OpenManage Integration for VMware vCenter Version 4.0

Web クライアントユーザーズガイド

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

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

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

2017 - 02

Rev. A00

目次

1

はじめに

VMware vCenter は、IT 管理者が VMware vSphere ESX/ESXi ホストを管理、監視する際の中心的な役割を果たすコンソールです。OpenManage Integration for VMware vCenter（OMIVV）が提供する展開、管理、監視、およびアップグレードの優れた機能を活用することより、VMware Web クライアントからの Dell ホスト管理が容易になります。

本リリースの新機能

OpenManage Integration for VMware vCenter のこのリリースでは、次の機能を提供しています。

- vSphere 6.5 および 6.0 U2 のサポート
- vSphere 6.5 Proactive HA および Dell ホストとシャーシコンポーネントの重大度をカスタマイズする機能のサポート
- 複数のクラスタ上でのファームウェアの並行アップデートジョブのサポート
- vRealize Operations との統合のサポート
- OMSA 8.3 および OMSA 8.4 のサポート
- OMIVV の最新バージョンが利用可能になった場合の通知
- 単一の vCenter インスタンスまたは複数の vCenter を使用した最大 1000 台のホストに対するサポート
- すべての第 13 世代プラットフォームのサポート

OpenManage Integration for VMware vCenter の機能

OpenManage Integration for VMware vCenter（OMIVV）アプライアンスの機能について、次に説明します。

表 1. OMIVV の機能

機能	説明
インベントリ	インベントリ機能では、次の項目が提供されます。 • Dell PowerEdge サーバの詳細（メモリの数量や種類、NIC、PSU、プロセッサ、RAC、保証情報、サーバ、クラスタ、およびデータセンターレベルビューなど）。 • シャーシの詳細（シャーシ管理コントローラの情報、シャーシの電源、KVM の状態、ファンや温度の詳細、保証情報、空のスイッチやサーバの詳細など）。
アラートの監視および送信	監視とアラートには、次のような機能が含まれています。 • 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）を実行する。 • サーバの問題を診断するための、インベントリやイベント、アラームなどの情報を提供する。
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。

機能	説明
展開とプロビジョニング	ハードウェアプロファイルおよびハイパーバイザープロファイルを作成し、PXE を使用せずに VMware vCenter を使用して、ベアメタルの Dell PowerEdge サーバにリモートで OS を展開する。
サーバー情報	デルの保証データベースから Dell サーバおよび関連するシャーシの保証情報を取得して、オンラインで簡単に保証をアップグレードできるようにする。
セキュリティの役割および許可	標準の vCenter 認証、規則、および許可との統合。

メモ: OMIVV 4.0 以降では、VMware vSphere Web クライアントのみがサポートされ、vSphere Desktop クライアントはサポートされません。

メモ: vCenter 6.5 以降、OMIVV アプライアンスは、フラッシュバージョンでのみ使用できます。OMIVV アプライアンスは、HTML5 バージョンでは使用できません。

2

管理コンソールについて

OpenManage Integration for VMware vCenter およびその仮想環境の管理を実現するには、次の 2 つの管理ポータルを使用します。

- ウェブベース管理コンソール
- 個々のサーバのコンソールビュー（ OMIVV アプライアンスの仮想マシンコンソール ）

管理ポータルの使用

管理ポータルを使用して、次のタスクを実行できます。

- vCenter サーバを登録する。「vCenter サーバの登録」を参照してください。
- vCenter のログイン資格情報を変更する。「vCenter ログイン資格情報の変更」を参照してください。
- SSL 証明書をアップデートする。「登録済み vCenter サーバの SSL 証明書のアップデート」を参照してください。
- ライセンスをアップロードまたは購入する。デモライセンスを使用している場合は、**ソフトウェア購入** リンクが表示されます。このリンクをクリックすることで、ここから複数のホストを管理するためのフルバージョンのライセンスを購入できます。「管理ポータルへのライセンスのアップロード」を参照してください。
- OMIVV をアップデートします。「仮想アプライアンスの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」を参照してください。
- トラブルシューティングバンドルを生成します。「トラブルシューティングバンドルのダウンロード」を参照してください。
- OMIVV を再起動します。「仮想アプライアンスの再スタート」を参照してください。
- バックアップおよび復元を実行します。「バックアップおよび復元によるアプライアンスのアップデート」を参照してください。
- アラートを設定します。「グローバルアラートの設定」を参照してください。

非管理者ユーザーによる vCenter サーバの登録

vCenter の Administrator 資格情報があるか、または必要な権限を持つ Administrator 以外のユーザーであれば、OMIVV アプライアンス用の vCenter サーバを登録できます。

このタスクについて

必要な権限を持つ Administrator 以外のユーザーが vCenter サーバを登録できるようにするには、次の手順を実行します。

手順

1. ある役割に対して選択された権限を変更するため、役割を追加してその役割に必要な権限を選択するか、既存の役割を変更します。
   VMware vSphere マニュアルで役割の作成や変更に必要な手順を参照の上、vSphere ウェブクライアントで権限を選択します。役割に必要なすべての権限を選択する方法については、「Administrator 以外のユーザーに必要な権限」を参照してください。

   メモ: vCenter の管理者が役割を追加または変更する必要があります。
2. 役割を定義し、その役割の権限を選択したら、新しく作成した役割にユーザーを割り当てます。
   vSphere ウェブクライアントでの権限の割り当てについての詳細は、VMware vSphere マニュアルを参照してください。

   メモ: vCenter の管理者が vSphere クライアントの権限を割り当てる必要があります。

   これで、必要な権限のある Administrator 以外の vCenter サーバユーザーが、vCenter の登録や登録解除、資格情報の変更、資格情報のアップデートを実行できるようになります。
3. 必要な権限を持つ管理者以外のユーザーを使用して vCenter サーバを登録します。「必要な権限を持つ Administrator 以外のユーザーによる vCenter サーバの登録」を参照してください。
4. 手順 1 で作成または変更した役割に、デルの権限を割り当てます。「vSphere ウェブクライアントでの役割へのデルの権限の割り当て」を参照してください。

これで、必要な権限のある Administrator 以外のユーザーが Dell ホストの OMIVV 機能を利用できるようになります。

Administrator 以外のユーザーに必要な権限

vCenter で OMIVV を登録する場合、Administrator 以外のユーザーには次の権限が必要です。

メモ: Administrator 以外のユーザーが OMIVV で vCenter サーバを登録する際に、次の権限が設定されていないとエラーメッセージが表示されます。

- アラーム
  - アラームの作成
  - アラームの変更
  - アラームの削除
- 内線番号
  - 拡張子の登録
  - 拡張子の登録解除
  - 拡張子の更新
- Global（グローバル）
  - タスクのキャンセル
  - ログイベント
  - 設定

  メモ: VMware vCenter 6.5 を使用している場合は、次の正常性のアップデート権限を割り当てます。
- 正常性アップデートプロバイダ
  - 登録
  - 登録解除
  - アップデート
- Host（ホスト）
  - CIM
    - CIM インタラクション
  - 設定
    - 詳細設定
    - 接続
    - メンテナンス
    - パッチの問い合わせ
    - セキュリティプロファイルとファイアウォール

    メモ: VMware vCenter 6.5 を使用している場合は、次の権限を割り当てます。
    - Host.Config
      - 詳細設定
      - 接続
      - メンテナンス
      - パッチの問い合わせ
      - セキュリティプロファイルとファイアウォール
  - インベントリ
    - クラスタにホストを追加

    * スタンドアロンホストの追加
- ホストプロファイル
  - 編集
  - 表示
- 許可
  - 権限の変更
  - 役割の変更
- セッション
  - セッションの検証
- タスク
  - タスクの作成
  - タスクの更新

必要な権限のある Administrator 以外のユーザーによる vCenter サーバの登録

必要な権限のある Administrator 以外のユーザーを使用して、OMIVV アプライアンス用の vCenter サーバを登録することができます。Administrator 以外のユーザーを使用して、または Administrator として vCenter サーバの登録を行う方法については、vCenter サーバの登録を参照してください。

既存の役割へのデルの権限の割り当て

このタスクについて
既存の役割を編集し、デルの権限を割り当てることができます。

メモ: 管理者権限のあるユーザーとしてログインしていることを確認します。

手順

1. 管理者権限のあるユーザーとして vSphere Web Client にログインします。
2. vSphere Web Client で、**管理**、**役割** の順に移動します。
3. **役割プロバイダ** ドロップダウンリストから、vCenter サーバシステムを選択します。
4. **役割** リストから役割を選択して、 アイコンをクリックします。
5. 選択した役割に対するデルの権限を次のうちから選択し、**OK** をクリックします。
   - Dell.Configuration
   - Dell.Deploy — プロビジョニング
   - Dell.Inventory
   - Dell.Monitoring
   - Dell.Reporting

   vCenter 内で使用できる OMIVV 役割の詳細については、「セキュリティの役割および許可」を参照してください。

権限と役割の変更は直ちに有効になります。以上で、必要な権限を持つユーザーが、OpenManage Integration for VMware vCenter の操作を実行できるようになります。

メモ: すべての vCenter 操作で、OMIVV は、ログインしているユーザーの権限ではなく、登録されているユーザーの権限を使用します。

メモ: OMIVV の特定のページに、デルの権限が割り当てられていないログインユーザーがアクセスした場合は、2000000 エラーが表示されます。

vCenter サーバの登録

このタスクについて
OMIVV アプライアンスを登録するには、その前に OpenManage Integration for VMware vCenter をインストールします。OpenManage Integration for VMware vCenter は、管理者ユーザーアカウント、または vCenter を操作するのに必要な権限を持つ管理者以外のユーザーア

カウントを使用します。OpenManage Integration for VMware vCenter では、リンクモードにある単一の vCenter インスタンスまたは複数の vCenter サーバが動作する最大 1000 のホストがサポートされます。

新規 vCenter サーバを登録するには、次の手順を実行します。

手順

1. サポートされているブラウザから、**管理ポータル** を開きます。

   管理ポータルを開くには、OpenManage Integration for VMware vCenter の **ヘルプとサポート** タブで、**管理コンソール** の下のリンクをクリックするか、Web ブラウザを起動して **https:\\<アプライアンスの IP | ホスト名>** という URL を指定します。
2. 左ペインで **VCENTER 登録** をクリックし、**新規 vCenter サーバの登録** をクリックします。
3. **新規 vCenter の登録** ダイアログボックスの **vCenter 名** で、次の手順を実行します。
   a. **vCenter Server 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の FQDN を入力します。

      メモ: OMIVV を VMware vCenter に登録する際には、完全修飾ドメイン名（FQDN）を使用することをお勧めします。すべての登録において、vCenter のホスト名は DNS サーバで正しく解決される必要があります。次に、DNS サーバを使用する際のベストプラクティスを示します。

      - DNS に正しく登録されている OMIVV アプライアンスを展開する場合は、静的 IP アドレスとホスト名を割り当てます。静的 IP アドレスを割り当てると、システムが再起動しても、OMIVV アプライアンスの IP アドレスは変わりません。
      - OMIVV のホスト名エントリが、DNS サーバの前方ルックアップゾーンと逆引きルックアップゾーンの両方にあることを確認します。

   b. **説明** テキストボックスに、説明を入力します（オプション）。
4. **vCenter ユーザーアカウント** で、次の手順を実行します
   a. **vCenter ユーザー名** テキストボックスに、Administrator のユーザー名または必要な権限のある Administrator 以外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。
5. **Register**（登録）をクリックします。

vCenter サーバを登録した後は、OMIVV が vCenter プラグインとして登録され、Dell OpenManage Integration アイコンが vSphere ウェブクライアントに表示されます。このウェブクライアントから OMIVV 機能にアクセスできます。

メモ: すべての vCenter 操作で、OMIVV は、ログインしているユーザーの権限ではなく、登録されているユーザーの権限を使用します。

例

必要な権限を持つユーザー X が vCenter に OMIVV を登録し、ユーザー Y にはデルの権限のみがあります。ユーザー Y は vCenter にログインでき、OMIVV からファームウェアアップデートタスクをトリガできます。ファームウェアのアップデートタスクの実行中に、OMIVV はユーザー X の権限を使用して、ホストをメンテナンスモードにするか再起動します。

vCenter ログイン資格情報の変更

vCenter ログイン資格情報は、Administrator 権限を持つユーザー、または必要な権限を持つ Administrator 以外のユーザーが変更できます。

1. 管理ポータルを開くには、OpenManage Integration for VMware vCenter の **ヘルプとサポート** タブで、**管理コンソール** の下のリンクをクリックするか、Web ブラウザを起動して **https:\\<アプライアンスの IP | ホスト名>** という URL を指定します。
2. **ログイン** ダイアログボックスにパスワードを入力して、**ログイン** をクリックします。
3. 左ペインで、**VCENTER の登録**をクリックします。

   登録済み vCenter サーバが **vCenter サーバ接続の管理** ウィンドウの右ペインに表示されます。**ユーザーアカウントの変更** ウィンドウを開くには、**資格情報** で、登録済み vCenter 用の **変更** をクリックします。
4. vCenter の **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。
5. パスワードを変更するには、**適用**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。

メモ: 入力されたユーザー資格情報に必要な権限がない場合は、エラーメッセージが表示されます。

登録済み vCenter サーバの SSL 証明書のアップデート

OpenManage Integration for VMware vCenter は、OpenSSL API と 2,048 ビットキー長の RSA 暗号化標準を使用して、証明書署名要求（CSR）を生成します。OMIVV によって生成された CSR は、信頼された認証局からデジタル署名付き証明書を取得します。OpenManage Integration for VMware vCenter は、Web サーバで SSL を有効にし、デジタル証明書を使用したセキュアな通信を行います。

このタスクについて

SSL 証明書が vCenter サーバ上で変更された場合は、次の手順で OpenManage Integration for VMware vCenter の新しい証明書をインポートします。

手順

1. 管理ポータルを開くには、OpenManage Integration for VMware vCenter の **ヘルプとサポート** タブで、**管理コンソール** の下のリンクをクリックするか、Web ブラウザを起動して **https:\\<アプライアンスの IP | ホスト名>** という URL を指定します。
2. 左ペインで、**VCENTER の登録**をクリックします。

   登録済み vCenter サーバが右ペインに表示されます。
3. vCenter サーバ IP またはホスト名の証明書を更新するには、**アップデート** をクリックします。

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

このタスクについて

OpenManage Integration for VMware vCenter を削除するには、管理コンソールを使用して vCenter サーバから OMIVV の登録を解除します。

メモ: インベントリ、保証、または展開ジョブが実行中の場合は、vCenter サーバから OMIVV の登録を解除しないようにします。

手順

1. 管理ポータルを開くには、OpenManage Integration for VMware vCenter の **ヘルプとサポート** タブで、**管理コンソール** の下のリンクをクリックするか、Web ブラウザを起動して **https:\\<アプライアンスの IP | ホスト名>** という URL を指定します。
2. **VCENTER 登録** ページの **vCenter Server IP またはホスト名** テーブルで、**登録解除** をクリックします。

   メモ: 複数の vCenter が存在する場合があるため、必ず正しい vCenter を選択してください。
3. 選択した vCenter サーバの登録解除を確認するには、**VCENTER 登録の解除** ダイアログボックスで、**登録の解除** をクリックします。

メモ: クラスタで Proactive HA を有効にしたことがある場合は、Proactive HA がクラスタで無効になっていることを確認します。Proactive HA を無効にするには、設定 → サービス → vSphere 可用性 を選択し、編集 をクリックして、クラスタの Proactive HA の障害と対応 画面にアクセスします。リモート HA を無効にするには、次の手順を実行します。

Proactive HA の障害と対応 画面で、**Dell Inc** プロバイダのチェックボックスをオフにします。

管理ポータルへのライセンスのアップロード

このタスクについて

OMIVV のライセンスをアップロードすることで、サポートされている同時登録済み vCenter インスタンスおよび管理対象ホストの数を変更することができます。また、ホストをさらに追加する必要がある場合は、次の手順を実行してライセンスを追加することもできます

手順

1. 管理ポータルを開くには、OpenManage Integration for VMware vCenter の **ヘルプとサポート** タブで、**管理コンソール** の下のリンクをクリックするか、Web ブラウザを起動して **https:\\<アプライアンスの IP | ホスト名>** という URL を指定します。
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。

   登録済み vCenter サーバが右ペインに表示されます。
4. **ライセンスのアップロード** をクリックします。
5. **ライセンスのアップロード** ダイアログボックスで **参照** をクリックし、ライセンスファイルを参照して **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が変更または編集された場合、OMIVV アプライアンスではファイルが破損しているとみなすため、ライセンスファイルは機能しなくなります。

仮想アプライアンスの管理

このタスクについて
仮想アプライアンスの管理により、OpenManage Integration for VMware vCenter のネットワークやバージョン、NTP および HTTPS 情報を管理できます。これによって、管理者は次の操作ができます。

- 仮想アプライアンスの再起動。「仮想アプライアンスの再スタート」を参照してください。
- 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の場所の設定。仮想アプライアンスの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。
- NTP サーバのセットアップ。「ネットワークタイムプロトコル（NTP）サーバのセットアップ」を参照してください。
- HTTPS 証明書のアップロード。「HTTPS 証明書のアップロード」を参照してください。

OpenManage Integration for VMware vCenter で、次の手順を実行して管理ポータルから **アプライアンス管理** ページにアクセスします。

手順

1. 管理ポータルを開くには、OpenManage Integration for VMware vCenter の **ヘルプとサポート** タブで、**管理コンソール** の下のリンクをクリックするか、Web ブラウザを起動して **https:\\<アプライアンスの IP | ホスト名>** という URL を指定します。
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. アプライアンス管理セクションを設定するには、左側のペインで **アプライアンス管理** をクリックします。

仮想アプライアンスの再スタート

1. **アプライアンス管理** ページで、**仮想アプライアンスの再起動** をクリックします。
2. 仮想アプライアンスを再起動するには、**仮想アプライアンスの再起動** ダイアログボックスで **適用** をクリックします。キャンセルするには **キャンセル** をクリックします。

仮想アプライアンスのホスト名の変更

このタスクについて
次の手順を実行します。

手順

1. **アプライアンスの管理** ページで、**ホスト名の変更** をクリックします。
2. 更新されたホスト名を入力します。
   次のフォーマットでドメイン名を入力します：<ホスト名>。
3. **ホスト名のアップデート** をクリックします。
   アプライアンスのホスト名が更新され、メインメニューに戻ります。
4. アプライアンスを再起動するには、**アプライアンス再起動** をクリックします。

メモ: すべての vCenter サーバをアプライアンスに登録した場合は、すべての vCenter インスタンスの登録を解除し、再度登録します。

メモ: iDRAC、DRM でのサーバのプロビジョニングなど、その環境内の仮想アプライアンスを参照するものはすべて、必ず手動で更新します。

仮想アプライアンスの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

前提条件
すべてのデータが保護されていることを確認するには、仮想アプライアンスのアップデートの前に OMIVV のデータベースのバックアップを実行します。「バックアップおよび復元の管理」を参照してください。

手順

1. **アプライアンス管理** ページの **アプライアンスアップデート** セクションで、使用可能な現在のバージョンを確認します。

メモ: OMIVV アプライアンスでは、使用可能なアップグレードのメカニズムを表示したり、RPM のアップグレードを実行したりするために、インターネット接続が必要となります。必ず OMIVV アプライアンスをインターネットに接続してください。ネットワークの設定により、ネットワークでプロキシが必要な場合は、プロキシを有効にしてプロキシ設定を入力します。「HTTP プロキシの設定」を参照してください。

メモ: リポジトリパスのアップデート が有効であることを確認します。

使用可能な仮想アプライアンスのバージョンについては、該当する RPM と OVF 仮想アプライアンスのアップグレードのメカニズムがチェック記号と共に表示されます。次に、使用可能なアップグレードのメカニズムのオプションを示します。いずれのアップグレードのメカニズムに関する作業を行ってもかまいません。

- チェック記号が RPM に対して表示された場合は、既存のバージョンからの使用可能な最新バージョンに RPM をアップグレードできます。「既存のバージョンから最新バージョンへのアップグレード」を参照してください。
- OVF に対してチェック記号が表示された場合は、既存のバージョンから OMIVV のデータベースをバックアップし、使用可能な最新バージョンのアプライアンスに復元することができます。「バックアップと復元によるアプライアンスのアップデート」を参照してください。
- RPM と OVF の両方に対してチェック記号が表示された場合は、前述のオプションのいずれかを実行してアプライアンスをアップグレードできます。このシナリオでは、RPM のアップグレードを推奨します。

2. 仮想アプライアンスをアップデートするには、OMIVV のバージョンから、前述したアップグレードメカニズムのタスクを必要に応じて実行します。

   メモ: 必ず、登録された vCenter サーバへのすべてのウェブクライアントセッションからログアウトしてください。

   メモ: 登録された vCenter サーバのいずれかにログインする前には必ず、同じプラットフォームサービスコントローラ（PSC）ですべてのアプライアンスを同時にアップデートしてください。

3. **アプライアンス管理** をクリックして、アップグレードメカニズムを検証します。

既存のバージョンから最新バージョンへの OMIVV のアップグレード

1. **APPLIANCE MANAGEMENT** ページで、お使いのネットワーク設定により、ネットワークでプロキシが必要な場合はプロキシを有効にしてプロキシ設定を入力します。「HTTP プロキシの設定」を参照してください。
2. OpenManage Integration のプラグインを既存のバージョンから現在のバージョンにアップグレードするには、次のいずれかの手順を実行します。
   - **リポジトリパスのアップデート** がパス http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ に設定されていることを確認します。パスが異なっている場合は、**アプライアンス管理** ウィンドウの **アプライアンスアップデート** 領域で、**編集** をクリックし、**リポジトリパスのアップデート** でパスを http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ にアップデートします。保存するには、**適用** をクリックします。
   - インターネット接続が利用できない場合は、すべてのファイルとフォルダを http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ パスからダウンロードし、HTTP 共有にコピーします。**アプライアンス管理** ウィンドウの **アプライアンスアップデート** セクションで、**編集** をクリックし、**リポジトリパスのアップデート** テキストボックスにオフライン HTTP 共有へのパスを入力して、**適用** をクリックします。
3. 利用可能な仮想アプライアンスのバージョンと現在の仮想アプライアンスのバージョンを比較し、利用可能な仮想アプライアンスのバージョンが、現在の仮想アプライアンスのバージョンより新しいことを確認します。
4. 仮想アプライアンスにアップデートを適用するには、**アプライアンスの設定**で、**仮想アプライアンスのアップデート** をクリックします。
5. **アプライアンスのアップデート** ダイアログボックスで、**アップデート** をクリックします。

   アップデート をクリックした後は、**管理コンソール** ウィンドウからログオフされます。
6. Web ブラウザを閉じます。

メモ: RPM のアップグレードが完了すると、OMIVV コンソールにログイン画面が表示されます。ブラウザを開いて、https:\\<アプライアンスの IP | ホスト名> リンクを入力し、アプライアンスアップデート 領域に移動します。使用可能な仮想アプライアンスと現在の仮想アプライアンスのバージョンが同じであることを確認できます。

バックアップおよび復元によるアプライアンスのアップデート

このタスクについて

OMIVV アプライアンスのバージョンを X から Y にアップデートするには、次の手順を実行します。

手順

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。
2. vCenter から、旧 OMIVV アプライアンスの電源を切ります。

   メモ: vCenter から OMIVV プラグインの登録を解除しないようにしてください。vCenter からプラグインの登録を解除すると、OMIVV プラグインによって vCenter に登録されたアラームと、そのアラームで実行されるカスタマイズ（アクションなど）がすべて削除されます。
3. 新しい OpenManage Integration バージョン Y の OVF を展開します。
4. OpenManage Integration バージョン Y のアプライアンスの電源を入れます。
5. バージョン Y のアプライアンスのネットワークやタイムゾーンなどをセットアップします。

   メモ: 新しい OpenManage Integration バージョン Y のアプライアンスの IP アドレスが、旧アプライアンスのものと同じであることを確認します。

   メモ: バージョン Y のアプライアンスの IP アドレスが旧アプライアンスのものと同じでない場合、OMIVV プラグインが正常に動作しない可能性があります。この場合、すべての vCenter インスタンスの登録を解除して、再度登録してください。
6. データベースを新しい OMIVV アプライアンスに復元します。「バックアップからの OMIVV データベースの復元」を参照してください。
7. アプライアンスを検証します。Dell.com/support/manuals で入手可能な『*OpenManage Integration for VMware vCenter* インストールガイド』の「インストールの検証」を参照してください。
8. 登録されたすべての vCenter サーバで **インベントリ** を実行します。

   メモ: アップグレード後に、プラグインで管理するすべてのホスト上でインベントリを再実行することを推奨します。インベントリをオンラインで実行するには、「インベントリジョブのスケジュール」を参照してください。

   メモ: 新しい OMIVV バージョン Y の IP アドレスが OMIVV バージョン X から変更された場合は、新規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します。第 12 世代以降のサーバの場合は、IP の変更がこれらの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。以前のバージョンに準拠していた 12 世代より前のホストでは、IP の変更が非準拠として表示されるため、Dell OpenManage Server Administrator（OMSA）を設定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。

トラブルシューティングバンドルのダウンロード

1. **アプライアンスの管理** ページで、**トラブルシューティングバンドルの生成** をクリックします。
2. **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。
3. **閉じる** をクリックします。

HTTP プロキシの設定

1. **アプライアンス管理** ページで **HTTP プロキシ設定** にスクロールダウンし、**編集** をクリックします。
2. 編集モードで次の手順を実行します。
   a. **有効**を選択して HTTP プロキシ設定の使用を有効にします。
   b. **プロキシサーバアドレス** に、プロキシサーバのアドレスを入力します。
   c. **プロキシサーバポート** に、プロキシサーバの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 **はい** を選択します。
   e. プロキシ資格情報を使用している場合は、**ユーザー名** にユーザー 名を入力します。
   f. **パスワード** にパスワードを入力します。
   g. **適用** をクリックします。

ネットワークタイムプロトコル（NTP）サーバのセットアップ

このタスクについて

NTP を使用すると、仮想アプライアンスクロックをネットワークタイムプロトコル（ NTP ）サーバと同期させることができます。

手順

1. **アプライアンス管理** ページで、**NTP 設定** 領域の **編集** をクリックします。
2. **有効** をクリックします。優先 NTP サーバとセカンダリ NTP サーバのホスト名または IP アドレスを入力し、**適用** をクリックします。

メモ: 仮想アプライアンスのクロックが NTP サーバーと同期するまでにおよそ 10 分かかります。

展開モードの設定

このタスクについて

必要な展開モードに対して次のシステム要件が満たされていることを確認します。

表 2. 展開モードのシステム要件

展開モード	ホストの数	CPU の数	メモリ（GB）
小規模	最大 250	2	8
中規模	最大 500	4	16
大	最大 1000	8	32

メモ: 上述の展開モードのいずれについても、予約機能を使用して OMIVV 仮想アプライアンスに十分なメモリリソースが確実に予約されているようにします。メモリリソースの予約についてのステップは、vSphere のマニュアルを参照してください。

お使いの環境内のノードの数に合わせて、適切な展開モードを選択して OMIVV を拡張できます。

手順

1. **アプライアンス管理** ページで、**展開モード** までスクロールダウンします。
   小規模、**中規模**、または **大規模** などの展開モードの設定値が表示されます。デフォルトでは、展開モードは **小規模** に設定されています。
2. 環境に基づいて展開モードを更新する場合は、**編集** をクリックします。
3. **編集** モードで、前提条件が満たされていることを確認してから、目的の展開モードを選択します。
4. **Apply（適用）** をクリックします。
   割り当てられた CPU とメモリが、設定された展開モードで必要な CPU とメモリに対して検証されます。その後、次のいずれかの動作が発生します。
   - 検証が失敗した場合は、エラーメッセージが表示されます。
   - 検証が成功した場合は、変更内容を確認した後に、OMIVV アプライアンスが再起動して展開モードが変更されます。
   - 必要な展開モードが設定済みの場合は、メッセージが表示されます。
5. 展開モードを変更した場合、変更内容を確定した後、展開モードが更新されるように OMIVV アプライアンスの再起動を続行します。

メモ: OMIVV アプライアンスの起動中は、割り当てられたシステムリソースが設定済みの展開モードに対して検証されます。割り当てられたシステムリソースが設定済みの展開モードより小さい場合、ログイン画面では OMIVV アプライアンスは起動しません。OMIVV アプライアンスを起動するには、OMIVV アプライアンスをシャットダウンし、システムリソースを設定済みの展開モードにアップデートして、「展開モードのダウングレード」のタスクを実行します。

展開モードのダウングレード

1. 管理コンソールにログインします。
2. 展開モードを目的のレベルに変更します。
3. OMIVV アプライアンスをシャットダウンし、システムリソースを目的のレベルに変更します。
4. OMIVV アプライアンスの電源を入れます。

証明書署名要求の生成

前提条件

vCenter で OMIVV を登録する前に、必ず証明書をアップロードしてください。

このタスクについて
新しい証明書署名要求 (CSR) を生成すると、前に生成された CSR で作成された証明書をアプライアンスにアップロードできなくなります。CSR を生成するには、次の手順を実行します。

手順

1. **アプライアンス管理** ページで、**HTTPS 証明書** 領域の **証明書署名要求の生成** をクリックします。
   新しい要求を生成すると、以前の CSR を使用して作成された証明書がアプライアンスにアップロードできなくなることを示すメッセージが表示されます。要求を続行するには **続行**、取り消すには **キャンセル** をクリックします。
2. 要求を続行した場合は、**証明書署名要求の生成** ダイアログボックスに、要求の **共通名**、**組織名**、**組織単位**、**地域**、**州名**、**国**、および **E- メール** を入力します。**続行** をクリックします。
3. **ダウンロード** をクリックして、生成された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

前提条件
証明書が PEM フォーマットを使用していることを確認してください。

このタスクについて
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できます。このタイプのセキュアな通信を設定するには、CSR 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、Firefox、または Chrome を使用できます。

手順

1. **アプライアンス管理** ページで、**HTTPS 証明書** 領域の **証明書のアップロード** をクリックします。
2. **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。
3. 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。
4. 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。

デフォルト *HTTPS* 証明書の復元

このタスクについて

メモ: アプライアンス向けにカスタム証明書をアップロードする場合は、必ず vCenter 登録前に新しい証明書をアップロードしてください。vCenter 登録後に新しいカスタム証明書をアップロードすると、ウェブクライアントに通信エラーが表示されます。この問題を修正するには、vCenter 登録を解除してから、もう一度登録します。

手順

1. **アプライアンス管理** ページの **HTTPS 証明書** 領域で **デフォルト証明書の復元** をクリックします。
2. **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

このタスクについて
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実行できます。

手順

1. 管理ポータルを開くには、OpenManage Integration for VMware vCenter の **ヘルプとサポート** タブで、**管理コンソール** の下のリンクをクリックするか、Web ブラウザを起動して **https:\\<アプライアンスの IP | ホスト名>** という URL を指定します。
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. 次のフィールドに対する数値を入力します。
   - **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**をクリックします。設定を取り消すには **キャンセル**をクリックします。

バックアップおよび復元の管理

このタスクについて
バックアップおよび復元の管理は、管理コンソールで行います。このページでは、次のタスクを実行できます。

- 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

OpenManage Integration for VMware vCenter で、次の手順を実行して、管理コンソールから **バックアップおよび復元設定** ページにアクセスします。

手順

1. 管理ポータルを開くには、OpenManage Integration for VMware vCenter の **ヘルプとサポート** タブで、**管理コンソール** の下のリンクをクリックするか、Web ブラウザを起動して **https:\\<アプライアンスの IP | ホスト名>** という URL を指定します。
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、**バックアップと復元**をクリックします。

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、OMIVV 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ます。そのバックアップは後で復元することができます。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。データロスに備えるため、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。

このタスクについて

メモ: NTP の設定は保存および復元されません。

手順

1. **バックアップおよび復元設定** ページで **編集** をクリックします。
2. ハイライトされた **設定と詳細** 領域で、以下の手順を実行します。
   a. **バックアップの場所** にバックアップファイルのパスを入力します。
   b. **ユーザー名** にユーザー名を入力します。
   c. **パスワード** にパスワードを入力します。
   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** のテキストボックスに、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 !@#$%* などの特殊文字を使用できます。
   e. **パスワードの確認** に暗号化パスワードを再度入力します。
3. これらの設定を保存するには、**適用**をクリックします。
4. バックアップスケジュールを設定します。「自動バックアップのスケジュール」を参照してください。

次の手順
この手順の後で、バックアップスケジュールを設定します。

自動バックアップのスケジュール

このタスクについて
バックアップの場所と資格情報の設定の詳細については、「バックアップおよび復元の設定」を参照してください。

手順

1. **バックアップおよび復元設定** ページで、**自動スケジュールされたバックアップの編集** をクリックします。
   関連フィールドが有効になります。
2. バックアップを有効化するには、**有効** をクリックします。
3. バックアップを実行したい曜日の **バックアップの日** チェックボックスを選択します。
4. **バックアップの時刻 （24 時間、HH:mm）** に、時刻を HH:mm 形式で入力します。
   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。

5. **Apply（適用）**をクリックします。

即時のバックアップの実行

1. **バックアップおよび復元設定** ページで、**今すぐバックアップ** をクリックします。
2. 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、**今すぐバックアップ** チェックボックスをオンにします。
3. **バックアップの場所**、**ユーザー名**、**パスワード**、および **暗号化用パスワード** に値を入力します。
   暗号化パスワードには、英数字および、!、@、#、$、%、* などの特殊文字を含めることができます。長さの制限はありません。
4. **バックアップ** をクリックします。

バックアップからの OMIVV データベースの復元

このタスクについて
復元の操作では、復元作業の完了後に仮想アプライアンスが再起動します。

手順
1. **バックアップおよび復元設定** ページを開きます。「バックアップおよび復元の管理」を参照してください。
2. **バックアップおよび復元設定** ページで、**今すぐ復元** をクリックします。
3. **今すぐ復元** ダイアログボックスで、**ファイルの場所** へのパスを入力し、バックアップの .gz ファイルを CIFS / NFS 形式で入力します。
4. 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、!、@、#、$、%、* などの特殊文字を含めることができます。長さの制限はありません。
5. 変更を保存するには、**適用** をクリックします。
   アプライアンスが再起動します。

メモ: アプライアンスが工場出荷時の設定にリセットされている場合は、OMIVV アプライアンスを再度登録してください。

vSphere クライアントコンソールについて

vSphere クライアントコンソールは仮想マシン上の vSphere 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ています。コンソールでは、次のタスクを実行できます。

- ネットワークの設定
- 仮想アプライアンスパスワードの変更
- NTP の設定と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
- コンソールからログアウトする
- 読み取り専用ユーザー役割の使用

OMIVV 仮想マシンコンソールを開く

手順
1. vSphere ウェブクライアント **ホーム** から、**vCenter** をクリックします。
2. **インベントリリスト** で、**仮想マシン** をクリックして、OMIVV 仮想アプライアンスを選択します。
3. 次のいずれかの手順を実行します。
   - **オブジェクト** タブで、**アクション** → **コンソールを開く** の順に選択します。
   - 選択した仮想マシンを右クリックし、**コンソールを開く** を選択します。

次の手順
仮想マシンコンソールを開いて、資格情報（ユーザー名：admin およびパスワード：アプライアンスの導入中に設定したパスワード）を入力した後で、コンソールを設定できます。

ネットワークの設定

このタスクについて

vSphere クライアントコンソール上でネットワーク設定を変更できます。

手順

1. 仮想マシンのコンソールを開きます。「vSphere クライアントコンソールを開く」を参照してください。
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** の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

このタスクについて

vSphere Web Client の仮想アプライアンスパスワードは、コンソールを使用して変更できます。

手順

1. 仮想マシンのコンソールを開きます。「vSphere クライアントコンソールを開く」を参照してください。
2. **コンソール** ウィンドウで、矢印キーを使って **管理パスワードの変更** を選択し、**ENTER** キーを押します。
3. **現在の管理パスワード** に値を入力して **ENTER** キーを押します。

   管理パスワードは、特殊文字 1 つ、数字 1 つ、大文字 1 つ、小文字 1 つを含む 8 文字以上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** キーを押します。
5. **管理パスワードを確認してください** に新パスワードを再度入力し、**ENTER** キーを押します。

NTP の設定とローカルのタイムゾーンの設定

1. 仮想マシンコンソールを開きます。「vSphere クライアントコンソールを開く」を参照してください。
2. OMIVV タイムゾーン情報を設定するには、**日付と時刻のプロパティ** をクリックします。
3. **日付と時刻** タブで、**ネットワーク上で日付と時間の同期化** を選択します。

   NTP サーバ ウィンドウが表示されます。
4. NTP サーバの IP またはホスト名を追加するには、**追加** ボタンをクリックして、**Tab** を押します。
5. **タイムゾーン** をクリックして、該当するタイムゾーンを選択し、**OK** をクリックします。

仮想アプライアンスの再起動

1. 仮想マシンのコンソールを開きます。「vSphere クライアントコンソールを開く」を参照してください。
2. **アプライアンス再起動** をクリックします。
3. アプライアンスを再起動するには はい をクリックします。キャンセルするには いいえ をクリックします。

仮想アプライアンスの工場出荷時設定へのリセット

1. 仮想マシンのコンソールを開きます。「vSphere クライアントコンソールを開く」を参照してください。
2. **設定のリセット** をクリックします。

   次のメッセージが表示されます。

   ```
   All the settings in the appliance will be Reset to Factory Defaults and the appliance
   will be rebooted. Do you still wish to continue?
   ```
3. アプライアンスをリセットするには はい をクリックします。キャンセルするには いいえ をクリックします。

   はい をクリックすると、OMIVV アプライアンスが工場出荷時設定にリセットされ、その他のすべての設定および既存のデータが失われます。

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ても、ネットワーク設定に行っ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。

vSphere コンソールからログアウトする

vSphere コンソールからログアウトするには、**ログアウト** をクリックします。

読み取り専用ユーザー役割

診断目的のシェルアクセス権を持つ、読み取り専用の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ます。読み取り専用ユーザーのパスワードは **readonly** に設定されています。読み取り専用ユーザー役割のユーザーのパスワードは、以前の OMIVV バージョン (1.0 ~ 2.3.1) では管理者パスワードと同じでしたが、バージョン 3.0 以降ではセキュリティ上の目的で変更されています。

3

複数アプライアンスの管理

同じプラットフォームサービスコントローラ (PSC) と同じ vCenter バージョン vCenter サーバに登録されている複数の OMIVV アプライアンスを、管理および監視することができます。

前提条件

ページがキャッシュされている場合は、グローバル更新を実行することをお勧めします。

手順

1. VMware vCenter のホームページで、**OpenManage Integration** アイコンをクリックします。
2. **ナビゲータ** で、**Dell** グループの下の **OMIVV アプライアンス** をクリックします。
3. **OMIVV アプライアンス** タブに、次の情報と監視アプライアンスが表示されます。

