい値を **25** に設定します。
12. **Apply Changes（変更の適用）**を選択すると、温度警告イベントが生成されます。別のイベントを発生させるには、同じ **Set to Values（値に設定）**オプションを使用して元の設定を復元します。イベントは警告として生成されてから、正常な状態になります。すべてが適切に動作している場合は、**vCenter Tasks & Events（vCenter タスクおよびイベント）**ビューに移動します。温度プローブ警告イベントが表示されています。

   メモ: 重複イベントにはフィルタがあり、連続して何度も同じイベントをトリガしても、受け取るイベントは 1 つだけです。すべてのイベントを表示するにはイベント間の間隔を少なくとも 30 秒にします。

Dell ホストシステムに OMSA エージェントをインストールしていますが、OMSA がインストールされていないというエラーメッセージが今でも表示されます。どうしたらよいですか?

この問題を解決するには、第 11 世代サーバで次の作業を行います。

1. ホストシステムに **OMSA** を **Remote Enablement（リモート有効化）**コンポーネントと共にインストールします。
2. コマンドラインを使用して OMSA をインストールする場合は、**-c オプション** を指定してください。OMSA がすでにインストールされている場合は、-c オプション付きで再インストールして、サービスを再起動してください。

   ```
   srvadmin-install.sh -c srvadmin-services.sh restart
   ```

   ESXi ホストの場合は、**VMware リモート CLI ツール** を使用して **OMSA VIB** をインストールし、システムを再起動する必要があります。

ロックダウンモードを有効にした状態で OpenManage Integration for VMware vCenter で ESX/ESXI をサポートできますか?

はい。ロックダウンモードは ESXi 4.1 以降のホストにおける本リリースでサポートされています。

再起動後、ロックダウンモードのホスト ESXi 4.0 Update2 および ESXi Update 3 でインベントリが失敗します。

ロックダウンモードでは ESXi 4.1 以降が必要です。これより前の ESXi バージョンを使用している場合に、ロックダウンモード中に何らかの理由でホストが再起動すると、再起動後にホストで次の手順を実行しない限り、インベントリが失敗し続けます。

ESXi 4.0 Update2 および Update3 向けの回避手順は、次のとおりです。

1. **vSphere Client（vSphere クライアント）**で **Hosts and Clusters（ホストとクラスタ）**を選択し、左のペインで **Host（ホスト）**を選択して **Configuration（設定）**タブをクリックします。
2. 左のペインの **Software（ソフトウェア）**で **Security Profile（セキュリティプロファイル）**をクリックします。
3. **Lockdown Mode（ロックダウンモード）**までスクロールダウンして、**Edit（編集）**をクリックします。
4. **Lockdown Mode（ロックダウンモード）**ダイアログボックスで、ロックダウンモードを無効にするために **Enable（有効化）**チェックボックスをクリアして、**OK** をクリックします。
5. ホストコンソールにログインして、**Restart Management Agents（管理エージェントの再起動）**を選択し、**<ENTER>** を押します。確認のために **<F11>** を押します。
6. ロックダウンモードを有効にするには、1 から 4 までの手順を繰り返しますが、今回は、**Enable（有効化）**チェックボックスを選択して **OK** をクリックします。

ロックダウンモードを使用しようとしたら、失敗しました。

ロックダウンモードで接続プロファイルにホストを追加したとき、インベントリが実行されましたが、「Remote Access Controller が見つからなかったか、インベントリがこのホスト上でサポートされていません」と表示されて失敗しました。インベントリはロックダウンモードのホストに対して動作するのではないのですか?

ホストをロックダウンモードにするか、ホストをロックダウンモードから削除する場合は、30 分待ってから、OpenManage Integration for VMware vCenter で次の操作を実行する必要があります。

ESXi 4.1 U1 で UserVars.CIMoeMProviderEnable にはどのような設定を使用すべきですか?

UserVars.CIMoemProviderEnabled を 1 に設定してください。

ハードウェアプロファイルの作成にリファレンスサーバーを使用していますが、失敗しました。どうしたらよいですか?

最低限の推奨バージョンの iDRAC ファームウェア、Lifecycle Controller ファームウェア、および BIOS がインストールされていることを確認してください。

リファレンスサーバーから取得したデータが現行のものであることを確認するには、**再起動時のシステムインベントリの収集（CSIOR）**を有効にして、データを抽出する前にリファレンスサーバーを再起動してください。「リファレンスサーバーでの CSIOR の設定」を参照してください。

ブレードサーバーに ESX/ESXi を展開しようとしていますが、失敗しました。どうしたらよいですか?

このエラーを解決するには、次の作業を実行します。

1. **ISO の場所（NFS パス）** とステージング **フォルダパス** が正しいことを確認します。
2. サーバー ID の割り当て時に選択された **NIC** が仮想アプライアンスと同じネットワーク上にあることを確認します。
3. **静的 IP アドレス** を使用している場合は、指定したネットワーク情報（サブネットマスクとデフォルトゲートウェイを含む）が正しいことを確認します。また、その IP アドレスがまだネットワーク上に割り当てられていることを確認します。
4. 少なくとも 1 つの **仮想ディスク** がシステムによって認識されていることを確認します。ESXi は内部 RIPS SD カードにもインストールされます。

ハイパーバイザー展開が R210 II マシンで失敗するのはなぜですか?

連結された ISO からの BIOS 起動の失敗が原因で、R210 II システムのタイムアウト問題がハイパーバイザー展開失敗エラーを引き起こします。この問題を解決するには、ハイパーバイザーを手動でマシンにインストールしてください。

展開ウィザードにモデル情報のない自動検出されたシステムが表示されるのはなぜですか?

