# OpenManage Integration for VMware vCenter

バージョン 5.1 インストール ガイド

DELL EMC

## メモ、注意、警告

**メモ:** 製品を使いやすくするための重要な情報を説明しています。

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

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



2020 - 04

Rev. A00

# 目次

# 1

# はじめに

本ガイドは、OpenManage Integration for VMware vCenter（OMIVV）をインストールして構成する手順を説明しています。OMIVV を使用することで、VMware vCenter を実行している PowerEdge サーバーの検出、モニター、管理が行えます。OMIVV のインストールが正常に完了した後に行う、インベントリー管理、モニタリングとアラート、ファームウェア アップデート、保証管理については、**https://www.dell.com/support** にある『*OpenManage Integration for VMware vCenter ユーザーズ ガイド*』を参照してください。

**トピック：**



# OpenManage Integration for VMware vCenter（OMIVV）のライセンス

OMIVV には、次の 2 種類のライセンスがあります。

- 評価ライセンス — OMIVV 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、OMIVV で 5 つのホスト（サーバー）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。この 90 日間評価バージョンは、出荷時に提供されるデフォルトのライセンスです。
- 標準ライセンス：OMIVV が管理するホストライセンスは、任意の数で購入できます。このライセンスには、製品サポートと OMIVV アプライアンスのアップデートも含まれています。

OMIVV は最大 15 の vCenter インスタンスをサポートします。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 Locker からライセンスファイルをダウンロードできます。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。

ライセンスを購入すると.XML ファイル（ライセンス キー）を **https://www.dell.com/support** の Dell Digital Locker 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、**https://www.dell.com/support** の「**オーダーサポートに問い合わせる**」ページに掲載されている、地域および製品ごとの Dell サポートの電話番号までお問い合わせください。

ライセンスによって、OMIVV 管理コンソールでは次の情報が提供されます。

- vCenter 接続ライセンスの最大数：最大 15 の登録済みおよび使用中の vCenter 接続が可能です。
- ホスト接続ライセンスの最大数：購入したホスト接続数です（1 つの OMIVV インスタンスで最大 2000 ホストをサポート）。

  認証情報プロファイルにホストを追加しようとする際に、ライセンスを保有するホスト数がライセンス数を超える場合、さらにホストを追加することはできません。OMIVV は、使用可能なホスト ライセンス数より多いホスト数の管理をサポートしていません。
- 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、この数はインベントリーされたホスト（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。

標準ライセンスは 3 年または 5 年間利用できます。追加のライセンスを購入すると、既存のライセンス期間が延長されます。

**メモ: OMIVV 5.x バージョンは、任意のアクティブなライセンスを使用できます。以前の OMIVV インスタンスからバックアップされたライセンスおよび Digital Locker から再ダウンロードしたライセンスは、現在の OMIVV インスタンスで使用できます。**

## ソフトウェア ライセンスの購入

1. **[ 設定 ]** > **[ ライセンス ]** > **[ ライセンスの購入 ]**、または **[ ダッシュボード ]** > **[ ライセンスの購入 ]**、または **[ 管理ポータル ]** > **[ vCenter の登録 ]** > **[ ライセンス ]** > **[ 今すぐ購入 ]** の順に移動します。
   Dell EMC のサポート ページが表示されます。

2. ライセンス ファイルをダウンロードし、既知の場所に保存します。
   ライセンスファイルは .zip ファイルにパッケージ化されている場合があります。.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。

# ライセンスの管理

## 新しく購入した製品のライセンスファイル

新しいライセンスを注文すると、注文の確認後に Dell EMC から E メールが送信されます。新しいライセンス ファイルのダウンロードは、**https://www.dell.com/suppot** の Dell EMC Digital Locker から行えます。ライセンスは XML ファイルとして送信されます。ZIP ファイルを受信した場合は、アップロードをする前に、XML ファイルを解凍しておきます。