   メモ: Dell アプライアンス タブでは、リストに表示されるアプライアンスの優先度は事前に定義されています。強調表示されたアプライアンスがアクティブなアプライアンスです。

   - **名前** - 各 OMIVV アプライアンスの IP アドレスまたは FQDN を使用したリンクが表示されます。アプライアンス固有の情報を表示および監視するには、特定のアプライアンス名のリンクをクリックします。アプライアンス名をクリックすると、OMIVV アプライアンスのメインコンテンツペインが表示され、OMIVV の操作を管理したり、特定のアプライアンスのホストやデータセンター、クラスタを監視したりすることができます。

     メモ: 複数のアプライアンスを使用している場合は、名前 をクリックするとメッセージボックスが表示され、キャッシュされたページ上でグローバル更新を実行するように要求されます。

     OMIVV の動作を管理しているアプライアンスを把握するには、次の操作を実行します。

     1. OpenManage Integration for VMware vCenter で、**ヘルプとサポート** タブをクリックします。
     2. 管理コンソールで、特定の OMIVV アプライアンスの IP を表示します。
   - **バージョン** - 各 OMIVV アプライアンスのバージョンを表示します。
   - **コンプライアンスステータス** - ロードされたプラグインにアプライアンスが対応しているかどうかを示します。

     メモ: アプライアンスの対応ステータスが表示されます。プラグインに OMIVV アプライアンスが対応していない場合は 非対応 と表示され、名前 リンクが無効になります。
   - **可用性ステータス** - プラグインからアプライアンスに到達できるかどうか、また必要なウェブサービスが OMIVV アプライアンスで動作しているかどうかを示すステータスが表示されます。

     メモ: アプライアンスの対応ステータスが 対応 で、アプライアンスの可用性ステータスが OK であれば、アプライアンスを選択できます。
   - **登録済み vCenter サーバ** - ログインしているセッションに対してアクセス可能で、アプライアンスに登録されているすべての vCenter が表示されます。複数の vCenter に 1 つのアプライアンスを登録すると、vCenter は展開 / 縮小可能なリストとして表示されます。vCenter のリンクをクリックすると **vCenter サーバ** ページが表示され、ナビゲータ ペインにすべての vCenter が一覧表示されます。

4

Web クライアントから OpenManage Integration へのアクセス

OMIVV のインストール後、VMware vCenter にログインすると、ホームページの **ホーム** タブの下にある、メインコンテンツエリアの **管理** グループの下に、**OpenManage Integration** アイコンが表示されます。**OpenManage Integration** アイコンを使用して **OpenManage Integration for VMware vCenter** ページへ移動します。**ナビゲータ** ペインに **Dell** グループが表示されます。

VMware vCenter のレイアウトは、次の 3 つの主なペインで構成されています。

表 3. OpenManage Integration for VMware vCenter のペイン

ペイン	説明
ナビゲータ	コンソール内のさまざまなビューにアクセスします。OpenManage Integration for VMware vCenter の vCenter メニューの下には、OpenManage Integration for VMware vCenter の主なアクセスポイントとして機能する特別なグループがあります。
メインコンテンツ	ナビゲータ ペインで選択したビューが表示されます。メインコンテンツ ペインは、ほとんどのコンテンツが表示される領域です。
通知	vCenter アラーム、タスク、および進行中の動作が表示されます。OpenManage Integration for VMware vCenter では vCenter のアラーム、イベント、およびタスクシステムが統合され、通知 ペインに情報が表示されます。

VMware vCenter Web クライアント内の移動

OpenManage Integration for VMware vCenter は、VMware vCenter の専用の **Dell** グループ内にあります。

1. VMware vCenter にログインします。
2. VMware vCenter のホームページで、**OpenManage Integration** アイコンをクリックします。
   ここでは、次の作業を実行できます。

   - メインコンテンツペインの各タブで、OpenManage Integration for VMware vCenter の接続プロファイルや製品設定の管理、サマリページの表示、その他の作業を行う。
   - **vCenter インベントリリスト** の下の ナビゲータ ペインで、ホストやデータセンター、クラスタを監視する。調べたいホストやデータセンター、クラスタを選択し、**オブジェクト** タブで監視対象のオブジェクトをクリックします。

Web クライアントのアイコン

製品のユーザーインタフェースには、実行するアクション用に、多くのアイコン式アクションボタンがあります。

表 4. 定義されているアイコンボタン

アイコンボタン	定義
	新しい項目を追加または作成する
	接続プロファイル、データセンターおよびクラスタにサーバを追加する
	ジョブを中止する
	リストを折りたたむ
	リストを展開する
	オブジェクトを削除する
	スケジュールを変更する
	編集
	ジョブをパージする
	ファイルをエクスポートする
	WBEM サービスを有効にする

ソフトウェアバージョンの特定

ソフトウェアのバージョンは OpenManage Integration for VMware vCenter の **はじめに** タブにあります。

1. VMware vCenter のホームページで、**OpenManage Integration** アイコンをクリックします。
2. OpenManage Integration for VMware vCenter の **はじめに** タブで、**バージョン情報** をクリックします。
3. **バージョン情報** ダイアログボックスでバージョン情報を確認します。
4. ダイアログボックスを閉じるには、**OK** をクリックします。

画面コンテンツの更新

VMware vCenter の **更新** アイコンを使用して、画面を更新します。

1. 更新したいページを選択します。
2. VMware vCenter タイトルバーで、**更新 （Ctrl+Alt+R）** アイコンをクリックします。
   更新 アイコンは、検索エリアの右側に表示され、時計回りの矢印のように見えます。

Dell ホストの表示

Dell ホストのみをすばやく表示したいときは、OpenManage Integration for VMware vCenter の ナビゲータ ペインで **Dell ホスト** を選択します。

1. VMware vCenter のホームページで、**OpenManage Integration** アイコンをクリックします。
2. **ナビゲータ** の **OpenManage Integration** で、**Dell ホスト** をクリックします。
3. **Dell ホスト** タブに、次の情報が表示されます。
   - **ホスト名** — 各 Dell ホストの IP アドレスを使用したリンクが表示されます。Dell ホスト情報を表示するには、特定のホストリンクをクリックします。
   - **vCenter** — この Dell ホストの vCenter IP アドレスが表示されます。

- **クラスタ** — Dell ホストがクラスタ内にある場合、クラスタ名が表示されます。
- **接続プロファイル** — 接続プロファイルの名前が表示されます。

OpenManage Integration for VMware vCenter ライセンス タブの表示

OpenManage Integration for VMware vCenter ライセンスをインストールすると、ホストと vCenter サーバのサポート可能な数が、このタブに表示されます。ページの上部には、OpenManage Integration for VMware vCenter のバージョンも表示されます。

ライセンスの下のページに **ライセンスの購入** リンクが表示されます。

ライセンス管理 セクションに表示される項目：

- **Product Licensing Portal（Digital Locker）**
- **iDRAC Licensing Portal**
- **管理コンソール**

OpenManage Integration for VMware vCenter の **ライセンス** タブには、次の情報が表示されます。

ライセンス タブ情報	説明
ホストのライセンス	• 使用可能なライセンス 使用可能なライセンスの数を表示します • 使用中のライセンス 使用中のライセンス数を表示します
vCenter **ライセンス**	• 使用可能なライセンス 使用可能なライセンスの数を表示します • 使用中のライセンス 使用中のライセンス数を表示します

ヘルプとサポートへのアクセス

製品について必要な情報を提供するため、OpenManage Integration for VMware vCenter には **ヘルプおよびサポート** タブがあります。このタブでは、次のような情報を得ることができます。

表 5. ヘルプおよびサポート タブの情報

名前	説明
製品ヘルプ	次のリンク • **OpenManage Integration for VMware vCenter ヘルプ** — 製品内にある製品ヘルプへのリンクを提供します。目次または検索を使って、必要な情報を探してください。 • **バージョン情報** - このリンクは **バージョン情報** ダイアログボックスを表示します。ここで製品のバージョンを確認することができます。
Dell マニュアル	次のリンクを提供します： • **サーバー マニュアル** • **OpenManage Integration for VMware vCenter マニュアル**
管理コンソール	管理コンソールへのリンクを提供します。
その他のヘルプおよびサポート	次のリンクを提供します：

名前	説明
	• **Lifecycle Controller 使用 iDRAC のマニュアル** • **Dell VMware マニュアル** • **OpenManage Integration for VMware vCenter 製品ページ** • **Dell ヘルプおよびサポートのホーム** • **Dell TechCenter**
サポート電話のヒント	Dell サポートへの連絡方法と正しい電話の転送についてヒントが記載されています。
トラブルシューティング バンドル	トラブルシューティングバンドルを作成し、ダウンロードするためのリンクを提供します。テクニカルサポートへ連絡するときに、このバンドルを提供するか、参照できます。詳細については、「トラブルシューティングバンドルのダウンロード」を参照してください。
Dell 推奨	Dell Repository Manager (DRM) へのリンクを提供します。DRM を使用して、お使いのシステムで使用可能なすべてのファームウェアアップデートを検索およびダウンロードします。
iDRAC のリセット	iDRAC が応答しないときに使用できる、iDRAC をリセットするためのリンクです。このリセットでは、通常の iDRAC の再起動が実行されます。

トラブルシューティングバンドルのダウンロード

このタスクについて

トラブルシューティングバンドル情報を使用して、トラブルシューティングを支援したり、その情報をテクニカルサポートに送信したりすることができます。トラブルシューティング情報を取得するには、次の手順を実行します。

手順

1. OpenManage Integration for VMware vCenter で、**ヘルプとサポート** タブをクリックします。
2. **トラブルシューティングバンドル** の下で、**トラブルシューティングバンドルの作成およびダウンロード** をクリックします。
3. **作成** ボタンをクリックします。
4. ファイルを保存するには、**ダウンロード** をクリックします。
5. **ファイルダウンロード** ダイアログボックスで、**保存** をクリックします。
6. **名前をつけて保存** ダイアログボックスで、ファイルを保存する場所に移動して、**保存** をクリックします。
7. 終了するには、**閉じる** をクリックします。

iDRAC のリセット

iDRAC のリセット リンクは、**ヘルプおよびサポート** タブにあります。iDRAC をリセットすると、iDRAC は通常の再起動を実行します。iDRAC の再起動では、ホストは再起動されません。リセットを実行した後、使用可能な状態に復帰するには最大 2 分かかります。このリセット操作は、iDRAC が OpenManage Integration for VMware vCenter で反応しなくなった場合に使用してください。

このタスクについて

メモ: デルでは、ホストをメンテナンスモードにした後で、iDRAC をリセットされることをお勧めします。このリセット処置を適用できるホストは、接続プロファイルに含まれ、少なくとも 1 回、インベントリ操作を行っているホストに限ります。このリセット処置では iDRAC を使用可能な状態に戻せないことがあります。このシナリオでは、ハードリセットが必要です。ハードリセットの詳細については、iDRAC のマニュアルを参照してください。

iDRAC の再起動中、以下が見られる場合があります。

- OpenManage Integration for VMware vCenter がその正常性ステータスを取得する間に、通信エラーのわずかな遅延が発生する。
- iDRAC とのオープンセッションがすべて閉じられる。
- iDRAC の DHCP アドレスが変わる。

  iDRAC の IP アドレスに DHCP を使用している場合は、IP アドレスが変わる可能性があります。IP アドレスが変わった場合、ホストのインベントリジョブを再度実行して、インベントリデータで新規 iDRAC IP アドレスを取得します。

手順

1. OpenManage Integration for VMware vCenter で、**ヘルプとサポート** タブをクリックします。
2. iDRAC のリセット で、**iDRAC のリセット** をクリックします。
3. iDRAC のリセット の下にある **iDRAC のリセット** ダイアログボックスに、ホストの IP アドレス / 名前を入力します。
4. iDRAC のリセットプロセスを理解していることを確認するため、**iDRAC のリセットについて理解しました。iDRAC のリセットを続行します** を選択します。
5. **iDRAC のリセット** をクリックします。

オンラインヘルプを開く

オンラインヘルプは、**ヘルプおよびサポート** タブから開くことができます。ヘルプのドキュメントを検索すれば、トピックや手順を理解できます。

1. OpenManage Integration for VMware vCenter で、**製品ヘルプ** の下にある **ヘルプとサポート** をクリックし、**OpenManage Integration for VMware vCenter ヘルプ** をクリックします。
   オンラインヘルプのコンテンツがブラウザのウィンドウに表示されます。
2. 左ペインの目次を使用するか検索機能を使用して、トピックを検索します。
3. オンラインヘルプを閉じるには、ブラウザのウィンドウの右上隅にある **X** をクリックします。

管理コンソールの起動

OpenManage Integration for VMware vCenter は VMware vCenter ウェブクライアント内から起動できます。管理コンソールは **ヘルプとサポート** タブから開きます。

1. OpenManage Integration for VMware vCenter で、**ヘルプとサポート** タブの **管理コンソール** の下にあるコンソールへのリンクをクリックします。
2. **管理コンソール** ログインダイアログボックスで、管理者パスワードを使用してログインします。
   管理コンソールでは、次の操作を実行できます。
   - vCenter の登録または登録解除、資格情報の変更、証明書の更新。
   - ライセンスのアップロード。
   - 登録済みで使用可能な vCenter の数、使用中 / 使用可能な最大ホストライセンス数についての概要の表示。
   - 仮想アプライアンスの再起動。
   - 最新バージョンへのアップデートまたはアップグレード。
   - ネットワーク設定の表示（読み取り専用モード）。
   - アプライアンスをアップグレードしたり、http://downloads.dell.com/published/Pages/index.html に接続したりするための Dell サーバへの接続の HTTP プロキシ設定。
   - NTP 設定。NTP サーバーを有効化または無効化、および優先またはセカンダリ NTP サーバーの設定が可能です。
   - 証明書署名要求（CSR）の生成、証明書のアップロード、または HTTPS 証明書のデフォルト証明書の復元。
   - 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。保存するアラートの最大数、アラートの保持日数、および重複アラートのタイムアウトを設定することができます。
   - すべての vCenter インスタンスに対するアラートの保存方法に関するグローバル設定。
   - バックアップまたは復元の開始。
   - ネットワーク共有へのバックアップ場所の設定、そのバックアップファイル用の暗号化パスワードの設定（ネットワーク接続のテストも行います）。
   - 定期的なバックアップのスケジュール。

ログ履歴の表示

ログのページでは、OMIVV が生成するログを表示できます。

このページの内容は、2 つのドロップダウンリストを使用してフィルタリングしたり、並べ替えたりすることができます。最初のドロップダウンリストでは、次のログタイプをもとにログの詳細をフィルタリングおよび表示できます。

- すべてのカテゴリ
- 情報
- 警告
- エラー

2 つ目のドロップダウンリストでは、次の日付と時刻の頻度を基準にしてログを並べ替えることができます。

- 過去 1 週間
- 過去 1 か月
- 過去 1 年間
- カスタム範囲
  - **カスタム範囲** を選択した場合は、フィルタリングしたい最初の日付と最後の日付を指定して、**適用** をクリックします。

グリッドテーブルには、次の情報が表示されます。

- カテゴリ — ログのカテゴリのタイプを表示します
- 日付と時刻 — ユーザーアクションの日時を表示します
- 説明 — ユーザーアクションの説明を表示します

行のヘッダーをクリックすることで、データグリッドの行を昇順または降順でソートできます。**フィルタ** テキストボックスを使用して、コンテンツの中を検索します。ページのグリッドの下には次の情報が表示されます。

表 6. ログ履歴

ログ情報	説明
合計項目数	すべてのログ項目の合計項目数を表示します
画面ごと項目数	表示された画面ページ上のログ項目の数を表示します。ドロップダウンボックスを使用して、ページあたりの項目数を設定します。
ページ	現在ログ情報を表示しているページを示します。テキストボックスにページ数を入力するか、**前へ** および **次へ** ボタンを使用して、希望のページへ移動します。
前へ または 次へ ボタン	次または前のページに移動します
すべてをエクスポートアイコン	ログの内容を CSV ファイルにエクスポートします

ログの表示

1. OpenManage Integration for VMware vCenter で **監視** タブをクリックします。
2. **ログ** タブに、OpenManage Integration for VMware vCenter のユーザーアクションのログが表示されます。表示されたログの詳細については、「ログ履歴」を参照してください。
3. グリッド内のデータを並べ替えるには、行のヘッダーをクリックします。
4. カテゴリまたは時間ブロックを使用して並べ替えるには、グリッドの前にあるドロップダウンリストを使用します。
5. ログアイテムのページ間を移動するには、**前へ** ボタンと **次へ** ボタンを使用します。

ログファイルのエクスポート

OpenManage Integration for VMware vCenter は、データテーブルからの情報のエクスポートにカンマ区切り値（CSV）ファイル形式を使用します。

1. OpenManage Integration for VMware vCenter で **監視** タブをクリックします。
2. ログの内容を CSV ファイルにエクスポートするには、画面右下角で  アイコンをクリックします。

3. **ダウンロードする場所の選択** ダイアログボックスを選択し、ログ情報の保存先の場所を参照します。
4. **ファイル名** テキストボックスで、デフォルトのファイル名の ExportList.csv を承諾するか、.CSV 拡張子がついた独自のファイル名を入力します。
5. **Save（保存）** をクリックします。

5

OpenManage Integration for VMware vCenter ライセンス

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

- 評価ライセンス — OMIVV バージョン 4.x アプライアンスの初回電源投入時に、自動的にインストールされます。評価バージョンには、OpenManage Integration for VMware vCenter で 5 つのホスト（サーバ）を管理することを可能にする評価ライセンスが含まれています。評価ライセンスは、Dell サーバの第 11 世代以降のバージョンにのみ適用される、90 日の試用期間用のデフォルトライセンスです。
- 標準ライセンス — 完全製品バージョンには、最高 10 の vCenter サーバ用の標準ライセンスが含まれ、OMIVV が管理するホスト接続をいくつでも購入できます。

評価ライセンスから完全標準ライセンスにアップグレードすると、注文の確認に関する電子メールが届きます。その後、Dell Digital ストアからライセンスファイルをダウンロードができます。ライセンス .XML ファイルをローカルシステムに保存し、**管理コンソール**を使用して新しいライセンスファイル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 接続ライセンス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。

メモ: 標準ライセンス期間は 3 年間または 5 年間のみです。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。

ライセンスを購入すると、.XML ファイル（ライセンスキー）を、Dell Digital ストアからダウンロードできるようになります。ライセンスキーをダウンロードできない場合は、www.dell.com/support/softwarecontacts に掲載されている、地域および製品ごとのデルサポートの電話番号までお問い合わせください。

ソフトウェアライセンスの購入およびアップロード

完全製品版にアップグレードするまでは、試用版ライセンスで実行しています。製品の **ライセンスの購入** リンクを使用して Dell ウェブサイトに移動し、ライセンスを購入してください。購入後に、**管理コンソール** を使用してアップロードします。

このタスクについて

メモ: ライセンスの購入 オプションは、試用版ライセンスを使用している場合にのみ表示されます。

手順

1. OpenManage Integration for VMware vCenter で、次のいずれかタスクを実行します。
   - **ライセンス** タブの **ソフトウェアライセンス** の横にある、**ライセンスの購入** をクリックします。
   - **はじめに** タブの **基本タスク** で、**ライセンスの購入** をクリックします。
2. Dell Digital ストアからダウンロードした既知のロケーションに、ライセンスファイルを保存します。
3. ウェブブラウザで、管理コンソールの URL を入力します。
   `https://<ApplianceIPAddress>` の形式を使用してください。
4. **管理コンソール** の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. **ライセンスのアップロード** 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、ライセンスファイルに移動して **参照** をクリックします。
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。

メモ: ライセンスファイルは zip ファイルの形式で送信される場合があります。zip ファイルを解凍し、ライセンスファイル（xml ファイル）のみをアップロードするようにしてください。ライセンスファイルには通常、123456789.xml など、注文番号に基づいた名前が付いています。

6

VMware vCenter 用のアプライアンスの設定

OMIVV の基本インストールと vCenter の登録が完了した後で、OMIVV アイコンをクリックすると**初期設定ウィザード** が表示されます。次の方法のいずれかを使用して、アプライアンス設定を行うことができます。

- **初期設定ウィザード** でアプライアンスを設定する。
- OMIVV の **設定** タブでアプライアンスを設定する。

最初の起動時に、**初期設定ウィザード** を使用して OMIVV アプライアンス設定を行うことができます。それ以降のインスタンスでは、**設定** タブを使用します。

メモ: いずれの方法もユーザーインタフェースは似ています。

設定ウィザードを使用した設定タスク

メモ: DNS 設定を変更した後で、OMIVV 関連タスクの実行中にウェブ通信エラーが表示された場合は、ブラウザのキャッシュをクリアし、ウェブクライアントから一旦ログアウトして、ログインし直します。

設定ウィザードを使用して、次のタスクを表示および実行できます。

- 設定ウィザード ようこそ ページを表示します。
- vCenter を選択します。「vCenter の選択」を参照してください。
- 接続プロファイルを作成します。「接続プロファイルの作成」を参照してください。
- イベントとアラームを設定します。「イベントおよびアラームの設定」を参照してください。
- インベントリジョブをスケジュールします。「インベントリジョブのスケジュール」を参照してください。
- 保証取得ジョブを実行します。「保証取得ジョブの実行」を参照してください。

設定ウィザードの ようこそ ダイアログボックスの表示

vCenter でインストールと登録を行った後に OMIVV を設定するには、次の手順を実行して **初期設定ウィザード** を表示します。

1. vSphere ウェブクライアントで、**ホーム**、**OpenManage Integration** アイコンの順にクリックします。
   次のオプションのいずれかを実行して、初期設定ウィザードにアクセスします。
   - 初めて **OpenManage Integration** アイコンをクリックすると、**初期設定ウィザード** が自動的に表示されます。
   - **OpenManage Integration** → **はじめに** の順にクリックして、**初期設定ウィザードの開始** をクリックします。
2. **ようこそ** ダイアログボックスで手順を確認し、**次へ** をクリックします。

vCenter の選択

このタスクについて
vCenter 選択 ダイアログボックスでは、次の vCenter を設定することができます。

- 特定の vCenter
- すべての 登録済み vCenter

vCenter 選択 ダイアログボックスにアクセスするには、次の手順を実行します。

手順

1. **初期設定ウィザード** の **ようこそ** ダイアログボックスで、**次へ** をクリックします。
2. **vCenters** ドロップダウンリストから、1 つの vCenter またはすべての登録済み vCenter を選択します。

   vCenter がまだ設定されていないか、またはお使いの環境に vCenter を追加した場合は、vCenter を選択します。vCenter 選択 ページでは、1 つまたは複数の vCenter を選択して設定できます。
3. **接続プロファイルの説明** ダイアログボックスで、**次へ** をクリックします。

   メモ: 同じシングルサインオン（SSO）に属する複数の vCenter サーバがある場合、また単一の vCenter サーバを構成することを選択した場合は、それぞれの vCenter が設定されるまで手順 1 ~ 3 を繰り返します。

接続プロファイルの作成

前提条件

接続プロファイルで Active Directory 資格情報を使用する前に、次のことを確認してください。

- Active Directory ユーザーアカウントが Active Directory に存在する。
- iDRAC およびホストが Active Directory ベースの認証用に設定されている。

このタスクについて

接続プロファイルには、OMIVV が Dell サーバに接続する際に使用する iDRAC およびホストの資格情報が保存されます。それぞれの Dell サーバは、OMIVV で管理される接続プロファイルに関連付ける必要があります。単一の接続プロファイルに複数のサーバを割り当てることが可能です。接続プロファイルは、設定ウィザードを使用するか、**OpenManage Integration for VMware vCenter** → **設定** タブで作成できます。iDRAC およびホストにログインするには、Active Directory 資格情報を使用します。

メモ: Active Directory 資格情報は iDRAC とホストの両方に同じものを設定することも、別々に設定することもできます。

メモ: 追加されたホストの数が接続プロファイルの作成に対するライセンス制限を超過する場合は、接続プロファイルを作成できません。

ESXi 6.5 以降を実行しているすべてのホストには、ウェブベースのエンタープライズ管理（WBEM）サービスがあり、デフォルトでは無効になっています。OMIVV では、このサービスがホストとの通信のために実行中であることを必要とします。このサービスは、接続プロファイル ウィザードで有効にできます。OMIVV では、WBEM サービスを使用して ESXi ホストおよび iDRAC の関係を正しく同期します。

手順

1. **接続プロファイルの説明** ダイアログボックスで、**次へ** をクリックします。
2. **接続プロファイルの名前と資格情報** ダイアログボックスで、接続の **プロファイル名** および接続プロファイルの **説明**（オプション）を入力します。
3. **接続プロファイルの名前と資格情報** ダイアログボックスの **iDRAC 資格情報** の下で、iDRAC を設定する際に Active Directory を使用するかどうかによって、次のいずれかの操作を行います。

   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** を選択します。それ以外は、iDRAC 資格情報の設定までスクロールダウンします。
     1. Active Directory の **ユーザー名** 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** かユーザー名@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。
     2. Active Directory の **パスワード** 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。
     3. **パスワードの 確認** にパスワード をもう一度入力します。
     4. 必要に応じて、次のいずれかの操作を実行します。
        - iDRAC 証明書をダウンロードおよび保存して、今後すべての接続でその証明書の検証を行うには、**証明書チェックを有効にする** を選択します。
        - iDRAC 証明書を保存せず、今後すべての接続で iDRAC 証明書チェックを実行しないようにするには、**証明書チェックを有効にする** チェックボックスのチェックを外します。
   - Active Directory なしで iDRAC 資格情報を設定するには、次のいずれかのタスクを実行します。

1. **ユーザー名** 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。
2. **パスワード** 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。
3. **パスワードの 確認** にパスワード をもう一度入力します。
4. 次のいずれかの手順を実行します。
   - iDRAC 証明書をダウンロードおよび保存して、今後すべての接続でその証明書の検証を行うには、**証明書チェックを有効にする** を選択します。
   - iDRAC 証明書を保存せず、今後すべての接続で iDRAC 証明書チェックを実行しないようにするには、**証明書チェックを有効にする** チェックボックスのチェックを外します。

4. **ホストルート** で、次のいずれかの手順を実行します。
   - 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** を選択し、以下の手順を実行します。それ以外の場合は、ホスト資格情報 を設定します。

     1. Active Directory の **ユーザー名** 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** かユーザー名@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。

        メモ: ホストユーザー名とドメインの制限については、下記を参照してください。

        ホストユーザー名の要件：
        - 1 ~ 64 文字長
        - 印刷不可の文字なし
        - " / \ [ ] : ; | = , + * ? < > @ などの無効な文字なし

        ホストドメイン要件：
        - 1 ~ 64 文字長
        - 最初の文字はアルファベットであることが必須
        - スペースは使用不可
        - " / \ [ ] : ; | = , + * ? < > @ などの無効な文字なし
     2. Active Directory の **パスワード** 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。
     3. **パスワードの 確認** にパスワード をもう一度入力します。
     4. 次のいずれかの手順を実行します。
        - ホスト証明書をダウンロードおよび保存して、今後すべての接続でその証明書の検証を行うには、**証明書チェックを有効にする** を選択します。
        - iDRAC 証明書を保存せず、今後すべての接続で iDRAC 証明書チェックを実行しないようにするには、**証明書チェックを有効にする** チェックボックスのチェックを外します。

   - Active Directory なしでホスト資格情報を設定するには、次のタスクを実行します。

     1. **ユーザー名** にあるユーザー名は `root` です。これはデフォルトのユーザー名で、変更することはできませんが、Active Directory が設定されている場合、root に限らず任意の Active Directory ユーザー名を選択することができます。
     2. **パスワード** 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 の資格情報は、ESXi ホストに使われる資格情報と同じです。
     3. **パスワードの 確認** にパスワード をもう一度入力します。
     4. 次のいずれかの手順を実行します。
        - ホスト証明書をダウンロードおよび保存して、今後すべての接続でその証明書の検証を行うには、**証明書チェックを有効にする** を選択します。
        - ホスト証明書を保存せず、今後すべての接続で iDRAC 証明書チェックを実行しないようにするには、**証明書チェックを有効にする** チェックボックスのチェックを外します。

5. **Next**（次へ）をクリックします。
6. **接続プロファイルの関連ホスト** ダイアログボックスで、接続プロファイルのホストを選択して **OK** をクリックします。

メモ: ESXi 6.5 以降を実行しているホストを選択する場合は、 アイコンをクリックして、すべてのホスト上の WBEM サービスを有効にします。

7. 接続プロファイルをテストするには、1 台または複数のホスト **を選択し、次に接続性テスト** をクリックします。

メモ: この手順は任意です。この手順で、ホストおよび iDRAC の資格情報が正しいかどうかを確認します。この手順は任意ですが、接続プロファイルをテストすることをお勧めします。

メモ: WBEM サービスが ESXi 6.5 以降のホストで有効になっていないと、テスト接続は失敗します。

8. プロファイルの作成を完了するには、**次へ** をクリックします。

次へ をクリックすると、ウィザードに入力した詳細情報はすべて保存され、ウィザードから変更できなくなります。設定ウィザードで設定を完了した後であれば、**管理** → **プロファイル** の **接続プロファイル** ページで、この vCenter の詳細情報の接続プロファイルを変更したり、追加で作成したりすることができます。接続プロファイルの変更を参照してください。

メモ: iDRAC Express または Enterprise カードがないサーバでは、このシステムに該当しないという iDRAC テスト接続の結果が出ます。

インベントリジョブのスケジュール

このタスクについて

インベントリスケジュール設定は、設定ウィザードを使用するか、**OpenManage Integration** → **管理** → **設定** タブにある OpenManage Integration で行うことができます。

メモ: OMIVV が常に最新の情報を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のリソースで実行でき、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。

メモ: すべてのホストのインベントリが実行されると、シャーシが自動的に検出されます。シャーシがシャーシのプロファイルに追加されると、シャーシのインベントリが自動的に実行されます。複数の vCenter サーバを持つ SSO 環境では、スケジュールされた時刻にいずれかの vCenter でインベントリが実行されると、すべての vCenter でシャーシのインベントリが自動的に実行されます。

メモ: このページの設定は、設定ウィザードが呼び出されるたびにデフォルトにリセットされます。事前にインベントリに対してスケジュール設定をした場合、以前のスケジュールがデフォルトの設定で上書きされないように、ウィザード機能を完了させる前に、必ずこのページの以前のスケジュールを複製してください。

手順

1. **初期設定ウィザード** の **インベントリのスケジュール** ダイアログボックスで、**インベントリデータ取得の有効化** を選択します（有効でない場合）。デフォルトでは、**インベントリデータ取得の有効化** は有効です。
2. **インベントリデータの取得スケジュール** で、次の手順を実行します。
   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。
      デフォルトでは、**すべての曜日** が選択されています。
   b. **データ取得時刻** テキストボックスに、時刻を HH:MM 形式で入力します。
      入力する時刻は現地時間です。したがって、仮想アプライアンスのタイムゾーンでインベントリを実行したい場合は、現地時間と仮想アプライアンスのタイムゾーンの時間との差を計算して、適切な時刻を入力してください。
   c. 変更内容を適用して続行するには、**次へ** をクリックします。

次へ をクリックすると、ウィザードに入力した詳細情報はすべて保存され、ウィザードから変更できなくなります。設定ウィザードで設定を完了した後であれば、**管理** → **設定** タブからホストのインベントリのスケジュールの詳細を変更することができます。「インベントリジョブスケジュールの変更」を参照してください。Dell.com/support/manuals で入手可能な『*OpenManage Integration for VMware vCenter User's Guide*』（OpenManage Integration for VMware vCenter ユーザーズガイド）の

保証取得ジョブの実行

このタスクについて

保証取得ジョブ設定は、OMIVV の 設定 タブから実行できます。さらに、**ジョブキュー** → **保証** から保証取得ジョブを実行またはスケジュールすることもできます。スケジュールされたジョブは、ジョブキューにリストされています。複数の vCenter サーバが存在する SSO 環境では、シャーシの保証は、いずれかの vCenter の保証が実行されるときに、すべての vCenter で自動的に実行されます。ただし、シャーシプロファイルに追加されていない場合、保証は自動的に実行されません。

メモ: このページの設定は、設定ウィザードが呼び出されるたびにデフォルトにリセットされます。事前に保証取得ジョブの設定をした場合、以前の保証取得ジョブがデフォルトの設定で上書きされないように、ウィザード機能を完了させる前に、必ずこのページで以前のスケジュールした保証取得ジョブを複製してください。

手順

1. **保証のスケジュール** ダイアログボックスで **保証データの取得を有効化** を選択します。
2. **保証データの取得スケジュール** で、次の操作を実行します。
   a. 保証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. 時刻を HH:MM フォーマットで入力します。

      入力する時刻は現地時間です。したがって、仮想アプライアンスのタイムゾーンでインベントリを実行したい場合は、現地時間と仮想アプライアンスのタイムゾーンの時間との差を計算して、適切な時刻を入力してください。
3. 変更内容を適用して続行するには、**次へ** をクリックして、**イベントとアラーム** 設定に進みます。

   次へ をクリックすると、ウィザードに入力した詳細情報はすべて保存され、ウィザードから変更できなくなります。設定ウィザードで設定を完了した後であれば、**設定** タブから保証ジョブスケジュールを変更することができます。保証ジョブスケジュールの変更を参照してください。

イベントおよびアラームの設定

初期設定ウィザード またはイベントとアラームの **設定** タブからイベントおよびアラームの設定を行うことができます。サーバからイベントを受信するため、OMIVV がサーバからのトラップ送信先として設定されています。第 12 世代ホストおよびそれ以降では、SNMP トラップ送信先を iDRAC で設定されるようにします。第 12 世代より前のホストでは、トラップ送信先を OMSA で設定されるようにします。

このタスクについて

メモ: OMIVV は第 12 世代以降のホストで SNMP v1 および v2 アラートをサポートし、第 12 世代より前のホストでは SNMP v1 アラートのみをサポートしています。

手順

1. **初期設定ウィザード** 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を掲載します。これが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** をオンにします。

   メモ: アラームが有効にされている Dell ホストはいくつかの特定の重大イベントに反応してメンテナンスモードに入るため、必要に応じてアラームを修正することができます。

   Dell アラーム警告の有効化 ダイアログボックスが表示されます。
3. 変更内容を適用するには **続行**、変更を取り消すには **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 をオンにした場合のみ実行してください。
4. すべての管理されている Dell サーバで、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。

   メモ: アプライアンスの復元後、イベントおよびアラームの設定は、GUI で有効と表示されていても有効化されていません。設定 タブから、イベントおよびアラーム 設定を再度有効化することができます。
5. **Apply（適用）** をクリックします。

設定 タブを使用した設定タスク

設定 タブを使用して、次の設定タスクを表示および実行できます。

- OMSA リンクを有効化します。「OMSA リンクの有効化」を参照してください。

- 保証期限通知を設定します。「保証期限通知の設定」を参照してください。
- ファームウェアアップデートリポジトリを設定します。「ファームウェアアップデートリポジトリの設定」を参照してください。
- 最新のアプライアンスバージョンの通知を設定します。「アプライアンスの最新バージョン通知の設定」を参照してください。
- イベントとアラームを設定および表示します。「イベントおよびアラームの設定」を参照してください。
- インベントリおよび保証のデータ取得スケジュールを表示します。「インベントリおよび保証のデータ取得スケジュールの表示」を参照してください。

アプライアンスの設定

このセクションでは、OMIVV アプライアンスに関する以下の設定を行います。

- 保証期限通知
- ファームウェアアップデートリポジトリ
- 最新のアプライアンスバージョン通知
- 資格情報の展開

保証期限通知の設定

1. OpenManage Integration for VMware vCenter の **管理** → **設定** タブで、**アプライアンス設定** の下にある **保証期限通知** をクリックします。
2. **保証期限通知** を展開すると、次の項目が表示されます。
   - **保証期限通知** — 設定が有効か無効か
   - **警告** — 初回の警告までの日数の設定
   - **重大度** — 初回の重大警告までの日数の設定
3. 保証期限に関する警告の保証期限しきい値を設定するには、 アイコン（ **保証期限通知** の右側 ）をクリックします。
4. **保証期限通知** ダイアログボックスで、次の手順を実行します。
   a. この設定を有効にするには、**ホストの保証期限通知を有効にする** をオンにします。
   チェックボックスを選択すると、保証期限通知が有効化されます。
   b. **最小日数しきい値アラート** の下で、次の手順を実行します。
      1. **警告** ドロップダウンリストで、保証期限の何日前に警告したいかを日数で選択します。
      2. **重要** ドロップダウンリストで、保証期限の何日前に警告したいかを日数で選択します。
5. **Apply（適用）** をクリックします。

ファームウェアアップデートリポジトリの設定

このタスクについて
OMIVV の **設定** タブで、ファームウェアアップデートリポジトリを設定できます。

手順

1. OpenManage Integration for VMware vCenter で、**管理** → **設定** タブの下、**ファームウェアアップデートリポジトリ** の右側にある **アプライアンス設定** の下で、 アイコンをクリックします。
2. **ファームウェアアップデートリポジトリ** ダイアログボックスで、次のいずれかを選択します。
   - **デルオンライン** - デルのファームウェアアップデートリポジトリを使用する場所（ Ftp.dell.com ）にアクセスできます。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 Dell リポジトリからダウンロードし、管理対象ホストをアップデートします。

     メモ: ネットワーク設定に基づいて、ネットワークでプロキシが必要な場合はプロキシ設定を有効にします。
   - **共有のネットワークフォルダ** - ファームウェアのローカルリポジトリを、CIFS ベースまたは NFS ベースのネットワーク共有に置くことができます。このリポジトリは、デルが定期的にリリースするサーバアップデートユーティリティ（ SUU ）のダンプでも、DRM を使用して作成されたカスタムリポジトリでもかまいません。このネットワーク共有は、OMIVV によってアクセスできるようにする必要があります。

     メモ: CIFS 共有を使用している場合は、リポジトリのパスワードは 31 文字以内にしてください。

3. **共有のネットワークフォルダ** を選択した場合は、次の形式を使用して **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

   メモ: CIFS 共有を使用する場合は、OMIVV によりユーザー名とパスワードを入力が求められます。文字「@、%、,」は、共有ネットワークフォルダのユーザー名またはパスワードには使用できません。
4. ダウンロードが完了したら、**適用** をクリックします。

メモ: ソースからのカタログの読み込みと OMIVV データベースのアップデートには、最長で 20 分かかる場合があります。

アプライアンスの最新バージョン通知の設定

このタスクについて

OMIVV の最新バージョン（RPM、OVF、RPM / OVF）の可用性に関する通知を定期的に受信するには、次の手順を実行して、最新バージョンの通知を設定します。