これは通常、システムにインストールされているファームウェアのバージョンが、推奨される最低要件を満たしていないことを示しています。場合によっては、ファームウェアアップデートがシステム上に登録されていないこともあります。この問題は、システムのコールドブートまたはブレードの再装着によって解決されます。iDRAC 上で新たに有効化されたアカウントは無効にする必要があり、そうすると自動検出が再開始され、OpenManage Integration for VMware vCenter にモデル情報と NIC 情報を提供します。

ESX/ESXI ISO で NFS 共有がセットアップされていますが、共有の場所をマウントするときのエラーで失敗します。

解決法を見つけるには、次の手順を行います。

1. iDRAC がアプライアンスに対して ping を実行できることを確認します。
2. ネットワークの稼働速度が遅すぎないことを確認します。

仮想アプライアンスを強制削除するにはどのようにしたらよいですか?

1. **https://<vcenter_serverIPAddress>/mob** にアクセスします。
2. **コンテンツ** をクリックします。
3. **ExtensionManager** をクリックします。
4. **UnregisterExtension** をクリックします。
5. 延長キーを入力して com.dell.plugin OpenManage Integration for VMware vCenter を登録解除し、**メソッドの呼び出し** をクリックします。
6. vSphere ウェブクライアントで OpenManage Integration for VMware vCenter の電源をオフにしてから削除します。

今すぐバックアップ画面にパスワードを入力するとエラーメッセージが表示されます

解像度の低いモニターを使用すると、暗号化パスワード フィールドが 今すぐバックアップ ウィンドウから見えなくなります。ページを下にスクロールして暗号化パスワードを入力する必要があります。

vSphere Web Client で Dell サーバー管理ポートレットまたは Dell アイコンをクリックすると、404 エラーが返されます。

アプライアンスが稼働しているかどうかをチェックして、稼働していない場合は、vSphere Web クライアントから起動します。仮想アプライアンス Web サービスが起動するまで数分待ってから、ページを更新します。引き続きエラーが発生する場合は、コマンドラインから IP アドレスまたは完全修飾ドメイン名を使用してアプライアンスに対して ping を実行してください。ping が通らない場合は、ネットワーク設定を見直して、正しく設定されていることを確認してください。

ファームウェアアップデートが失敗しました。どうしたらよいですか?

仮想アプライアンスログをチェックして、タスクがタイムアウトしていないか確認してください。タイムアウトしている場合は、コールドリブートを実行して iDRAC をリセットする必要があります。システムが起動して稼働し始めたら、インベントリを実行するか、Firmware（ファームウェア）タブを使用して、アップデートが正常に完了したかどうかを確認してください。

vCenter の登録が失敗しました。どうしたらよいですか?

vCenter 登録は通信の問題により失敗することがあるため、このような問題が発生した場合の解決法の一つとして、静的 IP アドレスを使用することができます。静的 IP アドレスを使用するには、OpenManage Integration for VMware vCenter の コンソール タブで、**ネットワークの設定 → デバイスの編集** を選択して、正しい **ゲートウェイ** と **FQDN**（完全修飾ドメイン名）を入力します。DNS 設定の編集で DNS サーバー名を入力します。

メモ: 仮想アプライアンスが入力された DNS サーバーを解決できることを確認してください。

接続プロファイルの資格情報テスト中、パフォーマンスが非常に遅くなったり、応答しなくなります。

サーバー上の iDRAC のユーザーが 1 人だけ（たとえば、*root* のみ）であり、そのユーザーが無効状態であるか、すべてのユーザーが無効状態になっています。無効状態のサーバーへの通信を行うと、遅延が発生します。この問題を解決するには、サーバーの無効状態を解決、またはサーバー上の iDRAC をリセットして root ユーザーをデフォルト設定に再有効化することができます。

無効状態のサーバーを修正するには、次の手順を行います。

1. Chassis Management Controller コンソールを開いて、無効になっているサーバーを選択します。
2. iDRAC コンソールを自動的に開くには、**Launch iDRAC GUI（iDRAC GUI の起動）** をクリックします。
3. iDRAC コンソールでユーザーリストまで移動して、次のいずれかを選択します。
   - iDRAC 6：**iDRAC settings（iDRAC 設定）→ Network/Security tab（ネットワーク / セキュリティタブ）→ Users tab（ユーザータブ）** を選択します。
   - iDRAC 7：**User authentication（ユーザー認証）** を選択します。
4. 設定を編集するには、User ID（ユーザー ID）列で、管理者（root）ユーザーのリンクをクリックします。
5. **Configure User（ユーザーの設定）** をクリックして、**Next（次へ）を**クリックします。

6. 選択されたユーザーの User Configuration（ユーザー設定）ページで、Enable user（ユーザーの有効化）の横にあるチェックボックスを選択して、**Apply（適用）**をクリックします。

OpenManage Integration for VMware vCenter は、VMware vCenter Server アプライアンスをサポートしていますか？

はい、OpenManage Integration for VMware vCenter は VMware vCenter Server アプライアンスをサポートしています。

OpenManage Integration for VMware vCenter は vSphere Web Client をサポートしていますか?