## ライセンスのスタッキング

OMIVV では、標準ライセンスを複数スタックしておき、アップロードしたライセンスの合計ホスト数までサポート対象ホスト数を増やすことが可能です。評価ライセンスはスタックできません。デフォルトでは、OMIVV は最大 15 の vCenter をサポートします。15 を超える vCenter を管理する場合は、複数のアプライアンスを使用します。

既存の標準ライセンスの有効期限が切れる前に、新しい標準ライセンスをアップロードした場合は、ライセンスはスタックされます。それ以外の場合、ライセンスの有効期限が切れている状態で新しいライセンスをアップロードすると、新しいライセンスでのホストの数のみがサポートされます。すでに複数のライセンスがアップロードされている場合、サポートされるホストの数は、最後にライセンスをアップロードした時点で期限の切れていないライセンスでのホスト合計数になります。

## 期限切れのライセンス

サポート期間 ( 通常、お買い上げの日付から 3~5 年 ) を経過したライセンスは、アップロードがブロックされます。アップロード後にライセンスの有効期限が切れた場合、一部の機能が動作しないことがあります。OMIVV の新しいバージョンへのアップグレードはブロックされます。

## ライセンスの交換

ご注文に関する問題があり、Dell EMC から交換用のライセンスを受け取った場合、交換用のライセンスの資格 ID は以前のライセンスと同じになります。交換用のライセンスをアップロードする際、同じ資格 ID のライセンスがすでにアップロードされていると、そのライセンスは置き換えられます。

# 強制

## アプライアンスのアップデート

すべてのライセンスが失効している場合、アプライアンスでの新しいバージョンへの更新は許可されません。新しいライセンスを取得してアップロードした後で、アプライアンスをアップグレードします。

## 評価用ライセンス

評価ライセンスの有効期限が切れると、いくつかの主要な領域の動作が停止し、エラー メッセージが適宜表示されます。

# 参照用の重要なメモ

- OMIVV 5.0 以降では、VMware vSphere Client ( HTML5 ) のみがサポートされ、vSphere Web Client ( Flex ) はサポートされません。
- DNS サーバーを使用するために推奨されるベスト プラクティスは次のとおりです。
  - OMIVV は IPv4 IP アドレスのみをサポートします。静的 IP 割り当てと DHCP 割り当ての両方がサポートされていますが、静的 IP アドレスを割り当てることをお勧めします。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。

vSphere での DNS の要件の詳細については、次の VMware のリンクを参照してください。

- vSphere 6.5 および Platform Services Controller アプライアンスの DNS 要件
- Windows での vSphere 6.7 および Platform Services Controller の DNS 要件

- OMIVV アプライアンスのモードについては、お使いの仮想化環境に合った適切なモードで OMIVV を導入するようにします。詳細については、「展開モードの設定」を参照してください。
- ポート要件に一致するようにネットワークを設定します。詳細については、「ポート情報」を参照してください。

# ハードウェア要件

OMIVV は、Dell EMC PowerEdge サーバーをフル サポートしており、iDRAC Express および Enterprise の全機能に対応しています。お使いのホストサーバが適格であることを確認するには、以降のセクションに記載されている次の項目を参照してください。

- 対応サーバーと最小 BIOS
- サポートされる iDRAC バージョン ( 導入および管理の両方 )
- OMIVV の対応メモリー、CPU、ストレージ スペース

OMIVV には、iDRAC、CMC または OME モジュラー型システム管理ネットワークおよび vCenter 管理ネットワークにアクセスできる、マザーボードまたはネットワーク付属カード上の LAN が必要です。詳細については、「OMIVV アプライアンスの設定」および「2 つのネットワーク インターフェイス コントローラー ( NIC ) を用いた OMIVV アプライアンスの設定」を参照してください。

# 対応 BIOS バージョン

OpenManage Integration for VMware vCenter の機能を有効にするには、次のバージョンの BIOS および Lifecycle Controller 搭載 iDRAC が必要です。

OMIVV を使用する前に、Repository Manager、または Lifecycle Controller のプラットフォームを使用して作成されたブータブル ISO を使用してお使いのサーバのバージョンを次のいずれかにアップデートすることをお勧めします。