手順

1. OpenManage Integration for VMware vCenter で、**管理設定** タブの **アプライアンスの設定** の下、**最新バージョンの通知** の右側にある アイコンをクリックします。

   デフォルトでは、最新バージョンの通知は無効になっています。
2. **最新バージョンの通知および取得のスケジュール** ダイアログボックスで、次の手順を実行します。
   a. 最新バージョンの通知を有効にするには、**最新バージョンの通知を有効化** チェックボックスをオンにします。
   b. **最新バージョンの取得スケジュール** の下で、当該のジョブを実行する曜日を選択します。
   c. **最新バージョンの取得時刻** で、必要なローカル時刻を指定します。

      ここで指定する時刻は現地時間です。このタスクが正しい時刻に OMIVV アプライアンスで動作するためには、時差があれば必ず計算するようにしてください。
3. 設定を保存するには **適用**、設定をリセットするには **クリア** をクリックします。操作を中止するには **キャンセル** をクリックします。

展開用の資格情報の設定

展開用の資格情報を使用することで、OS 展開が完了するまでの間、自動検出を使用して検出されたベアメタルシステムと安全に接続するための資格情報を設定できます。iDRAC と安全に接続するため、OMIVV では最初の検出時から展開プロセスの終了まで、展開用の資格情報を使用します。OS の展開プロセスが正常に完了すると、iDRAC 資格情報が OMIVV によって接続プロファイル内で提供されたとおりに変更されます。展開用の資格情報を変更した場合、その時点以降に新しく検出されたすべてのシステムが、新しい資格情報でプロビジョニングされます。ただし、展開用の資格情報の変更前に検出されたサーバ上の資格情報は、この変更の影響を受けません。

このタスクについて

メモ: OMIVV はプロビジョニングサーバとして機能します。展開用の資格情報を使用すれば、自動検出プロセス内でプロビジョニングサーバとして OMIVV を使用する iDRAC と通信することが可能になります。

手順

1. OpenManage Integration for VMware vCenter で、**管理** → **設定** タブの **アプライアンスの設定** の下、**展開用の資格情報** の右側にある アイコンをクリックします。
2. **ベアメタルサーバ展開用の資格情報** の **資格情報** の下に、次の値を入力します。
   - **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。
   - **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。

     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。

     パスワードが一致していることを確認します。
3. 指定した資格情報を保存するには、**適用** をクリックします。

vCenter 設定

このセクションでは、次の vCenter 設定を構成します。

- OMSA リンクを有効化します。「OMSA リンクの有効化」を参照してください。
- イベントとアラームを設定します。「イベントおよびアラームの設定」を参照してください。
- インベントリおよび保証のデータ取得スケジュールを設定します。「インベントリおよび保証のデータ取得スケジュールの表示」を参照してください。

OMSA リンクの有効化

前提条件

OMSA リンクを有効化する前に、OMSA ウェブサーバをインストールおよび設定してください。使用中の OMSA のバージョン、および OMSA ウェブサーバのインストールおよび設定方法については、『*OpenManage Server Administrator* インストールガイド』を参照してください。

このタスクについて

メモ: OMSA が必要なのは、Dell PowerEdge 第 11 世代とこれ以前の世代のサーバーのみです。

手順

1. OpenManage Integration for VMware vCenter にある **管理** → **設定** タブの、**vCenter 設定** の下、OMSA ウェブサーバの URL の右側で アイコンをクリックします。
2. **OMSA ウェブサーバー URL** ダイアログボックスに URL を入力します。
   必ず、HTTPS およびポート番号 1311 を含めた完全な URL を入力してください。

   https://<OMSA サーバ IP または fqdn>:1311
3. OMSA の URL をすべての vCenter サーバに適用するには、**これらの設定をすべての vCenter に適用する** を選択します。

   メモ: このチェックボックスを選択しないと、OMSA の URL は 1 つの vCenter にしか適用されません。
4. 入力した OMSA の URL リンクが動作することを確認するには、ホストの **サマリ** タブへ移動して、**Dell ホスト情報** セクション内で OMSA コンソールのリンクが動作していることを確認します。

イベントおよびアラームの設定

このタスクについて

Dell Management Center のイベントおよびアラーム ダイアログボックスでは、すべてのハードウェアアラームの有効化または無効化を行うことができます。現在のアラートのステータスは、vCenter アラーム タブに表示されます。重要イベントは、データロスが実際に起こったか差し迫っていること、またはシステムの不具合を示しています。警告イベントは、必ずしも重要であるとは限りませんが、将来問題になる可能性があるものを示します。イベントとアラームの有効化は、VMware Alarm Manager を使って行うこともできます。イベントは、ホストとクラスタ ビューの vCenter のタスクおよびイベント タブに表示されます。サーバからイベントを受信するには、OMIVV を SNMP トラップ先として設定します。第 12 世代およびそれ以降のホストでは、SNMP トラップ先は iDRAC で設定されます。第 12 世代より前のホストでは、トラップ先は OMSA で設定されます。イベントおよびアラームの設定は、**管理** → **設定** タブから OpenManage Integration for VMware vCenter を使用して行います。Dell ホストの vCenter アラーム（有効 または 無効）、およびイベント掲載レベルを表示するには、vCenter の **設定** の下で、**イベントおよびアラーム** の見出しを展開します。

メモ: OMIVV は、第 12 世代以降ホストに対して SNMP v1 および v2 アラートをサポートしています。12 世代以前のホストについては、OMIVV がサポートするのは SNMP v1 アラートです。

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します。

手順

1. OpenManage Integration for VMware vCenter の **管理** → **設定** タブで、**vCenter 設定** の下にある **イベントとアラーム** を展開します。
   現在の **Dell ホストの vCenter アラーム**（有効 または 無効）またはすべての vCenter アラーム、および **イベント掲載レベル** が表示されます。
2. アイコン（**イベントとアラーム** の右側にあるアイコン）をクリックします。
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** を選択します。

メモ: アラームが有効にされている Dell ホストは重大イベントに反応してメンテナンスモードに入るため、必要に応じてアラームを修正することができます。

4. すべての管理されている Dell サーバで、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。
   このステップでは変更が有効になるまでに最大 1 分かかります。また、**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利用できます。
5. **イベント掲載レベル** で、すべてのイベントを掲載しない、すべてのイベントを掲載する、重要および警告イベントのみ掲載する、または 仮想化関連の重要および警告イベントのみ掲載する のいずれかを選択します。詳細については、「イベント、アラームおよび正常性の監視」を参照してください。
6. この設定をすべての vCenter に適用したい場合、**これらの設定をすべての vCenter に適用する** を選択します。

   メモ: このオプションを選択すると、既存のすべての vCenter の設定が上書きされます。

   メモ: すでに、設定 タブで 登録済みのすべての vCenter をドロップダウンリストから選択している場合は、このオプションは使用できません。
7. 保存するには、**適用** をクリックします。

インベントリおよび保証のデータ取得スケジュールの表示

1. OpenManage Integration for VMware vCenter の **管理** → **設定** タブで、**vCenter 設定** の下にある **データ取得スケジュール** をクリックします。
   データ取得スケジュール をクリックすると展開して、インベントリおよび保証の編集オプションが表示されます。
2. アイコン（**インベントリの取得** または **保証の取得**）をクリックします。
   インベントリ / 保証データの取得 ダイアログボックスで、インベントリまたは保証の取得について、次の情報を表示できます。
   - インベントリおよび / または保証の取得オプションが有効になっているか無効にされているか。
   - 有効にされている曜日。
   - その日の有効にされている時間。
3. データ取得スケジュールを編集するには、「インベントリジョブスケジュールの変更」または「保証ジョブスケジュールの変更」を参照してください。
4. **データ取得スケジュール** を再度クリックしてインベントリと保証のスケジュールを折りたたみ、1 行で表示します。

7

プロファイル

資格情報プロファイル を使用することで、接続プロファイルとシャーシプロファイルの管理および設定が可能になります。一方、**導入用テンプレート** を使用することで、ハードウェアとハイパーバイザープロファイルの管理および設定が可能になります。

接続プロファイルについて

接続プロファイルでは、仮想アプライアンスが Dell サーバに接続する際に使用する資格情報を含む接続プロファイルを管理および設定できます。それぞれの Dell サーバは、OpenManage Integration for VMware vCenter で管理される 1 つの接続プロファイルのみに関連付ける必要があります。単一の接続プロファイルに複数のサーバを割り当てることができます。**初期設定ウィザード** を実行すると、OpenManage Integration for VMware vCenter から次のタスクを実行して接続プロファイルを管理できるようになります。

- 接続プロファイルの表示
- 接続プロファイルの作成
- 接続プロファイルの変更
- 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表示

接続プロファイルを表示するには、接続プロファイルがすでに存在するか、事前に作成する必要があります。1 つまたは複数の接続プロファイルを作成すると、**接続プロファイル** ページで表示できるようになります。OpenManage Integration for VMware vCenter では、プロファイル内で提供された資格情報を使用して Dell ホストと通信します。

1. OpenManage Integration for VMware vCenter で、**管理** をクリックします。
2. **プロファイル** をクリックして、**資格情報プロファイル** をクリックします。
3. **資格情報プロファイル** を展開して、**接続プロファイル** タブをクリックします。

   作成したすべての接続プロファイルを表示できます。

表 7. 接続プロファイル情報

接続プロファイルのフィールド	説明
プロファイル名	接続プロファイルの名前を表示します。
説明	説明が表示されます (入力されている場合)。
vCenter	FQDN またはホスト名を表示、またはコンテキストに応じて vCenter の IP アドレスを表示します。
関連ホスト	この接続プロファイルに関連付けられたホストが表示されます。複数ある場合、展開アイコンを使ってすべて表示します。
iDRAC 証明書チェック	iDRAC 証明書チェックが有効か無効かを表示します。
ホストルート証明書チェック	ホストルート証明書チェックが有効か無効かを表示します。
作成日	接続プロファイルが作成された日付を表示します。
変更日	接続プロファイルが変更された日付を表示します。

接続プロファイルのフィールド	説明
前回変更担当者	接続プロファイルを修正したユーザーの詳細を表示します。

接続プロファイルの作成

このタスクについて

複数のホストを 1 つの接続プロファイルに関連付けることができます。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。

メモ: この手順中に表示される vCenter ホストは、同じシングルサインオン（SSO）で認証されています。vCenter ホストが表示されない場合、別の SSO にあるか、バージョン 5.5 より前の VMware vCenter を使用していることが考えられます。

ESXi 6.5 以降を実行しているすべてのホストには、ウェブベースのエンタープライズ管理（WBEM）サービスがあり、デフォルトでは無効になっています。OMIVV では、このサービスがホストとの通信のために実行中であることを必要とします。このサービスは、接続プロファイル ウィザードで有効にできます。OMIVV では、WBEM サービスを使用して ESXi ホストおよび iDRAC の関係を正しく同期します。

手順

1. OpenManage Integration for VMware vCenter で、**管理**、**プロファイル**、**資格情報プロファイル**、**接続プロファイル** タブの順に移動し、 アイコンをクリックします。
2. **ようこそ** ページで **次へ** をクリックします。
3. **接続プロファイル** ページで、次の詳細情報を入力します。
   a. **プロファイル** の下で、**プロファイル名** および **説明**（オプション）を入力します。
   b. **vCenter** の下で、プロファイルの作成対象となる vCenter をドロップダウンリストから選択します。
   このオプションでは、各 vCenter に対して 1 つの接続プロファイルを作成できます。
   c. **iDRAC 資格情報** 領域で、次のいずれかの作業を実行します。

      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** を選択します。それ以外の場合は、次の手順に進みます。
        - **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**と**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。
        - iDRAC 証明書の検証については、次のいずれかを選択します。
          * iDRAC 証明書をダウンロードおよび保存して、今後すべての接続でその証明書の検証を行うには、**証明書チェックを有効にする** を選択します。
          * 証明書を検証せず、保存しない場合は、**証明書チェックを有効にする** をオフにします。
      - Active Directory を使用せずに iDRAC 資格情報を設定するには、次の操作を実行します。
        - **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。
        - iDRAC 証明書の検証については、次のいずれかを選択します。
          * iDRAC 証明書をダウンロードおよび保存して、今後すべての接続でその証明書の検証を行うには、**証明書チェックを有効にする** を選択します。

* 証明書を検証せず、保存しない場合は、**証明書チェックを有効にする** を選択しないでください。

d. **ホストルート** エリアで、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。それ以外の場合は、ホスト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**と**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。
  - 証明書の確認のため、次のいずれかを選択します。
    * ホスト証明書をダウンロードおよび保存して、今後すべての接続でその証明書の検証を行うには、**証明書チェックを有効にする** を選択します。
    * ホスト証明書をチェックせず、保存しない場合は、**証明書チェックを有効にする** を選択しないでください。
- Active Directory を使用せずにホスト資格情報を設定するには、次のいずれかの操作を実行します。
  - **ユーザー名** テキストボックスでは、ユーザー名が root です。

    root のユーザー名はデフォルトのユーザー名であり、変更はできません。

    メモ: Active Directory が設定されている場合、root でないどのような Active Directory ユーザー名も選択できます。
  - **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。
  - **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。
  - 証明書の確認のため、次のいずれかを選択します。
    * ホスト証明書をダウンロードおよび保存して、今後すべての接続でその証明書の検証を行うには、**証明書チェックを有効にする** を選択します。
    * ホスト証明書をチェックせず、保存しない場合は、**証明書チェックを有効にする** を選択しないでください。

メモ: OMSA 資格情報は、ESXi ホストに使われたものと同じです。

4. **次へ** をクリックします。
5. **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、**OK** をクリックします。
6. **関連ホスト** ページで、接続プロファイル用のホストを 1 つまたは複数追加します (必要な場合)。

   ホストを追加するには、 アイコンをクリックし、次に **OK** をクリックします。

   メモ: ESXi 6.5 以降を実行しているホストを選択する場合は、 アイコンをクリックして、すべてのホスト上の WBEM サービスを有効にします。
7. 接続プロファイルをテストするには、1 台または複数のホストを選択し、**接続テスト** アイコンをクリックします。

   メモ: このステップは任意です。このステップで、ホストおよび iDRAC の資格情報が正しいかどうかを検証します。任意であっても、接続プロファイルをテストすることをお勧めします。

   メモ: WBEM サービスが ESXi 6.5 以降のホストで有効になっていないと、テスト接続は失敗します。
8. プロファイルの作成を完了するには、**次へ** をクリックします。

   iDRAC Express または Enterprise カードがないサーバでは、このシステムに対する iDRAC テスト接続結果は **該当なし** と表示されます。

接続プロファイルの変更

接続プロファイルを作成した後に、プロファイル名、説明、関連ホストと iDRAC、およびホストの資格情報を編集することができます。

このタスクについて

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 5.5 以前の VMware vCenter を使用しているためと考えられます。

メモ: インベントリ、保証、または展開ジョブが実行中の場合は、接続プロファイルを更新しないようにします。

メモ: インベントリ、保証、または展開ジョブが実行中の場合は、接続プロファイルに関連付けられているホストを別の接続プロファイルに移動したり、接続プロファイルからホストを削除したりしないようにします。

手順

1. OpenManage Integration for VMware vCenter で、**管理** をクリックします。
2. **プロファイル** をクリックし、**資格情報プロファイル** をクリックします。
3. **資格情報プロファイル** を展開してから、**接続プロファイル** をクリックします。
4. プロファイルを選択して、 アイコンをクリックします。
5. **接続プロファイル** ウィンドウの **ようこそ** タブで、情報を読んで **次へ**をクリックします。
6. **名前と資格情報** タブで、次の手順を実行します。

   a. **プロファイル** の下で、**プロファイル名** と **説明** （ オプション ）を入力します。

   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、前記の注記を参照してください。

   c. **iDRAC 資格情報** の下で、次のいずれかの手順を実行します。

   - Active Directory を使用する iDRAC アカウントが、Active Directory に対してすでに設定および有効化されている場合は、**Active Directory を使用する** を選択します。
     - **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。
     - 証明書の確認のため、次のいずれかを選択します。
       * iDRAC 証明書をダウンロードおよび保存して、今後すべての接続でその証明書の検証を行うには、**証明書チェックを有効にする** を選択します。
       * 証明書をチェックせず、保存しない場合は、**証明書チェックを有効にする** を選択しないでください。
   - Active Directory なしで iDRAC 資格情報を設定するには、次のいずれかを入力します。
     - **ユーザー名** - ユーザー名を、**ドメイン\ユーザー名**と**ドメイン@ユーザー名**のいずれかの形式で入力します。
       ユーザー名に使用できる文字は、/ (スラッシュ) 、& (アンパサンド) 、\ (バックスラッシュ) 、. (ピリオド) 、" (引用符) 、@ (アットマーク) 、% (パーセント) です (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) 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** - パスワードを入力します。
       / (スラッシュ) 、& (アンパサンド) 、\ (バックスラッシュ) 、. (ピリオド) 、" (引用符) は、パスワードに使用できません。
     - **パスワードの確認** - パスワードを再入力します。
     - **証明書チェックを有効にする** - デフォルトでは、このチェックボックスはオフになっています。iDRAC 証明書 をダウンロードおよび保存して、今後のすべての接続中に証明書を検証するには、**証明書チェックを有効にする** をオンにします。証明書のチェックを行わず、保存も行わない場合は、**証明書チェックを有効にする** チェックボックスをオンにしないでください。

       メモ: Active Directory を使用する場合は、証明書チェックを有効にする をオンにします。

   d. **ホストルート** で、次のタスクを実行します。

   - Active Directory に関連するすべてのコンソールにアクセスするには、**Active Directory を使用する** チェックボックスをオンにします。
   - **ユーザー名** - デフォルトのユーザー名は root であるため変更できません。**Active Directory を使用する** を選択していれば、任意の Active Directory ユーザー名を使用できます。

メモ: ユーザー名 は root であるため、Active Directory を使用する を選択しないとこのエントリは変更できません。iDRAC ユーザーが root 資格情報を使用することは強制ではないため、Active Directory が設定されている場合は、管理権限を持つどのユーザーでも使用可能です。

- **パスワード** - パスワードを入力します。

  / (スラッシュ) 、& (アンパサンド) 、\ (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。
- **パスワードの確認** - パスワードを再入力します。
- **証明書チェックを有効にする** - デフォルトでは、このチェックボックスはオフになっています。iDRAC 証明書をダウンロードおよび保存して、今後のすべての接続中に証明書を検証するには、**証明書チェックを有効にする** をオンにします。証明書のチェックを行わず、保存も行わない場合は、**証明書チェックを有効にする** チェックボックスをオフにします。

  メモ: Active Directory を使用する場合は、証明書チェックを有効にする をオンにします。

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

  メモ: iDRAC Express または Enterprise カードがないホストの場合、このシステムに対する iDRAC テスト接続結果は 該当なし と表示されます。

7. **次へ**をクリックします。
8. **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。
9. **OK** をクリックします。

   関連ホスト ダイアログボックスで、選択したサーバ上の iDRAC とホストの資格情報をテストできます。

   メモ: ESXi 6.5 以降を実行しているホストを選択する場合は、 アイコンをクリックして、すべてのホスト上の WBEM サービスを有効にします。
10. 次のいずれかの手順を実行します。
    - 資格情報のテストを行わずに接続プロファイルを作成するには、**終了** をクリックします。
    - 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。

      メモ: WBEM サービスが ESXi 6.5 以降のホストで有効になっていないと、テスト接続は失敗します。

      テストが完了したら、**終了** 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、**終了** をクリックします。

メモ: 変更日 と 最終変更者 フィールドには、接続プロファイルのウェブクライアントインタフェースを介して実行する変更が含まれます。OMIVV アプライアンスのそれぞれの接続プロファイルに対して実行するすべての変更は、これら 2 個のフィールドの詳細には影響しません。

接続プロファイルの削除

このタスクについて

メモ: インベントリ、保証、または展開ジョブが実行中の場合は、ホストに関連付けられている接続プロファイルを削除しないようにします。

手順

1. OpenManage Integration for VMware vCenter で、**管理** をクリックします。
2. **プロファイル** をクリックし、**資格情報プロファイル** をクリックします。
3. **資格情報プロファイル** を展開し、**接続プロファイル** タブをクリックして、削除するプロファイルを選択します。
4. 詳細を表示するには、 アイコンをクリックします。
5. プロファイルを削除するには、削除確認メッセージの **はい** をクリックするか、**いいえ** をクリックして、削除操作をキャンセルします。

メモ: OMIVV は、削除した接続プロファイルの一部であるホストは、それらのホストが別の接続プロファイルに追加されるまで管理しません。

接続プロファイルのテスト

1. OpenManage Integration for VMware vCenter で、**管理** をクリックします。
2. **プロファイル** をクリックし、**資格情報プロファイル** をクリックします。
3. **資格情報プロファイル** を展開し、**接続プロファイル** タブをクリックして、接続プロファイルを選択します。
4. **接続プロファイルのテスト** ダイアログボックスで、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。
   接続プロファイルを選択しない場合、テスト接続の実行にある程度の時間がかかります。
5. 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、**すべてのテストを中止** をクリックします。**テストの中止** ダイアログボックスで、**OK** 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。

シャーシプロファイルについて

OMIVV は Dell サーバに関連付けられたすべての Dell シャーシを監視できます。シャーシの監視にはシャーシプロファイルが必要です。シャーシプロファイルは以下のタスクを実行することで管理できます。

- シャーシプロファイルを表示します。「シャーシプロファイルの表示」を参照してください。
- シャーシプロファイルを作成します。「シャーシプロファイルの作成」を参照してください。
- シャーシプロファイルを編集します。「シャーシプロファイルの編集」を参照してください。
- シャーシプロファイルを削除します。「シャーシプロファイルの削除」を参照してください。
- シャーシプロファイルをテストします。「シャーシプロファイルのテスト」を参照してください。

シャーシプロファイルの表示

前提条件
表示する前に、シャーシのプロファイルを作成しているか、またはシャーシプロファイルが存在することを確認します。

このタスクについて
1 つ、または複数のシャーシプロファイルを作成した後、シャーシプロファイル ページでこれらのプロファイルを表示することができます。

手順

1. OpenManage Integration for VMware vCenter で、**管理** をクリックします。
2. **プロファイル** をクリックし、**資格情報プロファイル** をクリックします。
3. **資格情報プロファイル** を展開して、**シャーシプロファイル** タブをクリックします。
   シャーシプロファイルが表示されます。
4. 複数のシャーシがシャーシプロファイルに関連付けられている場合、関連するすべてのシャーシを表示するには、 アイコンをクリックします。
5. **シャーシプロファイル** ページに、シャーシの情報が表示されます。

表 8. シャーシプロファイル情報

シャーシのフィールド	説明
プロファイル名	シャーシプロファイルの名前が表示されます
説明	説明が表示されます（入力されている場合）
シャーシ IP / ホスト名	シャーシの IP アドレスまたはホスト名が表示されます
シャーシサービスタグ	シャーシに割り当てられた固有の識別子が表示されます
変更日	シャーシプロファイルが変更された日付が表示されます

シャーシプロファイルの作成

シャーシプロファイルは、シャーシの監視に必要です。シャーシ資格情報プロファイルを作成して、単一または複数のシャーシと関連付けることができます。

このタスクについて

iDRAC とホストには Active Directory の資格情報を使用してログインすることができます。

手順

1. OpenManage Integration for VMware vCenter で、**管理** をクリックします。
2. **プロファイル** をクリックし、**資格情報プロファイル** をクリックします。
3. **資格情報プロファイル** を展開して、**シャーシプロファイル** タブをクリックします。
4. **シャーシプロファイル** ページで、 アイコンをクリックして、**新しいシャーシプロファイル**を作成します。
5. **シャーシプロファイルウィザード** ページで、次の手順を実行します。

   名前と資格情報 セクションの **シャーシプロファイル** で、次の操作を行います。

   a. **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。
   b. **説明** テキストボックスに説明を入力します。この操作はオプションです。

   資格情報 セクションで、次の操作を行います。

   a. **ユーザー名** テキストボックスに管理者権限のあるユーザー名を入力します。これはシャーシ管理コントローラへのログインに通常使用されるものです。
   b. **パスワード** テキストボックスに対応するユーザー名の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** テキストボックスに入力したものと同じパスワードを入力します。パスワードは一致する必要があります。

   メモ: 資格情報は、ローカルまたは Active Directory のものを使用できます。シャーシプロファイルに 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、シャーシ管理コントローラが Active Directory ベースの認証用に設定されている必要があります。

6. **Next（次へ）** をクリックします。

   シャーシの選択 ページが表示され、使用可能なすべてのシャーシが表示されます。

   メモ: シャーシが検出され、任意のモジュラーホストの正常なインベントリ実行がそのシャーシで認められた後に、初めてシャーシプロファイルに関連付けることができます。

7. 個々のシャーシまたは複数のシャーシのどちらかを選択するには、**IP/ ホスト名** 列の横にある対応するチェックボックスを選択します。

   選択したシャーシがすでに別のプロファイルの一部である場合は、選択したシャーシがプロファイルに関連付けられていることを示す警告メッセージが表示されます。

   たとえば、シャーシ A に関連付けられている **テスト** というプロファイルがあるとします。別のプロファイル **テスト 1** を作成してシャーシ A を **テスト 1** に関連付けようとすると、警告メッセージが表示されます。

8. **OK** をクリックします。

   関連付けられたシャーシ ページが表示されます。

9. シャーシの接続性をテストするには、シャーシを選択し、**接続テスト** アイコンをクリックします。これによって資格情報が検証され、その結果が **テスト結果** 列に **合格** または **失敗** として表示されます。
10. プロファイルを完了するには、**終了** をクリックします。

シャーシプロファイルの編集

シャーシプロファイルの作成後、プロファイル名、説明、関連シャーシ、および資格情報を編集することができます。

1. OpenManage Integration for VMware vCenter で、**管理** をクリックします。
2. **プロファイル** をクリックし、**資格情報プロファイル** をクリックします。

3. **資格情報プロファイル** を展開して、**シャーシプロファイル** タブをクリックし、シャーシプロファイルを選択します。
4. メインメニューで、 アイコンをクリックします。
   シャーシプロファイルの編集 ウィンドウが表示されます。
5. **シャーシプロファイル** では、**プロファイル名** および **説明** （ オプション ）を編集できます。
6. **資格情報** エリアで、**ユーザー名**、**パスワード** および **パスワードの確認** を編集できます。
   パスワードの確認 に入力するパスワードは、**パスワード** フィールドに入力したものと同じである必要があります。入力する資格情報は、シャーシの管理者権限を持っている必要があります。
7. 変更を保存するには、**適用** をクリックします。
   関連シャーシ タブでは、選択したシャーシ上でシャーシと資格情報をテストできます。次のいずれかの手順を実行します。
   - テストを開始するには、チェック対象のシャーシを 1 つまたは複数選択して、**テスト接続** アイコンをクリックします。**テスト結果** 列に、テスト接続が正常に行われたかどうかが表示されます。
   - 1 つまたは複数のシャーシを、シャーシプロファイルに追加または削除することができます。

メモ: シャーシがインベントリされていない場合は、IP/ ホスト名とサービスタグのみが表示されます。シャーシ名 フィールド と モデル フィールドは、シャーシがインベントリされると表示されます。

シャーシプロファイルの削除

1. OpenManage Integration for VMware vCenter で、**管理** をクリックします。
2. **プロファイル** をクリックし、**資格情報プロファイル** をクリックします。
3. **資格情報プロファイル** を展開して、**シャーシプロファイル** タブをクリックします。
4. 削除するシャーシプロファイルを選択して、 アイコンをクリックします。
   警告メッセージが表示されます。
5. 削除を続行するには **はい**、キャンセルするには **いいえ** をクリックします。
   シャーシプロファイルに関連付けられているすべてのシャーシがクリアされるか、別のプロファイルに移動された場合は、削除の確認メッセージが表示され、シャーシプロファイルに関連するシャーシが存在しないためにシャーシプロファイルが削除されることが示されます。シャーシプロファイルを削除するには、削除の確認メッセージの **OK** をクリックします。

メモ: 削除したシャーシプロファイルに関連付けられているシャーシが他のシャーシプロファイルに追加されない限り、OMIVV では当該のシャーシを監視しません。

シャーシプロファイルのテスト

1. OpenManage Integration for VMware vCenter で、**管理** をクリックします。
2. **プロファイル** をクリックし、**資格情報プロファイル** をクリックします。
3. **資格情報プロファイル** を展開し、**シャーシプロファイル** タブをクリックして、テスト対象となる単一または複数のシャーシプロファイルを選択します。
   この操作には数分かかることがあります。
4. **シャーシプロファイルのテスト** ダイアログボックスで、テストするシャーシを選択してから、**テスト接続** アイコンをクリックします。
5. 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、**すべてのテストを中止** をクリックします。**テストの中止** ダイアログボックスで、**OK** 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。

8

インベントリおよび保証の管理

OMIVV を設定すると、**監視** タブで、インベントリや保証ジョブの監視、導入ジョブの管理、およびファームウェアアップデートジョブを管理できるようになります。インベントリと保証は、**初期設定ウィザード** または **設定** タブで設定します。

ジョブキュー ページでは、次のジョブを管理します。

- 送信されたサーバ展開やファームウェアアップデートジョブの表示
- ファームウェアのアップデートまたは展開ジョブ、またはインベントリ / 保証履歴キューの更新
- インベントリまたは保証ジョブのスケジュール設定
- ファームウェアのアップデートまたは展開ジョブのキュー項目のページ

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、最低でも週に 1 回は、インベントリ / 保証ジョブの実行をスケジュールしてください。

このページで実行できるタスクには、次のようなものがあります。

- 展開ジョブの管理
- ファームウェアアップデートジョブの管理
- インベントリジョブの管理
- 保証ジョブの管理

メモ: 記述されているすべてのジョブで、アプライアンスの時刻を将来の日付に変更して、元に戻す場合は再度スケジュールされていることを確認してください。

メモ: 正常性の基本的な監視には、OMIVV アプライアンスを再起動してください。正常性の拡張的な監視には、拡張監視 を無効にし、OMIVV 管理コンソールから有効にしてください。

インベントリジョブ

インベントリジョブは、**設定** タブまたは **初期設定ウィザード** を使用して設定します。**インベントリ履歴** タブを使用して、すべてのインベントリジョブを表示します。このタブで実行できるタスクには、次のようなものがあります。

- ホストまたはシャーシのインベントリの表示
- インベントリジョブスケジュールの変更
- シャーシのインベントリジョブを今すぐ実行する

ホストインベントリの表示

データを収集するには、インベントリが正常に完了している必要があります。インベントリが完了すると、データセンター全体または個別のホストシステムに関するインベントリ結果を表示できます。インベントリビューの行は、昇順または降順にソートできます。

このタスクについて

メモ: ホストデータが取得および表示できない場合に考えられる理由を、以下にいくつか示します。

- ホストに接続プロファイルが関連付けられていないため、インベントリジョブを実行できない。
- データを収集するインベントリジョブがホストで実行されていないので、表示できるデータがない。
- 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使用可能な追加ライセンスが必要。
- このホストに、Dell PowerEdge サーバの第 12 世代以降に必要な正しい iDRAC ライセンスがないため、正しい iDRAC ライセンスを購入する必要がある。
- 資格情報が誤っている可能性がある。
- ホストに到達可能でない場合がある。

ホストインベントリの詳細を表示するには、次の手順を実行します。

手順

1. OpenManage Integration for VMware vCenter で **監視** タブをクリックします。
2. **ジョブキュー** をクリックし、**インベントリ履歴** を展開し、次に **ホストインベントリ** をクリックします。
   vCenter の情報は上部のグリッドに表示されます。
3. 選択した vCenter でのホスト情報を表示するには、表示する vCenter を選択して関連するホストのすべての詳細情報を表示します。
4. ホストインベントリ情報を確認します。

表 9. vCenter とホスト情報

vCenter	
vCenter	vCenter アドレスを表示します
ホスト合格	合格したホストを表示します
最新のインベントリ	最新のインベントリスケジュールが実行された日付と時刻を表示します
次のインベントリ	次のインベントリスケジュールが実行される日付と時刻を表示します
ホスト	
ホスト	ホストのアドレスを表示します。
ステータス	ステータスが表示されます。オプションには以下のものがあります。 • 成功 • Failed（失敗） • 進行中 • スケジュール済み
継続時間（MM:SS）	ジョブの継続時間を分と秒で表示します
開始日時	インベントリスケジュールが開始した日付と時刻を表示します
終了日時	インベントリスケジュールが終了した時刻を表示します

シャーシインベントリの表示

正常に完了したインベントリは、データを収集する必要があります。インベントリビューの列は、昇順または降順に並べ替えることができます。

1. OpenManage Integration for VMware vCenter で **監視** タブをクリックします。
2. **ジョブキュー** をクリックし、**インベントリ履歴** を展開して、**シャーシインベントリ** をクリックします。
3. シャーシインベントリ情報を確認します。

表 10. シャーシ情報

シャーシインベントリ	
シャーシ IP	シャーシ IP アドレスが表示されます
Service Tag	シャーシのサービスタグを表示します。サービスタグは、サポートとメンテナンスのためにメーカーが提供する一意の識別子です
ステータス	シャーシのステータスが表示されます
継続時間 （MM:SS）	ジョブの継続時間を分と秒で表示します
開始日時	インベントリスケジュールが開始した日付と時刻を表示します
終了日時	インベントリスケジュールが終了した時刻を表示します

インベントリジョブスケジュールの変更

インベントリに最新のホスト情報が含まれていることを確認するため、最低でも週に 1 回はインベントリジョブの実行をスケジュールします。インベントリ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。インベントリジョブのスケジュールの変更は、**初期設定ウィザード** または **監視** タブから行います。

このタスクについて

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

- 毎週の特定の時刻と曜日
- 一定の期間ごと

ホストシステムでインベントリを実行するには、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ます。

手順

1. Dell OpenManage Integration for VMware vCenter で **監視** タブをクリックします。
2. **ジョブキュー**、**インベントリ履歴**、**ホストインベントリ** の順にクリックします。
3. vCenter を選択し、 アイコンをクリックします。
4. **インベントリデータの取得** ダイアログボックスで、次の手順を行います。
   a. **インベントリデータ** の下にある **インベントリデータ取得の有効化** チェックボックスを選択します。
   b. **インベントリデータの取得スケジュール** の下からジョブを実行する曜日を選択します。
   c. **インベントリデータの取得時間** テキストボックスで、このジョブに対するローカル時刻を入力します。
   場合によっては、ジョブ設定とジョブ実装の時間差を考慮する必要があります。
5. 設定を保存するには **適用**、設定をリセットするには **クリア** をクリックします。操作を中止するには **キャンセル** をクリックします。
6. すぐにジョブを実行するには、OpenManage Integration for VMware vCenter の **監視** → **ジョブキュー** タブで、**インベントリ履歴** → **ホストインベントリ** の順にクリックします。
7. をクリックし、**成功** ダイアログボックスで **閉じる** をクリックします。

メモ: モジュラーホストのインベントリを実行すると、対応するシャーシが自動的に検出されます。シャーシがすでにシャーシプロファイルに含まれていれば、ホストのインベントリの後にシャーシのインベントリが自動的に実行されます。

インベントリジョブをすぐにスケジュールすると、インベントリジョブがキューに入ります。単一ホストに対するインベントリは実行できません。すべてのホストに対してインベントリジョブが開始されます。

インベントリジョブの実行

1. **設定ウィザード** を終了すると、接続プロファイルに追加されたすべてのホストについて、自動的にインベントリが開始されます。それ以降にインベントリをオンデマンドで実行するには、**ジョブキュー** → **インベントリ** → **今すぐ実行** の順にクリックしてインベントリジョブを実行します。
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
- 保管時
- ファームウェア
- 電源モニタ

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

シャーシのインベントリのジョブを今すぐ実行する

Chassis Inventory（シャーシインベントリ）タブで、シャーシインベントリジョブを表示および実行することができます。

1. Dell OpenManage Integration for VMware vCenter で **監視** タブをクリックします。
2. **ジョブキュー**、**インベントリ履歴**、**シャーシインベントリ** の順にクリックします。
   最後のインベントリジョブのシャーシとステータスのリストが表示されます。

   メモ: スケジュールされたシャーシインベントリは、スケジュールされたホストインベントリと同時に実行されます。
3. をクリックします。
   アップデートされたインベントリ済みシャーシのリストが表示され、各シャーシに対して **成功** または **失敗** ステータスが示されます。

保証ジョブ

ハードウェア保証情報はデルオンラインから取得され、OMIVV によって表示されます。サーバに関する保証情報の収集には、サーバのサービスタグが使用されます。保証データの取得ジョブを設定するには、**初期設定ウィザード**を使用します。
このタブで実行できるタスクには、次のようなものがあります。

- 保証履歴の表示
- 保証ジョブスケジュールの変更
- 保証ジョブを今すぐ実行する
- シャーシ保証ジョブを今すぐ実行する

保証履歴の表示

保証ジョブは、すべてのシステムに関する保証情報を Support.dell.com から取得するためにスケジュールされたタスクです。インベントリビューの行は、昇順または降順で並べ替えることができます。

このタスクについて

メモ: 保証情報を抽出するには、OMIVV アプライアンスがインターネットに接続している必要があります。OMIVV アプライアンスがインターネットに接続していることを確認してください。ネットワークの設定によっては、インターネットに接続して保証情報を取得するために、OMIVV でプロキシ情報が必要になる可能性があります。プロキシの詳細は管理コンソールで更新できます。詳細については、「HTTP プロキシの設定」を参照してください。

手順

1. Dell OpenManage Integration for VMware vCenter で **監視** タブをクリックします。
2. **ジョブキュー** をクリックし、**保証履歴** をクリックします。

3. **保証履歴** を拡張して、**ホスト保証** および **シャーシ保証** を表示します。
4. 対応する保証ジョブ履歴情報を表示するには、**ホスト保証** を選択し、vCenter を選択して、関連するすべてのホストの詳細を表示します。

表 11. vCenter およびホスト履歴情報

vCenter 履歴	
vCenters	vCenters のリストが表示されます
ホスト合格	合格した vCenter ホスト数が表示されます
前の保証	最後の保証ジョブを実行した日付と時刻が表示されます
次の保証	次回の保証ジョブを実行する日付と時刻が表示されます
ホストの履歴	
ホスト	ホストのアドレスが表示されます
ステータス	ステータスが表示されます。オプションには以下のものがあります。 • 成功 • Failed（失敗） • 進行中 • スケジュール済み
継続時間（MM:SS）	保証ジョブの継続時間が MM:SS 単位で表示されます
開始日時	保証ジョブが開始された日付と時刻が表示されます
終了日時	保証ジョブが終了した時刻が表示されます

シャーシ保証の表示

保証ジョブは、すべてのシステムに関する保証情報を Support.dell.com から取得するためにスケジュールされたタスクです。インベントリビューの行は、昇順または降順で並べ替えることができます。

1. Dell OpenManage Integration for VMware vCenter で **監視** タブをクリックします。
2. **ジョブキュー** をクリックし、**保証履歴** をクリックします。
3. **保証履歴** を拡張して、**ホスト保証** および **シャーシ保証** を表示します。
4. **シャーシ保証** をクリックします。
5. シャーシ保証の詳細を表示します。