はい、OpenManage Integration for VMware vCenter は VMware vSphere ウェブクライアントをサポートしています。

ベアメタル展開の問題

本項では、展開プロセスで見つかった問題の処理について説明します。

自動検出とハンドシェイクの前提条件

- 自動検出とハンドシェイクを実行する前に、iDRAC と Lifecycle Controller ファームウェア、および BIOS が推奨される最低バージョンの要件を満たしていることを確認してください。
- CSIOR は、システムまたは iDRAC で少なくとも 1 度は実行されている必要があります。

ハードウェア設定の失敗

- 展開タスクを開始する前に、システムが CSIOR を完了していて、再起動中ではないことを確認してください。
- リファレンスサーバーが全く同じシステムになるように、BIOS 設定をクローンモードで実行することを強く推奨します。
- 一部のコントローラでは、1 台のドライブでの RAID 0 アレイの作成を許可しません。この機能は高性能のコントローラでのみサポートされており、このようなハードウェアプロファイルの適用は失敗の原因になり得ます。

新たに購入したシステムでの自動検出の有効化

ホストシステムの自動検出機能はデフォルトでは有効になっておらず、購入時に有効化を請求する必要があります。購入時に自動検出の有効化が請求されると、iDRAC 上で DHCP が有効化され、管理者アカウントが無効になります。iDRAC に静的 IP アドレスを設定する必要はなく、これはネットワーク上の DHCP サーバーから取得されます。自動検出機能を利用するには、検出プロセスをサポートするように DHCP サーバーまたは DNS サーバー（または両方）を設定する必要があります。CSIOR は出荷プロセスですでに実行されています。自動検出をサポートするようにネットワークをセットアップするための方法の詳細については、**http://attachments.wetpaintserv.us/xBUlrs4t%2B2TzbrwqYkblvQ%3D%3D2 62254** にある『Lifecycle Controller 自動検出ネットワークセットアップ仕様』を参照してください。

購入時に自動検出を請求しなかった場合は、次の手順で有効にすることができます。

1. 起動プロセス中に **<Ctrl-E>** を押します。
2. iDRAC セットアップウィンドウで、NIC を有効にします（ブレードサーバーのみ）。
3. Auto-Discovery（自動検出）を有効にします。
4. DHCP を有効にします。
5. 管理者アカウントを無効にします。
6. **Get DNS server address from DHCP（DHCP から DNS サーバーアドレスを取得）**を有効にします。

7. **Get DNS domain name from DHCP（DHCP から DNS ドメイン名を取得）**を有効にします。
8. **Provisioning Server（プロビジョニングサーバー）**フィールドに次を入力します。
   `<OpenManage Integration virtual appliance IPaddress>:4433`

デルへのお問い合わせ

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

デルでは、オンラインまたは電話によるサポートとサービスのオプションを複数提供しています。サポートやサービスの提供状況は国や製品ごとに異なり、国 / 地域によってはご利用いただけないサービスもございます。デルのセールス、テクニカルサポート、またはカスタマーサービスへは、次の手順でお問い合わせいただけます。

1. **dell.com/support** にアクセスします
2. サポートカテゴリを選択します。
3. ページの上部にある「国/地域の選択」ドロップダウンメニューで、お住まいの国または地域を確認します。
4. 必要なサービスまたはサポートのリンクを選択します。

OpenManage Integration for VMware vCenter の関連情報

- PowerEdge™ サーバー用 Dell サーバーマニュアルの表示またはダウンロード
  http://www.dell.com/poweredgemanuals
- Dell OpenManage システム管理者マニュアル
  http:// www.delltechcenter.com/omsa
- Dell Lifecycle Controller マニュアル
  http://www.dell.com/enterprisemanagement

8

仮想化—第 11 世代および第 12 世代 Dell Poweredge サーバー関連のイベント

次の表は、イベント名、説明、重要度を含む仮想化関連の重要イベントおよび警告イベントを示しています。

表 7. 第 11 世代および第 12 世代 Dell PowerEdge サーバーのイベント

イベント名	説明	重大度	推奨処置
Dell-Current sensor detected a warning value	指定したシステムの電流センサーが警告しきい値を超えました。	警告	処置は不要
Dell-Current sensor detected a failure value	指定したシステムの電流センサーが障害しきい値を超えました。	Error（エラー）	システムをメンテナンスモードにしてください
Dell-Current sensor detected a non-recoverable value	指定したシステムの電流センサーが回復不可能なエラーを検出しました	Error（エラー）	処置は不要
Dell-Redundancy regained	センサーが正常値に戻りました	Info（情報）	処置は不要
Dell-Redundancy degraded	指定したシステムの冗長性センサーが、冗長性ユニットのいずれかのコンポーネントで障害が発生したが、ユニットは引き続き冗長であることを検出しました。	警告	処置は不要
Dell - Redundancy lost	指定したシステムの冗長性センサーが、冗長性ユニットのコンポーネントのひとつが切断された、故障した、または存在しないことを検出しました。	Error（エラー）	システムをメンテナンスモードにしてください
Dell - Power supply returned to normal	センサーが正常値に戻りました	Info（情報）	処置は不要
Dell - Power supply detected a warning	指定したシステムの電源装置センサー読み取り値がユーザー定義可能な警告しきい値を超えました。	警告	処置は不要
Dell - Power supply detected a failure	電源装置の接続が切断されているか、故障しました。	Error（エラー）	システムをメンテナンスモードにしてください