**表 1. 12G PowerEdge サーバーの対応 BIOS バージョン**

| サーバー | 必要最小 BIOS バージョン |
|---|---|
| T320 | 1.0.1 以降 |
| T420 | 1.0.1 以降 |
| T620 | 1.2.6 以降 |
| M420 | 1.2.4 以降 |
| M520 | 1.2.6 以降 |
| M620 | 1.2.6 以降 |
| M820 | 1.2.6 以降 |
| R220 | 1.0.3 以降 |
| R320 | 1.2.4 以降 |
| R420 | 1.2.4 以降 |
| R520 | 1.2.4 以降 |
| R620 | 1.2.6 以降 |
| R720 | 1.2.6 以降 |
| R720xd | 1.2.6 以降 |
| R820 | 1.7.2 以降 |
| R920 | 1.1.0 以降 |

**表 2. 13G PowerEdge サーバーの対応 BIOS バージョン**

| サーバー | 必要最小 BIOS バージョン |
|---|---|
| R630 | 1.0.4 以降 |

| サーバー | 必要最小 BIOS バージョン |
|---|---|
| R730 | 1.0.4 以降 |
| R730xd | 1.0.4 以降 |
| R430 | 1.0.4 以降 |
| R530 | 1.0.2 以降 |
| R830 | 1.0.2 以降 |
| R930 | 1.0.2 以降 |
| R230 | 1.0.2 以降 |
| R330 | 1.0.2 以降 |
| T630 | 1.0.2 以降 |
| T130 | 1.0.2 以降 |
| T330 | 1.0.2 以降 |
| T430 | 1.0.2 以降 |
| M630 | 1.0.0 以降 |
| M830 | 1.0.0 以降 |
| FC430 | 1.0.0 以降 |
| FC630 | 1.0.0 以降 |
| FC830 | 1.0.0 以降 |

**表 3. iDRAC9 ベース PowerEdge サーバーの対応 BIOS バージョン**

| サーバー | 必要最小 BIOS バージョン |
|---|---|
| R240 | 1.0.0 以降 |
| R340 | 1.0.0 以降 |
| R940 | 1.0.0 以降 |
| R940xa | 1.0.0 以降 |
| R740 | 1.0.0 以降 |
| R740xd | 1.0.0 以降 |
| R740xd2 | 1.0.0 以降 |
| R640 | 1.0.0 以降 |
| R840 | 1.0.0 以降 |
| R440 | 1.0.0 以降 |
| M640 | 1.0.0 以降 |
| T140 | 1.0.0 以降 |
| T340 | 1.0.0 以降 |
| T640 | 1.0.0 以降 |
| T440 | 1.0.0 以降 |
| R540 | 1.0.0 以降 |
| FC640 | 1.0.0 以降 |
| R6415 | 1.0.0 以降 |
| R7425 | 1.0.0 以降 |

| サーバー | 必要最小 BIOS バージョン |
|---|---|
| R7415 | 1.0.0 以降 |
| XR2 | 2.2.11 以降 |
| MX740C | 1.0.0 以降 |
| MX840C | 1.0.0 以降 |
| R6515 | 1.0.3 以降 |
| R7515 | 1.0.3 以降 |
| R6525 | 1.0.0 以降 |
| R7525 | 1.2.4 以降 |

**表 4. vSAN Ready Nodes の対応 BIOS バージョン**

| vSAN Ready Node | 必要最小 BIOS バージョン |
|---|---|
| R740xd | 1.0.0 以降 |
| R640 | 1.0.0 以降 |
| R440 | 1.0.0 以降 |
| R6415 | 1.0.0 以降 |
| C6420 | 1.0.0 以降 |
| R840 | 1.0.0 以降 |