表 12. シャーシ情報

シャーシ履歴	
シャーシ IP	シャーシ IP アドレスが表示されます
Service Tag	シャーシのサービスタグを表示します。サービスタグは、サポートとメンテナンスのためにメーカーが提供する一意の識別子です
ステータス	シャーシのステータスが表示されます
継続時間（MM:SS）	保証ジョブの継続時間が MM:SS 単位で表示されます
開始日時	保証ジョブが開始された日付と時刻が表示されます
終了日時	保証ジョブが終了した時刻が表示されます

保証ジョブスケジュールの変更

保証ジョブは **初期設定ウィザード** で最初に設定します。**設定** タブから、保証ジョブスケジュールを変更できます。

1. Dell OpenManage Integration for VMware vCenter で **監視** タブをクリックします。
2. **ジョブキュー** をクリックし、**保証履歴** をクリックします。
3. **保証履歴** を拡張して、**ホスト保証** および **シャーシ保証** を表示します。
4. 対応する保証ジョブ履歴情報を表示するには、**ホスト保証** または **シャーシ保証** のいずれかを選択します。
5. アイコンをクリックします。
6. **保証データの取得** ダイアログボックスで、次の手順を行います。
   a. **保証データ** の下にある **保証データの取得を有効化** チェックボックスを選択します。
   b. **保証データの取得スケジュール** の下から保証ジョブを実行する曜日を選択します。
   c. **保証データの取得時間** テキストボックスで、このジョブを実行するローカル時刻を入力します。
   このジョブを正しい時刻に実行するために、時差を計算する必要がある場合があります。
7. **Apply（適用）** をクリックします。

ホスト保証ジョブを今すぐ実行する

保証ジョブは、最低でも週に 1 回実行してください。

1. Dell OpenManage Integration for VMware vCenter で **監視** タブをクリックします。
2. **ジョブキュー** をクリックし、**保証履歴** をクリックします。
3. **保証履歴** を拡張して、**ホスト保証** および **シャーシ保証** を表示します。
4. 対応する保証ジョブ履歴情報を表示するには、**ホスト保証** または **シャーシ保証** のいずれかを選択します。
5. 実行したい保証ジョブを選択して、 アイコンをクリックします。
6. **成功** ダイアログボックスで **閉じる** をクリックします。
   これで、保証ジョブがキューに入ります。

メモ: ホストの保証の実行が開始すると、すべてのシャーシに対するシャーシの保証が自動的に実行されます。複数の vCenters を持つ SSO 環境では、いずれかの vCenter で保証が手動で実行されると、すべての vCenter でシャーシの保証が自動的に実行されます。

シャーシ保証ジョブを今すぐ実行する

保証ジョブは、最低でも週に 1 回実行してください。

1. OpenManage Integration for VMware vCenter で、**監視** → **ジョブキュー** タブの順に移動します。
2. 実行する保証ジョブを選択するには、**保証履歴**、**シャーシ保証** の順にクリックします。
3. アイコンをクリックします。
4. **成功** ダイアログボックスで **閉じる** をクリックします。
   これで、保証ジョブがキューに入ります。

単一ホストの監視

OpenManage Integration for VMware vCenter では、単一ホストの詳細情報を表示できます。ナビゲータ ペインにすべてのベンダーのすべてのホストが表示され、ここから VMware vCenter 内のホストにアクセスできます。より詳細な情報を検索するには、特定の Dell ホストをクリックします。Dell ホストのリストを表示するには、OpenManage Integration for VMware vCenter の ナビゲータ ペインで **Dell ホスト** をクリックします。

ホストサマリ詳細の表示

このタスクについて

個々のホストのホストサマリ詳細は、**ホストサマリ** ページで表示できます。このページにはさまざまなポートレットが表示され、そのうちの 2 つが OpenManage Integration for VMware vCenter に適用されます。2 つのポートレットとは次のものです。

- Dell ホストの正常性
- Dell ホスト情報

これら 2 つのポートレットは希望する位置にドラッグ & ドロップすることができ、要件に応じて 2 つのポートレットを他のポートレットと同様にフォーマットおよびカスタマイズすることができます。ホストサマリの詳細を表示するには、次の手順を実行します。

手順

1. OpenManage Integration for VMware vCenter の ナビゲータ ペインで、**ホスト** をクリックします。
2. **オブジェクト** タブで、確認したい特定のホストを選択します。
3. **サマリ** タブをクリックします。
4. ホストサマリの詳細を表示します。

   表 13. ホストサマリ情報

情報	説明
代替システム	ステータスエリアの下、ポートレットの前にある黄色のボックスに OpenManage Integration for VMware vCenter に対するアラートが表示されます。
タスクトレイ	右側パネルエリアに Dell 製品の統合情報が表示されます。次の情報が表示されます。 • 最近のタスク • 進行中の作業 • アラーム タスクトレイポートレットに Dell のアラーム情報が表示されます。

5. スクロールダウンすると、Dell Server Management ポートレットが表示されます。

   表 14. Dell サーバ管理ポートレット

情報	説明
サービスタグ	お使いの Dell PowerEdge サーバのサービスタグが表示されます。この ID は、サポートに電話をする際に使用します。
モデル名	サーバのモデル名を表示します。
耐障害性メモリ	BIOS 属性の状態が表示されます。BIOS 属性は、サーバの初回セットアップ中に BIOS で有効化され、サーバのメモリ動作モードを表示します。メモリ動作モード値を変更するときはシステムを再スタートします。これは、耐障害性メモリ(FRM)オプション対応で、ESXi 5.5 以降のバージョンを実行する PowerEdge サーバの第 12 世代以降に該当します。BIOS 属性の値は次の 4 つです。 • 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 : この値はオペレーティングシステムのバージョンが ESXi 5.5 未満のシステムをサポートすることを示しています。

情報	説明
	• 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、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。
ID	次が表示されます： • ホスト名 — Dell ホストの名前が表示されます • 電源状態 — 電源がオンかオフかが表示されます • iDRAC IP — iDRAC の IP アドレスが表示されます • 管理 IP — 管理 IP アドレスが表示されます • 接続プロファイル — このホストの接続プロファイル名が表示されます • モデル — Dell サーバのモデルが表示されます • サービスタグ — サーバのサービスタグが表示されます • 資産タグ — 資産タグが表示されます • 保証残日数 — 保証の残りの日数が表示されます • 最終インベントリスキャン — 最終インベントリスキャンの日付と時刻が表示されます
ハイパーバイザー & ファームウェア	次が表示されます： • ハイパーバイザー — ハイパーバイザーのバージョンが表示されます • BIOS バージョン — BIOS バージョンが表示されます • リモートアクセスカードバージョン — リモートアクセスカードバージョンが表示されます
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。 • Remote Access Console（iDRAC）の起動 — 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。 • OMSA コンソールの起動 — OMSA コンソールを起動して OpenManage Server Administrator ユーザーインタフェースにアクセスします。
ホストアクション	さまざまな間隔で点滅するように、物理サーバを設定します。「インジケータライトの点滅」を参照してください。

6. Dell ホストの正常性のポートレットの表示：

表 15. Dell ホストの正常性

情報	説明
Dell ホストの正常性	コンポーネントの正常性は、すべての主要なホストサーバコンポーネントの状態を、図式で表したものです。サーバグローバルステータス、サーバ、電源装置、温度、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、電源とメモリがあります。シャーシの正常性パラメータは、VRTX バージョン 1.0 以降、バージョン 4.4 以降がインストールされている M1000e のモデルに適用されます。バージョン 4.3 より以前では、2 つの正常性インジケータのみが表示され、それらは 正常 および 警告または重大（逆三角形にオレンジ

情報	説明
	色の感嘆符)となります。全般的な正常性は、正常性パラメータが最も少ないシャーシに基づいた正常性を示します。次のオプションが含まれます。 • 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です。

例えば、正常記号が 5 つ、警告記号が 1 つある場合には、全般的な正常性は警告として表示されます。

単一ホストのハードウェアの詳細の表示

このタスクについて

Dell ホスト情報 タブで、単一ホストのハードウェア詳細を表示できます。このページに情報を表示するには、インベントリジョブを実行します。ハードウェアビューでは、OMSA および iDRAC からのデータを直接レポートします。「インベントリジョブの実行」を参照してください。

手順

1. OpenManage Integration for VMware vCenter の ナビゲータ ペインで、**ホスト** をクリックします。
2. **ホスト** タブで、ハードウェア：<会社名> 詳細を表示するホストを選択します。
3. **監視** タブで、**Dell ホスト情報** タブを選択します。

   ハードウェア：<会社名> サブタブに、各コンポーネントに関する次の情報が表示されます。

表 16. 単一ホストのハードウェア情報

ハードウェア：コンポーネント	情報
ハードウェア：FRU	• **パーツ名** — FRU のパーツ名が表示されます • **パーツ番号** — FRU のパーツ番号が表示されます • **製造元** — 製造元の名前が表示されます • **シリアルナンバー** — 製造元のシリアルナンバーが表示されます • **製造日** — 製造日が表示されます
ハードウェア：プロセッサ	• **ソケット** — スロット番号が表示されます • **速度** — 現在の速度が表示されます • **ブランド** — プロセッサのブランドが表示されます • **バージョン** — プロセッサのバージョンが表示されます • **コア** — このプロセッサ内のコアの数が表示されます
ハードウェア：電源装置	• **タイプ** — 電源装置のタイプが表示されます。電源装置には、次のタイプがあります。 – 不明 – リニア – スイッチング – BATTERY – UPS – コンバータ – レギュレータ

ハードウェア：コンポーネント	情報
	– AC – DC – VRM • **場所** — スロット 1 など、電源装置の場所が表示されます • **出力（ワット）** — ワット単位で電力が表示されます
ハードウェア: メモリ	• **メモリスロット** — 使用済み、合計、および使用可能なメモリ数が表示されます • **メモリ容量** — インストール済みメモリ、総メモリ容量、および利用可能なメモリが表示されます • **スロット** — DIMM スロットが表示されます • **サイズ** — メモリサイズが表示されます • **タイプ** — メモリのタイプが表示されます
ハードウェア: NIC	• **合計** — 使用可能なネットワークインタフェースカードの合計数が表示されます • **名前** — NIC 名が表示されます • **製造元** — 製造元の名前のみが表示されます • **MAC アドレス** — NIC の MAC アドレスが表示されます
ハードウェア: PCI スロット	• **PCI スロット** — 使用済み、合計、および使用可能な PCI スロット数が表示されます • **スロット** — スロットが表示されます • **製造元** — PCI スロットのメーカー名が表示されます • **説明** — PCI デバイスの説明が表示されます • **タイプ** — PCI スロットタイプが表示されます • **幅** — データバス幅が表示されます（該当する場合）
ハードウェア: リモートアクセスカード	• **IP アドレス** — リモートアクセスカードの IP アドレスが表示されます • **MAC アドレス** — リモートアクセスカードの MAC アドレスが表示されます • **RAC タイプ** — リモートアクセスカードのタイプが表示されます • **URL** — このホストに関連付けられた動作している iDRAC の URL が表示されます

単一ホストのストレージ詳細の表示

このタスクについて

Dell ホスト情報 タブで、単一ホストのストレージ詳細を表示できます。このページで情報を表示させるには、インベントリジョブを実行します。ハードウェアにより OMSA および iDRAC からのデータが直接報告されます。「インベントリジョブの実行」を参照してください。ページに表示されるオプションは、**表示** ドロップダウンリストで選択した項目によって異なります。**物理ディスク** を選択すると、別のドロップダウンリストが表示されます。次のドロップダウンリストをフィルタといい、物理ディスクのオプションをフィルタリングできます。ストレージ詳細を表示するには、次の手順を実行します。

手順

1. OpenManage Integration for VMware vCenter の ナビゲータ ペインで、**ホスト** をクリックします。
2. **オブジェクト** タブで、ストレージ：物理ディスク詳細を表示したいホストを選択します。
3. **監視** タブで、**Dell ホスト情報** タブを選択します。

   ストレージ サブタブで、次の項目を表示します。

表 17. 単一ホストのストレージ詳細

コンポーネント	情報
保管時	仮想ディスク、コントローラ、エンクロージャ、および関連する物理ディスク(グローバルホットスペアおよび専用ホットスペア数とともに)の数が表示されます。表示 ドロップダウンリストからオプションを選択すると、そのオプションがハイライトされます。
表示	このホストに対して表示するオプションが表示されます。 • 仮想ディスク • 物理ディスク • コントローラ • エンクロージャ

表示オプションのストレージ詳細の表示

ホストストレージ ページのストレージオプションは、**表示** ドロップダウンリストで選択した項目によって異なります。
表示 ドロップダウンリストから前述のオプションのいずれかを選択し、次の項目を表示します。

表 18. 単一ホストのストレージ詳細

情報	説明
仮想ディスク	• **名前** — 仮想ディスクの名前が表示されます • **デバイス FQDD** — FQDD が表示されます • **物理ディスク** — 仮想ディスクが配置されている物理ディスクが表示されます • **容量** — 仮想ディスクの容量が表示されます • **レイアウト** — 仮想ストレージのレイアウトタイプ、すなわちこの仮想ディスクに設定された RAID のタイプが表示されます • **メディアタイプ** — SSD と HDD のいずれかが表示されます • **コントローラ ID** — コントローラ ID が表示されます • **デバイス ID** — デバイス ID が表示されます • **ストライプサイズ** — ストライプサイズが表示されます。ストライプサイズは、各ストライプが単一ディスク上で消費する容量です • **バスプロトコル** — 仮想ディスクに含まれる物理ディスクが使用する技術を表示します。表示される可能性のある値は次のとおりです。 – SCSI – SAS – SATA • **デフォルト読み取りポリシー** — コントローラでサポートされているデフォルト読み取りポリシーが表示されます。オプションには次のようなものがあります。 – 先読み – 先読みなし – 適応先読み – 読み取りキャッシュが有効 – 読み取りキャッシュが無効 • **デフォルト書き込みポリシー** — コントローラでサポートされているデフォルト書き込みポリシーが表示されます。オプションには次のようなものがあります。 – ライトバック – ライトバックの強制 – ライトバックが有効 – ライトスルー

情報	説明
	– 書き込みキャッシュ有効、保護 – 書き込みキャッシュが無効 • **キャッシュポリシー** — キャッシュポリシーが有効かどうかが表示されます
物理ディスク — このオプションを選択すると、**フィルタ** ドロップダウンリストが表示されます。 次のオプションに基づいて、物理ディスクをフィルタリングできます。 • すべての物理ディスク • グローバルホットスペア • 専用ホットスペア • 最後のオプションでは、カスタム名の仮想ディスクが表示されます	• **名前** — 物理ディスクの名前が表示されます • **デバイス FQDD** — デバイス FQDD が表示されます • **容量** — 物理ディスクの容量が表示されます • **ディスクステータス** — 物理ディスクのステータスが表示されます。オプションには次のようなものがあります。 – オンライン – 準備完了 – 劣化 – エラー – オフライン – 再構成中 – 互換性なし – 削除済み – クリア済み – SMART アラートが検知されました – 不明 – 外部 – サポートなし • **設定済み** — ディスクが設定されているかどうかが表示されます • **ホットスペアタイプ** — ホットスペアのタイプを示します。オプションには次のようなものがあります。 – いいえ — ホットスペアなし – グローバル — ディスクグループの一部であるが未使用のバックアップディスク – 専用 — 単一の仮想ディスクに割り当てられた未使用のバックアップディスク。仮想ディスク内の物理ディスクが故障すると、ホットスペアが有効化されて故障した物理ディスクと交換されるため、システムが中断することや、ユーザー介入が必要になることがありません。 • **仮想ディスク** — 仮想ディスクの名前が表示されます • **バスプロトコル** — バスプロトコルが表示されます • **コントローラ ID** — コントローラ ID が表示されます • **コネクタ ID** — コネクタ ID が表示されます • **エンクロージャ ID** — エンクロージャの ID が表示されます • **デバイス ID** — デバイス ID が表示されます • **モデル** — 物理ストレージディスクのモデル番号が表示されます • **パーツ番号** — ストレージのパーツ番号が表示されます • **シリアル番号** — ストレージのシリアル番号が表示されます • **ベンダー** — ストレージのベンダー名が表示されます
コントローラ	• **コントローラ ID** — コントローラ ID が表示されます • **名前** — コントローラの名前が表示されます • **デバイス FQDD** — デバイスの FQDD が表示されます • **ファームウェアバージョン** — ファームウェアのバージョンが表示されます • **最低限必要なファームウェア** — 最低限必要なファームウェアが表示されます。ファームウェアが古くなっていて、新しいバージョンが使用可能な場合に、この列に値が表示されます

情報	説明
	• **ドライババージョン** — ドライバのバージョンが表示されます • **巡回読み取り状況** — 巡回読み取り状況が表示されます • **キャッシュサイズ** — キャッシュサイズが表示されます
エンクロージャ	• **コントローラ ID** — コントローラ ID が表示されます • **コネクタ ID** — コネクタ ID が表示されます • **エンクロージャ ID** — エンクロージャの ID が表示されます • **名前** — エンクロージャの名前が表示されます • **デバイス FQDD** — デバイス FQDD が表示されます • **サービスタグ** — サービスタグが表示されます

ウェブクライアントでのシステムイベントログについて

システムイベントログ（SEL）では、OMIVV で検出されたハードウェアのステータス情報が提供され、次の基準に基づいて情報が表示されます。

ステータス 情報（青色の感嘆符）、警告（感嘆符の付いた黄色の三角形）、エラー（赤色の X）、および不明（? の付いたボックス）など、数種類のアイコンがあります。

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 OMIVV の操作が正常に完了しました。

警告 OMIVV 操作の一部が正常に完了しておらず、一部だけ成功しました。

エラー OMIVV の操作に失敗しました。

外部 CSV ファイルとして、ログを保存できます。「個別ホストに対するシステムイベントログの表示」を参照してください。

単一ホストのイベントログの表示

このタスクについて

イベントを表示するには、次の手順を実行します。

手順

1. **監視** タブにアクセスし、**システムイベントログ** サブタブを開くには、次の手順のいずれかを実行します。

オプション	説明
OMIVV から	このオプションでは、次の手順を実行します。 a. OpenManage Integration for VMware vCenter の ナビゲータ ペインで、**ホスト** をクリックします。 b. **オブジェクト** タブで、SEL ログを表示したい特定のホストをダブルクリックします。
ホーム ページから	**ホーム** ページで、**ホストとクラスタ** をクリックします。

2. **監視** タブで、**Dell ホスト情報** → **システムイベントログ** の順に選択します。

   最近のシステムログ項目には、最新の 10 個のシステムイベントログのエントリが表示されます。
3. **システムイベントログ** を更新するには、グローバル更新を実行します。
4. イベントログ項目数を制限（フィルタ）するには、以下のいずれかのオプションを選択します。
   - 検索フィルタテキストボックスで、ログエントリを動的にフィルタするには、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クリアするには、**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。
5. すべてのイベントログ項目をクリアするには、**ログのクリア** をクリックします。

すべてのログエントリが消去された後で、すべてのログエントリが削除されることを示すメッセージが表示され、次のオプションのいずれかを選択できます。

- ログの消去に同意する場合は、**ログのクリア** 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。

6. イベントログを CSV ファイルにエクスポートするには、  をクリックします。
7. 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。

単一ホストの追加ハードウェアの詳細の表示

このタスクについて

Dell ホスト情報 タブで、単一ホストのファームウェア、電源モニタおよび保証ステータスの詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行します。ハードウェアビューには OMSA および iDRAC からのデータを直接報告します。「シャーシのインベントリジョブを今すぐ実行する」を参照してください。

手順

1. OpenManage Integration for VMware vCenter の ナビゲータ ペインで、**ホスト** をクリックします。
2. **オブジェクト** タブで、<会社名> の詳細を表示したいホストを選択します。
3. **監視** タブで、**Dell ホスト情報** タブを選択します。

   ハードウェア：<会社名> サブタブに、各コンポーネントに関する次の情報が表示されます。

   表 19. 単一ホストの情報

コンポーネント	情報
ファームウェア ホストページでは、検索やフィルタを使用したり、ファームウェア情報の CSV ファイルをエクスポートしたりすることが可能です。	• **名前** — このホスト上のすべてのファームウェアの名前が表示されます • **タイプ** — ファームウェアの種類が表示されます • **バージョン** — このホスト上のすべてのファームウェアのバージョンが表示されます • **インストール日** — インストール日が表示されます
電源モニタ **メモ: ここで使用するホスト時刻は、ホストが位置する現地時刻を指しています。**	• **一般情報** — 電力バジェットおよび現在のプロファイル名が表示されます • **しきい値** — 警告および失敗のしきい値がワット単位で表示されます • **予備電源容量** — インスタントおよびピークの予備電源容量がワット単位で表示されます **エネルギー統計** • **タイプ** — エネルギー統計のタイプが表示されます • **測定開始時刻（ホスト時刻）** — ホストが電力消費を開始した日付と時刻が表示されます • **測定終了時刻（ホスト時刻）** — ホストが電力消費を停止した日付と時刻が表示されます • **読み取り値** — 1 分間に測定した平均値が表示されます • **ピーク時刻（ホスト時刻）** — ホストのピーク電流の日付と時刻が表示されます • **ピーク読み取り値** — システムピーク電力の統計、すなわちシステムが消費するピーク電力がワット単位で表示されます
保証	• **プロバイダ** — 保証のプロバイダ名が表示されます • **説明** — 説明が表示されます • **開始日** — 保証の開始日が表示されます • **終了日** — 保証の終了日が表示されます • **残日数** — 保証の残り日数が表示されます

コンポーネント	情報
メモ: 保証ステータスを表示するためには、保証ジョブを必ず実行します。「保証取得ジョブの実行」を参照してください。保証ステータス ページで、保証の期限の日付を監視できます。サーバの保証情報をデルからオンラインで取得する際には、保証設定によって保証のスケジュールを有効化または無効化したり、最小日数しきい値アラートを設定したりして制御します。	• **最終更新日** — 保証が最後に更新された日時

クラスタおよびデータセンターでのホスト監視

OpenManage Integration for VMware vCenter では、データセンターやクラスタに含まれるすべてのホストの詳細情報を表示できます。データグリッドの行のヘッダーをクリックすることで、データをソートできます。データセンターおよびクラスタのページでは、情報を CSV ファイルにエクスポートすることが可能で、データグリッドでのフィルタ機能や検索機能もあります。

データセンターおよびクラスタの概要の表示

このタスクについて

Dell データセンター / クラスタ情報 タブで、データセンターまたはクラスタのホストの詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行します。表示されるデータは、どのビューのデータにアクセスしているかによって異なる場合があります。ハードウェアビューは OMSA および iDRAC からのデータを直接報告します。「インベントリジョブの実行」を参照してください。

メモ: データセンターとクラスタのページでは、情報を CSV ファイルにエクスポートすることが可能です。ここにはデータグリッドでのフィルタまたは検索機能があります。

手順

1. OpenManage Integration for VMware vCenter の ナビゲータ ペインで、**vCenter** をクリックします。
2. **データセンター** または **クラスタ** をクリックします。
3. **オブジェクト** タブで、ホストの詳細を表示したい特定のデータセンターまたはクラスタを選択します。
4. **監視** タブで、**Dell データセンター / クラスタ情報** → **概要** タブを選択して、詳細を表示します。

メモ: 詳細の完全なリストを表示するには、データグリッドから特定のホストを選択します。

表 20. データセンターおよびクラスタの概要

情報	説明
データセンター / クラスタ情報	次が表示されます： • データセンター / クラスタ名 • Dell の管理対象ホスト数 • 合計エネルギー消費量
ハードウェアリソース	次が表示されます： • 合計プロセッサ数 • Total Memory（総メモリ量） • Virtual Disk Capacity（仮想ディスク容量）
保証サマリ	選択したホストの保証ステータスを表示します。ステータスには次のようなものがあります。 • 期限切れ保証 • アクティブな保証

情報	説明
	• 不明な保証
Host（ホスト）	ホスト名を表示します
Service Tag	ホストのサービスタグを表示します
モデル	Dell PowerEdge のモデルを表示します
Asset Tag	設定すると、アセットタグが表示されます
シャーシサービスタグ	シャーシのサービスタグを表示します（ある場合）
OS バージョン	ESXi OS のバージョンを表示します
場所	ブレードのみ：スロットロケーションが表示されます。その他の場合は、「該当なし」と表示されます。
iDRAC IP	iDRAC の IP アドレスを表示します
サービスコンソール IP	サービスコンソールの IP を表示します
CMC URL	CMC の URL（ブレードサーバのシャーシの URL）を表示します。それ以外の場合は「該当なし」と表示されます
CPU	CPU の数を表示します
メモリ	ホストのメモリを表示します
電源状況	ホストに電源があるかを表示します
最新のインベントリ	最後のインベントリジョブの日付と時刻が表示されます
接続プロファイル	接続プロファイルの名前を表示します
リモートアクセスカードバージョン	リモートアクセスカードのバージョンを表示します
BIOS ファームウェアバージョン	BIOS のファームウェアバージョンを表示します

データセンターおよびクラスタのハードウェアの詳細の表示

このタスクについて

Dell データセンター / クラスタ情報 タブで単一ホストのハードウェア詳細を表示できます。このページに情報を表示するには、インベントリジョブを実行します。データセンターおよびクラスタのページでは、情報を CSV ファイルにエクスポートし、データグリッドでフィルタまたは検索機能が利用できます。表示されるデータは、データにアクセスするビューによって異なる場合があります。ハードウェアビューでは、OMSA および iDRAC からデータを直接報告します。「インベントリジョブの実行」を参照してください。

手順

1. OpenManage Integration for VMware vCenter の ナビゲータ ペインで、**vCenter インベントリリスト** をクリックします。
2. **データセンター** または **クラスタ** をクリックします。
3. **オブジェクト** タブで、コンポーネント固有の詳細を表示する特定のデータセンターまたはクラスタを選択します。
4. **監視** タブで、**Dell データセンター / クラスタ情報** タブを選択します。

   ハードウェア：<会社名> サブタブに、各コンポーネントに関する次の情報が表示されます。

   表 21. データセンターとクラスタのハードウェア情報

ハードウェア：コンポーネント	情報
ハードウェア：FRU	• **ホスト** — ホスト名が表示されます • **サービスタグ** — ホストのサービスタグが表示されます • **パーツ名** — FRU のパーツ名を表示します

ハードウェア：コンポーネント	情報
	• **パーツ番号** — FRU のパーツ番号を表示します • **製造元** — 製造元の名前を表示します • **シリアルナンバー** — 製造元のシリアルナンバーを表示します • **製造日** — 製造日を表示します
ハードウェア：プロセッサ	• **ホスト** — ホスト名が表示されます • **サービスタグ** — ホストのサービスタグが表示されます • **ソケット** — スロット番号を表示します • **速度** — 現在の速度を表示します • **ブランド** — プロセッサのブランドを表示します • **バージョン** — プロセッサのバージョンを表示します • **コア** — このプロセッサ内のコアの数が表示されます
ハードウェア：電源装置	• **ホスト** — ホスト名が表示されます • **サービスタグ** — ホストのサービスタグが表示されます • **タイプ** — 電源装置のタイプが表示されます。電源装置には、次のタイプがあります。 – 不明 – リニア – スイッチング – BATTERY – UPS – コンバータ – レギュレータ – AC – DC – VRM • **場所** — スロット 1 など、電源装置の場所が表示されます • **出力（ワット）** — ワット単位で電力が表示されます • **ステータス** — 電源装置の状態が表示されます。次の状態があります。 – その他 – 不明 – OK – 重要 – 非重要 – 回復可能 – 回復不可能 – 高 – 低
ハードウェア: メモリ	• **ホスト** — ホスト名が表示されます • **サービスタグ** — ホストのサービスタグが表示されます • **スロット** — DIMM スロットが表示されます • **サイズ** — メモリサイズが表示されます • **タイプ** — メモリのタイプが表示されます

ハードウェア：コンポーネント	情報
ハードウェア: NIC	• **ホスト** — ホスト名が表示されます • **サービスタグ** — ホストのサービスタグが表示されます • **名前** — NIC 名が表示されます • **製造元** — 製造元の名前のみが表示されます • **MAC アドレス** — NIC の MAC アドレスが表示されます
ハードウェア: PCI スロット	• **ホスト** — ホスト名が表示されます • **サービスタグ** — ホストのサービスタグが表示されます • **スロット**— スロットを表示します • **製造元** — PCI スロットのメーカー名が表示されます • **説明** — PCI デバイスの説明が表示されます • **タイプ** — PCI スロットタイプが表示されます • **幅** — データバス幅が表示されます（該当する場合）
ハードウェア: リモートアクセスカード	• **ホスト** — ホスト名が表示されます • **サービスタグ** — ホストのサービスタグが表示されます • **IP アドレス** — リモートアクセスカードの IP アドレスが表示されます • **MAC アドレス** — リモートアクセスカードの MAC アドレスが表示されます • **RAC タイプ** — リモートアクセスカードのタイプが表示されます • **URL** — このホストに関連付けられた動作している iDRAC の URL が表示されます

データセンターおよびクラスタのストレージの詳細の表示

このタスクについて

Dell データセンター / クラスタ情報 タブで、データセンターまたはクラスタの物理ストレージの詳細を表示できます。このページで情報を表示させるには、インベントリジョブを実行します。データセンターとクラスタのページでは、情報を CSV ファイルにエクスポートすることが可能で、データグリッドでのフィルタ / 検索機能が提供されます。ハードウェアビューは OMSA および iDRAC からのデータを直接報告します。「インベントリジョブの実行」を参照してください。

手順

1. OpenManage Integration for VMware vCenter の ナビゲータ ペインで、**vCenter インベントリリスト** をクリックします。
2. **データセンター** または **クラスタ** をクリックします。
3. **オブジェクト** タブで、特定のデータセンターまたはクラスタを選択します。
4. **監視** タブで、**Dell データセンター / クラスタ情報** タブを選択し、**ストレージ** → **物理ディスク / 仮想ディスク** に移動します。

   詳細の完全なリストを表示するには、データグリッドから特定のホストを選択します。

表 22. データセンターとクラスタのストレージの詳細

ストレージ：ディスク	説明
物理ディスク	• **ホスト** — ホスト名が表示されます • **サービスタグ** — ホストのサービスタグが表示されます • **容量** — 物理ディスクの容量が表示されます • **ディスクステータス** — 物理ディスクのステータスが表示されます。オプションには次のようなものがあります。 – オンライン – 準備完了

ストレージ：ディスク	説明
	– 劣化 – エラー – オフライン – 再構成中 – 互換性なし – 削除済み – クリア済み – SMART アラート検知 – 不明 – 外部 – サポートなし **メモ: これらのアラートの意味についての詳細は、dell.com/support にある『OpenManage Server Administrator Storage Management ユーザーズガイド』を参照してください。** • **モデル番号** — 物理ストレージディスクのモデル番号が表示されます • **最終インベントリ** — インベントリが最後に実行された日、月、時刻が表示されます • **ステータス** — ホストのステータスが表示されます • **コントローラ ID** — コントローラ ID が表示されます • **コネクタ ID** — コネクタ ID が表示されます • **エンクロージャ ID** — エンクロージャの ID が表示されます • **デバイス ID** — デバイス ID が表示されます • **バスプロトコル** — バスプロトコルが表示されます • **ホットスペアタイプ** — ホットスペアのタイプを示します。オプションには次のようなものがあります。 – いいえ — ホットスペアなし – グローバル — ディスクグループの一部であるが未使用のバックアップディスク – 専用 — 単一の仮想ディスクに割り当てられた未使用のバックアップディスク。仮想ディスク内の物理ディスクが故障すると、ホットスペアが有効化されて故障した物理ディスクと交換されるため、システムが中断することや、ユーザー介入が必要になることがありません • **パーツ番号** — ストレージのパーツ番号が表示されます • **シリアル番号** — ストレージのシリアル番号が表示されます • **ベンダー名** — ストレージのベンダー名が表示されます
仮想ディスク	• **ホスト** — ホストの名前が表示されます • **サービスタグ** — ホストのサービスタグが表示されます • **名前** — 仮想ディスクの名前を表示します • **物理ディスク** — 仮想ディスクが配置されている物理ディスクが表示されます • **容量** — 仮想ディスクの容量を表示します • **レイアウト** — 仮想ストレージのレイアウトタイプが表示されます。これは、この仮想ディスクに設定された RAID のタイプです • **最終インベントリ** — インベントリが最後に実行された曜日、日付および時刻が表示されます • **コントローラ ID** — コントローラ ID が表示されます • **デバイス ID** — デバイス ID が表示されます • **メディアタイプ** — SSD と HDD のいずれかが表示されます • **バスプロトコル** — 仮想ディスクに含まれる物理ディスクが使用する技術を表示します。表示される可能性のある値は次のとおりです。

ストレージ：ディスク	説明
	– SCSI – SAS – SATA • **ストライプサイズ** — ストライプサイズが表示されます。ストライプサイズは、各ストライプが単一ディスク上で消費する容量です • デフォルト読み取りポリシー — コントローラでサポートされているデフォルト読み取りポリシーが表示されます。オプションには次のようなものがあります。 – 先読み – 先読みなし – 適応先読み – 読み取りキャッシュが有効 – 読み取りキャッシュが無効 • **デフォルト書き込みポリシー** — コントローラでサポートされているデフォルト書き込みポリシーが表示されます。オプションには次のようなものがあります。 – ライトバック – ライトバックの強制 – ライトバックが有効 – ライトスルー – 書き込みキャッシュ有効、保護 – 書き込みキャッシュが無効 • **ディスクキャッシュポリシー** — コントローラでサポートされているデフォルトのキャッシュポリシーが表示されます。オプションには次のようなものがあります。 – 有効 — キャッシュ I/O – 無効 — ダイレクト I/O

データセンターおよびクラスタの追加ハードウェアの詳細の表示

このタスクについて

Dell データセンター / クラスタ情報 タブで、データセンターおよびクラスタのファームウェアや電源モニタ、保証ステータスの詳細を表示できます。このページで情報を表示させるには、インベントリジョブを実行します。データセンターとクラスタのページでは、情報を CSV ファイルにエクスポートすることが可能で、データグリッドでのフィルタ / 検索機能が提供されます。ハードウェアビューは OMSA および iDRAC からのデータを直接報告します。「インベントリジョブを今すぐ実行する」を参照してください。

手順

1. OpenManage Integration for VMware vCenter の ナビゲータ ペインで、**vCenter** をクリックします。
2. **データセンター** または **クラスタ** をクリックします。
3. **オブジェクト** タブで、ホストのコンポーネントの詳細を表示したい特定のデータセンターまたはクラスタを選択します。
4. **監視** タブで、**Dell データセンター / クラスタ情報** タブを選択します。

   <会社名> サブタブに、各コンポーネントに関する次の情報が表示されます。

   表 23. 単一ホストの情報

コンポーネント	情報
ファームウェア	• **ホスト** — ホストの名前が表示されます • **サービスタグ** — ホストのサービスタグが表示されます • **名前** — このホスト上のすべてのファームウェアの名前が表示されます

コンポーネント	情報
	• **バージョン** — このホスト上のすべてのファームウェアのバージョンが表示されます
電源モニタ **メモ: 詳細の完全なリストを表示するには、データグリッドから特定のホストを選択します。**	• **ホスト** — ホストの名前が表示されます • **サービスタグ** — ホストのサービスタグが表示されます • **現在のプロファイル** — お使いのシステムのパフォーマンスを最大化して電力を節約するための電源プロファイルが表示されます • **エネルギー消費量** — ホストのエネルギー消費量が表示されます • **ピーク予約容量** — 電力のピーク予約容量が表示されます • **電力バジェット** — このホストの電力上限が表示されます • **警告しきい値** — お使いのシステムの温度プローブの警告しきい値の設定最大値が表示されます • **障害しきい値** — お使いのシステムの温度プローブの障害しきい値の設定最大値が表示されます • **インスタント予約容量** — ホストのインスタントヘッドルーム容量が表示されます • **エネルギー消費開始日** — ホストが電力消費を開始した日付と時刻が表示されます • **エネルギー消費終了日** — ホストが電力消費を停止した日付と時刻が表示されます • **システムピーク電力** — ホストのピーク電力が表示されます • **システムピーク電力開始日** — ホストのピーク電力が開始した日付と時間が表示されます • **システムピーク電力終了日** — ホストのピーク電力が終了した日付と時間が表示されます • **システムピーク電流** — ホストのピーク電流が表示されます • **システムピーク電流開始日** — ホストのピーク電流が開始した日付と時間が表示されます • **システムピーク電流終了日** — ホストのピーク電流が終了した日付と時間が表示されます
保証サマリ **メモ: 保証ステータスを表示するためには、保証ジョブを必ず実行します。「保証取得ジョブの実行」を参照してください。保証概要 ページで、保証の期限の日付を監視できます。サーバの保証情報をデルからオンラインで取得する際には、保証設定によって保証のスケジュールを有効化または無効化したり、最小日数しきい値アラートを設定したりして制御します。**	• **保証概要** — ホストの保証概要が表示されます。ここでは、アイコンを使用して、各ステータスカテゴリ内のホスト数が視覚的に示されます • **ホスト** — ホスト名が表示されます • **サービスタグ** — ホストのサービスタグが表示されます • **説明** — 説明が表示されます • **保証ステータス** — ホストの保証ステータスが表示されます。ステータスのオプションには、次のようなものがあります。 – アクティブ — ホストが保証されており、いずれのしきい値も超過していません – 警告 — ホストはアクティブですが、警告しきい値を超過しています – 重要 — 警告と同様ですが、重要なしきい値です – 期限切れ — このホストの保証期限が切れています – 不明 — 保証ジョブが実行されていない、データ取得中にエラーが発生した、システムに保証がない、のいずれかであるため、OpenManage Integration for VMware vCenter が保証ステータスを取得しません • **残日数** — 保証の残り日数が表示されます

物理サーバインジケータライトの点滅の設定

このタスクについて

大規模なデータセンター環境で物理サーバを見つけやすくするため、設定した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。

手順

1. OpenManage Integration for VMware vCenter のナビゲータエリアにあるインベントリリストで、**ホスト** をクリックします。
2. **オブジェクト** タブで、希望のホストをダブルクリックします。
3. **サマリ** タブで、Dell Server Management ポートレットまでスクロールダウンします。
4. **ホスト処理** で、**インジケータライトの点滅** を選択します。
5. 次のいずれかを選択します。
   - 点滅をオンにして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。
   - 点滅をオフにするには、**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。

9

ファームウェアアップデートについて

OMIVV アプライアンスでは、BIOS とファームウェアのアップデートジョブを管理対象ホストで実行できます。複数のクラスタまたは非クラスタホストで同時にファームウェアアップデートジョブを実行できます。同じクラスタの 2 つのホストでファームウェアアップデートを同時に実行することはできません。

次の表は、さまざまな展開モードで同時に実行できるファームウェアアップデートジョブの数を示します。ただし、スケジュールできるファームウェアアップデートジョブの数に制限はありません。