Dell - Power supply sensor detected a non-recoverable value	指定したシステムの電源装置センサーが回復不可能なエラーを検出しました	Error（エラー）	処置は不要
Dell - Memory Device Status warning	メモリデバイスの修正レートが許容値を超えました。	警告	処置は不要
Dell - Memory Device error	メモリデバイスの修正レートが許容値を超えた、メモリスペアバンクがアクティブになった、またはマルチビットの ECC エラーが発生しました。	Error（エラー）	システムをメンテナンスモードにしてください
Dell - Fan enclosure inserted into system	センサーが正常値に戻りました	Info（情報）	処置は不要
Dell - Fan enclosure removed from system	指定したシステムからファンエンクロージャが取り外されました。	警告	処置は不要
Dell - Fan enclosure removed from system for an extended amount of time	ユーザー定義可能な時間にわたって、指定したシステムからファンエンクロージャが取り外されたままになっています。	Error（エラー）	処置は不要
Dell - Fan enclosure sensor detected a non-recoverable value	指定したシステムのファンエンクロージャセンサーが回復不可能なエラーを検出しました	Error（エラー）	処置は不要
Dell - AC power has been restored	センサーが正常値に戻りました	Info（情報）	処置は不要
Dell - AC power has been lost warning	AC 電源コードが電源を失いましたが、これを警告として分類するだけの十分な冗長性があります。	警告	処置は不要
Dell - An AC power cord has lost its power	AC 電源コードが電源を失っており、冗長性不足のため、これをエラーとして分類する必要があります。	Error（エラー）	処置は不要
Dell - Processor sensor returned to a normal value	センサーが正常値に戻りました	Info（情報）	処置は不要
Dell - Processor sensor detected a warning value	指定したシステムのプロセッサセンサーがスロットル状態です。	警告	処置は不要
Dell - Processor sensor detected a failure value	指定したシステムのプロセッサセンサーが無効になっている、設定エラー	Error（エラー）	処置は不要

	がある、またはサーマルトリップが発生しました。		
Dell - Processor sensor detected a non-recoverable value	指定したシステムのプロセッサセンサーが故障しました。	Error（エラー）	処置は不要
Dell - Device configuration error	指定したシステムのプラグ可能デバイスで設定エラーが検出されました。	Error（エラー）	処置は不要
Dell - Battery sensor returned to a normal value	センサーが正常値に戻りました	Info（情報）	処置は不要
Dell - Battery sensor detected a warning value	指定したシステムのバッテリセンサーが、バッテリが予測不具合状態にあることを検出しました。	警告	処置は不要
Dell - Battery sensor detected a failure value	指定したシステムのバッテリセンサーが、バッテリの故障を検出しました。	Error（エラー）	処置は不要
Dell - Battery sensor detected a nonrecoverable value	指定したシステムのバッテリセンサーが、バッテリの故障を検出しました。	Error（エラー）	処置の必要なし
Dell - Thermal shutdown protection has been initiated	このメッセージは、システムがエラーイベントによるサーマルシャットダウンに設定されたときに生成されます。温度センサー読み取り値がシステムで設定されたエラーしきい値を超えると、オペレーティングシステムがシャットダウンし、システムの電源がオフになります。このイベントは、システムからファンエンクロージャが長い時間取り外されている場合にも、特定のシステムで発生することがあります。	Error（エラー）	処置は不要
Dell - Temperature sensor returned to a normal value	センサーが正常値に戻りました	Info（情報）	処置は不要
Dell - Temperature sensor detected a warning value	指定したシステムのバックプレーン基板、システム基板、CPU、またはドライブキャリア上の温度センサーが警告しきい値を超えました。	警告	処置は不要

Dell - Temperature sensor detected a failure value	指定したシステムのバックプレーン基板、システム基板、またはドライブキャリア上の温度センサーが障害しきい値を超えました。	Error（エラー）	システムをメンテナンスモードにしてください
Dell - Temperature sensor detected a non-recoverable value	指定したシステムのバックプレーンボード、システム基板、またはドライブキャリアの温度センサーが回復不可能なエラーを検出しました。	Error（エラー）	処置は不要
Dell - Fan sensor returned to a normal value	センサーが正常値に戻りました	Info（情報）	処置は不要
Dell - Fan sensor detected a warning value	ホスト <x> のファンセンサー読み取り値が警告しきい値を超えました。	警告	処置の必要なし
Dell - Fan sensor detected a failure value	指定したシステムのファンセンサーが 1 つまたは複数のファンの障害を検出しました。	Error（エラー）	システムをメンテナンスモードにしてください
Dell - Fan sensor detected a nonrecoverable value	ファンセンサーが回復不可能なエラーを検出しました。	Error（エラー）	処置は不要
Dell - Voltage sensor returned to a normal value	センサーが正常値に戻りました	Info（情報）	処置は不要
Dell - Voltage sensor detected a warning value	指定したシステムの電圧センサーが警告しきい値を超えました。	警告	処置は不要
Dell - Voltage sensor detected a failure value	指定したシステムの電圧センサーが障害しきい値を超えました。	Error（エラー）	システムをメンテナンスモードにしてください
Dell - Voltage sensor detected a nonrecoverable value	指定したシステムの電圧センサーが回復不可能なエラーを検出しました	Error（エラー）	処置は不要
Dell - Current sensor returned to a normal value	センサーが正常値に戻りました	Info（情報）	処置は不要
Dell - Storage: storage management error	ストレージ管理がデバイス依存のエラー状態を検出しました。	Error（エラー）	システムをメンテナンスモードにしてください
Dell - Storage: Controller warning	コントローラの警告です。詳細に関しては、vSphere クライアントのタスクとイベント タブを参照して下さい。	警告	処置は不要