# 対応する Lifecycle Controller 搭載 iDRAC のバージョン

**表 5. 導入に対応する Lifecycle Controller 搭載 iDRAC**

| サーバー | Lifecycle Controller 搭載 iDRAC |
|---|---|
| 12G | 2.50.50.50 以降 |
| 13G | 2.50.50.50 以降 |
| iDRAC9 ベース サーバー | 3.00.00.00 以降 |

**表 6. クラウドサーバの BIOS と iDRAC の要件**

| モデル | BIOS | Lifecycle Controller 搭載 iDRAC |
|---|---|---|
| C6320 | 1.0.2 | 2.50.50.50 以降 |
| C4130 | 1.0.2 | 2.50.50.50 以降 |
| C6420 | 1.0.0 以降 | 3.00.00.00 以降 |
| C4140 | 1.0.0 以降 | 3.00.00.00 以降 |
| C6525 | 1.0.0 以降 | 3.42.42.42 以降 |

# PowerEdge サーバーでサポートされる機能

OpenManage Integration for VMware vCenter によって管理されているホスト上では、次の機能がサポートされています。

**表 7. PowerEdge サーバーでサポートされる機能**

| 機能 | プラットフォーム | |
|---|---|---|
| | 第 12 世代 および第 13 世代 | iDRAC9 ベース サーバー |
| ハードウェアインベントリ | Y | Y |

| 機能 | プラットフォーム | |
|---|---|---|
| イベントとアラーム | はい ( SNMP v1 および v2 ) | はい ( SNMP v1 および v2 ) |
| コンポーネント毎の正常性監視* | Y | Y |
| BIOS / ファームウェアアップデート# | Y | Y |
| Proactive HA | Y | Y |
| 保証情報 | Y | Y |
| 管理対応性 | Y | Y |
| 設定コンプライアンス | Y | Y |
| ベアメタルサーバの自動 / 手動検出 | Y | Y |
| ベアメタル準拠 | Y | Y |
| ハードウェア構成 | Y | Y |
| OS 導入 | Y | Y |
| サーバー LED の点滅 | Y | Y |
| SEL ログの表示 / クリア | Y | Y |
| iDRAC のリンクと起動 | Y | Y |
| iDRAC のリセット | Y | Y |
| システムロックダウンモード | 無 | Y |
| システムプロファイル | Y | Y |
| クラスタプロファイル | Y | Y |
| 統合シャーシ IP を使用したホスト管理 | 無 | Y@ |
| OEM サーバのサポート | Y~ | Y |
| vSphere Lifecycle Manager | Y ( 13G のみ ) | Y |

* モデル番号 C6320 のクラウドでは、メザニンカードの正常性監視はサポートされていません。

# モデル番号 C6320 のクラウドでは、メザニンカードのファームウェアアップデートはサポートされていません。

@ MX シャーシホストにのみ適用されます。インベントリ、モニタリング、Proactive HA、ファームウェアのアップデート機能がサポートされています。

~ ラックサーバでのみサポートされています。

# PowerEdge シャーシでサポートされる機能

このトピックには、PowerEdge シャーシでサポートされる機能に関する情報が記載されています。

**表 8. モジュールインフラストラクチャでサポートされる機能**

| 機能 | M1000e | VRTX | FX2S | MX |
|---|---|---|---|---|
| SNMP アラート | Y | Y | Y | Y |
| ハードウェアインベントリ | Y | Y | Y | Y |
| CMC または管理モジュールのリンクと起動 | Y | Y | Y | Y |
| ライセンス情報 | 該当なし | Y | Y | Y |
| 保証情報 | Y | Y | Y | Y |
| 正常性レポート | Y | Y | Y | Y |

| 機能 | M1000e | VRTX | FX2S | MX |
|---|---|---|---|---|
| マルチシャーシ管理グループの関係情報 | N | N | N | Y |
| ファームウェアアップデート | 無 | N | N | Y |