表 24. さまざまな展開モードにおけるファームウェアアップデートジョブ数

小規模展開モード	中規模展開モード	大規模展開モード
5	10	15

以下にファームウェアアップデートを実行できる 2 つの方法を示します。

- 単一 DUP - DUP 場所 (CIFS 共有または NFS 共有) を直接指定して、iDRAC、BIOS、または LC に対するファームウェアアップデートを実行します。単一 DUP 方法は、ホストレベルでのみ使用できます。
- リポジトリ - BIOS およびすべてのサポートされるファームウェアアップデートを実行します。この方法は、ホストレベルとクラスタレベルの両方で使用できます。次に、リポジトリの 2 つの場所を示します。
  - Dell オンライン - 場所として、デルのファームウェアアップデートリポジトリ (ftp.dell.com) を使用します。OpenManage Integration for VMware vCenter は、指定されたファームウェアアップデートをデルのリポジトリからダウンロードして、管理対象ホストをアップデートします。

    メモ: ネットワークの設定に基づき、ネットワークにプロキシが必要な場合は、プロキシを有効にします。
  - 共有ネットワークフォルダ - ファームウェアのローカルリポジトリは、CIFS ベースまたは NFS ベースのネットワーク共有に配置できます。このリポジトリとしては、デルが定期的にリリースする Server Update Utility (SUU) のダンプ、または DRM を使用して作成されたカスタムリポジトリのいずれかを使用できます。このネットワーク共有は、OMIVV からアクセスできる必要があります。

    メモ: CIFS 共有を使用している場合は、リポジトリのパスワードは 31 文字以内にしてください。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リポジトリのセットアップについての情報は、「ファームウェアアップデートリポジトリの設定」を参照してください。

ファームウェアの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、BIOS、および Lifecycle Controller の最低ファームウェアレベルの詳細については、『*OpenManage Integration for VMware vCenter Compatibility Matrix*』(OpenManage ntegration for VMware vCenter 互換性マトリックス) を参照してください。iDRAC、Lifecycle Controller、および BIOS の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プロセスにより、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バージョンに対するアップデートが可能になります。

単一ホスト用のファームウェアのアップデートウィザードの実行

このタスクについて

単一ホスト用のファームウェアアップデートを実行するには、次の手順を実行します。

メモ: ファームウェアのアップデート処理中は、次のものを削除しないことを推奨します。

- ファームウェアのアップデートジョブが進行中の vCenter のホスト
- ファームウェアのアップデートジョブが進行中のホストの接続プロファイル

手順

1. ファームウェアアップデートウィザードにアクセスするには、OpenManage Integration で **ホスト** をクリックし、次のいずれかの操作を実行します。
   - ホストを右クリックし、**すべての OpenManage Integration アクション** → **ファームウェアアップデート** の順に選択します。
   - **ホスト** ページでホストをクリックし、**すべての OpenManage Integration アクション** → **ファームウェアアップデート** の順に選択します。
   - **ナビゲータ** ペインで、ホストを選択し、**サマリ** → **Dell ホスト情報** → **ファームウェアウィザードを実行** の順にクリックします。
   - **ナビゲータ** ペインで、ホストを選択し、**監視** → **Dell ホスト情報** → **ファームウェア** → **ファームウェアウィザードを実行** の順にクリックします。

   OMIVV が、ホストのコンプライアンスおよび、同じクラスタ内のホストで他のファームウェアアップデートジョブが進行中かどうかを確認します。検証後、**ファームウェアアップデート** ウィザードが表示され、**ようこそ** ページが表示されます。

   メモ: OMIVV を以前のバージョンから使用可能なバージョンにアップグレードするときに、そのファームウェアのアップデートジョブがすでにスケジュールされていた場合は、OMIVV データベースをバックアップし、利用可能なバージョンに復元した後に同じホスト上でファームウェアのアップデートウィザードを起動することができます。
2. **次へ**をクリックします。
   アップデートソースの選択 画面が表示されます。
3. **アップデートソースの選択** 画面で、次のいずれかを選択します。
   - **現在のリポジトリの場所** を選択し、**アップデートバンドルの選択** ドロップダウンリストから、ファームウェアアップデートのバンドルを選択します。

     メモ: 64 ビットバンドルは、iDRAC バージョン 1.51 以前を搭載した第 12 世代ホストではサポートされていません。

     メモ: 64 ビットバンドルは、すべての iDRAC バージョンの第 11 世代ホストでサポートされていません。

     メモ: OMIVV では、ファームウェアアップデート用の 32 ビットおよび 64 ビットのバンドルをサポートします。同じリリース ID のカタログで複数のバンドルが使用可能な場合は、OMIVV が前述のバンドルの他にハイブリッドバンドルも作成します。
   - 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するには、**単一 DUP** を選択します。単一 DUP は、仮想アプライアンスがアクセスできる CIFS または NFS 共有上に存在することができます。**ファイルの場所** を以下のいずれかの形式で入力します。
     - NFS 共有 — <host>:/<share_path/FileName.exe
     - CIFS 共有 — \\<host accessible share path>\<FileName>.exe

       CIFS 共有の場合、共有ドライブにアクセスできるドメイン形式でユーザー名とパスワードを入力するように要求するプロンプトが OMIVV から表示されます。

       メモ: 共有ネットワークフォルダのユーザー名またはパスワードには、@、%、および、, 文字は使用できません。
4. **単一 DUP** を選択した場合は、手順 7 に進みます。
5. **次へ**をクリックします。
   コンポーネントの選択 画面が表示され、コンポーネントのファームウェアの詳細が一覧表示されます。画面には、選択したホストのホスト名やサービスタグ、モデル名、コンポーネント、バージョン、アップデートのバージョン、重要度、リブートが必要かどうか (はい / いいえ)、その他の詳細情報が表示されます。

   メモ: OMIVV を以前のバージョンから使用可能なバージョンにアップグレードすると、ファームウェアアップデートのリポジトリを更新しない限り、リブートが必要かどうかを指定するフィールドですべてのコンポーネントについて「いいえ」と表示されます。
6. チェックボックスを使用して、リストから 1 つ以上のコンポーネントを選択し、**次へ** をクリックします
   ダウングレード中、または現在アップデート用にスケジュールされているコンポーネントは選択できません。**フィルタ** フィールドを使用すれば、データグリッドのさまざまなコンポーネントの内容からカンマ区切り値をフィルタリングすることができます。また、コンポーネントデータグリッド内で行をドラッグアンドドロップすることもできます。ウィザードからエクスポートするには、**CSV にエクスポート** ボタンを使用します。**ファームウェアのダウングレードを許可** チェックボックスをオンにした場合は、コンポーネントを選択して、ダウングレード対象に一覧で指定します。

メモ: 再起動を必要とするコンポーネントを選択した場合、作業負荷を移行できるように vCenter 環境が設定されていることを確認します。

7. **次へ**をクリックします。
   ファームウェアアップデートのスケジュール 画面が表示されます。

   a. **ファームウェアアップデートジョブ名** フィールドでジョブ名を指定し、**ファームウェアアップデートの説明** フィールドに説明を入力します。このフィールドへの入力はオプションです。
      ファームウェアアップデートのジョブの名前は必須です。ここでは、すでに使用されている名前は使用しないようにしてください。ファームウェアアップデートのジョブ名をパージすれば、そのジョブ名を再度使用できます。
   b. 次のいずれかのオプションを選択します。
      - **今すぐアップデート** を選択すると、ファームウェアアップデートジョブが直ちに開始されます。
      - ファームウェアアップデートジョブを後で実行するには、**アップデートのスケジュール** を選択します。ファームウェアアップデートジョブのスケジュールは、現在の時刻から 30 分後に設定可能です。
        - カレンダー ボックスで 月と日 を選択します。
        - 時刻テキストボックスに、HH:MM 形式で時刻を入力します。この時刻は、OMIVV アプライアンスの時刻です。
      - サービスの中断を避けるため、**次回の再起動時にアップデートを適用** を選択します。
      - ホストがメンテナンスモードでなくてもアップデートを適用して再起動するには、**アップデートを適用、そしてメンテナンスモードに入らずに再起動を強制** を選択します。ただし、この方法は推奨されません。
8. **次へ**をクリックします。
   サマリ ページが表示され、ファームウェアアップデートに対するすべてのコンポーネントの詳細が表示されます。
9. **終了** をクリックします。

ファームウェアアップデートジョブが完了するまでは数分かかります。この時間は、ファームウェアアップデートジョブの対象に含まれるコンポーネントの数によって異なります。**ジョブキュー** ページで、ファームウェアアップデートジョブの状態を表示することができます。ジョブキュー ページにアクセスするには、OpenManage Integration で **監視** → **ジョブキュー** → **ファームウェアアップデート** の順に選択します。ファームウェアのアップデートタスクが完了すると、選択されたホスト上でインベントリが自動的に実行され、ホストが自動的にメンテナンスモードを終了します。ただし、この動作は **ファームウェアアップデートのスケジュール** 画面で当該のオプションが選択されている場合に限ります。

クラスタ用のファームウェアのアップデートウィザードの実行

OMIVV では、クラスタのすべてのホスト上で BIOS とファームウェアのアップデートを実行できます。このウィザードでアップデートされるのは、接続プロファイルに含まれ、ファームウェア、CSIOR ステータス、ハイパーバイザー、および OMSA ステータス (第 11 世代サーバのみ) に関して準拠するホストのみです。Distribute Resource Scheduling (DRS) がクラスタ上で有効である場合、ホストがメンテナンスモードに入る際やメンテナンスモードを終了する際にワークロードを移行することで、OMIVV がクラスタ対応のファームウェアのアップデートを実行します。

前提条件

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、次の条件が満たされていることを確認してください。

- アップデートリポジトリのファームウェアがすでに設定されている。ファームウェアアップデートリポジトリのセットアップについては、「ファームウェアアップデートリポジトリの設定」を参照してください。
- 更新中のクラスタの下のホストに対して、アクティブなファームウェアアップデートジョブが存在しない。

このタスクについて

メモ: VMware では、同一のサーバハードウェアでクラスタを構築することを推奨します。

メモ: ファームウェアのアップデート処理中は、次のものを削除しないことを推奨します。

- ファームウェアのアップデートジョブが進行中の vCenter のクラスタのホスト
- ファームウェアのアップデートジョブが進行中のクラスタのホストの接続プロファイル

手順

1. ファームウェアアップデート ウィザードを起動するには、OpenManage Integration で **クラスタ** をクリックし、次のいずれかの手順を実行します。
   - クラスタをクリックし、**アクション** → **すべての OpenManage Integration アクション** → **ファームウェアアップデート** の順に選択します。

- **オブジェクト** タブで、**アクション** → **すべての OpenManage Integration アクション** → **ファームウェアアップデート** の順に選択します。
- クラスタをクリックして、**監視** → **Dell クラスタ情報** → **ファームウェア** の順に選択します。**ファームウェア** 画面で、**ファームウェアウィザードを実行** リンクをクリックします。
- クラスタを右クリックして、**アクション** → **すべての OpenManage Integration アクション** → **ファームウェアアップデート** の順に選択します。

ファームウェアアップデートウィザードの **ようこそ** ページが表示されます。

2. **ようこそ** ページを表示し、**次へ** をクリックします。
   サーバの選択 画面が表示されます。
3. **サーバの選択** ウィンドウの **名前** ツリービューで、チェックボックスを使用してホストを選択します。
4. **次へ**をクリックします。
   アップデートソースの選択 画面が表示されます。ここでバンドルを選択できます。リポジトリの場所も表示されます。
5. **アップデートソースの選択** 画面で、**バンドルの選択** 領域に表示される一覧から、選択されたホストのモデル名を選択します。
   選択されたホストの各モデルにつき、ホスト名の横にドロップダウンリストがあり、そこから必要なバンドルを選択できます。1 つのファームウェアアップデートにつき、最低 1 つのバンドルを選択します。

   メモ: OMIVV では、ファームウェアアップデート用の 32 ビットおよび 64 ビットのバンドルをサポートします。同じリリース ID のカタログで複数のバンドルが使用可能な場合は、OMIVV がこれらのバンドルの他にハイブリッドバンドルも作成します。

   メモ: 64 ビットバンドルは、iDRAC バージョン 1.51 以前を搭載した第 12 世代ホストではサポートされていません。

   メモ: 64 ビットバンドルは、すべての iDRAC バージョンの第 11 世代ホストでサポートされていません。
6. **次へ**をクリックします。
   コンポーネントの選択 画面が表示されます。画面には、選択したホストのクラスタやモデル、ホスト名、サービスタグ、コンポーネント、バージョン、アップデートのバージョン、重要度、リブートが必要かどうか（はい / いいえ）、その他の詳細情報が表示されます。
7. **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リストから 1 つ以上のコンポーネントを選択し、**次へ** をクリックして続行します。
   フィルタ フィールドを使用すれば、データグリッドのさまざまなコンポーネントの内容からカンマ区切り値をフィルタリングすることができます。また、コンポーネントデータグリッド内で行をドラッグアンドドロップすることもできます。ウィザードからエクスポートするには、**CSV にエクスポート** ボタンを使用します。**ファームウェアのダウングレードを許可** チェックボックスをオンにすることで、現在のバージョンよりも古いバージョンのファームウェアを選択できます。
8. **ファームウェアアップデート情報** ページに、すべてのファームウェアのアップデートの詳細が表示されます。
9. **次へ**をクリックします。
   ファームウェアアップデートのスケジュール 画面が表示されます。

   a. ファームウェアアップデートジョブ名を **ファームウェアアップデートジョブ名** フィールドに入力します。
      ファームウェアアップデートのジョブの名前は必須であり、すでに使用されている名前を使用しません。ファームウェアアップデートのジョブの名前をパージすれば、その名前を再度使用できます。
   b. **ファームウェアアップデートの説明** フィールドにファームウェアアップデートの説明を入力します。
      説明はオプションです。
   c. **ファームウェアアップデートのスケジュール** の下で、次のうちからオプションを選択します。
      - 今すぐアップデートジョブを実行するには、**今すぐアップデート** をクリックします。
      - アップデートジョブを後で実行するには、**アップデートのスケジュール** をクリックして、次のタスクを実行します。

        a. **カレンダー** ボックスで 月と日 を選択します。
        b. **時刻** テキストボックスに、時刻を HH:MM 形式で入力します。
10. **次へ**をクリックします。
    Summary（サマリ）ページが表示されます。
11. **サマリ** ページで、**終了** をクリックします。**ファームウェアアップデートジョブが正常に作成されました** というメッセージが表示されます。

ファームウェアアップデートジョブが完了するまでは数分かかります。この時間は、選択されているホストの数と、各ホスト内のコンポーネントの数によって異なります。**ジョブキュー** ページで、ファームウェアアップデートジョブ状態を見ることができます。ジョブキュー ページにアクセスするには、

OpenManage Integration で **監視** → **ジョブキュー** → **ファームウェアアップデート** の順に選択します。ファームウェアのアップデート作業が完了すると、選択されたホスト上でインベントリが自動的に実行され、ホストが自動的にメンテナンスモードを終了します。

ファームウェアアップデートジョブの管理

前提条件
このページで情報を表示するには、クラスタのファームウェアアップデートジョブを実行します。「クラスタ用のファームウェアのアップデートウィザードの実行」を参照してください。

このタスクについて
このページにはすべてのファームウェアアップデートジョブが表示されます。このページで、ファームウェアアップデートジョブを表示、更新、パージ、または中止できます。

手順

1. OpenManage Integration で、**監視** → **ジョブキュー** → **ファームウェアアップデート** を選択します。
2. 最近の情報を表示するには、**更新** アイコンをクリックします。
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。
   - ステータス
   - スケジュールされた時刻
   - 名前
   - 説明
   - vCenter
   - コレクションサイズ（ファームウェアインベントリジョブにおけるサーバの台数）
   - 進捗状況サマリ（ファームウェアアップデートの進捗状況詳細）
4. 特定のジョブについてのよりくわしい詳細を表示するには、特定のジョブのデータグリッドでジョブを選択します。
   ここでは、次の詳細を確認できます。
   - ホスト名
   - ステータス
   - 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、中止するジョブを選択し、 をクリックします。

   メモ: すでに iDRAC に送信済みのファームウェアアップデートジョブを中止する場合、そのファームフェアは引き続きホストでアップデートする必要がありますが、OMIVV ではそのジョブがキャンセルされたと報告されます。

6. 以前のファームウェアアップデートジョブまたは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、 をクリックします。
   ファームウェアアップデートジョブのパージ ダイアログボックスが表示されます。パージできるのは、キャンセルされたジョブ、成功したジョブ、または失敗したジョブのみで、スケジュール済みジョブやアクティブなジョブはパージできません。
7. **ファームウェアアップデートジョブのパージ** ダイアログボックスで **これより古い** を選択し、**適用** をクリックします。
   その後、選択したジョブがキューからクリアされます。

10

イベント、アラームおよび正常性の監視

ハードウェア管理の目的は、管理者が OMIVV プラグインまたは vCenter を離れずに、重要なハードウェアイベント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。

データセンターおよびホストシステムの監視では、vCenter の **タスク** タブと **イベント** タブにハードウェア（サーバとストレージ）および仮想化関連イベントを表示することにより、Administrator がインフラストラクチャの正常性を監視できるようになります。また、重要なハードウェアアラートは OpenManage Integration for VMware vCenter アラームをトリガすることができます。Dell 仮想化関連イベントに対して定義されているいくつかのアラームは、管理対象ホストシステムをメンテナンスモードに移行させることができます。

サーバからイベントを受信するため、すべての監視対象デバイス上で OMIVV がトラップ送信先として設定されます。トラップ送信先には次のようなものがあります。

- SNMP トラップ送信先は、第 12 世代以降のホストの iDRAC で設定されます。
- 第 12 世代以前のホストでは、トラップ送信先は OMSA 内に設定されます。
- シャーシでは、トラップ送信先は CMC 内に設定されます。

メモ: OMIVV は、第 12 世代以降ホストに対して SNMP v1 および v2 アラートをサポートしています。12 世代以前のホストについては、OMIVV がサポートするのは SNMP v1 アラートのみです。

監視するには、次の手順を実行します。

- **イベントとアラーム** を設定します。
- 必要に応じて、SNMP OMSA トラップの送信先 を設定します。
- 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。

ホストのイベントおよびアラームについて

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を選択、Dell ホストに対するアラームを有効にする、またはデフォルトアラームを復元することができます。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 vCenter に対して一括で設定することもできます。

次に 4 つのイベント掲載レベルを示します。

表 25. イベント掲載レベル

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 に転送することを許可しません。
すべてのイベントを掲載する	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する	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する	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イベントです。

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。有効にすると、重要なハードウェアアラームによって OMIVV アプライアンスは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別のホストシステムに移行します。OpenManage Integration for

VMware vCenter は管理下の Dell ホストから受信したイベントを転送し、それらのイベントに対するアラームを生成します。このアラームを使い、vCenter に対し、再起動、メンテナンスモードまたは移行などの措置を起動できます。

たとえば、デュアル電源が故障しアラームが出された場合、その結果の措置として、そのマシンがメンテナンスモードになり、ワークロードはクラスタ内の別のホストに移行されます。

クラスタ外のすべてのホスト、または VMware Distributed Resource Scheduling (DRS) が起動されていないクラスタにあるすべてのホストでは、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。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するには、DRS と Dell アラームが設定されたクラスタを使用します。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。イベントとアラームを有効にする前に、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復元できる便利なオプションです。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: Dell イベントを受信するには、イベントを有効にしてください。

メモ: OpenManage Integration for VMware vCenter は、ホストが仮想マシンを正常に実行するのに不可欠な仮想化関連イベントをあらかじめ選択します。Dell ホストアラームはデフォルトで無効にされています。Dell アラームを有効にする場合、クラスタで DRS を使用し、重要イベントを送信する仮想マシンが自動的に移行されるようにする必要があります。

シャーシのイベントおよびアラームについて

シャーシに対応するイベントとアラームは、vCenter のレベルでのみ表示されます。すべての vCenter でのホストに対するイベントおよびアラームの設定は、シャーシレベルでも適用されます。イベントおよびアラームの設定は、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を選択したり、Dell ホストやシャーシのアラームを有効化したり、デフォルトのアラームを復元したりすることが可能です。vCenter ごとに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 vCenter に対して一度にイベントとアラームを設定することもできます。

シャーシイベントの表示

1. 左ペインで vCenter を選択し、vCenter サーバをクリックします。
2. 任意の vCenter をクリックします。
3. **監視** → **イベント** タブをクリックします。
4. さらにイベント詳細を表示したい場合、特定のイベントを選択します。

シャーシアラームの表示

1. 左ペインで vCenter を選択し、vCenter サーバをクリックします。
2. 任意の vCenter をクリックします。
   アラームが表示されます。表示されるのは最初の 4 つのアラームのみです。
3. 完全なリストを表示するには、**すべて表示** をクリックすると、詳細なリストが **監視** タブに **すべての問題** として表示されます。
4. **トリガされたアラーム** で、**アラーム** をクリックしてアラーム定義を表示します。

仮想化関連のイベント

次の表には、仮想化関連の重要イベントおよび警告イベントが記載されていて、イベント名、説明、重大度レベル、および推奨処置が含まれます。

表 26. 仮想化イベント

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	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	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	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 1 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	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	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	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	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	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	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	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	エラー	処置は不要

イベント名	説明	重大度	推奨処置
Dell-AC power has been restored	センサーが正常値に戻りました	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	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	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か、設定エラーがあるか、またはサーマルトリップが発生しました	エラー	処置は不要
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。	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	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	情報	処置は不要
Dell-Battery sensor detected a warning value	指定され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	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	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	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	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ボード、システム基板、CPU、またはドライブキャリア上の温度セン	警告	処置は不要

イベント名	説明	重大度	推奨処置
	サーが、警告しきい値を超えました		
Dell-Temperature sensor detected a failure 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上の温度センサーが、障害しきい値を超えました	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	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	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	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	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	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	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	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	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	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	物理ディスクの一部が破損しています。	警告	処置は不要
Dell-Storage: Controller failure	物理ディスクの一部が破損しています。	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	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	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	エラー	システムをメンテナンスモードにしてください

イベント名	説明	重大度	推奨処置
Dell-Storage: Array disk failure	アレイディスク障害です	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	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	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。	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	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。	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。	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	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-Fluid Cache Disk failure	Fluid Cache ディスクの障害です	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-Cable failure or critical event	ケーブルの故障、または重要なイベントです	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-Chassis Management Controller detected a warning	シャーシ管理コントローラが警告を検出しました	警告	処置は不要
Dell-Chassis Management Controller detected an error	シャーシ管理コントローラがエラーを検出しました	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-IO Virtualization failure or critical event	I/O 仮想化の失敗または重要なイベントです	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-Link status warning	リンク状態に関する警告です	警告	処置は不要
Dell-Link status failure or critical event	リンク状態のエラーか、重要なイベントです	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-Security warning	セキュリティ警告です	警告	処置は不要
Dell-System: Software configuration warning	システム : ソフトウェア設定の警告です	警告	処置は不要
Dell-System: Software configuration failure	システム : ソフトウェア設定に障害が発生しています	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 Security warning	ストレージセキュリティの警告です	警告	処置は不要

イベント名	説明	重大度	推奨処置
Dell-Storage Security failure or critical event	ストレージセキュリティのエラー、または重要なイベントです	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-Software change update warning	ソフトウェアの変更アップデートに関する警告です	警告	処置は不要
Dell-Chassis Management Controller audit warning	シャーシ管理コントローラの監査に関する警告です	警告	処置は不要
Dell-Chassis Management Controller audit failure or critical event	シャーシ管理コントローラの監査エラー、または重要なイベントです	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-PCI device audit warning	PCI デバイスの監査に関する警告です	警告	処置は不要
Dell Power Supply audit warning	電源装置の監査の警告です	警告	処置は不要
Dell-Power Supply audit failure or critical event	電源装置の監査エラー、または重要なイベントです	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 usage audit warning	消費電力の監査の警告です	警告	処置は不要
Dell-Power usage audit failure or critical event	消費電力の監査エラー、または重要なイベントです	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-Security configuration warning	セキュリティ設定に関する警告です	警告	処置は不要
Dell-Configuration: Software configuration warning	設定：ソフトウェア設定に関する警告です	警告	処置は不要
Dell-Configuration: Software configuration failure	設定：ソフトウェア設定に障害が発生しています	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-Virtual Disk Partition failure	仮想ディスクのパーティションの障害です	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-Virtual Disk Partition warning	仮想ディスクのパーティションに関する警告です	警告	処置は不要
iDRAC イベント **メモ: クラスタの一部である Proactive HA が有効化されたすべてのホストでは、次の仮想化されたイベントが Proactive HA イベントにマッピングされます。ただし、「ファンは冗長ではありません」および「電源装置が冗長ではありません」のイベントはマッピングされません。**			
ファンが冗長です	なし	情報	処置は不要
ファンの冗長性が失われました	1 つまたは複数のファンが故障したか、取り外されたか、または追加のファンが必要になる構成の変更が発生しました	重要	故障したファンを取り外してから再度取り付けるか、追加のファンを取り付けます
ファンの冗長性が劣化しています	1 つまたは複数のファンが故障したか、取り外されたか、または追加のファンが必要になる構成の変更が発生しました。	警告	故障したファンを取り外してから再度取り付けるか、追加のファンを取り付けます
ファンが冗長ではありません	1 つまたは複数のファンが故障したか取り外された、または追加のファンが必要になる構成の変更が発生しました	情報	故障したファンを取り外してから再度取り付けるか、追加のファンを取り付けます

イベント名	説明	重大度	推奨処置
ファンは冗長ではありません。正常な動作を維持するためのリソースが不足しています	1 つまたは複数のファンが故障したか取り外された、または追加のファンが必要になる構成の変更が発生しました	重要	故障したファンを取り外してから再度取り付けるか、追加のファンを取り付けます
電源装置は冗長です	なし	情報	処置は不要
電源装置の冗長性が失われました	電源装置の例外、電源装置のインベントリの変更、システム電源インベントリの変更などのため、現在の電源動作モードには冗長性がありません。以前、システムは電源冗長モードで動作していました	重要	電源ユニットの障害が発生していないか、イベントログを確認します。システム構成と電力消費を確認します
電源装置の冗長性が劣化しています	電源装置の例外、電源装置のインベントリの変更、システム電源インベントリの変更などのため、現在の電源動作モードには冗長性がありません。以前、システムは電源冗長モードで動作していました	警告	電源ユニットの障害が発生していないか、イベントログを確認します。システム構成と電力消費を確認します
電源装置が冗長ではありません	現在の電源装置構成は、冗長性を有効にするプラットフォーム要件を満たしていません。1 台の電源装置に障害が発生すると、システムがシャットダウンするおそれがあります。	情報	意図した状態でない場合は、システム構成と電力消費を確認し、電源ユニットを正しい構成で取り付けます。電源ユニットのステータスにエラーがないか確認します
電源装置が冗長ではありません。正常な動作を維持するためのリソースが不足しています	システムの電源が切れるか、またはパフォーマンスが低下した状態で動作する可能性があります	重要	電源ユニットの障害が発生していないか、イベントログを確認します。システム構成と電力消費を確認し、電源ユニットを正しくアップグレードするか、または正しく取り付けます
内蔵デュアル SD モジュールが冗長です	なし	情報	処置は不要
内蔵デュアル SD モジュールの冗長性が失われました	片方または両方の SD カードが正常に機能していません	重要	障害の発生した SD カードを交換します
内蔵デュアル SD モジュールの冗長性が劣化しています	片方または両方の SD カードが正常に機能していません	警告	障害の発生した SD カードを交換します
内蔵デュアル SD モジュールが冗長性を欠いています	なし	情報	冗長性が必要な場合は、追加の SD カードを取り付け、冗長構成にします
シャーシイベント			
電源装置の冗長性が失われました	電源装置の例外、電源装置のインベントリの変更、システム電源インベントリの変更などのため、現在の電源動作モードには冗長性がありません。以前、システムは電源冗長モードで動作していました	重要	電源ユニットの障害が発生していないか、イベントログを確認します。システム構成と電力消費を確認します
電源装置の冗長性が劣化しています	電源装置の例外、電源装置のインベントリの変更、システム電源インベントリの変更などのため、	警告	電源ユニットの障害が発生していないか、イベントログを確認しま

イベント名	説明	重大度	推奨処置
	現在の電源動作モードには冗長性がありません。以前、システムは電源冗長モードで動作していました		す。システム構成と電力消費を確認します
電源装置は冗長です	なし	情報	処置は不要
電源装置が冗長ではありません	現在の電源装置構成は、冗長性を有効にするプラットフォーム要件を満たしていません。1 台の電源装置に障害が発生すると、システムがシャットダウンするおそれがあります。	情報	意図した状態でない場合は、システム構成と電力消費を確認し、電源ユニットを正しい構成で取り付けます。電源ユニットのステータスにエラーがないか確認します
電源装置が冗長ではありません。正常な動作を維持するためのリソースが不足しています	システムの電源が切れるか、またはパフォーマンスが低下した状態で動作する可能性があります	重要	電源ユニットの障害が発生していないか、イベントログを確認します。システム構成と電力消費を確認し、電源ユニットを正しくアップグレードするか、または正しく取り付けます
ファンの冗長性が失われました	1 つまたは複数のファンが故障したか取り外された、または追加のファンが必要になる構成の変更が発生しました	重要	故障したファンを取り外してから再度取り付けるか、追加のファンを取り付けます
ファンの冗長性が劣化しています	1 つまたは複数のファンが故障したか取り外された、または追加のファンが必要になる構成の変更が発生しました。	警告	故障したファンを取り外してから再度取り付けるか、追加のファンを取り付けます
ファンが冗長です	なし	情報	処置は不要
ファンが冗長ではありません	1 つまたは複数のファンが故障したか取り外された、または追加のファンが必要になる構成の変更が発生しました	情報	故障したファンを取り外してから再度取り付けるか、追加のファンを取り付けます
ファンは冗長ではありません。正常な動作を維持するためのリソースが不足しています	1 つまたは複数のファンが故障したか取り外された、または追加のファンが必要になる構成の変更が発生しました	重要	故障したファンを取り外してから再度取り付けるか、追加のファンを取り付けます

Proactive HA のイベント

次の表は、正常性アップデート ID、コンポーネントのタイプ、および説明を含む Proactive HA の 重要、正常、および警告イベントを示します。

表 27. Proactive HA のイベント

Dell Inc プロバイダのイベント ID	Component Type（コンポーネントタイプ）	説明
DellServerFan	ファン	ファンの冗長性イベント
DellServerPower	電源	電源の冗長性イベント
DellServerIDSDM	保管時	IDSDM の冗長性イベント
DellChassisFan	ファン	シャーシファンのシミュレーション冗長性イベント
DellChassisPower	電源	シャーシ電源のシミュレーション冗長性イベント

アラームおよびイベントの設定の表示

このタスクについて
アラームおよびイベントを設定したら、ホストの vCenter アラームが有効になっているか、また、設定 タブでどのイベントの掲載レベルが選択されているかを表示することができます。

手順

1. OpenManage Integration for VMware vCenter の **管理** → **設定** タブで、**vCenter 設定** の下にある **イベントとアラーム** を展開します。次の詳細が表示されます。
   - Dell ホスト用の vCenter アラーム — **有効** または **無効** が表示されます。
   - イベント掲載レベル
2. イベントとアラームを設定します。「イベントおよびアラームの設定」を参照してください。

次の手順
イベント掲載レベルを表示するには、「ホストのイベントおよびアラームについて」を参照してください。

イベントの表示

前提条件
イベントを **イベント** タブで表示する前に、必ずイベントを設定します。「イベントおよびアラームの設定」を参照してください。

このタスクについて
ホスト、クラスタ、またはデータセンターのイベントを、イベント タブに表示します。

手順

1. OpenManage Integration for VMware vCenter ナビゲータで、**ホスト**、**データセンター**、または **クラスタ** をクリックします。
2. **オブジェクト** タブで、イベントを表示したいホスト、データセンター、またはクラスタを選択します。
3. **監視** タブで、**イベント** をクリックします。
4. イベント詳細を表示したい場合、特定のイベントを選択します。

ハードウェアコンポーネントの正常性 - Proactive HA

Proactive HA は、OMIVV で動作する vCenter（vCenter 6.5 以降）機能です。Proactive HA を有効にすると、この機能がホスト内の冗長コンポーネント障害時にプロアクティブに対応することによりワークロードを保護します。

メモ: Dell PowerEdge 第 12 世代以降のすべてのホスト、および接続プロファイルの一部で、正常にインベントリされた ESXi バージョン v6.0 以降は、Proactive HA に対して有効です。

冗長ホストサーバコンポーネントのステータスを評価するために、OMIVV アプライアンスはホストコンポーネントの正常性ステータスの変化を vCenter サーバにアップデートします。電源装置、ファン、内蔵デュアル SD モジュール（IDSDM）などの主なホストサーバコンポーネントについて、次のようなステータス状態が得られます。

- 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。

（トラップまたはポーリング経由で）コンポーネントの正常性ステータスの変更が OMIVV で検出されると、コンポーネントの正常性アップデート通知がステータスと共に、vCenter サーバに転送されます。vCenter サーバでは通知に基づき、構成に応じて手動または自動のいずれかのアクションが実行されます。vCenter サーバでは、次のいずれかのアクションが実行されます。

- ホストを隔離モードにする
- ホストをメンテナンスモードにする

ラックサーバの Proactive HA の設定

このタスクについて
ラックサーバを設定するには、次の手順を実行します。

手順

1. 接続プロファイルおよび接続プロファイルと関連付けるホストを作成します。「接続プロファイルの作成」を参照してください。
2. ホストインベントリが正常に完了したことを確認します。「ホストインベントリの表示」を参照してください。
3. iDRAC での SNMP トラップ送信先が OMIVV アプライアンスの IP アドレスとして設定されていることを確認します。
4. クラスタで Proactive HA を有効にします。「クラスタでの Proactive HA の有効化」を参照してください。

モジュラーサーバの Proactive HA の設定

このタスクについて
モジュラーサーバ用に設定するには、次の手順を実行します。

手順

1. 接続プロファイルおよび接続プロファイルと関連付けるホストを作成します。「接続プロファイルの作成」を参照してください。
2. ホストインベントリが正常に完了したことを確認します。「ホストインベントリの表示」を参照してください。
3. 関連シャーシのシャーシプロファイルを作成します。「シャーシプロファイルの作成」を参照してください。
4. シャーシインベントリが正常に完了したことを確認します。「シャーシインベントリの表示」を参照してください。
5. CMC を起動し、シャーシのトラップ送信先が OMIVV アプライアンスの IP アドレスとして設定されていることを確認します。
6. **シャーシ管理コントローラ** で、**設定** → **全般** に移動します。
7. **一般シャーシ設定** ページで、**拡張シャーシロギングおよびイベントを有効にする** をクリックします。
8. クラスタで Proactive HA を有効にします。「クラスタでの Proactive HA の有効化」を参照してください。

クラスタでの Proactive HA の有効化

前提条件
クラスタで Proactive HA を有効にする前に、次の条件が満たされていることを確認します。

- vCenter コンソールに DRS が有効にされているクラスタが作成され、設定されます。クラスタで DRS を有効にするには、VMware のマニュアルを参照してください。
- クラスタの一部であるすべてのホストは、接続プロファイルの一部であり、正常にインベントリされる必要があります。

手順

1. OpenManage Integration で、**クラスタ** をクリックします。
2. **クラスタ** の下でクラスタをクリックし、**設定** → **vSphere の可用性** の順に選択し、次に **編集** クリックします。
   クラスタ設定の編集 ウィザードが表示されます。
3. **vSphere DRS** をクリックし、選択されていない場合は、**vSphere DRS をオンにする** を選択します。
4. **vSphere の可用性** をクリックし、**Proactive HA をオンにする** を選択します (選択されていない場合)。
5. 左側のペインの **vSphere の可用性** の下で、**Proactive HA の障害と対応** をクリックします。
   Proactive HA の障害と対応 画面が表示されます。
6. **Proactive HA の障害と対応** 画面で、**自動化レベル** を展開します。
7. **自動化レベル**で、**手動** または **自動化** を選択します。
8. **修正** に、重要度のステータスに基づいて、隔離モード、メンテナンスモード、または隔離とメンテナンスモードの両方の組み合わせを選択します。詳細については、VMware のマニュアルを参照してください。
9. **Proactive HA のプロバイダ** では、クラスタのデルのプロバイダを選択するチェックボックスを使用します。
10. 選択した Dell プロバイダに対して **編集** をクリックします。
    Proactive HA のプロバイダに **ブロックされた障害状態の編集** ダイアログボックスが表示されます。
11. 障害状態がイベントを掲載するのをブロックするには、チェックボックスを使用して、**障害状態** の表から (トラップまたはポーリングを介して生成された) イベントを選択します。

フィルタは障害状態データグリッドのコンテンツは、**フィルタ** フィールドを使用するか、障害状態データグリッド内の行をドラッグアンドドロップして、フィルタできます。障害状態は、クラスタレベルまたはホストレベルで適用できます。

12. クラスタ内のすべての現在および今後のホストで適用するには、**クラスタレベル** チェックボックスを選択します。
13. ホストで適用するには、チェックボックスを使用して、**適用対象** 表から部分的障害プロバイダにホストを選択します。
    フィルタ フィールドを使用して、データグリッドのコンテンツをフィルタできます。
14. 変更を適用するには、**ブロックされた障害状態の編集** で **OK** をクリックし、キャンセルするには **キャンセル** をクリックします。
15. 変更を保存するには **OK** をクリックし、キャンセルするには **キャンセル** をクリックします。

次の手順
これで、OMIVV は、Dell サーバからのイベントを介してコンポーネントの正常性アップデート通知を vCenter サーバに転送できます。通知に基づいて、vCenter サーバは、**修正** に選択された手動または自動アクションを実行します。

Dell サーバの正常性ポーリング

前提条件
毎時間 OMIVV がポーリングする前に、次の条件が満たされていることを確認します。

- 接続プロファイルがホストに割り当てられている。
- ホストシステムは、正常に完了したインベントリを使用できる。

このタスクについて
以下は、正常性ポーリングイベントです：
表 28. ポーリングイベント

イベント名	重大度	推奨処置
ポーリング - ファンの冗長性が正常状態	情報	処置は不要
ポーリング - ファンの冗長性が警告状態	警告	ファンを交換します
ポーリング - ファンの冗長性が重要状態	重要	ファンを交換します
ポーリング - 電源の冗長性が正常状態	情報	処置は不要
ポーリング - 電源の冗長性が警告状態	警告	電源装置ユニットを交換します
ポーリング - 電源の冗長性が重要状態	重要	電源装置ユニットを交換します

ポーリングは毎時間実行され、ポーリングスケジュールを設定することはできません。ポーリングは、トラップの損失の可能性に対応するためのフェールセーフメカニズムとして使用できます。