Dell - Storage: Controller failure	コントローラの障害です。詳細に関しては、vSphere の タスクとイベント タブを参照して下さい。	Error（エラー）	システムをメンテナンスモードにしてください
Dell - Storage: Channel Failure	チャネル障害です。	Error（エラー）	システムをメンテナンスモードにしてください
Dell - Storage: Enclosure hardware information	エンクロージャハードウェア情報です。	Info（情報）	処置は不要
Dell - Storage: Enclosure hardware warning	エンクロージャハードウェア警告です。	警告	処置は不要
Dell - Storage: Enclosure hardware failure	エンクロージャハードウェアエラーです。	Error（エラー）	システムをメンテナンスモードにしてください
Dell - Storage: Array disk failure	アレイディスク障害です。	Error（エラー）	システムをメンテナンスモードにしてください
Dell - Storage: EMM failure	EMM 障害です。	Error（エラー）	システムをメンテナンスモードにしてください
Dell - Storage: power supply failure	電源装置障害です。	Error（エラー）	システムをメンテナンスモードにしてください
Dell - Storage: temperature probe warning	物理ディスク温度プローブ警告で、低温すぎるか高温すぎます。	警告	処置は不要
Dell - Storage: temperature probe failure	物理ディスク温度プローブエラーで、低温すぎるか高温すぎます。	Error（エラー）	システムをメンテナンスモードにしてください
Dell - Storage: Fan failure	ファン障害です。	Error（エラー）	システムをメンテナンスモードにしてください
Dell - Storage: Battery warning	バッテリ警告です。	警告	処置は不要
Dell - Storage: Virtual disk degraded warning	仮想ディスクの劣化警告です。	警告	処置は不要
Dell - Storage: Virtual disk degraded failure	仮想ディスク劣化障害です。	Error（エラー）	システムをメンテナンスモードにしてください
Dell - Storage: Temperature probe information	温度プローブ情報です。	Info（情報）	処置は不要
Dell - Storage: Array disk warning	アレイディスク警告です。	警告	処置は不要
Dell - Storage: Array disk information	アレイディスク情報です。	Info（情報）	処置は不要
Dell - Storage: Power supply warning	電源装置警告です。	警告	処置は不要

Dell - Chassis Intrusion - Physical Security Violation	シャーシイントルージョン - 物理的なセキュリティ違反です。	エラー	処置の必要なし
Dell - Chassis Intrusion(Physical Security Violation) Event Cleared	シャーシイントルージョン（物理的セキュリティ違反）イベントがクリアされました	info	処置の必要なし
Dell - CPU Presence (Processor Presence detected)	CPU 存在（プロセッサの存在が検出されています）	info	処置の必要なし
Dell - System Event Log (SEL) Full (Logging Disabled)	システムイベントログ（SEL）がフルです（ログが無効になっています）	エラー	処置の必要なし
Dell - System Event Log (SEL) Cleared	システムイベントログ（SEL）がクリアされました	info	処置の必要なし
Dell - SD Card redundancy Has Returned to Normal	SD カードの冗長性が正常に戻りました	info	処置の必要なし
Dell - SD Card Redundancy has been Lost	SD カードの冗長性が失われました	エラー	処置の必要なし
Dell - SD Card Redundancy Degraded	SD カードの冗長性が劣化しています	警告	処置の必要なし
Dell - Module SD Card Present (SD Card Presence Detected)	モジュール SD カードが存在します（SD カードの存在が検出されました）	info	処置の必要なし
Dell - Module SD Card Failed (Error)	モジュール SD カードの不具合（エラー）です	エラー	処置の必要なし
Dell - Module SD Card Write Protect(Warning)	SD カードモジュールが書き込み保護されています（警告）	警告	処置の必要なし
Dell - Module SD Card not Present	SD カードモジュールが存在しません	info	処置の必要なし
Dell - Watchdog Timer Expired	ウォッチドッグタイマーが期限切れです	エラー	処置の必要なし
Dell - Watchdog Reset	ウォッチドッグがリセットされました	エラー	処置の必要なし
Dell - Watchdog Power Down	ウォッチドッグの電源が切れています	エラー	処置の必要なし
Dell - Watchdog Power cycle	ウォッチドッグのパワーサイクルです	エラー	処置の必要なし
Dell - System Power Exceeds PSU Wattage	システム消費電力が PSU のワット数を超過しています	エラー	処置の必要なし

Dell - System Power Exceeds Error Cleared	システム消費電力超過のエラーがクリアされました	info	処置の必要なし
Dell - Power Supply Inserted	電源装置が挿入されました	info	処置の必要なし
Dell - Internal Dual SD Module is present	内蔵デュアル SD モジュールが存在します	info	処置の必要なし
Dell - Internal Dual SD Module is online	内蔵デュアル SD モジュールがオンラインです	info	処置の必要なし
Dell - Internal Dual SD Module is operating normally	内蔵 デュアル SD モージュールが正常に動作しています	info	処置の必要なし
Dell - Internal Dual SD Module is write protected	内蔵デュアル SD モジュールが書込み防止になっています	警告	処置の必要なし
Dell - Internal Dual SD Module is writable	内蔵ディアル SD モジュールが書き込み可能です	info	処置の必要なし
Dell - Integrated Dual SD Module is absent	内蔵デュアル SD モジュールが不在です	エラー	処置の必要なし
Dell - Integrated Dual SD Module redundancy is lost	内蔵デュアル SD モジュールの冗長性が失われました	エラー	処置の必要なし
Dell - Internal Dual SD Module is redundant	内蔵デュアル SD モジュールが冗長です	info	処置の必要なし
Dell - Internal Dual SD Module is not redundant	内蔵デュアル SD モジュールが冗長性を欠いています	info	処置の必要なし
Dell - Integrated Dual SD Module failure	内蔵デュアル SD モジュールエラーです	エラー	処置の必要なし
Dell - Internal Dual SD Module is redundant	内蔵デュアル SD モジュールがオフラインです	警告	処置の必要なし
Dell - Integrated Dual SD Module redundancy is lost	内蔵デュアル SD モジュールの冗長性が劣化しています	警告	処置の必要なし
Dell - SD card device has detected a warning	SD カードデバイスが警告を検出しました	警告	処置の必要なし
Dell - SD card device has detected a failure	SD カードデバイスがエラーを検出しました	エラー	処置の必要なし
Dell - Integrated Dual SD Module warning	内蔵デュアル SD モジュールの警告です	警告	処置の必要なし
Dell - Integrated Dual SD Module information	内蔵デュアル SD モジュールの情報です	info	処置の必要なし