# プロビジョニングされたストレージに必要なストレージ容量

OMIVV 仮想アプライアンスでは、プロビジョニングされたストレージ用に 95 GB 以上のディスク容量が必要です。

## デフォルトの仮想アプライアンスの設定

OMIVV 仮想アプライアンスは、8 GB の RAM と 2 個の仮想 CPU でプロビジョニングされます（小規模展開モード）。

# ソフトウェア要件

vSphere 環境が、仮想アプライアンスのシステム要件と、ポート アクセス、クロックの同期化、リスニング ポートの各要件を完全に満たすようにしてください。

OMIVV の機能へのアクセスには、Google Chrome を使用することをお勧めします。OMIVV は、Google Chrome と Mozilla Firefox をサポートしています。Microsoft Internet Explorer はサポートされていません。

**VMware vSphere Client（HTML-5）の要件**

vCenter 6.5 U2 以降

OpenManage Integration for VMware vCenter は、次の vCenter サーババージョンのすべてをサポートします。

**表 9. サポートされている vCenter サーババージョン**

| vCenter バージョン | クライアント サポート |
|---|---|
| 6.5 U2 | Y |
| 6.5 U3 | Y |
| 6.7 | Y |
| 6.7 U1 | Y |
| 6.7 U2 | Y |
| 6.7 U3 | Y |
| 7.0 | Y |

OMIVV 5.1 アプライアンスは CentOS バージョン 7 で実行されます。

# 管理対象ホスト上のサポートされている ESXi バージョン

次の表は、管理対象ホスト上でサポートされている ESXi バージョンに関する情報を提供するものです。

**表 10. サポートされている ESXi バージョン**

| ESXi バージョン | プラットフォーム | | |
|---|---|---|---|
| | 12G | 13G | iDRAC9 ベース サーバー |
| 6.0 U3 | Y | Y | 無 |
| 6.5 | Y | Y | 無 |
| 6.5 U1 | Y | Y | Y |
| 6.5 U2 | Y | Y | Y |

| ESXi バージョン | プラットフォーム | | |
|---|---|---|---|
| 6.5 U3 | Y | Y | Y |
| 6.7 | 無 | Y | Y |
| 6.7 U1 | 無 | Y | Y |
| 6.7 U2 | 無 | Y | Y |
| 6.7 U3 | 無 | Y | Y |
| 7.0 | 無 | Y | Y |

メモ: **PowerEdge MX ホストは、ESXi 6.5 U2 以降で使用されている場合にのみサポートされます。**

# ポート情報

本項には、仮想アプライアンスと管理対象ノードの設定に関するポート要件がすべてリストされています。

**表 11. 仮想アプライアンス**

| 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 | 送信先 | 使用状況 | 説明 |
|---|---|---|---|---|---|---|---|
| 53 | DNS | TCP | なし | 出力 | OMIVV アプライアンスから DNS サーバへ | DNS クライアント | DNS サーバへの接続またはホスト名の解決。 |
| 68 | DHCP | UDP | なし | 入力 | DHCP サーバーから OMIVV アプライアンスへ | 動的ネットワーク設定 | IP、ゲートウェイ、ネットマスク、DNS などのネットワーク詳細情報の入手に使用。 |
| 69 | TFTP | UDP | 128 ビット | 出力 | OMIVV から iDRAC へ | トリビアルファイル転送 | ベアメタル サーバーの対応する最小ファームウェア バージョンへのアップデートに使用。 |
| 123 | NTP | UDP | なし | 入力 | NTP から OMIVV アプライアンスへ | 時刻の同期 | 特定のタイムゾーンと同期。 |
| 162 | SNMP エージェント | UDP | なし | 入力 | iDRAC または CMC、もしくは OME-Modular から OMIVV アプライアンスへ | SNMP エージェント ( サーバー ) | 管理対象ノードからの SNMP トラップ受信用。 |
| 80/443 | HTTP/HTTPS | TCP | なし | 出力 | OMIVV アプライアンスからインターネットへ | Dell オンラインデータアクセス | オンライン ( インターネット ) 保証、ファームウェア、最新 RPM 情報への接続。 |
| 443 | HTTPS | TCP | 128 ビット | 入力 | OMIVV UI から OMIVV アプライアンスへ | HTTPS サーバー | OMIVV が提供する Web サービス。vSphere Client および Dell 管理ポータルで使用。 |
| 443 | HTTPS | TCP | 128 ビット | 入力 | ESXi サーバから OMIVV アプライアンスへ | HTTPS サーバー | OMIVV アプライアンスと通信するためのポストインストールスクリプト用のオペレーティングシステム導入フローで使用。 |
| 443 | HTTPS | TCP | 128 ビット | 入力 | iDRAC から OMIVV アプライアンスへ | 自動検出 | 管理対象ノードの自動検出に使用するプロビジョニングサーバ。 |
| 443 | WSMAN | TCP | 128 ビット | 入力 / 出力 | OMIVV アプライアンスと iDRAC 間 | iDRAC 通信 | 管理対象ノードの管理および監視に使用する iDRAC、CMC、または OME-Modular 通信。 |