メモ: ポーリングは、IDSDM コンポーネントの冗長性情報を vCenter サーバに提供しません。

正常性のオーバーライド重大度のアップデート通知

お使いの環境に合わせた、カスタマイズした重大度で Dell ホストおよびシャーシのシステムの重大度を設定することができます。デフォルトの重大度は、システムの重大度と同じです。

このタスクについて
以下は、重大度レベルです。

- **情報**
- **中程度の低下**
- **深刻な低下**

メモ: 情報 重大度レベルではコンポーネントの重大度をカスタマイズできません。

手順

1. OpenManage Integration for VMware vCenter の **管理** タブで、**Proactive HA 設定** → **Proactive HA イベント** の順にクリックします。
2. **Proactive HA イベント** ページで、Dell ホストおよびシャーシコンポーネントのリストの iDRAC および CMC の情報を表示します。

上部および下部のデータグリッドに、イベント ID、イベントの説明、現在のシステムの重大度、およびホストとシャーシコンポーネントのオーバーライド重大度を含むすべてのポーリングおよび Proactive HA イベントが表示されます。

メモ: IDSDM コンポーネントの重大度はカスタマイズできません。そのため、IDSDM は、イベントリストに表示されません。

3. ホストまたはシャーシコンポーネントの重大度を変更するには、**オーバーライド重大度** 列で、ドロップダウンリストから目的のステータスを選択します。
4. カスタマイズが必要なすべてのイベントについて、ステップ 6 を繰り返します。
5. 次のいずれかのアクションを実行します。
   a. カスタマイズを保存するには、**変更の適用** をクリックします。
   b. 重大度レベルを選択した後で、オーバーライドされた重大度に戻すには、**キャンセル** をクリックします。
   c. デフォルトの重大度をオーバーライドされた重大度に適用するには、**デフォルトの重大度にリセット** をクリックします。

管理コンソールの起動

Dell Server Management ポートレットから起動できる管理コンソールは、次の 3 つです。

- iDRAC ユーザーインタフェースにアクセスするには、Remote Access Console を起動します。「Remote Access Console（iDRAC）の起動」を参照してください。
- OpenManage Server Administrator ユーザーインタフェースにアクセスするには、OMSA コンソールを起動します。OMSA コンソールを起動する前に、Open Management Integration for VMware vCenter で OMSA URL を設定する必要があります。「OMSA コンソールの起動」を参照してください。
- シャーシのユーザーインタフェースにアクセスするには、ブレードシャーシコンソールをクリックします。「シャーシ管理コントローラ（CMC）コンソールの起動」を参照してください。

メモ: ブレードシステムを使っている場合、CMC コンソール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、シャーシ管理コントローラユーザーインタフェースは表示されません。

Remote Access Console（iDRAC）の起動

このタスクについて

Dell Server Management ポートレットから、iDRAC ユーザーインタフェースを起動できます。

手順

1. OpenManage Integration for VMware vCenter のナビゲータエリアにあるインベントリリストで、**ホスト** をクリックします。
2. **オブジェクト** タブで、希望のホストをダブルクリックします。
3. **サマリ** タブで、Dell Server Management ポートレットまでスクロールダウンします。
4. **管理コンソール → Remote Access Console（iDRAC）** をクリックします。

OMSA コンソールの起動

このタスクについて

OMSA コンソールを起動する前に、OMSA URL をセットアップし、OMSA ウェブサーバをインストールおよび設定してください。OMSA URL のセットアップは、**設定** タブから行うことができます。

メモ: 第 11 世代の Dell PowerEdge サーバを監視および管理するために、OpenManage Integration for VMware vCenter を使用して、OMSA をインストールします。

手順

1. OpenManage Integration for VMware vCenter のナビゲータエリアにあるインベントリリストで、**ホスト** をクリックします。
2. **オブジェクト** タブで、希望のホストをダブルクリックします。
3. **サマリ** タブで、**Dell ホスト情報** までスクロールダウンします。
4. **Dell ホスト情報** セクションで、**OMSA コンソール** をクリックします。

シャーシ管理コントローラ（CMC）コンソールの起動

このタスクについて

Dell Server Management ポートレットから、シャーシのユーザーインタフェースを起動できます。

手順

1. OpenManage Integration for VMware vCenter のナビゲータエリアにあるインベントリリストで、**ホスト** をクリックします。
2. **オブジェクト** タブで、希望のホストをダブルクリックします。
3. **サマリ** タブで、Dell Server Management ポートレットまでスクロールダウンします。
4. **管理コンソール → シャーシ管理コントローラ（CMC）コンソール** の順にクリックします。

11

シャーシ管理

OMIVV では、モジュラーサーバに関連するシャーシに関する追加情報を表示できます。シャーシ情報 タブで、個々のシャーシのシャーシ概要の詳細や、ハードウェアインベントリ、ファームウェアおよび管理コントローラに関する情報、個々のシャーシコンポーネントの正常性、シャーシ保証情報を表示することができます。各シャーシについて、次の 3 つのタブが表示されます。シャーシのモデルによって、表示されるタブは異なります。

- サマリタブ
- 監視 タブ
- 管理 タブ

メモ: すべての情報を表示するには、シャーシがシャーシプロファイルに関連付けられ、シャーシインベントリが正常に完了していることを確認します。詳細については、「シャーシプロファイルについて」を参照してください。

シャーシサマリ詳細の表示

シャーシサマリ ページでは、個々のシャーシのシャーシサマリ詳細を表示することができます。

1. **ホーム** ページで **vCenter** をクリックします。
2. 左ペインの **OpenManage Integration** で、**Dell シャーシ** をクリックします。
3. 左ペインで、対応するシャーシ IP を選択します。
4. **サマリ** タブをクリックします。
   選択したシャーシについて、次の情報が表示されます。
   - 名前
   - モデル
   - ファームウェアバージョン
   - サービスタグ
   - CMC

   メモ: CMC リンクをクリックすると、Chassis Management Controller ページが表示されます。

   メモ: シャーシにインベントリジョブを実行しない場合は、サービスタグと CMC IP アドレスしか表示されません。
5. 選択したシャーシに関連付けられたデバイスの正常性ステータスを表示します。
   メインのペインには、シャーシの全般的な正常性が表示されます。有効な正常性インジケータは、**正常**、**警告**、**重要**、**なし** です。**シャーシの正常性** のグリッドビューには、各コンポーネントの正常性が表示されます。シャーシの正常性パラメータは、VRTX バージョン 1.0 以降、M1000e バージョン 4.4 以降 のモデルに適用されます。4.3 より以前のバージョンでは、正常性インジケータは、正常 および 警告または重要（逆三角形にオレンジ色の感嘆符）など、2 つのみ表示されます。

   メモ: 全般的な正常性は、正常性パラメータが最も少ないシャーシに基づいた正常性を示します。例えば、正常記号が 5 つ、警告記号が 1 つある場合には、全般的な正常性は警告として表示されます。
6. シャーシの **CMC Enterprise** または **Express** とライセンスタイプおよび終了期限を表示します。
   詳細情報は M1000e シャーシには適用されません。
7. **保証** アイコンをクリックし、残りの日数およびホストに使用済みの日数を表示します。
   保証が複数ある場合、保証の残りの日数は、最後の保証の最後の日として計算されます。
8. **シャーシの正常性** ページに表示される、シャーシの **アクティブエラー** 表リストでエラーを表示します。

メモ: M1000e のバージョン 4.3 以前では、アクティブエラーは表示されません。

シャーシのハードウェアインベントリ情報の表示

選択したシャーシ内のハードウェアインベントリについての情報を表示することができます。このページでその情報を表示するには、インベントリジョブを実行し、コンポーネント情報を含む CSV ファイルをエクスポートしてください。

1. **ホーム** ページで **vCenter** をクリックします。
2. 左ペインの **OpenManage Integration** で、**Dell シャーシ** をクリックします。
3. 左ペインで、対応するシャーシ IP を選択します。
4. **監視** タブをクリックします。

   関連するコンポーネントの情報を表示するには、OMIVV 内をナビゲーションします。

表 29. ハードウェアインベントリ情報

ハードウェアインベントリ：コンポーネント	OMIVV でのナビゲーション	情報
ファン	次のいずれかの方法を使用します。 • **概要** タブで **ファン** をクリックします。 • **監視** タブで左ペインを展開し、**ハードウェアインベントリ** をクリックしてから **ファン** をクリックします。	ファンに関する情報には、次のものがあります。 • 名前 • 存在 • 電源状況 • 読み取り • 警告しきい値 • 重要しきい値 – 最小 – 最大
電源装置	次のいずれかの方法を使用します。 • **概要** タブで **電源装置** をクリックします。 • **監視** タブで左ペインを展開し、**ハードウェアインベントリ** をクリックしてから **電源装置** をクリックします。	電源装置に関する情報には、次のものがあります。 • 名前 • 容量 • 存在 • 電源状況
温度センサー	次のいずれかの方法を使用します。 • **概要** タブで **温度センサー** をクリックします。 • **監視** タブで左ペインを展開し、**ハードウェアインベントリ** をクリックしてから **温度センサー** をクリックします。	温度センサーに関する情報には、次のものがあります。 • 場所 • 読み取り • 警告しきい値 – 最大 – 最小 • 重要しきい値 – 最大 – 最小 **メモ: PowerEdge M1000e シャーシでは、温度センサーについての情報がシャーシに対してのみ表示されます。他のシャーシでは、温度センサーについての情報がシャーシと関連するモジュラーサーバに対して表示されます。**

ハードウェアインベントリ：コンポーネント	OMIVV でのナビゲーション	情報
I/O モジュール	次のいずれかの方法を使用します。 • **概要** タブで **I/O モジュール** をクリックします。 • **監視** タブで左ペインを展開し、**ハードウェアインベントリ** をクリックしてから **I/O モジュール** をクリックします。	I/O モジュールに関する情報には、次のものがあります。 • スロット / 場所 • 存在 • 名前 • ファブリック • Service Tag • 電源状態 追加情報を表示するには、対応する I/O モジュールを選択します。次の情報が表示されます。 • 役割 • ファームウェアバージョン • ハードウェアバージョン • IP アドレス • サブネットマスク • ゲートウェイ • MAC アドレス • DHCP が有効
PCIe	次のいずれかの方法を使用します。 • **概要** タブで **PCIe** をクリックします。 • **監視** タブで左ペインを展開し、**ハードウェアインベントリ** をクリックしてから **PCIe** をクリックします。	PCIe に関する情報には、次のものがあります。 • PCIe スロット – スロット – 名前 – 電源ステータス – ファブリック • サーバスロット – 名前 – 番号 追加情報を表示するには、対応する PCIe を選択します。次の情報が表示されます。 • スロットタイプ • サーバマッピング • 割り当てステータス • スロットに割り当てられた電力 • PCI ID • Vendor ID (ベンダー ID) **メモ: PCIe 情報を M 1000 e シャーシには適用されません。**
iKVM	次のいずれかの方法を使用します。 • **概要** タブで **iKVM** をクリックします。 • **監視** タブで左ペインを展開し、**ハードウェアインベントリ** をクリックしてから **iKVM** をクリックします。	iKVM に関する情報には、次のものがあります。 • iKVM 名 • 存在 • ファームウェアバージョン • フロントパネル USB/ ビデオが有効

ハードウェアインベントリ：コンポーネント	OMIVV でのナビゲーション	情報
		• CMC CLI へのアクセスを許可 **メモ: iKVM についての情報は、PowerEdge M1000e シャーシに対してのみ表示できます。** **メモ: シャーシに iKVM モジュールが含まれている場合にのみ iKVM タブが表示されています。**

シャーシの追加ハードウェア構成の表示

選択したシャーシ内の保証、ストレージ、ファームウェア、管理コントローラ詳細についての情報を表示することができます。このページでその情報を表示するには、インベントリジョブを実行し、コンポーネント情報の CSV ファイルをエクスポートしてください。

このタスクについて

シャーシの保証、ストレージ、ファームウェア、管理コントローラの詳細を表示するには、次の手順を実行します。

手順

1. **ホーム** ページで **vCenter** をクリックします。
2. 左ペインの **OpenManage Integration** で、**Dell シャーシ** をクリックします。
3. 左ペインで、対応するシャーシ IP を選択します。
4. **監視** タブをクリックします。

   保証、ストレージ、ファームウェア、および管理コントローラの情報を表示するには、OMIVV 内をナビゲーションします。

表 30. ファームウェア詳細

ハードウェア設定	OMIVV でのナビゲーション	情報
ファームウェア	a. **監視** タブで、二重矢印マークをクリックして左ペインを展開してから、**ファームウェア** をクリックします。 b. **監視** タブで **CMC の起動** をクリックすると、**Chassis Management Controller** ページが表示されます。	ファームウェアに関する情報には、次のものがあります。 • コンポーネント • 現在のバージョン

表 31. 管理コントローラの詳細

ハードウェア設定	OMIVV でのナビゲーション	情報
管理コントローラ	a. **監視** タブで、二重矢印マークをクリックして左ペインを展開してから、**管理コントローラ** をクリックします。 b. **管理コントローラ** ページで追加情報を表示するには、矢印マークをクリックして左の列を展開します。	管理コントローラに関する情報には、次のものがあります。 • 一般 – 名前 – Firmware Version（ファームウェアバージョン） – 最終アップデート時刻 – CMC の場所 – ハードウェアバージョン • 共通ネットワーク – DNS ドメイン名 – DNS に DHCP を使用 – MAC アドレス

ハードウェア設定	OMIVV でのナビゲーション	情報
		– 冗長性モード • CMC IPv4 情報 – IPv4 が有効 – DHCP が有効 – IP アドレス – Subnet Mask（サブネットマスク ） – ゲートウェイ – 優先 DNS サーバー – 代替 DNS サーバー

表 32. ストレージ情報

ハードウェア設定	OMIVV でのナビゲーション	情報
保管時	**監視** タブで、**ストレージ** をクリックします。	ストレージに関する情報には、次のものがあります。 • 仮想ディスク • コントローラ • エンクロージャ • 物理ディスク • ホットスペア **メモ: ストレージでハイライト表示されたリンクをクリックすると、ビュー の表にそれぞれのハイライトされた項目の詳細が表示されます。ビューの表で、各ラインの項目をクリックすると、それぞれのハイライトされた項目の追加の詳細が表示されます。** M1000e シャーシでは、ストレージモジュールを使用する場合、次のストレージ詳細が、追加の情報なしでグリッドビューに表示されます。 • 名前 • モデル • Service Tag • IP アドレス（ストレージへのリンク ） • ファブリック • グループ名 • グループ IP アドレス（ストレージグループへのリンク

表 33. 保証情報

ハードウェア設定	OMIVV でのナビゲーション	情報
保証	**監視** タブで、**保証** をクリックします。	保証に関する情報には、次のものがあります。 • プロバイダ • 説明 • ステータス • 開始日 • 終了日 • 残日数 • 最終更新日

ハードウェア設定	OMIVV でのナビゲーション	情報
		メモ: 保証ステータスを表示するには、保証ジョブを実行したことを確認します。「保証取得ジョブの実行」を参照してください。

シャーシに関連するホストの表示

選択したシャーシに関連するホストについての情報は、**管理** タブで表示することができます。

1. **ホーム** ページで **vCenter** をクリックします。
2. 左ペインの **OpenManage Integration** で、**Dell シャーシ** をクリックします。
3. 左ペインで、対応するシャーシ IP を選択します。
4. **管理** タブをクリックします。
   関連ホストについて、次の情報が表示されます。
   - ホスト名（選択したホスト IP をクリックすると、ホストについての詳細が表示されます。）
   - Service Tag
   - モデル
   - iDRAC IP
   - スロットの場所
   - 最新のインベントリ

12

ハイパーバイザーの展開

OMIVV では、ハイパーバイザーを導入し、vCenter 内の指定されたデータセンターとクラスタに追加するとともにサポートされるベアメタルサーバで次のコンポーネントを設定することができます。

- 起動順序の設定
- RAID 設定
- BIOS 設定
- iDRAC 設定

PXE を使用することなく VMware vCenter を使用して、ベアメタル Dell PowerEdge サーバ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を作成できます。

ハードウェアをプロビジョニングし、展開を実行するには、物理サーバが展開ウィザードに表示されることを確認します。すべての物理サーバが次の要件に沿っていることを確認します。

- 『*OpenManage Integration for VMware vCenter* の互換性マトリックス』で利用できる特定のハードウェアサポート情報を満たす。
- iDRAC ファームウェア、Lifecycle Controller、および BIOS の対応最小バージョンを満たす。具体的なファームウェアサポート情報については、『*OpenManage Integration for VMware vCenter* の互換性マトリックス』を参照してください。
- 展開後に手動で PCI スロットの NIC を設定します。アドオンの NIC を使用している場合は、システムでホストのマザーボード上の LAN（LOM）が有効化されネットワークに接続されている必要があります。OMIVV では、内蔵または組み込みの LOM のみを使用して、展開がサポートされます。
- iDSDM のストレージの仕様を満たす。iDSDM のストレージ仕様について知るには、VMware のマニュアルを参照してください。BIOS から iDSDM を有効にしていることを確認してから、OMIVV とともにハイパーバイザーを展開します。OMIVV では、iDSDM またはローカルハードドライブでの展開が可能です。
- vCenter と iDRAC が異なるネットワークに接続されている場合、vCenter のネットワークと iDRAC のネットワーク間にルートがあることを確認します。
- Collect System Inventory On Reboot（CSIOR）が有効になっていることを確認します。また、自動 / 手動検出を開始する前に、システムの電源を完全に切断してからシステムに電源を入れ（ハード再起動）、取得データが最新のものであることを確認します。
- 自動検出とハンドシェイクオプションが工場出荷時に事前設定された Dell サーバの注文を選択します。サーバでこれらのオプションで事前設定されていない場合、手動で OMIVV IP アドレスを入力するか、または、ローカルネットワークを設定してこの情報を提供します。
- ハードウェアの設定に OMIVV が使用されない場合は、ハイパーバイザーの展開開始前に、次の条件が満たされていることを確認します。
  - 仮想化テクノロジ（VT）フラグを BIOS で有効にする。
  - 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 iDSDM に設定します。
- ハードウェア設定に OMIVV 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ていることを検証します。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。
- すべての Dell ドライバを含むカスタム ESXi イメージが、展開で使用可能なことを確認します。デルの「**ドライバおよびダウンロード**」ページに移動し、展開プロセス中に OMIVV がアクセスできる CIFS または NFS 共有場所にカスタムイメージを保存することによって、正しいイメージを **support.dell.com** から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、『*OpenManage Integration for VMware vCenter Compatibility Matrix*』（OpenManage Integration for VMware vCenter の互換性マトリックス）を参照してください。正しいイメージを使用するには、「カスタム Dell ISO イメージのダウンロード」を参照してください。
- 参照ハードウェアプロファイルで BIOS モードを選択していることを確認してから、ハイパーバイザープロファイルを適用します。これは、OMIVV では、ターゲットサーバ上でハイパーバイザーを自動展開するために、BIOS モードのみをサポートしているからです。ハードウェアプロファイルを選択していない場合、起動モードを手動で BIOS に設定し、サーバを再起動してから、ハイパーバイザープロファイルを適用するようにします。

メモ: 対象のシステムで起動モードが UEFI に設定されている場合、OMIVV は OS の展開に失敗します。

サーバが Dell PowerEdge 第 12 世代サーバより前のバージョンの場合、展開プロセスは次のタスクを実行します。

- ターゲットシステムに OMSA パッケージをインストールします。
- OMSA で OMIVV をポイントするように SNMP トラップの宛先を自動的に設定します。

デバイス検知

検出とは、サポートされている Dell PowerEdge ベアメタルサーバを追加するプロセスです。サーバが検出されたら、これをハイパーバイザーおよびハードウェアの導入に使用できます。導入に必要な PowerEdge サーバのリストは、『*OpenManage Integration for VMware vCenter* の互換性マトリックス』を参照してください。デルのベアメタルサーバの iDRAC から OMIVV 仮想マシンへのネットワーク接続が必要です。

メモ: OMIVV では、既存のハイパーバイザーを持つホストを検出せず、その代わりに、vCenter に追加してください。接続プロファイルに追加してから、ホストコンプライアンスウィザードを使用して OpenManage Integration for VMware vCenter との調整を行います。

メモ: ベアメタルサーバは OMIVV 4.0 よりも前に検出されました。ベアメタルサーバリストからマシンを削除して再検出します。

手動検出

検出プロセスで追加されなかったベアメタルサーバは、手動で追加することができます。追加されると、サーバは展開ウィザードのサーバリストに表示されます。

1. OpenManage Integration for VMware vCenter の **管理** → **導入** タブで、 アイコンをクリックします。
   サーバの追加 ダイアログボックスが表示されます。
2. **サーバの追加** 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. **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。
3. **サーバの追加** をクリックします。
   サーバの追加タスクを完了するには、数分かかる場合があります。

OpenManage Integration for VMware vCenter での自動検出

自動検出とは、第 11 世代、第 12 世代、および第 13 世代の Dell PowerEdge ベアメタルサーバを追加するプロセスです。サーバが検出されたら、これをハイパーバイザーおよびハードウェアの導入に使用します。自動検出は、OMIVV からベアメタルサーバを手動で検出する必要を排除する iDRAC 機能です。

自動検出の前提条件

Dell PowerEdge ベアメタルサーバの第 11 世代、第 12 世代、またはそれ以降の世代の検出を行う前に、OMIVV が既にインストールされていることを確認してください。ベアメタルサーバのプールで検出することができるのは、iDRAC Express または iDRAC Enterprise を搭載した第 11 世代、第 12 世代、第 13 世代の PowerEdge サーバです。Dell ベアメタルサーバの iDRAC から OMIVV アプライアンスへのネットワーク接続があること確認します。

メモ: OMIVV では、既存のハイパーバイザーを持つホストを検出しないでください。その代わりに、ハイパーバイザーを接続プロファイルに追加してから、ホストコンプライアンスウィザードを使用して OMIVV との調整を行います。

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 - 必ずサーバをコンセントに接続してください。サーバ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とポート 4433 経由で通信していることを確認します。IP アドレスは、DHCP サーバを使用して、または手動で iDRAC 設定ユーティリティで指定できます。
- 追加のネットワーク設定 - DHCP を使用している場合、DNS 名前解決が行われるように、DHCP から DNS サーバアドレスを取得 の設定を有効にするようにします。
- 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の IP アドレスまたはホスト名が既知であることを確認します。「プロビジョニングサービスの場所」を参照してください。

- アカウントアクセス無効 - 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てください。自動検出が正常に完了したら、iDRAC 管理者アカウントを再度有効にします。
- 自動検出有効 — 自動検出処理が開始できるように、サーバの iDRAC で自動検出が有効にされていることを確認します。

プロビジョニングサービスの場所

自動検出中に、次のオプションを使用して、iDRAC によりプロビジョニングサービスの場所を取得します。

- iDRAC で手動で指定 — LAN ユーザー設定、プロビジョニングサーバの下の iDRAC 設定ユーティリティで、手動で場所を指定します。
- DHCP スコープオプション — DHCP スコープオプションを使用して、場所を指定します。
- DNS サービスレコード — DNS サービスレコードを使用して場所を指定します。
- DNS の既知の名前 — DNS サーバが、既知の名前 DCIMCredentialServer を使用してサーバの IP アドレスを指定します。

プロビジョニングサービスの値が iDRAC コンソールで手動で指定されていない場合、iDRAC は DHCP スコープオプション値を使用しようとします。DHCP スコープオプションが存在しない場合、iDRAC は DNS からサービスレコードの値を使用しようと試みます。

DHCP スコープオプションと DNS サービスレコードの設定方法の詳細については、「http://en.community.dell.com/techcenter/extras/m/white_papers/20178466」で「Dell 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。

iDRAC 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処理中、無効にする必要があります。自動検出のセットアップを正しく行ったら、iDRAC GUI に戻り、ルート以外の、オフにしていた管理者アカウントを再度有効にします。

このタスクについて

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できます。非管理者アカウントを使用すると、自動検出に失敗した場合にリモートアクセスが可能です。

手順

1. ブラウザで、**iDRAC IP アドレス**を入力します。
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。
   - iDRAC8：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. **Next（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. **Apply（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後、各管理者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、ここでは **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 世代の PowerEdge サーバでの自動検出の手動設定

前提条件

iDRAC およびホストの IP アドレスがあることを確認します。

このタスクについて

お使いのベアメタルアプライアンスの自動検出の使用を工場出荷時に設定されるように注文していない場合は、これを手動で設定できます。

ベアメタルサーバの自動検出が正しく行われると、新しい AutoAdministrator 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 AutoAdministrator アカウントは、有効になりません。AutoAdministrator アカウントは、正しく自動検出が行われた後で必ず再度有効にしてください。「iDRAC の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 AutoAdministrator 以外の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 AutoAdministrator 以外の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。

手順

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** ダイアログボックスで、**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 回押します。

   認証が必要です ダイアログボックスが表示されます。
6. **認証が必要です** ダイアログボックスで、表示された名前を確認して、**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 を押すようプロンプトが表示されます。ここで即座に **CTRL + E** を押します。

    下のダイアログボックスが表示された場合、操作は正しく行われており、表示されない場合、電源 メニューに移動して、電源をオフにし、再度電源をオンにしてこのステップを繰り返します。

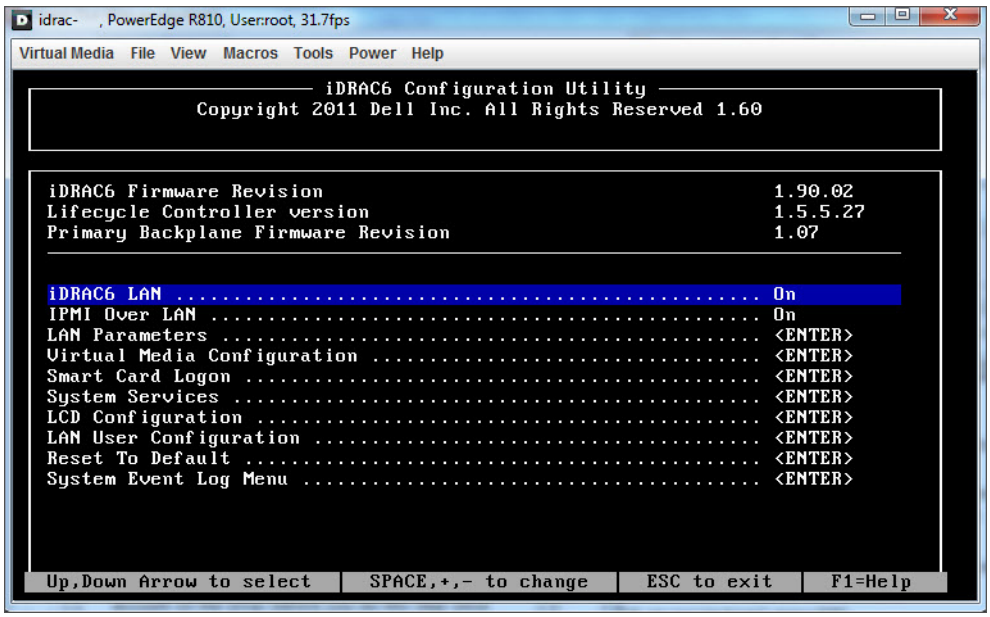

図 1. iDRAC 設定ユーティリティ

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 世代以降の PowerEdge サーバの自動検出を手動設定する

前提条件

iDRAC アドレスがあることを確認します。

このタスクについて

デルにサーバを注文し、プロビジョニングサーバの IP アドレスを入力した後、サーバで自動検出機能を有効にするように依頼できます。プロビジョニングサーバの IP アドレスは OMIVV の IP アドレスである必要があります。この場合は、Dell からサーバを受け取った後に iDRAC をマウントして接続した後に電源をオンにすると、サーバは自動検出され、サーバは展開ウィザードの最初のページに一覧表示されます。

メモ: 自動検出されたサーバについては、管理 → 設定 → 展開用の資格情報 で提供される資格情報が管理者資格情報として設定され、OS の展開が完了するまでの間のサーバとの通信に使用されます。OS の展開が正しく完了したら、関連する接続プロファイルで提供される iDRAC 資格情報が設定されます。

ターゲットマシンで自動検出を手動で有効にするには、第 12 世代以降のサーバについて以下の手順を実行します。

手順

1. システムセットアップに進み、ターゲットシステムを起動 / 再起動し、初期起動中に F2 を押します。
2. **iDRAC 設定** → **ユーザー設定** に移動して、ルートユーザーを無効にします。ルートユーザーを無効にするときに、この iDRAC アドレスにアクティブな Administrator 権限を持つユーザーが他にいないことを必ず確認してください。
3. **戻る** をクリックしてから **Remote Enablement** をクリックします。
4. **自動検出を有効にする** を **有効** に設定し、**プロビジョニングサーバ** を OMIVV の IP アドレスとして設定します。
5. 設定を保存します。
   次回のサーバ起動時にサーバが自動検出されます。自動検出が正常に完了した後、ルートユーザーが有効になり、**自動検出を有効にする** フラグは自動的に無効になります。

ベアメタルサーバの取り外し

自動検出または手動で追加されたサーバは、手動で取り外すことができます。

1. OpenManage Integration for VMware vCenter で **管理** → **導入** タブを選択します。
2. **ベアメタルサーバ** ページでサーバを選択し、✖。

プロビジョニング

すべての自動 / 手動検出対応ベアメタルシステムは、ハードウェアのプロビジョニングとハイパーバイザー展開のために OMIVV で利用できます。プロビジョニングと展開の準備をするには、次の手順を実行します。

表 34. 展開の準備

手順	説明
ハードウェアプロファイルの作成	新しいサーバの展開に使われる参照サーバから収集したハードウェア設定が含まれます。「ハードウェアプロファイルを作成するための参照サーバのカスタマイズ」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	ESXi の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。「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。
導入用テンプレートの作成	オプションで、ハイパーバイザープロファイル、またはハードウェアプロファイルとハイパーバイザープロファイルの両方が含まれます。これらのプロファイルは保存して、必要に応じて利用可能なすべてのデータセンターサーバで再利用することができます。 **メモ: ハードウェアプロファイルのみの展開はサポートされません。**

導入用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、ジョブキューからジョブステータスを表示し、保留中の展開ジョブを変更します。

ハードウェアプロファイルの設定

サーバ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します。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。

表 35. ハードウェアプロファイルを作成するための要件

要件	説明
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。 **メモ: OpenManage Integration for VMware vCenter は、参照サーバの設定にかかわらず、すべての展開サーバにおける 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を使用する前に、参照サーバの 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。**
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が含まれます。
RAID 設定	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は次の 2 つの RAID 設定オプションが構成されています。** 1. RAID 1 + を適用して、必要に応じて専用ホットスペアを作成する — デフォルトの RAID 設定をターゲットサーバに適用したい場合は、このオプションを使用します。 2. 参照サーバから RAID 構成をクローンする - このオプションは、参照サーバの設定をクローンしたい場合に使用します。「参照サーバをカスタマイズしてハードウェアプロファイルを作成する」を参照してください。

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。

- 参照サーバにおける CSIOR の有効化
- 参照サーバをカスタマイズしてハードウェアプロファイルを作成する
- ハードウェアプロファイルのクローン

参照サーバにおける CSIOR の有効化

前提条件

参照サーバ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。

このタスクについて

CSIOR を有効化するには、次の 2 つの方法があります。

表 36. CSIOR を有効にする方法

方法	説明
ローカル	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	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 TechCenter*」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。

手順

1. システムに電源を入れ、POST 中に **F2** 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。

参照サーバをカスタマイズしてハードウェアプロファイルを作成する

手順

1. OpenManage Integration for VMware vCenter の **管理** → **導入** タブで、**導入用テンプレート** → **ハードウェアプロファイル** を選択します。
2. アイコンをクリックします。
3. **ハードウェアプロファイルウィザード** の **ようこそ** ページで **次へ** をクリックして、次の手順を実行します。
   - **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、説明を入力します。説明は省略可能です。
4. **Next（次へ）** をクリックします。

   参照サーバ ダイアログボックスが表示されます。ダイアログボックスから直接参照サーバを選択することも、参照サーバ ウィンドウの 参照 ボタンを使用して選択することもできます。
5. 次のいずれかの手順を実行して参照サーバを選択します。
   - **参照サーバ** ダイアログボックスで、正しい参照サーバを選択し、参照サーバに対応する **選択** リンクをクリックします。

     設定を抽出中、という **抽出確認** ダイアログボックスが表示されます。参照サーバからハードウェア構成を抽出するには、**抽出確認** ダイアログボックスで **はい** をクリックすると、数分で抽出が完了します。
   - **参照サーバ** ページで **参照** をクリックして、OMIVV または対応ベアメタルサーバで管理され、正しくインベントリが行われた対応参照サーバを選択します。

     参照サーバからハードウェア構成を抽出するには、**抽出確認** ダイアログボックスで **はい** をクリックします。

   選択されたサーバ名、iDRAC IP アドレス、モデル、およびサービスタグが、**参照サーバ** ページに表示されます。
6. **参照サーバ** ページで、参照サーバの設定をカスタマイズするには、**参照サーバの設定をカスタマイズ** をクリックし、オプションとして含め、カスタマイズできる次の設定を選択します。
   - **RAID 設定**
   - **BIOS 設定**
   - **起動順序**
   - **iDRAC Settings（iDRAC 設定）**
     - **ネットワーク設定**
     - **ユーザーリスト**
7. **RAID 設定** ウィンドウで、次のいずれを選択し、**次へ** をクリックします。

- **RAID1 + を適用して、必要に応じて専用ホットスペアを作成する** - デフォルトの RAID 設定をターゲットサーバに適用したい場合はこのオプションを使用します。RAID の設定タスクは、RAID1 対応可能のオンボードコントローラの最初の 2 つのドライブが RAID1 にデフォルト設定されます。また、RAID 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。
- **以下のように参照サーバから RAID 構成をクローンする** - このオプションは、参照サーバの設定をクローンしたい場合に使用します。

8. **BIOS 設定** ページで、プロファイルに BIOS 設定情報を含めるには、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をアップデートします。
   - **システム情報**
   - **メモリ設定**
   - **プロセッサ設定**
   - **SATA 設定**
   - **UEFI Boot Settings（UEFI 起動設定）**
   - **One-Time Boot（1 回限りの起動）**
   - **内蔵デバイス**
   - **Slot Disablement（スロット無効化）**
   - **シリアル通信**
   - **システムプロファイル設定**
   - **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を行ったら、**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、選択したサーバの『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。
9. **起動順序** ページで、次を実行して、**次へ** をクリックします。
   a. 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** をクリックして以下のアップデートを行います。
      1. **起動モード** リストで、`BIOS` または `UEFI` を選択します。
      2. **起動デバイスのシーケンス** の下の **表示** リストで、表示されている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。
      3. **起動順序の再試行の有効化** を選択し、サーバが自動的に起動シーケンスのリトライを行うようにします。
      4. 変更を適用するには **OK** をクリックし、変更を取り消すには **キャンセル** をクリックします。
   b. ハードドライブ順オプションを表示するには、**ハードドライブのシーケンス** を展開して、**編集** をクリックします。以下をアップデートします。
      1. 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。
      2. 変更を適用するには **OK** をクリックし、変更を取り消すには **キャンセル** をクリックします。

   メモ: Dell 13 世代の PowerEdge サーバでは、現在の起動モードの詳細のみがハードウェアプロファイルに表示されます。

   メモ: ターゲットマシンの起動モードが UEFI に設定されている場合、OMIVV からのオペレーティングシステム導入は失敗します。
10. **iDRAC 設定** ページで、次の手順を実行します。
    a. 設定オプションを表示するカテゴリを展開して、**編集** をクリックします。

       次のいずれかをアップデートします。
       - **ネットワーク設定**
       - **ネットワーク**
       - **仮想メディア**

    b. iDRAC のローカル **ユーザーリスト** の下で、次のいずれかを実行します。
       - **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。終了したら、変更を適用するには **適用** をクリックし、キャンセルするには **キャンセル** をクリックします。
       - **ユーザーの削除** - 選択したユーザーを削除します。ユーザーを選択するには、マウスを使用して **削除** をクリックします。削除を確定するには、**はい** をクリックします。

- **ユーザーの編集** - 手動で iDRAC ユーザーの情報を編集します。終了したら、設定を適用するには **適用** をクリックし、キャンセルするには **キャンセル** をクリックします。

カテゴリ内のすべてのアップデートを行ったら、**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、選択したサーバの『*iDRAC* ユーザーズガイド』を参照してください。

11. **Next（次へ）** をクリックします。
12. **概要** ページで **終了** をクリックします。

次の手順

このプロファイルは自動的に保存され、**ハードウェアプロファイル** ウィンドウに表示されます。

新規ハードウェアプロファイルのクローン

1. OpenManage Integration for VMware vCenter の **管理** → **導入** タブで、**導入用テンプレート** → **ハードウェアプロファイル** を選択します。
2. アイコンをクリックします。
3. **ハードウェアプロファイルウィザード** の **ようこそ** ページで **次へ** をクリックして、次の操作を実行します。
   - **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、説明を入力します。説明は省略可能です。
4. **Next（次へ）** をクリックします。
5. 規定に準拠し、vCenter で管理され、Dell OpenManage プラグインで正常にインベントリが行われている参照サーバを選択するには、**参照サーバ** ページで **参照** をクリックします。
6. 参照サーバからすべてのハードウェア設定を抽出するには、**参照サーバ設定のクローン** オプションをクリックします。
7. **Next（次へ）** をクリックします。

   設定の抽出には数分かかります。
8. **Next（次へ）** をクリックします。

   設定が表示され、選択されたサーバ名、iDRAC IP アドレス、およびサービスタグが参照サーバの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** の下の **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の管理

ハードウェアプロファイルは、参照サーバを使ってサーバのハードウェア設定を定義します。OpenManage Integration for VMware vCenter からは、以下を含め、既存のハードウェアプロファイルで実行できる複数の管理処理があります。

- 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削除

ハードウェアプロファイルの表示または編集

1. OpenManage Integration for VMware vCenter の **管理** → **導入** タブで、**導入用テンプレート** → **ハードウェアプロファイル** を選択します。

   ハードウェアプロファイルが表示されます。
2. プロファイルを編集するには、プロファイルを選択して、 をクリックします。
3. **ハードウェアプロファイル** ウィザードで、別の値で設定するには、**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、変更を取り消すには **キャンセル** をクリックします。

ハードウェアプロファイルの削除

このタスクについて

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、削除タスクが失敗する原因になる可能性があります。

手順

1. OpenManage Integration for VMware vCenter の **管理** → **導入** タブで、**導入用テンプレート** → **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、 をクリックします。
3. プロファイルを削除するには、確認ダイアログボックスで **はい**、キャンセルするには **いいえ** をクリックします。

ハイパーバイザープロファイルの作成

前提条件

ESXi をサーバ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します。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 Dell のカスタム 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
- プラグインがサーバを展開する vCenter のクラスタまたはデータセンター