Dell - Integrated Dual SD Module redundancy information	内蔵デュアル SD モジュールの冗長性情報です	info	処置の必要なし
Dell - Network failure or critical event	ネットワークエラーまたは重要なイベントです	エラー	処置の必要なし
Dell - Network warning	ネットワークの警告です	警告	処置の必要なし
Dell - Network information	ネットワーク情報です	info	処置の必要なし
Dell - Physical disk failure	物理ディスクの障害です	エラー	処置の必要なし
Dell - Physical disk warning	物理ディスクの警告です	警告	処置の必要なし
Dell - Physical disk information	物理ディスクの情報です	info	処置の必要なし
Dell - An error was detected for a PCI device	PCI デバイスでエラーが検出されました	エラー	処置の必要なし
Dell - A warning event was detected for a PCI device	PCI デバイスで警告イベントが検出されました	警告	処置の必要なし
Dell - An informational event was detected for a PCI device	PCI デバイスで情報イベントが検出されました	info	処置の必要なし

A

自動検出について

自動検出とは、第 11 世代 および第 12 世代の Dell PowerEdge ベアメタルサーバーを、OpenManage Integration for VMware vCenter で使用するために、使用可能なサーバーのプールに追加する手順です。サーバーが検出されたら、これをハイパーバイザーおよびハードウェアの展開に使用します。本付録は、自動検出について、システム設定に役立つ十分な情報を提供します。自動検出は、コンソールを使用して新規サーバーをセットアップし登録するための、Lifecycle Controller の機能です。この機能を使用する利点は、面倒な手動での新規サーバーのローカル設定を排除し、コンソールで新しいサーバー（ネットワークに接続されて電源プラグを差し込み済み）を自動的に検出できる点にあります。

自動検出は、実行される処理にちなんで、*検出とハンドシェイク* とも呼ばれます。自動検出を有効にしたサーバーを AC 電源に接続して、ネットワークに接続すると、Dell サーバーの Lifecycle Controller が、Dell プロビジョニングサーバーに統合された展開コンソールの*検出*を試みます。次に、自動検出機能により、プロビジョニングサーバーと Lifecycle Controller 間で*ハンドシェイク*が開始されます。

OpenManage Integration for VMware vCenter は、統合プロビジョニングサーバーの展開コンソールです。プロビジョニングサーバーの場所は、異なる方法で iDRAC に提供されます。プロビジョニングサーバーの場所の IP アドレスまたはホスト名は、OpenManage Integration for VMware vCenter アプライアンス仮想マシンの IP アドレスまたはホスト名に設定されます。

メモ: 自動検出で設定された新規サーバーは、24 時間の間 90 秒間隔で、プロビジョニングサーバーの場所の解決を試行します。この後で、手動で自動検出を再度開始することができます。

自動検出要求を受信した OpenManage Integration for VMware vCenter for VMware vCenter は、SSL 証明書を検証し、クライアント側のセキュリティ証明書やホワイトリストによる検証といった、オプションで設定済みのセキュリティ手順を開始します。新規サーバーからの 2 回目の検証要求で、iDRAC に設定する一時ユーザー名 / パスワードの資格情報を返します。以降の呼び出しは、OpenManage Integration for VMware vCenter for VMware vCenter が開始し、サーバーに関する情報を収集して一時資格情報を削除し、管理者がアクセスするためのより永続的な資格情報をユーザーの定義により設定します。

自動検出が正しく行われると、検出時に 設定 > 展開用資格情報 と選択したページで提供された展開用の資格情報がターゲットの iDRAC 上で作成されます。続いて、自動検出機能はオフになります。これで、サーバーが、Dell Management Center で展開 の下にある使用可能なベアメタルサーバーのプール内に表示されます。

自動検出は、現在、vSphere.Net クライアントを使用して実行することができます。

自動検出の必要条件

第 11 世代または第 12 世代の Dell PowerEdge ベアメタルサーバーの検出を行う前に、OpenManage Integration for VMware vCenter をインストールします。iDRAC Express または iDRAC Enterprise を搭載した第 11 世代以降の Dell PowerEdge サーバーのみを、OpenManage Integration for VMware vCenter のベアメタルサーバーのプールで検出することができます。Dell ベアメタルサーバーの iDRAC から OpenManage Integration for VMware vCenter 仮想マシンへのネットワーク接続が必要です。

メモ: ハイパーバイザーが既にあるホストは OpenManage Integration for VMware vCenter で検出せずに、このハイパーバイザーを接続プロファイルに追加して、ホストの準拠 ウィザードを使用して OpenManage Integration for VMware vCenter で調整します。