| 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 | 送信先 | 使用状況 | 説明 |
|---|---|---|---|---|---|---|---|
| 445/139 | SMB | TCP | 128 ビット | 出力 | OMIVV アプライアンスから CIFS へ | CIFS 通信 | Windows 共有との通信用。 |
| 2049/111 | NFS | UDP/TCP | なし | 入力 / 出力 | OMIVV アプライアンスから NFS へ | パブリック共有 | OMIVV アプライアンスによって管理対象ノードに公開される NFS パブリック共有。ファームウェアアップデートおよびオペレーティングシステム導入のフローで使用。 |
| 4001 ~ 4004 | NFS | UDP/TCP | なし | 入力 / 出力 | OMIVV アプライアンスから NFS へ | パブリック共有 | これらのポートは、NFS サーバの V2 および V3 プロトコルによって statd、quotd、lockd および mountd サービスを実行するため、継続的に開いている必要があります。 |
| ユーザー定義 | 任意 | UDP/TCP | なし | 出力 | OMIVV アプライアンスからプロキシサーバへ | プロキシ | プロキシサーバとの通信 |

**表 12. 管理対象ノード ( ESXi )**

| 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 | 送信先 | 使用状況 | 説明 |
|---|---|---|---|---|---|---|---|
| 162 | SNMP | UDP | なし | 出力 | ESXi から OMIVV アプライアンスへ | ハードウェアイベント | ESXi から送信される非同期 SNMP トラップ。ESXi からこのポートを開く必要あり。 |
| 443 | WSMAN | TCP | 128 ビット | 入力 | OMIVV アプライアンスから ESXi へ | iDRAC 通信 | 管理ステーションへの情報提供に使用。ESXi からこのポートを開く必要あり。 |
| 443 | HTTPS | TCP | 128 ビット | 入力 | OMIVV アプライアンスから ESXi へ | HTTPS サーバー | 管理ステーションへの情報提供に使用。ESXi からこのポートを開く必要あり。 |

iDRAC および CMC ポート情報の詳細については、**https://www.dell.com/support** にある『*Integrated Dell Remote Access Controller ユーザーズガイド*』および『*Dell Chassis Management Controller ユーザーズガイド*』を参照してください。

OME-Modular ポート情報の詳細については、**https://www.dell.com/support** にある『*Dell EMC OME-Modular ユーザーズガイド*』を参照してください。

# Dell Online の参照 URL

**表 13. Dell Online の参照 URL**

| 特長 | 参照 URL |
|---|---|
| 保証 | https://apigtwb2c.us.dell.com |
| ファームウェアアップデート | https://downloads.dell.com |
| RPM アップグレード | https://linux.dell.com |

# 2

# OMIVV のインストールと設定

すべての要件が満たされており、必要な VMware vCenter が実行されていることを確認します。詳細については、「ハードウェア要件」および「ソフトウェア要件」を参照してください。