手順

1. OpenManage Integration for VMware vCenter の **管理** → **導入** タブで、**導入用テンプレート** → **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、 アイコンをクリックします。
3. **ハイパーバイザープロファイル** ダイアログボックスで、次のサブタスクを実行します。
   - **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説明を入力します。この操作はオプションのエントリです。
4. **参照 ISO パスおよびバージョンの選択** の下の、**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入力します。

   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できます。

   - NFS **フォーマット：** host:/share/hypervisor_image.iso
   - CIFS **フォーマット：** ¥¥host¥share¥hypervisor.iso

   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。パスワードが一致していることを確認します。
5. **バージョンの選択** リストで、ESXi の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導入されたすべてのサーバには、このイメージが付きます。サーバが第 12 世代より前のバージョンの場合、OMSA の最新の推奨バージョンもインストールされます。
6. パスと認証を検証するには、**設定のテスト** の下で **テストの開始** をクリックします。
7. **Apply（適用）** 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

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。

- 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削除

ハイパーバイザープロファイルの表示または編集

1. OpenManage Integration for VMware vCenter の **管理** → **導入** タブで、**導入用テンプレート** → **ハイパーバイザープロファイル** を選択します。

ハイパーバイザープロファイルが表示されます。

2. プロファイルを選択して、 アイコンをクリックします。
3. **ハイパーバイザープロファイル** ダイアログボックスに、アップデートされた値を入力します。
4. 変更を適用するには **保存** をクリックし、変更を取り消すには **キャンセル** をクリックします。

ハイパーバイザープロファイルの削除

このタスクについて

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。

手順

1. OpenManage Integration for VMware vCenter の **管理** → **導入** タブで、**導入用テンプレート** → **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、 アイコンをクリックします。
3. 確認のダイアログボックスで、プロファイルを削除するには **削除** をクリックし、キャンセルするには **キャンセル** をクリックします。

導入テンプレートの作成

このタスクについて

導入用テンプレートには、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。

手順

1. OpenManage Integration for VMware vCenter の **管理** → **導入** タブで、**導入用テンプレート**をクリックします。
2. アイコンをクリックします。
3. **導入用テンプレート** ダイアログボックスに、テンプレートの名前を入力します。
4. 導入用テンプレートの **説明** （ オプション ）を入力します。
5. **ハードウェアプロファイル** または **ハイパーバイザープロファイル** を選択します。
6. 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。

導入用テンプレートの管理

OpenManage Integration からは、既存の導入用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。

- 導入用テンプレートの表示または編集
- 導入用テンプレートの削除

導入用テンプレートの表示または編集

1. OpenManage Integration for VMware vCenter の **管理** → **導入** タブで、**導入用テンプレート** を選択します。
   導入用テンプレートプロファイルが表示されます。
2. **導入用テンプレート** ページでテンプレートを選択し、 アイコンをクリックします。
3. 変更するには、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が固有であることを確認します。

導入用テンプレートの削除

1. OpenManage Integration for VMware vCenter の **管理** → **導入** タブで、**導入用テンプレート**をクリックします。
2. **導入用テンプレート** ページで、テンプレートを選択し、 アイコンをクリックします。
3. テンプレートの削除を確定するには、メッセージボックスで、**削除** をクリックし、キャンセルするには、**キャンセル** をクリックします。

展開ウィザードについて

展開ウィザードは、以下の展開プロセスについて説明します。

- 対応ベアメタルサーバの選択。
- ハードウェアプロファイルとハイパーバイザープロファイルで構成される導入用テンプレートの選択。
- インストールのターゲット（ハードディスクまたは iDSDM ）の選択。
  ハイパーバイザーを展開する場合、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 OMIVV で展開する前に、BIOS で有効化されている必要があります。
- ホストに関連付ける接続プロファイルの選択。
- 各ホストへのネットワークの詳細の割り当て。
- vCenter、宛先データセンターまたはクラスタ、およびオプションのホストプロファイルの選択。
- サーバー展開ジョブ実行のスケジュール。

メモ: ハードウェアプロファイルのみを展開している場合、展開ウィザードの サーバ識別、接続プロファイル、ネットワーク詳細 の各オプションは省略され、展開のスケジュール設定 ページに直接進みます。

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。

VLAN サポート

OMIVV 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、VLAN サポートは展開ウィザードで設定できます。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 が指定されると、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これらの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を選択し、同じ VLAN ID をすべてのサーバに適用する場合、展開ウィザードのサーバ識別の箇所で、**選択したすべてのサーバに設定を適用** を使用します。このオプションでは、その他のネットワーク設定とともに同じ VLAN ID を、その展開ジョブのすべてのサーバに適用することができます。

メモ: OMIVV 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、サーバコンプライアンス、およびファームウェアアップデートが関わるワークフローに問題を生じる原因になります。

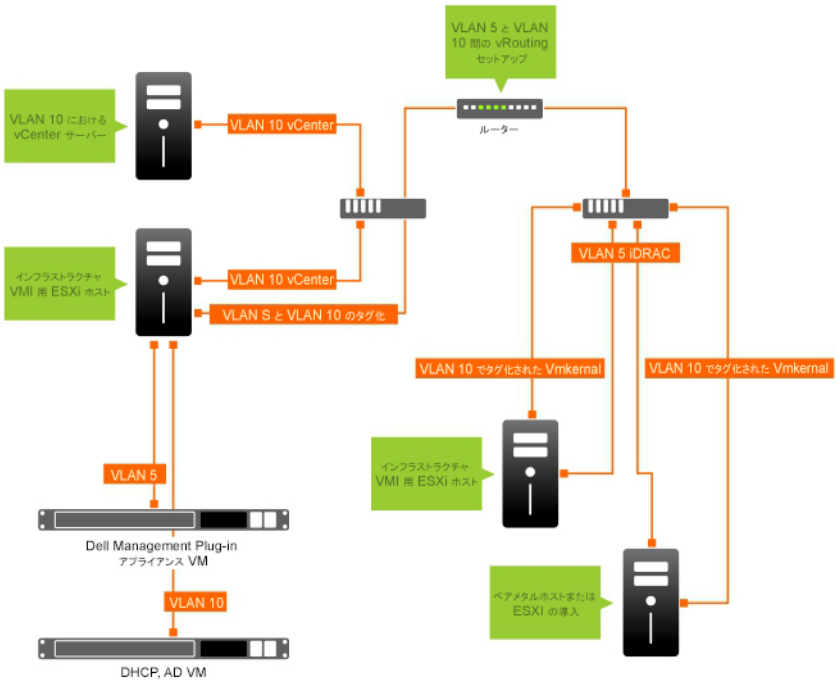

図 2. VLAN ネットワーク。

このネットワークの例では、展開されている vCenter と ESXi ホストの VMkernal は VLAN 10 にありますが、OMIVV アプライアンスは VLAN 5 にあります。OMIVV 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にされていない場合、展開は失敗します。

展開ウィザードの実行

前提条件

展開ウィザードを実行する前に、導入用テンプレートを、ハードウェアプロファイルとハイパーバイザープロファイル、および vCenter の接続プロファイルを使用して作成します。

このタスクについて

展開ウィザードを実行するには、次の手順を実行します。

手順

1. OpenManage Integration for VMware vCenter で **管理** → **導入** タブを選択します。
2. **ベアメタルサーバ** ウィンドウで、**展開ウィザードを実行** リンクをクリックします。
   展開ウィザードの **ようこそ** ページが表示されます。
3. **ようこそ** ページで、情報を表示してから **次へ** をクリックします。
4. **展開用サーバを選択します** ページで、対応ベアメタルサーバを展開ジョブに割り当てるには、サーバのリストの横にあるチェックボックスをクリックします。
5. **次へ**をクリックします。
6. **テンプレート / プロファイルの選択** ページで、次の手順を実行します。
   a. **導入用テンプレート** の下で、選択したサーバに導入用テンプレートを割り当てるには、**導入用テンプレートの選択** から既存の導入用テンプレートを選択します。
   ドロップダウンリストから、次の導入用テンプレートのいずれかを選択できます。
   - サーバハードウェアの設定だけを実行する導入用テンプレートのみのハードウェアプロファイルを選択している場合は、手順 10 に進みます。
   - ハイパーバイザーを導入するハイパーバイザープロファイルの導入用テンプレートを選択している場合は、手順 6（B）以降から続行します。

メモ: 展開のみのハードウェアプロファイルを選択している場合は、展開のスケジュール設定 ページに情報を含めるためのプロンプトが自動的に表示されます。

b. **ハイパーバイザーのインストール** の下で、次のオプションのいずれかを選択します。

- **ハードディスク** - ハードドライブ上にハイパーバイザーを導入します。
- **内蔵デュアル SD モジュール** — IDSDM にハイパーバイザーを導入します。

メモ: 選択されたサーバの少なくとも 1 台で IDSDM が使用できる場合は、内蔵デュアル SD モジュール オプションが有効になっています。使用できない場合は、ハードディスク オプションのみが使用できます。

選択したサーバのいずれも IDSDM に対応していない場合、または IDSDM が導入中に存在しない場合は、次のいずれかの操作を実行します。

– ハイパーバイザーをサーバ上の最初のハードディスクに導入する場合は、**ハイパーバイザーを使用可能な内蔵デュアル SD モジュールのないサーバの最初のハードディスクに導入する** チェックボックスを選択します。

注意: このオプションを選択してハイパーバイザーをサーバの最初のハードディスクドライブに導入すると、ディスクドライブ上のデータはすべて消去されます。

– 選択したサーバでの導入を省略し、次のサーバでハイパーバイザーの導入を続行するには、**ハイパーバイザーを使用可能な内蔵デュアル SD モジュールのないサーバの最初のハードディスクに導入する** チェックボックスをクリアします。

c. **資格情報プロファイル** の下で、次のいずれかの操作を実行します。

- **この資格情報プロファイルをすべてのサーバに使用** オプションボタンを選択し、すべてのサーバを同じ既存プロファイルに割り当てるには、ドロップダウンリストから、接続プロファイルを選択します。
- **各サーバの接続プロファイルの選択** オプションボタンをクリックし、ドロップダウンリストから各サーバの接続プロファイルを選択します。

7. **次へ**をクリックします。

サーバ識別 ページが表示されます。

サーバ識別情報は、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 (IP アドレス、サブネットマスク、およびゲートウェイ) を入力します。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 DNS サーバを設定します。ホストを vCenter に追加する場合は、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 OMIVV プラグイン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 サーバが逆引き要求に対応するように設定します。展開ジョブを実行するスケジュールを作成する前に、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。

8. **サーバ識別** ページで、次の手順を実行します。

このページでは、VLAN ID を指定するオプションが利用できます。VLAN ID を指定すると、導入中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に VLAN ID でタグ付けできます。サーバ識別 では、導入されたサーバに新しい名前とネットワーク ID が割り当てられます。「VLAN サポート」を参照してください。

a. 個々のサーバ情報を展開して表示するには、**選択済みサーバ** の下で をクリックします。
b. **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。
c. **管理タスク用 NIC** ドロップダウンリストで、サーバ管理に使用する NIC を選択します。
d. IP アドレス、サブネットマスク、デフォルトゲートウェイ、および DNS の詳細を入力するか、または **DHCP を使用して取得** チェックボックスを選択します。
e. 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。

f. 導入するすべてのサーバに手順 a ~ h を繰り返すか、または **選択したすべてのサーバに設定を適用** チェックボックスを選択します。

選択したすべてのサーバに設定を適用 を選択した場合、他のサーバには FQDN 名および IP アドレスを入力します。

メモ: サーバの FQDN 名を指定するとき、必ず各サーバに固有のホスト名を指定してください。

9. **次へ**をクリックします。

10. **展開のスケジュール設定** ページで、次の操作を実行します。
    a. **ジョブ名**と **ジョブの説明** を入力します。
    b. **vCenter 設定** に、次の項目を入力します。
        1. **vCenter インスタンス** で、展開後にホストを管理するサーバインスタンスを表示します。
        2. **vCenter 宛先コンテナ** で **参照** をクリックして vCenter の展開先を検索します。
        3. **vCenter ホストプロファイル** で、ホスト設定をカプセル化し、ホスト設定を管理しやすくするプロファイルを選択します(オプション)。
    c. ジョブのスケジュールを選択して、展開ジョブを実行するときを決定します。
        1. **展開ジョブのスケジュール設定** を選択します
            - カレンダーコントロールを使用して日付を選択します。
            - 時間を入力します。
        2. ただちにジョブを開始するには、**展開ジョブを今すぐ実行** を選択します。

    展開ジョブが開始された後でジョブキューに移動するには、**ジョブが送信された後、ジョブキュー に移動します** を選択します。
11. **終了** をクリックします。

次の手順
展開ウィザードのタスクが完了したら、**ジョブキュー** を使用して展開ジョブを管理できます。

ジョブキューを使用した展開ジョブの管理

1. OpenManage Integration for VMware vCenter の **監視** → **ジョブキュー** タブで、**展開ジョブ** をクリックします。
   展開ジョブに関する次の詳細情報が、上のグリッドに表示されます。
   - 名前
   - 説明
   - スケジュールされた時刻
   - ステータス
   - コレクションサイズ
   - 進捗状況サマリ
2. **展開ジョブの詳細**をアップデートするには、**更新** アイコンをクリックします。
3. 展開ジョブに含まれるサーバの詳細情報を含む、展開ジョブの詳細を表示するには、上のグリッドで展開ジョブを選択します。
   次の詳細情報が下のグリッドに表示されます。
   - サービスタグ
   - iDRAC の IP アドレス
   - ジョブのステータス
   - 展開ジョブの詳細 (上でマウスを動かすと詳しい情報が表示されます)
   - 開始および終了時刻

   展開ジョブについての情報全体をテキストのポップアップとして表示するには、ジョブを選択し、その展開ジョブの **詳細** 行の上にカーソルを置きます。
4. 展開ジョブを中止するには、 アイコンをクリックします。
5. メッセージが表示されたら、**ジョブの中止** をクリックし、キャンセルするには、**ジョブを中止しない** をクリックします。
6. **展開ジョブキューのパージ** ウィンドウを表示するには、 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。
   その後、選択したジョブがキューからクリアされます。

展開ジョブのタイミング

ベアメタルサーバのプロビジョニングと展開には、複数の要因により、完了まで 30 分か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。以下の表に、展開ジョブにかかるおおよその時間のガイドラインを示します。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 37. おおよその展開時間

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

展開シーケンス中のサーバ状態

インベントリジョブの実行時に、自動 / 手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か、保留中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。

表 38. 展開シーケンス中のサーバ状態

サーバの状態	説明
未設定	サーバは OMIVV に接続し、設定されるのを待機しています。
設定済み	サーバは、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で設定されています。

カスタム Dell ISO イメージのダウンロード

前提条件
展開に必要なすべての Dell ドライバを含むカスタム ESXi イメージです。

手順

1. support.dell.com にアクセスします。
2. **製品の参照** で、**製品の表示** をクリックします。
3. **製品の選択** で、**サーバ、ストレージ、ネットワーキング** をクリックして、**PowerEdge** を選択します。
4. Dell PowerEdge サーバモデルをクリックします。
5. サーバモデルの **ドライバおよびダウンロード** ページをクリックします。
6. **OS を変更** リンクをクリックして、必要な ESXi システムを選択します。
7. **エンタープライズソリューション** をクリックします。
8. **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、**ダウンロード** をクリックします。

13

ホスト、ベアメタルおよび iDRAC 対応について

ホストおよびベアメタルサーバを OMIVV 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は、OMIVV で正しく管理できません。OMIVV は、ベアメタルまたはホスト上の非対応についての詳細を表示し、該当する場所で非対応の修正を可能にします。

それぞれの場合、以下のいずれかを実行して対応問題を表示して解決できます。

- vSphere ホスト対応問題を表示して解決するには、「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を表示して解決するには、「非対応のベアメタルサーバ解決ウィザードの実行」を参照してください。

vSphere ホストの対応性のレポートおよび修正

前提条件
次の場合、ホストは非対応です。

- ホストが接続プロファイルに割り当てられていない。
- 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。OMSA をインストールまたはアップデートした場合は、ESXi ホストの再起動が必要。

△ **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。このようなシナリオでは、警告メッセージが表示されます。**

このタスクについて
非対応 vSphere ホストの修正ウィザードを実行して、非対応ホストを修正できます。一部の非対応 ESXi ホストでは再起動が必要です。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、次の処理が行われます。

- 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 がインストールされていないホストの場合、または OMSA のサポート対象外のバージョンを実行している場合は、次のようになります。
  - OMSA がホストにインストールされます。
  - ホストは、メンテナンスモードに入り、再起動されます。
  - 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。
  - ホストはメンテナンスモードを終了します。
  - インベントリが実行され、データが更新されます。
- OMSA ステータスについては、サポート対象バージョンの OMSA の修正がインストールされていますが、次のように設定する必要があります。
  - OMSA がホストにインストールされます。
  - インベントリが実行され、データが更新されます。

非対応ホストを表示および修正するには、次の手順を実行します。

手順

1. OpenManage Integration for VMware vCenter の **管理** タブで、**コンプライアンス** → **vSphere ホスト** をクリックします。

a. **vSphere ホスト** ページで、非対応ホストのリストを表示します。

ホスト IP またはホスト名、モデル、接続プロファイル、CSIOR ステータス、OMSA ステータス、ハイパーバイザー、および iDRAC ライセンスのステータスとともに非対応ホストをリストする表が表示されます。

b. 非対応ホストの詳細を表示するには、非対応ホストを選択します。

c. 表内で列を置き換えるには、データグリッド内で行をドラッグアンドドロップします。

2. 非対応ホストを修正するには、**非対応 vSphere ホストの修正** をクリックします。

非対応 vSphere ホストの修正 ウィザードが起動されます。これはダイナミックウィザードで、選択した非対応ホストに関連したページにのみが表示されます。

選択したすべての非対応ホストは CSIOR 対応です。ウィザードで、**CSIOR をオンにする** ページを表示できます。

3. **非対応 vSphere ホストの修正** ウィザードの **ようこそ** ページで **次へ** をクリックします。
4. **対応性を修正する vSphere ホストの選択ウィザード** ページで、解決したいホストのチェックボックスを選択します。
5. **Next（次へ）** をクリックします。

接続プロファイルに割り当てられていない選択されたホストがあると、警告メッセージが表示され、コンプライアンスウィザードを続行するか、対応性を修正 ウィザードをキャンセルするかを尋ねるプロンプトが表示されます。接続プロファイルの非対応を修正するには、次のいずれかを実行します。

- 接続プロファイルが割り当てられていないホストをコンプライアンスウィザードから除外するには、**コンプライアンスウィザードを続行** をクリックします。
- ウィザードを終了して、**接続プロファイル** ページからシステムを修正するには、**キャンセル** をクリックします。「接続プロファイルの作成」を参照してください。接続プロファイルを作成した後、ウィザードに戻ることができます。

6. 警告メッセージに対して **コンプライアンスウィザードを続行** をクリックした場合、**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. **Next（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** を解決するチェックボックスを選択します。
9. **Next（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。

OMSA をインストールまたはアップデートする場合は、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。

- 自動的にホストをメンテナンスモードにして、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。
- 手動で再起動する場合、OMSA をインストールした後、ホストを再起動し、ホストが稼働したら、手動でまたはコンプライアンスウィザードを使用して OMSA を設定します。OMSA が設定されていない場合、再度インベントリを実行します。「インベントリジョブの実行」を参照してください。

11. **Next（次へ）** をクリックします。
12. **概要** ウィンドウで、非対応ホストで行われるアクションを確認します。

概要 ページのアクションが適用されるには、手動再起動が必要です。

13. **Finish（終了）** をクリックします。

vSphere ホスト用の iDRAC ライセンス対応の修正

このタスクについて

vSphere ホスト対応のページにリストされる vSphere ホストは iDRAC ライセンスと互換性がないため、非対応です。表には、iDRAC ライセンスのステータスが表示されます。非対応のホストをクリックして、iDRAC ライセンスの残日数などさらに詳細な情報を表示できます。また、必要に応じて、詳細情報を更新できます。**インベントリジョブの実行** リンクが **vSphere ホスト** ページから無効にされている場合、iDRAC ライセンスのために非対応となっている vSphere ホストはありません。

手順

1. OpenManage Integration for VMware vCenter の **管理** タブで、**コンプライアンス** → **vSphere ホスト** をクリックします。
2. **iDRAC ライセンスのステータス** が **非対応** のホストを選択します。
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、対応する必要のあるホストに対してインベントリジョブが正常に完了した後で、このページに戻ります。

11 世代サーバとの OMSA の使用

Dell PowerEdge 第 11 世代サーバを管理するために、OMIVV ではこれらのサーバで実行する OMSA を必要とします。OMIVV を使用して展開される第 11 世代のホストでは、OMSA が自動的にインストールされます。手動で展開する第 11 世代ホストの場合は、次のいずれかを選択できます。

- OMIVV を使用して OMSA をインストールおよび設定します。「OMSA トラップ先の設定」を参照してください。
- OMSA を手動でインストールおよび設定します。「OMSA エージェントの ESXi システムへの展開」を参照してください。

メモ: OMIVV を使用して OMSA エージェントを導入すると、httpClient サービスが開始されてポート 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、ポートが閉じます。

メモ: 上記オプションの他に、OMSA エージェントをインストールして設定する、ウェブクライアントホストコンプライアンスを使用することができます。

OMSA エージェントの ESXi システムへの展開

このタスクについて

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前に OMSA を手動でホストにインストールします。OMSA 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。

手順

1. OMSA が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 <OMSA version X.X>
```

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

このタスクについて

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

メモ: OMSA が必要となるのは、第 12 世代 Dell PowerEdge サーバより前の Dell サーバのみです。

OMSA トラップ先を設定するには、以下を行います。

手順

1. URL として https://<HostIP>:1311/ を入力して、ウェブブラウザから 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、イベントが掲載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. OMIVV アプライアンスの IP アドレスを **送信先の 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. さらにイベントを設定するには、手順 1 ~ 8 を繰り返します。

ベアメタルサーバの対応性のレポートおよび修正

前提条件

ベアメタルサーバは次の場合には非対応です。

- サポートされているサーバではない。
- サポートされている iDRAC ライセンスがない (iDRAC Express が最小要件です)。
- iDRAC、BIOS、または LC のサポートされているバージョンがない。
- LOM または rNDC が存在しない。

このタスクについて

非対応のベアメタルサーバのリストを表示および修正するには、次の手順を実行します。

手順

1. OpenManage Integration for VMware vCenter で **管理** → **導入** タブを選択します。
   a. **ベアメタルサーバ** ページで、非対応サーバのリストを表示します。
      サービスタグ、モデル、iDRAC IP、サーバステータス、コンプライアンス状態、および iDRAC ライセンスステータスとともに非対応サーバをリストする表が表示されます。
   b. 非対応サーバの詳細を表示するには、非対応サーバを選択します。
   c. サーバの非対応情報を CSV ファイルにエクスポートするには、表の右隅で、 アイコンをクリックします。
   d. データグリッドのコンテンツをフィルタするには、**フィルタ** フィールドをクリックします。
   e. 表内で列を置き換えるには、データグリッド内で行をドラッグアンドドロップします。
2. 非対応サーバを修正するには、**非対応サーバの修正** をクリックします。
3. **ベアメタルの対応性を修正** ウィザードの **ようこそ** ページで **次へ** をクリックします。
4. **対応性を修正** ページで、解決するサーバのチェックボックスを選択します。
   非対応サーバがリストされ、非対応とされたサーバのファームフェアコンポーネントが表示されます。リストされた非対応サーバは、以下のファームフェアコンポーネントの少なくともいずれか 1 つでアップデートする必要があります。
   - iDRAC IP

     メモ: OMIVV から、iDRAC ライセンスが非対応のベアメタルサーバは修正できません。OMIVV 外部でそれらのサーバにサポートされる iDRAC ライセンスをアップロードし、ライセンス付与されたサーバの再確認 をクリックします。「ベアメタルサーバ対応性の再確認」を参照してください。
   - BIOS
   - LC
5. **次へ**をクリックします。
6. **概要** ウィンドウで、非対応ベアメタルサーバのファームフェアコンポーネントで行われる操作を確認します。
7. **終了** をクリックします。

ベアメタルサーバの iDRAC ライセンス対応の修正

このタスクについて

ベアメタルサーバ ページにリストされるベアメタルサーバは iDRAC ライセンスと互換性がないため、非対応です。表には、iDRAC ライセンスのステータスが表示されます。非対応のベアメタルサーバをクリックして、iDRAC ライセンスの残日数など、さらに詳細な情報を表示できます。また、必要に応じて、詳細情報を更新できます。**ライセンス付与されたサーバの再確認** リンクが **ベアメタルサーバ** ページで有効にされている場合は、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があります。

手順

1. OpenManage Integration for VMware vCenter で **管理** → **導入** タブを選択します。

ベアメタルサーバ ページで、表に示される非対応サーバのリストを表示します。

2. **iDRAC ライセンスのステータス** が、**非対応** または **不明** のベアメタルサーバを選択します。
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、**ライセンス付与されたサーバの再確認** をクリックします。

ベアメタルサーバ対応性の再確認

このタスクについて

OMIVV プラグイン以外で問題を提起したサーバについては、次の手動サーバ対応性の再確認を実行します。

手順

1. OpenManage Integration for VMware vCenter の **管理** → **導入** タブで、**ライセンス付与されたサーバの再確認** 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、**ライセンス付与されたサーバの再確認** をクリックします。

お使いのシステムを正常に修正した場合は、リストが更新され、システムが **対応**としてリストされます。正常に修正されない場合は、引き続き **非対応** としてリストされます。

14

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。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対するパスワードは一切提供されません。バックアップデータベースは、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。

デフォルトでは、Administrator グループ内のユーザーがすべての権限を有します。Administrator が、VMware vSphere ウェブクライアント内の OpenManage Integration for VMware vCenter のすべての機能を使用できます。必要な権限を持つユーザーに製品の管理を任せる場合、次の手順を実行します。

1. 必要な権限を持つ役割の作成
2. ユーザーの使用による vCenter サーバの登録
3. Dell 役割、Dell Operational Role および Dell インフラストラクチャ導入役割の両方を含めます。

データ整合性

OpenManage Integration for VMware vCenter、管理コンソール、および vCenter 間の通信は、HTTPS/SSL を使用して行います。OpenManage Integration for VMware vCenter は、vCenter とアプライアンス間での信頼された通信のために使用される SSL 証明書を生成します。また、通信前、および OpenManage Integration for VMware vCenter 登録前に vCenter サーバの証明書を検証し、信頼します。OpenManage Integration for VMware vCenter のコンソールタブは、キーが管理コンソールとバックエンドサービス間で交互に転送される間、不適切な要求を回避するためのセキュリティ手順を使用します。このタイプのセキュリティは、クロスサイトリクエストフォージェリを失敗させます。

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表示されます。この処置は、管理コンソールセッションの攻撃が可能な悪意ある URL をユーザーがクリックすることも防ぎます。

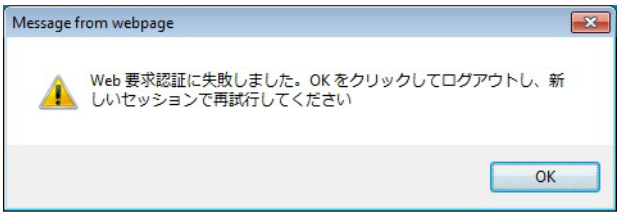

図 3. セキュリティエラーメッセージ

アクセス制御認証、承諾、および役割

vCenter 操作を実行するために、OpenManage Integration for VMware vCenter は、ウェブクライアントの現行のユーザーセッションと OpenManage Integration に保存された管理資格情報を使用します。OpenManage Integration for VMware vCenter は、vCenter サーバのビルトイン役割と権限モデルを使い、OpenManage Integration 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。

Dell Operational role

この役割には、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 サーバタスクの作成を含む、アプライアンスおよび vCenter サーバのタスクを実行する権限 / グループが含まれます。

この役割には次の特権グループが含まれます。

表 39. 権限グループ

グループ名	説明
特権グループ — Dell.Configuration	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
特権グループ — Dell.Inventory	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
特権グループ — Dell.Monitoring	監視の設定、監視
特権グループ — Dell.Reporting (使用されていません)	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導入役割

この役割には、ハイパーバイザー導入機能に関連した権限が含まれます。

この役割の特権は、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。

特権グループ — Dell.Deploy-Provisioning	テンプレートの作成、HW 設定プロファイルの設定、ハイパーバイザー導入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、導入

特権について

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
  - ステージング機能を使用してステージングフォルダを設定および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
  - HW 設定プロファイルの設定
  - ハイパーバイザ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
  - 導入
- 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

15

トラブルシューティング

本項では、トラブルシューティングの質問に対する回答を記載します。本項では、次の内容を説明します。

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。

Google Chrome の すべてエクスポート ボタンで .CSV ファイルへのエクスポートが失敗するのはなぜですか?

vCenter サーバの登録後、ホストを追加して接続プロファイルを作成し、次にホストのインベントリ詳細を表示すると、**すべてエクスポート** ボタンがエラーを返します。**すべてエクスポート** ボタンをクリックしても、情報は .CSV ファイルにエクスポートされません。

メモ:

Google Chrome ブラウザはどのバージョンでも、**シークレットモード**の場合、**すべてエクスポート** ボタンをクリックしても情報が .CSV ファイルにエクスポートされません。

対応処置：Google Chrome で **すべてエクスポート** ボタンを使用して情報を .CSV ファイルにエクスポートするには、Chrome ブラウザで**シークレットモード**を無効にします。

対象バージョン：4.0

非対応の vSphere ホストに対する iDRAC のライセンスタイプと説明が間違って表示されます

非対応のホストで CSIOR が無効であるか、実行されたことがない場合、有効な iDRAC ライセンスが利用できるにもかかわらず、間違った iDRAC ライセンス情報が表示されます。このため、ホストは vSphere ホストリストに表示されますが、詳細を表示するためにホストをクリックすると、**iDRAC ライセンスタイプ** には何も表示されず、**iDRAC ライセンス説明** には「お使いのライセンスはアップグレードする必要があります」が表示されます。

対応処置：この問題を解決するには、参照サーバで CSIOR を有効にします。

対象バージョン：4.0

古いバージョンの OMIVV から vCenter を登録解除し、その後にそれより新しいバージョンの OMIVV に同じ vCenter を登録すると、Dell アイコンは表示されません

古いバージョンの OMIVV から vCenter サーバを登録解除し、その後にそれより新しいバージョンの OMIVV に同じ vCenter サーバを登録した場合、vsphere-client-serenity フォルダに、古いバージョンの OMIVV からの古いデータであるエントリが残っています。このため、vCenter アプライアンスの vsphere-client-serenity フォルダに以前のバージョンの OMIVV に固有の古いデータが存在するので、より新しいバージョンの OMIVV に登録しても Dell アイコンは表示されません。

対応処置：以下の手順を行います。

1. vCenter アプライアンスの **/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity** フォルダに移動し、次のような古いデータが存在することを確認します。
   - com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-3.0.0.197
2. 古いバージョンの OMIVV に対応するフォルダを手動で削除します。
3. vCenter サーバで vSphere Web クライアントサービスを再起動します。

対象バージョン：すべて

設定ウィザードを起動するごとに設定がデフォルト設定で上書きされます

設定ウィザードを最初に起動した際にインベントリ、保証取得スケジュール、イベントとアラームを設定しても、設定ウィザードを再起動すると、以前に設定したインベントリおよび保証取得スケジュールが維持されません。インベントリおよび保証取得スケジュールは、設定ウィザードを起動するごとにデフォルト設定にリセットされます。ただし、イベントとアラームについては、更新された設定が維持されます。

対応処置 / 回避策：ウィザードの機能を完了する前に、以前のスケジュールを インベントリ ページと 保証取得スケジュール ページに複製し、以前のスケジュールがデフォルト設定で上書きされないようにします。

対象バージョン：3.0 以降

Dell プロバイダが正常性アップデートプロバイダとして表示されません

vCenter サーバを OMIVV に登録した後に、vCenter サーバのバージョンをたとえば vCenter 6.0 から vCenter 6.5 にアップグレードすると、**Proactive HA プロバイダ** リストに Dell プロバイダが表示されません。

対応処置：非管理者ユーザーまたは管理者ユーザーに対して登録済み vCenter をアップグレードできます。最新バージョンの vCenter サーバにアップグレードするには、VMware のマニュアルを参照して、状況に応じて次の選択肢のいずれかを実行します。

- 非管理者ユーザーの場合：
  a. 必要に応じて、非管理者ユーザーに追加の権限を割り当てます。「Administrator 以外のユーザーに必要な権限」を参照してください。
  b. 登録済み OMIVV アプライアンスを再起動します。
  c. Web クライアントからログアウトしてから再度ログインします。
- 管理者ユーザーの場合：
  a. 登録済み OMIVV アプライアンスを再起動します。
  b. Web クライアントからログアウトしてから再度ログインします。

これで、Dell プロバイダが **Proactive HA プロバイダ** リストに表示されるようになります。

対象バージョン：4.0

ESXi 5.x ホスト上でファームウェアアップデートタスクを実行するとインベントリが失敗するのはなぜですか?

vCenter サーバの登録後、ESXi 5.x ホストでファームウェアアップデートタスクを実行し、**コンポーネントの選択** 画面からコンポーネントとして iDRAC を選択すると、ホスト内の ESXi が新しい iDRAC IP と同期されず、無効な iDRAC IP が OMIVV に提供されることがあります。このため、そのホストではインベントリを正常に実行できません。

対応処置：この問題を解決するには、ESXi ホストで sfcdb デーモンを再起動します。詳細については、https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2077693 を参照してください。

対象バージョン：4.0

無効または不明な iDRAC IP が原因でホストインベントリまたはテスト接続が失敗します。有効な iDRAC IP を取得する方法を教えてください。

このタスクについて

無効または不明な iDRAC IP が原因でホストインベントリまたはテスト接続が失敗し、「ネットワーク遅延または到達不能ホスト」、「接続拒否」、「操作でタイムアウト」、「WSMAN」、「ホストへの経路無し」、「IP アドレス：NULL」などのメッセージが表示されます。

手順

1. iDRAC 仮想コンソールを開きます。
2. F2 キーを押して、**トラブルシューティングオプション** に移動します。
3. **トラブルシューティングオプション** で、**管理エージェントの再起動** に移動します。
4. F11 を押して、管理エージェントを再起動します。

これで、有効な iDRAC IP が使用できるようになります。

メモ: WBEM サービスが有効になっていない場合も、ホストインベントリは失敗することがあります。WBEM サービスの詳細については、「接続プロファイルの作成」を参照してください。

非対応の vSphere ホスト解決ウィザードの実行で、特定のホストのステータスが「不明」として表示されるのはなぜですか?

非対応の vSphere ホスト解決ウィザードを実行して非対応のホストを修正する際に、特定のホストのステータスが「不明」として表示されます。「不明」のステータスは iDRAC が到達できない場合に表示されます。

対応処置：iDRAC がホストに接続しており、インベントリが正常に実行されていることを確認します。

対象バージョン：4.0

OMIVV アプライアンスの登録中に割り当てられるデルの権限は OMIVV の登録を解除した後、削除されません

OMIVV アプライアンスに vCenter を登録した後、複数のデルの権限が vCenter 権限リストに追加されます。OMIVV アプライアンスから vCenter の登録を解除しても、デルの権限は削除されません。

メモ: デルの権限は削除されませんが、OMIVV の操作への影響はありません。

影響を受けるバージョン：3.1

重要度カテゴリをフィルタしようとすると、Dell Management Center に、関連するすべてのログが表示されません。すべてのログを表示するにはどうすればいいですか?

ドロップダウンから **すべてのカテゴリ** を選択し、重要度カテゴリを選択してログデータをフィルタするとき、特定のカテゴリに属しているすべてのログが正確に表示されます。ただし、ドロップダウンから **情報** を選択してフィルタする場合、ファームウェアアップデートログは表示されず、タスク開始ログのみが表示されます。

解決策：Dell Management Center ですべてのログを表示するには、フィルタ ドロップダウンから **すべてのカテゴリ** を選択します。

影響を受けるバージョン：3.1

VMware 認証局（VMCA）によるエラーコード 2000000 を解決する方法

vSphere 証明書マネージャを実行し、vCenter サーバまたはプラットフォームコントローラサービス (PSC) 証明書を新しい CA 証明書と vCenter 6.0 のキーで置き換えるとき、OMIVV にエラーコード 2000000 が表示され、例外が発生します。

解決策：例外を解決するには、サービスの ssl アンカーを更新する必要があります。ssl アンカーは、PSC で `ls_update_certs.py` スクリプトを実行してアップデートできます。スクリプトは古い証明書サムプリントを入力引数として使用し、新しい証明書がインストールされます。詳細については、http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 と

http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689 にアクセスしてください。

Windows vSphere 6.0 での ssl アンカーのアップデート

1. lstoolutil.py.zip ファイルを http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 からダウンロードします。
2. lstoolutil.py ファイルを %VMWARE_CIS_HOME%"\VMware Identity Services\lstool\scripts\ フォルダにコピーします。

メモ: vSphere 6.0 アップデート 1 を使用している場合は、lstoolutil.py ファイルを置き換えないでください。

次の関連する手順を使用して ssl アンカーをアップデートできます。

- Windows オペレーティングシステムにインストールされている vCenter 用 ssl アンカーのアップデート：vSphere 証明書マネージャユーティリティを使用して vCenter の Windows インストールにある証明書を置き換えます。「vCenter の Windows インストールでの証明書の置き換え」を参照してください。
- vCenter サーバアプライアンス用 ssl アンカーのアップデート：vSphere 証明書マネージャユーティリティを使用して vCenter サーバアプライアンスにある証明書を置き換えます。「vCenter サーバアプライアンスでの証明書の置き換え」を参照してください。

指定された手順から取得した出力には、それぞれ `24 個のサービスをアップデートしました` および `26 個のサービスをアップデートしました` と表示されます。出力に `0 個のサービスをアップデートしました` と表示される場合、古い証明書サムプリントが正しくありません。次のステップを実行して、古い証明書サムプリントを取得できます。また、証明書の置き換えに **vCenter 証明書マネージャ** を使用していない場合は、次の手順を使用して古い証明書サムプリントを取得します。

メモ: 取得した古いサムプリントで `ls_update_certs.py` を実行します。

1. 管理対象オブジェクトブラウザ（MOB）から古い証明書を取得します。「管理対象オブジェクトブラウザ（MOB）から古い証明書を取得する」を参照してください。
2. 古い証明書からサムプリントを抽出します。「古い証明書からのサムプリントの抽出」を参照してください。

影響を受けるバージョン：3.0 以降、vCenter 6.0 以降

vCenter の Windows インストールでの証明書の置き換え

このタスクについて

vSphere 証明書マネージャユーティリティを使用して、vCenter の Windows インストールで証明書を置き換えるには次のステップを実行します。

手順

1. リモートデスクトップ接続を通じて外付けのプラットフォームサービスコントローラに接続します。
2. 管理モードでコマンドプロンプトを開きます。
3. `mkdir c:\certificates` コマンドを使用して、c:\certificates フォルダを作成します。
4. 次のコマンドを使用して古い証明書を取得します。`"%VMWARE_CIS_HOME%"\vmafdd\vecs-cli entry getcert --store BACKUP_STORE --alias bkp___MACHINE_CERT --output c:\certificates\old_machine.crt`
5. 次のコマンドを使用して古い証明書サムプリントを取得します。`"%VMWARE_OPENSSL_BIN%" x509 -in C:\certificates\old_machine.crt -noout -sha1 -fingerprint`

   メモ: 取得した証明書サムプリントは次の形式です。`SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`

   サムプリントは一連の数字とアルファベットで、次のように表示されます。`13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`
6. 次のコマンドを使用して新しい証明書を取得します。`"%VMWARE_CIS_HOME%"\vmafdd\vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output c:\certificates\new_machine.crt`
7. 次の手順を実行します。
   a. `"%VMWARE _PYTHON_BIN%" ls_update_certs.py --url` コマンドを使用して、`ls_update_certs.py` を実行します。
   b. psc.vmware.com を Lookup_Service_FQDN_of_Platform_Services_Controller で置き換え、`https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile c:\certificates\new_machine.crt --user Administrator@vsphere.local`

`--password Password` コマンドを使用して、13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 サムプリントをステップ 5 で取得したサムプリントと置き換えます。

メモ: 必ず有効な資格情報を入力してください。

8. すべてのサービスが正常にアップデートされた後に、vCenter ウェブクライアントから一度ログアウトしてから再度ログインします。

次の手順
OMIVV が正常に起動します。

vCenter サーバアプライアンスでの証明書の置き換え

このタスクについて
vSphere 証明書マネージャユーティリティを使用して、vCenter サーバアプライアンスで証明書を置き換えるには次のステップを実行します。

手順

1. コンソールまたはセキュアシェル（SSH）セッションを介して、外付けのプラットフォームサービスコントローラアプライアンスにログインします。
2. 次のコマンドを実行して Bash シェルへのアクセスを有効にします。`shell.set --enabled true`
3. `shell` と入力し、**Enter** を押します。
4. `mkdir /certificates` コマンドを使用して、フォルダまたは証明書を作成します
5. 次のコマンドを使用して古い証明書を取得します。`/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store BACKUP_STORE --alias bkp___MACHINE_CERT --output /certificates/old_machine.crt`
6. 次のコマンドを使用して古い証明書サムプリントを取得します。`openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint`

   メモ: 取得した証明書サムプリントは次の形式です。`SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`

   サムプリントは一連の数字とアルファベットで、次のように表示されます。`13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`
7. 次のコマンドを使用して新しい証明書を取得します。`/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output /certificates/new_machine.crt`
8. `cd /usr/lib/vmidentity/tools/scripts/` コマンドを実行して、ディレクトリを変更します
9. 次の手順を実行します。
   a. `python ls_update_certs.py --url` コマンドを使用して、`ls_update_certs.py` を実行します。
   b. psc.vmware.com を Lookup_Service_FQDN_of_Platform_Services_Controller で置き換え、`https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile /certificates/new_machine.crt --user Administrator@vsphere.local --password "Password"` コマンドを使用して、13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 サムプリントをステップ 6 で取得したサムプリントと置き換えます。

   メモ: 必ず有効な資格情報を入力してください。
10. すべてのサービスが正常にアップデートされた後に、vCenter ウェブクライアントから一度ログアウトしてから再度ログインします。

次の手順
OMIVV が正常に起動します。

管理対象オブジェクトブラウザ（MOB）から古い証明書を取得する

管理対象オブジェクトブラウザ（MOB）を使用してプラットフォームサービスコントローラ（PSC）に接続することにより、vCenter サーバシステムの古い証明書を取得することができます。

このタスクについて
古い証明書を取得するには、次のステップを実行して、ArrayOfLookupServiceRegistrationInfo 管理対象オブジェクトの sslTrust フィールドを見つけます。

メモ: 本書では、すべての証明書を保存するために C:\certificates\ フォルダの場所が使用されます。

手順

1. `mkdir C:\certificates\` コマンドを使用して、PSC に C:\certificates\ フォルダを作成します。
2. ブラウザで次のリンクを開きます。https://<vCenter FQDN|IP address>/lookupservice/mob?moid=ServiceRegistration&method=List
3. `administrator@vsphere.local` のユーザー名でログインし、プロンプトが表示されたら、パスワードを入力します。

   メモ: vCenter シングルサインオン（SSO）ドメインにカスタム名を使用している場合は、そのユーザー名とパスワードを使用します。

4. **filterCriteria** で、値フィールドを変更してタグ **<filtercriteria></filtercriteria>** のみを表示し、**メソッドの呼び出し** をクリックします。
5. 置き換える証明書に応じて次のホスト名を検索します。

   表 40. 検索条件情報

トラストアンカー	検索条件
vCenter サーバ	Ctrl+F を使用して、ページで vc_hostname_or_IP.example.com を検索
プラットフォームサービスコントローラ	Ctrl+F を使用して、ページで psc_hostname_or_IP.example.com を検索

6. 対応する sslTrust フィールドの値を探します。sslTrust フィールドの値は、Base64 でエンコードされた古い証明書の文字列です。
7. プラットフォームサービスコントローラまたは vCenter サーバのトラストアンカーを更新する際には、次の例を使用します。

   メモ: 実際の文字列が大幅に短縮され、読みやすくなります。

   - vCenter サーバの場合

   表 41. vCenter サーバの例

名前	タイプ	値
url	anyURI	https://vcenter.vmware.local:443/sdk

   - プラットフォームサービスコントローラの場合

   表 42. プラットフォームサービスコントローラの例

名前	タイプ	値
url	anyURI	https://psc.vmware.local/sts/STSService/vsphere.local

8. sslTrust フィールドの内容をテキスト文書にコピーし、その文書を old_machine.txt として保存します。
9. テキストエディターで old_machine.txt を開きます。
10. 以下を、それぞれ old_machine.txt ファイルの最初と最後に追加します。