自動検出させるには、次の条件を満たしている必要があります。

- **電源：** サーバーをコンセントに接続します。サーバーの電源を入れる必要はありません。

- **ネットワーク接続：** サーバーの iDRAC がネットワークに接続され、プロビジョニングサーバーとポート 4433 経由で通信している必要があります。IP アドレスは、DHCP サーバーを使用して、または手動で iDRAC 設定ユーティリティで指定します。
- **追加のネットワーク設定：** DHCP を使用している場合、*DNS サーバーアドレスを DHCP から取得* 設定を有効にして DNS 名の解決が行われるようにします。
- **プロビジョニングサービスの場所：** iDRAC に対してプロビジョニングサービスサーバーの IP アドレスまたはホスト名が既知でなければなりません。
- **アカウントアクセスは無効：** iDRAC への管理者アカウントのアクセスを有効にし、管理者特権を持つ iDRAC アカウントがある場合は、先にこれを iDRAC ウェブコンソールから無効にします。自動検出が正しく完了したら、iDRAC 管理者アカウントを再度有効にします。
- **自動検出は有効：** サーバーの iDRAC で自動検出が有効にされており、自動検出処理が開始できる状態。

iDRAC サーバーの管理者アカウントを有効または無効にする

自動検出をセットアップする前に、ルート以外のすべての管理者アカウントを無効にします。ルートアカウントは、自動検出の進行中は無効にされます。自動検出のセットアップを正しく行ったら、Integrated Dell Remote Access Controller 6 の GUI に戻り、オフにしていたアカウントを再度有効にします。以上の手順は、第 11 世代および第 12 世代の PowerEdge サーバー用の手順です。

メモ: 自動検出に失敗しないようにするため、iDRAC 上の非管理者アカウントを有効にすることもできます。これにより、自動検出に失敗した場合でもリモートアクセスが可能です。

1. ブラウザで、**iDRAC IP アドレス**をタイプします。
2. **Integrated Dell Remote Access Controller GUI** にログインします。
3. 次の手順のいずれか 1 つを実行します。
   - iDRAC6： 左ペインで、**iDRAC 設定 → ネットワーク / セキュリティ → ユーザー** タブを順に選択します。
   - iDRAC7： 左ペインで、**iDRAC 設定 → ユーザー認証 → ユーザー** タブを順に選択します。
4. ユーザー タブで、ルート以外の管理者アカウントを探します。
5. アカウントを無効にするには、ユーザー ID の下で **ID** を選択します。
6. **次へ** をクリックします。
7. ユーザー設定 ページの 一般 の下で、**ユーザーを有効にする** チェックボックスのチェックを外します。
8. **適用** をクリックします。
9. 自動検出を正しくセットアップしたら、各アカウントを再度有効にするため、ステップ 1～8 を繰り返しますが、今回は **ユーザーを有効にする** チェックボックスを選択して **適用** をクリックします。

第 11 世代 PowerEdge サーバーでの自動検出の手動設定

iDRAC およびホストの IP アドレスが必要です。

お使いのベアメタルアプライアンスの工場出荷時に自動検出を使用するよう注文されていない場合は、これを手動で設定できます。iDRAC には 2 つのユーザーインタフェースがあり、設定する iDRAC の IP アドレスを使用して両方にアクセスすることができます。

ベアメタルサーバーの自動検出が正しく行われると、新しい管理者アカウントが作成されるか、ハンドシェイクサービスによって返された資格情報で既存アカウントが有効になります。自動検出以前に無効にされていた、その他すべての管理者アカウントは、有効になりません。これらのアカウントは、正しく自動検出が行われた後で再度有効にしてください。「iDRAC 上で管理者アカウントを有効または無効にする」を参照してください。

メモ: 何らかの理由で自動検出が正しく完了しなかった場合、iDRAC にリモートで接続する方法はありません。リモート接続には、iDRAC 上で非管理者アカウントを有効にしている必要があります。 iDRAC 上に有効になっているアカウントがない場合、iDRAC に接続する唯一の方法は、ボックスにローカルでログインして iDRAC 上でアカウントを有効にする方法です。

1. ブラウザで、**iDRAC IP** アドレスを入力します。
2. **iDRAC Enterprise GUI** にログインします。
3. **Integrated Dell Remote Access Controller 6— Enterprise → システム概要** タブの、仮想コンソールプレビューで、**起動** をクリックします。
4. 警告 — セキュリティ ダイアログで、**はい** をクリックします。
5. iDRAC ユーティリティコンソール で、**F12** を 1〜2 回押して、認証が必要です ダイアログボックスを表示します。
6. 認証が必要です ダイアログボックスで、名前 が表示されたら **Enter** を押します。
7. **パスワード** を入力します。
8. **Enter** を押します。
9. シャットダウン / 再起動 ダイアログボックスが表示されたら、**F11** を押します。
10. ホストが再開し、画面にメモリのロードに関する情報が表示され、さらに RAID、iDRAC が表示されて CTRL + E を押すようメッセージが表示されます。ここで即座に **CTRL + E** を押します。

    このダイアログボックスが表示されれば、操作は正しく行われています。表示されない場合、電源 メニューから 電源オフ して、再度電源をオンにしてこのステップを繰り返します。

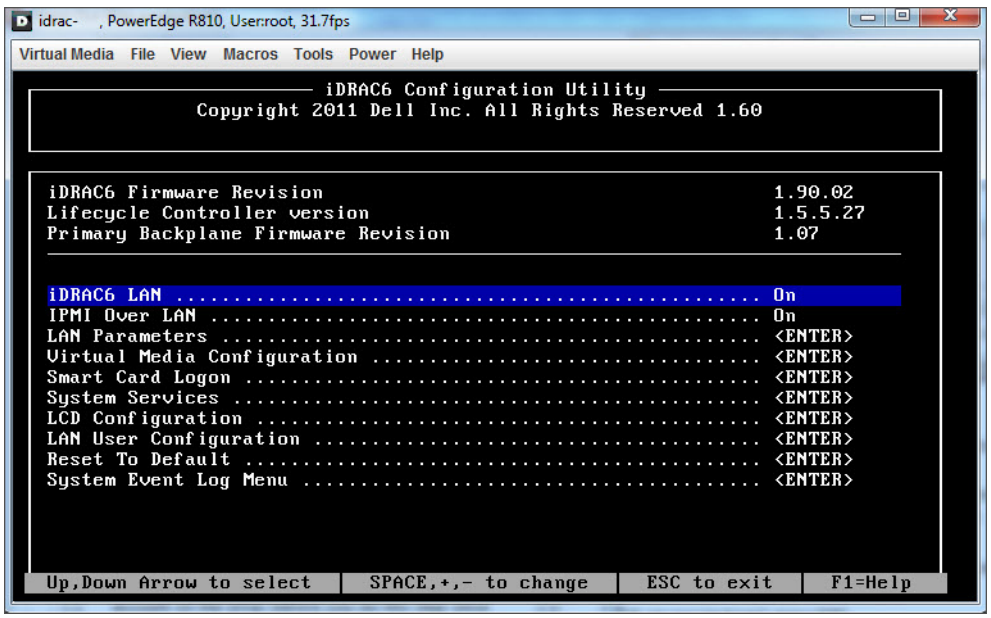

図 6. CTRL + E を押して、この画面をアクティブにします。

11. iDRAC6 設定ユーティリティ で、矢印キーを使用して **LAN パラメータ** を選択します。
12. **Enter** を押します。
13. このホストがブレードの場合、NIC を設定するにはスペースキーを押して **有効** に切り替えます。
14. DHCP を使用している場合、矢印キーを使用して **DHCP からのドメイン名** を選択します。
15. スペースキーでオプションを **オン** に切り替えます。
16. DHCP を使用している場合、矢印キーを使用して IPv4 の設定に移動し、**DHCP からの DNS サーバー** を選択します。

17. スペースキーでオプションを **オン** に切り替えます。
18. 終了するには、キーボードで **ESC** を押します。
19. 矢印キーで **LAN ユーザー設定** を選択します。
20. 矢印キーで **プロビジョニングサーバー** を選択します。
21. **Enter** を押します。
22. ホストの IP アドレスを入力します。
23. **ESC** を押します。
24. 矢印キーで **アカウントアクセス** を選択します。
25. スペースキーでオプションを **無効** に切り替えます。
26. 矢印キーで **自動検出** を選択します。
27. スペースキーでオプションを **有効** に切り替えます。
28. キーボードで **ESC** を押します。
29. 再び **Esc** を押します。

第 12 世代 PowerEdge サーバーでの自動検出の手動設定

iDRAC およびホストの IP アドレスが必要です。

お使いのベアメタルアプライアンスの工場出荷時に自動検出を使用するよう注文されていない場合は、これを手動で設定できます。iDRAC には 2 つのユーザーインタフェースがあり、設定する iDRAC の IP アドレスを使用して両方にアクセスすることができます。

ベアメタルサーバーの自動検出が正しく行われると、新しい管理者アカウントが作成されるか、ハンドシェイクサービスによって返された資格情報で既存アカウントが有効になります。自動検出以前に無効にされていた、その他すべての管理者アカウントは、有効になりません。これらのアカウントは、正しく自動検出が行われた後で再度有効にしてください。「iDRAC 上で管理者アカウントを有効または無効にする」を参照してください。

メモ: 何らかの理由で自動検出が正しく完了しなかった場合、iDRAC にリモートで接続する方法はありません。リモート接続には、iDRAC 上で非管理者アカウントを有効にしている必要があります。 iDRAC 上に有効になっているアカウントがない場合、iDRAC に接続する唯一の方法は、ボックスにローカルでログインして iDRAC 上でアカウントを有効にする方法です。

1. ブラウザで、**iDRAC IP アドレス**を入力します。
2. **iDRAC Enterprise GUI** にログインします。
3. **Integrated Dell Remote Access Controller 7— Enterprise → システム概要** タブの、仮想コンソールプレビューで、**起動** をクリックします。
4. 警告 — セキュリティ ダイアログで、**はい** をクリックします。
5. iDRAC ユーティリティコンソール で、**F12** を 1〜2 回押して、認証が必要です ダイアログボックスを表示します。
6. 認証が必要です ダイアログボックスで、名前 が表示されたら **Enter** を押します。
7. **パスワード** を入力します。
8. **Enter** を押します。
9. シャットダウン / 再起動 ダイアログボックスが表示されたら、**F11** を押します。
10. ホストが再開し、画面にメモリのロードに関する情報が表示され、さらに RAID、Dell 画面が表示されて F2 を押すようメッセージが表示されたら、即座に **F2** を押します。

    Dell セットアップユーティリティ 画面が表示されるのを待ちます。Dell セットアップユーティリティ画面 が表示されるまで、数分かかります。
11. Dell セットアップユーティリティ画面で、矢印キーを使用して **iDRAC 設定** を選択します。
12. 矢印キーで **リモートで有効にする** を選択します。

13. 自動検出を有効にするには、**有効にする** をクリックします。
14. **ESC** を押します。
15. **ESC** を押します。
16. 警告 画面で 終了 を確定して、**はい** をクリックします。