```
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
```

11. old_machine.txt を old_machine.crt として保存します。

次の手順

これでこの証明書からサムプリントを抽出できます。

古い証明書からのサムプリントの抽出

次のオプションを使用して、古い証明書からサムプリントを抽出し、プラットフォームサービス にアップロードできます。

- 証明書ビューアツールを使用して、サムプリントを抽出します。「証明書ビューアツールを使用した証明書サムプリントの抽出」を参照してください。
- アプライアンスでコマンドラインを使用して、サムプリントを抽出します。「コマンドラインを使用してサムプリントを抽出する」を参照してください。

証明書ビューアツールを使用した証明書サムプリントの抽出

このタスクについて

次のステップを実行して、証明書サムプリントを抽出します。

手順

1. Windows で、**old_machine.txt** ファイルをダブルクリックして、Windows 証明書ビューアで開きます。
2. Windows 証明書ビューアで、**SHA1 サムプリント** フィールドを選択します。
3. サムプリントの文字列をプレーンテキストエディターにコピーしてスペースをコロンで置き換えるか、文字列からスペースを削除します。
   たとえば、サムプリントの文字列は、次のいずれかのように表示されます。
   - ea87e150bb96fbbe1fa95a3c1d75b48c30db7971
   - ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71

コマンドラインを使用してサムプリントを抽出する

アプライアンスと Windows のインストールでコマンドラインを使用してサムプリントを抽出するには、次の項を参照してください。

vCenter サーバアプライアンスでコマンドラインを使用してサムプリントを抽出する

次の手順を実行します。

1. old_machine.crt 証明書を、古い証明書を取得するためのステップ 1 で作成した **C:\certificates\old_machine.crt** の場所にある PSC に移動またはアップロードします。Windows セキュアコピー（WinSCP）またはその他の SCP クライアントを使用して証明書を移動またはアップロードできます。
2. セキュアシェル（SSH）経由で外付けのプラットフォームサービスコントローラアプライアンスにログインします。
3. 次のコマンドを実行して Bash シェルへのアクセスを有効にします。`shell.set --enabled true`
4. `shell` と入力し、**Enter** を押します。
5. 次のコマンドを実行してサムプリントを抽出します。`openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint`

メモ: サムプリントは、等号に続く一連の数字とアルファベットで、次のように表示されます。`SHA1 Fingerprint= ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71`

Windows のインストールでコマンドラインを使用してサムプリントを抽出する

次の手順を実行します。

1. old_machine.crt 証明書を、古い証明書を取得するためのステップ 1 で作成した **C:\certificates\old_machine.crt** の場所にある PSC に移動またはアップロードします。Windows セキュアコピー（WinSCP）またはその他の SCP クライアントを使用して証明書を移動またはアップロードできます。
2. リモートデスクトップ接続を通じて外付けのプラットフォームサービスコントローラに接続します。
3. 管理モードでコマンドプロンプトを開きます。
4. 次のコマンドを実行してサムプリントを抽出します。`"%VMWARE_OPENSSL_BIN%" x509 -in c:\certificates\old_machine.crt -noout -sha1 -fingerprint`

メモ: サムプリントは、等号に続く一連の数字とアルファベットで、次のように表示されます。`SHA1 Fingerprint=09:0A:B7:53:7C:D9:D2:35:1B:4D:6D:B8:37:77:E8:2E:48:CD:12:1B`

古いサムプリントで ls_update_certs.py を実行します。すべてのサービスが正常にアップデートされた後に、vCenter ウェブクライアントから一度ログアウトしてから再度ログインします。デルプラグインが正常に起動します。

ファームウェアアップデートウィザードに、バンドルがファームウェアリポジトリから取得されていないというメッセージが表示されます。どうすればファームウェアアップデートを続行できますか?

ウェブクライアントでは、単一ホストにファームウェアアップデートウィザードを実行したとき、**コンポーネントの選択** 画面にコンポーネントのファームウェア詳細が表示されます。必要なファームウェアのアップデートを選択して、**戻る** を 2 回クリックし **ようこそ** ページに到着したときに **次へ** をクリックすると、**アップデートソースの選択** 画面に、バンドルがファームウェアリポジトリから取得されていないというメッセージが表示されます。

解決策：目的のファームウェアアップデートを選択し、**次へ** をクリックして、ファームウェアアップデートを続行できます。

影響を受けるバージョン：3.0 以降

管理コンソール で、アプライアンスを工場出荷時設定にリセットした後、リポジトリパスのアップデート がデフォルトに設定されないのはなぜですか?

アプライアンスをリセットした後、**管理コンソール** に移動し、左側のペインで **アプライアンス管理** をクリックします。**アプライアンスの設定** ページで、**リポジトリパスのアップデート** がデフォルトのパスに変更されていません。

対応処置：管理コンソール で、**デフォルトのアップデートリポジトリ** フィールドにあるパスを、**リポジトリパスのアップデート** フィールドに手動でコピーします。

クラスタレベルで 30 台のホスト用のファームウェアアップデートが失敗する理由

VMware では、クラスタを同一のサーバハードウェアで構築することをお勧めしています。ホスト数がクラスタの上限（ VMware 推奨 ）に近い状態のクラスタ、または異なるモデルの Dell サーバで構成されているクラスタでのクラスタレベルのファームウェアアップデートには、vSphere ウェブクライアントを使用します。

ジョブキュー ページから選択した際に、すべての vCenter の保証とインベントリスケジュールが適用されないのはなぜですか?

Dell Home → 監視 → ジョブキュー → 保証 / インベントリ履歴 → スケジュール に移動します。1 つの vCenter を選択して スケジュールの変更 ボタンを選択します。ダイアログが開くと、**すべての登録済み vCenter に適用する** というメッセージを持つチェックボックスが表示されます。チェックボックスを選択して **適用** を押すと、すべての vCenter ではなく、当初選択した特定の vCenter のみに設定が適用されます。**すべての登録済み vCenter に適用する** は、**ジョブキュー** ページから保証またはインベントリスケジュールが変更されるときには適用されません。

対応処置：ジョブキュー ページからのインベントリまたは保証スケジュールの変更は、選択した vCenter を変更する場合にのみ使用します。

影響を受けるバージョン：2.2 以降

OMIVV で、DNS 設定を変更した後、vCenter ウェブクライアントで、ウェブ通信エラーが発生したらどうすればよいですか?

DNS 設定を変更した後、OMIVV 関連タスクの実行中に vCenter ウェブクライアントで何らかのウェブ通信エラーが表示された場合は、次のいずれかの手順を実行します。

- ブラウザのキャッシュをクリアします。
- ログアウトしてウェブクライアントからログインします。

設定 ページから移動した後に戻った場合、設定 ページのロードに失敗するのはなぜですか?

vSphere v5.5 では、ウェブクライアントで **設定** ページから移動した後にページに戻ると、ページがロードに失敗し、スピナーが回転し続けることがあります。ロードの失敗は更新問題で、ページが正しく更新されていません。

対応処置：グローバル更新をクリックすると、画面が正しく更新されます。

影響を受けるバージョン：2.2 および 3.0

初期設定ウィザードのインベントリスケジュール / 保証スケジュール ページで「過去の時間にタスクをスケジュールすることはできません」と表示されるのはなぜですか?

ウェブクライアントでは、次の場合に「過去の時間にタスクをスケジュールすることはできません」エラーが表示されます。

- 初期設定ウィザードで すべての登録済み vCenter を選択し、ホストのない vCenter がいくつかある場合。
- いくつかの vCenter にインベントリまたは保証タスクがすでにスケジュールされている場合。

- インベントリまたは保証スケジュールがないいくつかの vCenter が未設定の場合。

解決方法：vCenter の **設定** ページから再度個別にインベントリと保証スケジュールの設定を実行します。

影響を受けるバージョン：2.2 以降

ファームウェアページで一部のファームウェアのインストール日が 12/31/1969 と表示されるのはなぜですか?

ウェブクライアントでは、ホスト向けのファームウェアページで一部のファームウェアアイテムのインストール日が 12/31/1969 と表示されます。ファームウェアのインストール日が使用不可である場合、この古い日付が表示されます。

対応処置：ファームウェアコンポーネントの一部にこの古い日付が表示される場合は、そのコンポーネントのインストール日が使用不可であると考えてください。

影響を受けるバージョン：2.2 以降

連続したグローバル更新によって最近のタスクウィンドウに例外が生成されます。このエラーの解決方法を教えてください。

連続して 更新 ボタンを押すと、VMware UI が例外を生成する場合があります。

解決方法：このエラーを無視して続行してかまいません。

影響を受けるバージョン：2.2 以降

IE 10 のデル画面のいくつかで Web クライアント UI が歪むのはなぜですか?

場合によっては、ポップアップダイアログが表示されると、バックグラウンドのデータが白色となり、歪んで表示されることがあります。

対応処置：ダイアログボックスを閉じると、画面は通常状態に戻ります。

影響を受けるバージョン：2.2 以降

vCenter へのプラグインの登録に成功したにもかかわらず、Web クライアントに OpenManage Integration アイコンが表示されないのはなぜですか?

OpenManage Integration アイコンは、vCenter Web クライアントサービスが再起動されるか、アプライアンスが再起動されない限り Web クライアントに表示されません。OpenManage Integration for VMware vCenter アプライアンスを登録すると、アプライアンスはデスクトップクライアントと Web クライアントの両方に登録されます。アプライアンスの登録を解除した後で、そのアプライアンスの同じバージョンの再登録、または新しいバージョンの登録のどちらかを行うと、両方のクライアントに正常に登録されますが、Dell アイコンが Web クライアントに表示されない場合があります。これは、VMware のキャッシュ問題によるものです。この問題を解決するには、vCenter サーバで Web クライアントサービスを再起動する必要があります。その後、プラグインが UI に表示されます。

対応処置：vCenter サーバで Web クライアントサービスを再起動します。

影響を受けるバージョン：2.2 以降

選択した 11G システム用のバンドルがリポジトリにあっても、ファームウェアアップデートでファームウェアアップデート用バンドルがないと表示されるのはなぜですか?

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すると、インベントリは起動されますが、「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」のメッセージが表示されて失敗します。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はずです。

ホストをロックダウンモードにした場合、またはホストのロックダウンモードを解除した場合は、30 分待ってから、次の操作を実行する必要があります。ファームウェアアップデート用に 11G ホストを使用すると、ファームウェアのアップデートウィザードでは、リポジトリにそのシステム用のバンドルがあっても、バンドルは何も表示されません。この問題が発生する場合、11G ホストで、OpenManage Integration にトラップを送信するように OMSA が構成されていない可能性があります。

対応処置：OpenManage Integration Web クライアントのホスト対応ウィザードを使用して、ホストが対応していることを確認します。対応していない場合は、ホスト対応の解決を使用してホストを対応させます。

影響を受けるバージョン：2.2 以降

アプライアンスの IP および DNS 設定が DHCP 値によって上書きされた場合、アプライアンスの再起動後に DNS 構成設定が元の設定に復元されるのはなぜですか?

これは、静的に割り当てられた DNS 設定が DHCP からの値で置き換えられるという既知の不具合です。これは、DHCP を使用して IP 設定が取得され、DNS 値が静的に割り当てられている場合に発生します。DHCP リースが更新されるか、アプライアンスが再起動すると、静的に割り当てられた DNS 設定が削除されます。

対応処置：DNS サーバの設定が 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

OMIVV を使用して、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をアップデートできません

これは、Dell PowerEdge 第 12 世代サーバ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との間に存在する既知の問題です。このファームウェアバージョンを搭載する一部の Intel ネットワークカードモデルに対して、Lifecycle Controller を使用してファームウェアアップデートを適用しようとすると、アップデートが失敗します。このバージョンのファームウェアを使用しているお客様は、オペレーティングシステムを使用して、ネットワークドライバソフトウェアをアップデートする必要があります。13.5.2 以外のファームウェアバージョンを搭載する Intel ネットワークカードは、OMIVV を使用してアップデートできます。詳細については、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、残りのサーバをアップデートするためのアップデートタスクが停止します。

Intel ネットワークカードを 14.5 または 15.0 から 16.x にアップデートするために OMIVV を使用すると、DUP からのステージング要件が原因でアップデートが失敗します

これは、NIC 14.5 および 15.0 の既知の問題です。ファームウェアを 16.x にアップデートする前に、カスタムカタログを使用してファームウェアを 15.5.0 をアップデートします。

対象バージョン：すべて

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、LC プロンプトのジョブステータスに「失敗」と表示されるのに、vCenter コンソールではハードウェアアップデートジョブステータスが何時間も失敗にもタイムアウトにもなりません。なぜこれが起きるのですか?

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 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：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ロケーションが表示されるのはなぜですか?

到達不能なアップデートリポジトリパスを指定すると、「失敗：URL....への接続時にエラー」エラーメッセージが アプライアンスアップデート ビューの上部に表示されます。ただし、リポジトリパスのアップデート はアップデート以前の値にクリアされません。

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

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な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は、ホストの再起動を必要としません。その場合、ファームウェアアップデートは、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。

一部の電源装置のステータスが重要に変更されても、シャーシのグローバル正常性が正常のままになっているのはなぜですか?

シャーシの電源装置に関するグローバル正常性は、冗長性ポリシーと、オンライン状態で機能している PSU がシャーシの電力必要量を満たしているかどうかに基づきます。PSU の一部で電力不足が発生しても、シャーシ全体の電力要件が満たされる場合、シャーシのグローバル正常性は正常のままになります。電源装置および電源管理の詳細については、Dell PowerEdge M1000e Chassis Management Controller Firmware に関するユーザーガイドを参照してください。

システム概要 ページの プロセッサ ビューで、プロセッサのバージョンが「該当なし」と表示されるのはなぜですか?

PowerEdge の第 12 世代以降の Dell サーバでは、プロセッサバージョンは ブランド 列に表示されます。それ以前の世代のサーバでは、プロセッサバージョンは バージョン 列に表示されます。

Web クライアントで接続プロファイルを編集した後に 終了 をクリックすると例外が返されるのはなぜですか?

これは、FQDN ではなく IP を使用して vCenter サーバがアプライアンスに登録されている場合に発生します。接続プロファイルは、Web クライアントで編集できます。
対応処置：vCenter サーバを同じアプライアンスに再登録しても問題は解決しません。FQDN で登録された新しいセットアップが必要です。

ホストが属する接続プロファイルが Web GUI で作成または編集する際に表示されないのはなぜですか?

これは、FQDN ではなく IP を使用して vCenter サーバがアプライアンスに登録されている場合に発生します。vCenter サーバを同じアプライアンスに再登録しても問題は解決しません。FQDN で登録された新しいセットアップが必要です。

接続プロファイルの編集時に、Web UI の ホストの選択 ウィンドウに何も表示されなくなるのはなぜですか?

これは、FQDN ではなく IP を使用して vCenter サーバがアプライアンスに登録されている場合に発生します。vCenter サーバを同じアプライアンスに再登録しても問題は解決しません。FQDN で登録された新しいセットアップが必要です。

ファームウェアリンクをクリックするとエラーメッセージが表示されるのはなぜですか?

このタスクについて
低速ネットワーク速度（9,600 bps）を使用している場合、通信エラーメッセージが表示されることがあります。このエラーメッセージは、OpenManage Integration for VMware vCenter の vSphere クライアントでファームウェアリンクをクリックすると表示されることがあります。ソフトウェアインベントリリストを取得する際に接続タイムアウトが発生すると、表示されます。Microsoft Internet Explorer は、このタイムアウトをトリガする

機能を備えています。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。この問題を解決するには、次の手順を実行します。

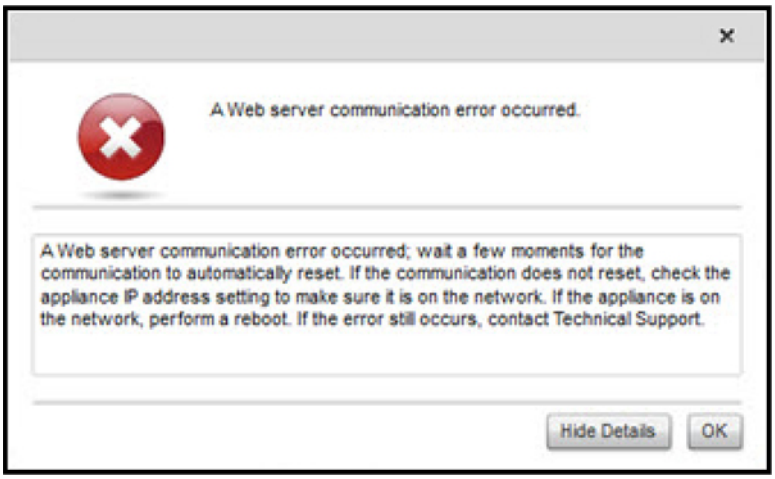

図 4. ファームウェアリンク通信エラー

手順

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。
   お使いの環境によっては、この値をさらに大きくすることが必要な場合があります。
5. Regedit を終了します。
6. Internet Explorer を再起動します。

メモ: 新しい Internet Explorer ウィンドウを開くだけでは、問題は解決しません。Internet Explorer ブラウザを再起動します。

OMIVV が SNMP トラップを設定およびサポートするのは、Dell サーバのどの世代ですか?

OMIVV は、第 12 世代より前の世代のサーバで OMSA SNMP トラップをサポートし、第 12 世代のサーバで iDRAC トラップをサポートしています。

OMIVV はどのような vCenter サーバを管理しますか?

OMIVV は、リンクモードまたは非リンクモードの登録済み vCenter サーバのみを管理します。

OMIVV はリンクモードの vCenter をサポートしますか?

OMIVV は、最大 10 台のリンクモードまたは非リンクモードの vCenter サーバをサポートします。リンクモードでの OMIVV の動作の詳細については、www.dell.com で提供されているホワイトペーパー『*OpenManage Integration for VMware vCenter: Working in Linked Mode*』（ OpenManage Integration for VMware vCenter ：リンクモードでの動作 ）を参照してください。

OMIVV ではどのようなポート設定が必要ですか?

メモ: OMIVV の 準拠 ウィンドウから 非対応の vSphere ホスト解決 リンクを使用して OMSA エージェントを展開すると、OMIVV により http クライアントサービスが起動され、ESXI 5.0 以降ではポート 8080 が有効化されます。その後、OMSA VIB がダウンロードおよびインストールされます。OMSA VIB のインストールが完了したら、サービスは自動的に停止し、ポートは閉じられます。

OMIVV では、次のポート設定を使用します。

表 43. 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	最大暗号化レベル	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	無
53	DNS	TCP	なし	出力	DNS クライアント	無
80	HTTP	TCP	なし	出力	Dell オンラインデータアクセス	無
80	HTTP	TCP	なし	入力	管理コンソール	無
162	SNMP エージェント	UDP	なし	入力	SNMP エージェント (サーバー)	無
11620	SNMP エージェント	UDP	なし	入力	SNMP エージェント (サーバー)	無
443	HTTPS	TCP	128 ビット	入力	HTTPS サーバー	無
443	WSMAN	TCP	128 ビット	入力 / 出力	iDRAC/OMSA 通信	無
4433	HTTPS	TCP	128 ビット	入力	自動検出	無
2049	ネットワーク ファイルシステム	UDP	なし	入力 / 出力	パブリック共有	無
4001 ~ 4004	ネットワーク ファイルシステム	UDP	なし	入力 / 出力	パブリック共有	無
11620	SNMP エージェント	UDP	なし	入力	SNMP エージェント (サーバー)	無

表 44. 管理対象ノード

ポート番号	プロトコル	ポートタイプ	最大暗号化レベル	方向	使用状況	設定可能
162、11620	snmp	UDP	なし	出力	ハードウェアイベント	無
443	WSMAN	TCP	128 ビット	入力	iDRAC/OMSA 通信	無
4433	HTTPS	TCP	128 ビット	出力	自動検出	無
2049	ネットワーク ファイルシステム	UDP	なし	入力 / 出力	パブリック共有	無
4001 ~ 4004	ネットワーク ファイルシステム	UDP	なし	入力 / 出力	パブリック共有	無
443	HTTPS	TCP	128 ビット	入力	HTTPS サーバー	無
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	無
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	無
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	無

ポート番号	プロトコル	ポートタイプ	最大暗号化レベル	方向	使用状況	設定可能
5353	mDNS	UDP/TCP		入力 / 出力	マルチキャスト DNS	無
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)	無
69	TFTP	UDP	128 ビット	入力 / 出力	トリビアルファイル転送	無
111	ネットワーク ファイルシステム	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)	無
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	無

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。

- Google Chrome バージョン 28 以降
- Microsoft Internet Explorer、バージョン 9 および 10
- Mozilla Firefox バージョン 22 以降
- 予約メモリ： 2 GB

  メモ: 最適なパフォーマンスを得るため、デルは 3 GB をお勧めします。
- ディスク： 44 GB
- CPU ： 2 つの仮想 CPU

iDRAC ユーザーリストに新しく変更された資格情報を持つユーザーが含まれたハードウェアプロファイルを正常に適用した後で、ベアメタル検出のために使用された同じユーザーのパスワードが変更されないのはなぜですか?

展開用にハードウェアプロファイルテンプレートのみが選択された場合、検出のために使用されたユーザーのパスワードは、新しい資格情報に変更されません。これは、将来の展開ニーズで、プラグインが iDRAC と通信できるようにするために、意図的に行われています。

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

対応処置 ： vSphere Web クライアントでファームウェアアップデートタスクが正常に完了したら、**ファームウェアアップデート** 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。このページに古いバージョンが表示される場合は、OpenManage Integration for VMware vCenter の **ホスト対応** ページに移動して、ホストの CSIOR ステータスをチェックします。CSIOR が有効になっていない場合は、CSIOR を有効にしてホストを再起動します。CSIOR が既に有効になっている場合、iDRAC コンソールにログインし、iDRAC をリセットします。数分待ってから、**ファームウェアアップデート** ページを更新します。

OMSA を使用して温度ハードウェア障害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を教えてください。

このタスクについて

イベントが正しく機能していることを確認するには、次の手順を実行します。

手順

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** に移動します。
2. **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. **最大警告しきい値** に、現在の読み取り値よりも低い値を設定します。
    たとえば、現在の読み取り値が 27 の場合、しきい値を **25** に設定します。
12. **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 **値に設定** オプションを使用して、元の設定を復元します。イベントが警告として生成され、その後、正常な状態になります。すべてが正常に動作している場合は、**vCenter タスクとイベント** 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 30 秒以上に設定します。

OMSA エージェントが OMIVV ホストシステムにインストールされているにもかかわらず、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表示されます。このエラーを解決する方法を教えてください。

このタスクについて
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。

手順

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 をインストールしている場合は、必ず **-c オプション**を使用するようにします。OMSA が既にインストールされている場合は、-c オプションを使用して再インストールし、サービスを再起動します。

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

ESXi ホストの場合は、**VMware Remote 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。

OMIVV はロックダウンモードが有効な ESXi をサポートできますか?

はい。本リリースでは、ロックダウンモードは ESXi 5.0 以降のホストにおいてサポートされています。

ロックダウンモードを使用しようとすると、失敗します

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ようとすると、インベントリは起動されますが、「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す。

ホストをロックダウンモードにした場合、またはホストのロックダウンモードを解除した場合は、30 分待ってから、OMIVV 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。

参照サーバを使用している際にハードウェアプロファイルの作成が失敗した場合はどうすればよいですか?

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。

参照サーバから取得したデータが最新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を再起動してください。

ブレードサーバで ESXi を導入しようとすると障害が発生するのはなぜですか?

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 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、設定されているネットワーク情報（サブネットマスクとデフォルトゲートウェイを含む）が正確であることを確認します。また、IP アドレスがまだネットワーク上で割り当てられていないことも確認します。
4. 1 つ以上の**仮想ディスク**がシステムで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。

Dell PowerEdge R210 II マシンでハイパーバイザー展開が失敗するのはなぜですか?

接続されている ISO からの BIOS 起動が失敗したために、Dell PowerEdge R210 II システムでタイムアウト問題が発生し、結果としてハイパーバイザー展開が失敗しています。

対応処置：手動でハイパーバイザーをマシンにインストールします。

展開ウィザードでは自動検出されたシステムのモデル情報が表示されないのはなぜですか?

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に登録されていない可能性があります。

対応処置：この問題を解決するには、システムをコールドブートするか、ブレードを抜き差しします。iDRAC で新たに有効化したアカウントを無効にする必要があります。その後、自動検出が再起動され、モデル情報と NIC 情報が OMIVV に提供されます。

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しようとするとエラーで失敗します

このタスクについて
解決法を見つけるには、次の手順を行います。

手順

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。
3. ポート 2049、4001 ~ 4004 が開いていること、ファイアウォールがそれに応じて設定されていることを確認します。

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. VMware vCenter のシステム管理者資格情報を入力します。
3. **コンテンツ** をクリックします。
4. **ExtensionManager** をクリックします。
5. **UnregisterExtension** をクリックします。
6. 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。
7. 延長キーを入力して com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient を登録解除し、**メソッドの呼び出し** をクリックします。
8. vSphere Web クライアントで OMIVV を無効にして削除します。登録解除用のキーは、Web クライアント用である必要があります。

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している場合、暗号化パスワード フィールドが 今すぐバックアップ ウィンドウに表示されないことがあります。ページをスクロールダウンして、暗号化パスワードを入力する必要があります。

vSphere Web クライアントで Dell サーバ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

OMIVV アプライアンスが実行されていることを確認します。実行されていない場合は、vSphere Web クライアントから再起動します。仮想アプライアンス Web サービスが開始するまで数分間待機し、その後、ページを更新します。エラーが継続する場合は、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 を試します。ping が失敗する場合は、お使いのネットワーク設定が正しいことを確認します。

ファームウェアアップデートに失敗した場合は、どうすればよいですか?

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たかどうかを確認します。タイムアウトしている場合、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。システムが起動したら、インベントリを実行するか、または **ファームウェア** タブを使用して、アップデートが正常に終了したことを確認します。

vCenter の登録が失敗した場合には何をすればよいですか?

vCenter の登録は通信の問題が原因で失敗することがあります。このため、このような問題が発生した場合は、対応処置として静的 IP アドレスを使用します。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、**ネットワークの構成** → **デバイスの編集** を選択し、正しい値を **ゲートウェイ** と **FQDN**（ 完全修飾ドメイン名 ）に入力します。DNS 構成の編集 の下に DNS サーバ名を入力します。

メモ: 入力した DNS サーバ名を仮想アプライアンスが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

このタスクについて

サーバ上の iDRAC に存在するユーザーが 1 人 (たとえば *root*) のみで、そのユーザーが無効になっている場合、またはすべてのユーザーが無効な場合に、無効状態のサーバとの通信で遅延が発生します。この問題を解決するには、サーバの無効状態を解決するか、サーバの iDRAC をリセットして、root ユーザーをデフォルト設定で再び有効化します。

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。

手順

1. Chassis Management Controller コンソールを開いて、無効状態のサーバを選択します。
2. iDRAC コンソールを自動的に開くには、**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、次のいずれかをクリックします。
   - iDRAC6：**iDRAC 設定** → **ネットワーク / セキュリティ タブ** → **ユーザー タブ** を選択します。
   - iDRAC7：**iDRAC 設定** → **ユーザー タブ** を選択します。
   - iDRAC8：**iDRAC 設定** → **ユーザー タブ** 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. **ユーザーの設定** をクリックして、**次へ** をクリックします。
6. 選択したユーザーの **ユーザーの設定** ページで、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、**適用** をクリックします。

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

はい、OMIVV はバージョン 2.1 以降で、VMware vCenter Server アプライアンスをサポートしています。

次回の再起動時にファームアップデートを適用するオプションでファームウェアのアップデートを行ってシステムを再起動したにも関わらず、ファームウェアのレベルがアップデートされないのはなぜですか?

ファームウェアをアップデートするには、再起動が完了した後にホストでインベントリを実行します。場合によっては、再起動イベントがアプライアンスに通知されずに、インベントリが自動的にトリガされないことがあります。このような状況では、インベントリを手動で再実行し、アップデートされたファームウェアのバージョン情報を取得する必要があります。

ホストを vCenter ツリーから削除した後でもシャーシにそのホストが引き続き表示されるのはなぜですか?

シャーシのホストはシャーシインベントリの一部として識別されます。シャーシインベントリが正常に終了すると、シャーシのホストリストがアップデートされます。このため、ホストが vCenter ツリーから削除されても、次のシャーシのインベントリが実行されるまで、そのホストはシャーシに表示されます。

管理コンソール で、アプライアンスを工場出荷時設定にリセットした後、リポジトリパスのアップデート がデフォルトに設定されないのはなぜですか?

アプライアンスをリセットした後、**管理コンソール** に移動し、左側のペインで **アプライアンス管理** をクリックします。**アプライアンスの設定** ページで、**リポジトリパスのアップデート** がデフォルトのパスに変更されていません。

対応処置 : 管理コンソール で、**デフォルトのアップデートリポジトリ** フィールドにあるパスを、**リポジトリパスのアップデート** フィールドに手動でコピーします。

OMIVV のバックアップおよび復元の後、アラーム設定が復元されないのはなぜですか?

OMIVV アプライアンスのバックアップを復元しても、一部のアラーム設定が復元されません。ただし、OpenManage Integration for VMware GUI の **アラームおよびイベント** フィールドには復元された設定が表示されます。

対応処置 : OpenManage Integration for VMware GUI の **管理** → **設定** タブで、**イベントおよびアラーム** 設定を手動で変更します。

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。
- 参照サーバがまった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必要があります。
- コントローラによっては、1 台のドライブでは RAID 0 アレイを作成できません。この機能はハイエンドのコントローラでのみサポートされており、そ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となることがあります。

新しく購入したシステムでの自動検出の有効化

このタスクについて

ホストシステムの自動検出機能はデフォルトで有効になっていません。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を請求した場合、iDRAC で DHCP が有効化され、管理アカウントが無効化されます。iDRAC 用に静的 IP アドレスを設定する必要はありません。ネットワーク上の DHCP サーバから取得されます。自動検出機能を使用するには、検出プロセスをサポートするように、DHCP サーバまたは DNS サーバ (または両方) を設定する必要があります。出荷処理中に、CSIOR が既に実行されている必要があります。

購入時に自動検出の有効化を請求しなかった場合は、次の手順で有効化できます。

手順

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`

16

関連マニュアル

このガイド以外にも、その他のガイドを利用できます (dell.com/support/manuals)。マニュアル ページで、**製品の参照** カテゴリの **製品の表示** をクリックします。**製品の選択** セクションで、**ソフトウェアとセキュリティ** → **仮想化ソリューション** の順にクリックします。**OpenManage Integration for VMware vCenter 4.0** をクリックして、次のドキュメントにアクセスします。

- 『*OpenManage Integration for VMware vCenter Version 4.0 Web Client User's Guide*』*(OpenManage Integration for VMware vCenter* バージョン *4.0 Web Client* ユーザーズガイド *)*
- 『*OpenManage Integration for VMware vCenter Version 4.0 Release Notes*』*(OpenManage Integration for VMware vCenter 4.0* リリースノート *)*
- 『*OpenManage Integration for VMware vCenter Version 4.0 Compatibility Matrix*』*(OpenManage Integration for VMware vCenter* バージョン *4.0* 互換性マトリクス *)*

delltechcenter.com では、ホワイトペーパーなどの技術に関する成果物を検索できます。Dell TechCenter Wiki のホームページで、**システム管理** → **OpenManage Integration for VMware vCenter** の順にクリックすると各記事を参照できます。

デルサポートサイトからの文書へのアクセス

必要なドキュメントにアクセスするには、次のいずれかの方法で行います。

- 次のリンクを使用します。
  - すべての Enterprise システム管理マニュアル — Dell.com/SoftwareSecurityManuals
  - OpenManage マニュアル — Dell.com/OpenManageManuals
  - リモートエンタープライズシステム管理マニュアル — Dell.com/esmmanuals
  - iDRAC および Lifecycle Controller マニュアル — Dell.com/idracmanuals
  - OpenManage Connection エンタープライズシステム管理マニュアル — Dell.com/OMConnectionsEnterpriseSystemsManagement
  - Serviceability Tool マニュアル — Dell.com/ServiceabilityTools
  - Client Command Suite システム管理マニュアル — Dell.com/DellClientCommandSuiteManuals
  - OpenManage 仮想化ソリューションマニュアル — Dell.com/VirtualizationSolutions
- Dell サポートサイトから、
  a. Dell.com/Support/Home に移動します。
  b. **製品の表示** をクリックし、**製品の選択** セクションで、**ソフトウェアとセキュリティ** をクリックします。
  c. **ソフトウェアとセキュリティ**グループボックスで、次の中から必要なリンクをクリックします。
     - **エンタープライズシステム管理**
     - **リモートエンタープライズシステム管理**
     - **Serviceability Tools**
     - **Dell Client Command Suite**
     - **接続クライアントシステム管理**

- **仮想化ソリューション**

d. ドキュメントを表示するには、必要な製品バージョンをクリックします。

- 検索エンジンを使用します。
  - 検索 ボックスに名前および文書のバージョンを入力します。