次の概要レベルの手順では、OMIVV のインストールおよび設定の全体的な手順についてのアウトラインが記載されています。

1. Dell サポート Web サイト（**https://www.dell.com/support**）から、*DellEMC_OpenManage_Integration_<バージョン番号>.<ビルド番号>.zip* ファイルをダウンロードします。OMIVV のダウンロードの詳細については、「OpenManage Integration for VMware vCenter のダウンロード」を参照してください。
2. ダウンロードしたファイルを保存した場所に移動し、ファイルの中身を解凍します。
3. vSphere Client（HTML-5）を使用して、OMIVV アプライアンスが入った Open Virtualization Format（OVF）ファイルを導入します。「OMIVV OVF の導入」を参照してください。
4. OVF の導入後に、タイム ゾーンと現在の日付と時刻を設定します。
5. ライセンスファイルをアップロードします。ライセンスの詳細については、「OMIVV 管理コンソールへのライセンスのアップロード」を参照してください。
6. 要件に応じて導入モードを設定します。詳細については、次を参照してください：展開モードの設定
7. 管理コンソールを使用して OMIVV アプライアンスを vCenter Server に登録します。「新しい vCenter サーバーの登録」を参照してください。
8. アプライアンス構成の設定を完了します。詳細については、次を参照してください：OMIVV アプライアンスの設定

**トピック：**

- 前提条件チェックリスト
- OpenManage Integration for VMware vCenter のダウンロード
- vSphere Client（HTML-5）を使用した OMIVV OVF の導入
- 証明書署名要求（CSR）の生成
- HTTPS 証明書のアップロード
- デフォルト HTTPS 証明書の復元
- 展開モードの設定
- 新しい vCenter サーバーの登録
- OMIVV アプライアンスの設定
- 登録済み vCenter バージョンのアップグレード後の OMIVV の再設定
- バックアップおよび復元の管理
- OMIVV アプライアンスとリポジトリーの場所のアップデート
- RPM を使用した OMIVV アプライアンスのアップグレード
- バックアップと復元を使用した OMIVV アプライアンスのアップグレード
- OpenManage Integration for VMware vCenter の登録解除
- 登録解除後の OMIVV の回復

# 前提条件チェックリスト

製品インストールを開始する前に、次のことを確認してください。

- vCenter Server のアクセスには OMIVV のユーザー名とパスワードが必要です。ユーザーは、すべての必要な権限を持つ管理者の役割を割り当てられたユーザーである場合もあれば、必要な権限を持つ非管理者ユーザーの場合もあります。OMIVV が動作するために必要な権限のリストの詳細については、「Administrator 以外のユーザーに必要な権限」を参照してください。
- ESXi ホスト システムの root パスワードか、ホストでの管理者権限がある Active Directory の資格情報が必要です。
- ユーザー名およびパスワードには、iDRAC での管理権限がある iDRAC Express または Enterprise との関連付けがされています。
- iDRAC での Administrator 権限を持っています。
- シンプル 2FA およびスマート カード ログオンは、iDRAC9 ベース サーバーの iDRAC では無効になっています。
- vCenter Server を実行中です。
- OMIVV のインストール ディレクトリーの場所が決まっています。
- OMIVV と vCenter Server は同じネットワーク上にあります。

- vCenter、OMIVV、iDRAC が異なるネットワークに接続されている場合、vCenter、OMIVV、iDRAC の各ネットワーク間にはルートがあります。これは、OMIVV アプライアンスが 2 つの NIC で設定されていない場合にのみ適用されます。
- VMware vSphere 環境は、仮想アプライアンスのシステム要件と、ポート アクセス、クロックの同期化、リスニング ポートの各要件に合致する必要があります。

**メモ: 仮想アプライアンスは通常の仮想マシンとして機能します。中断やシャットダウンは、いずれも仮想アプライアンスの全体的な機能に影響します。**

# OpenManage Integration for VMware vCenter のダウンロード

Dell EMC PowerEdge サーバのサービスタグを手元に置いておきますデルサポート用 Web サイトのすべてのサポートにアクセスするには、サービスタグを使用することをお勧めします。これにより、適切なバージョンのソフトウェアをプラットフォームにダウンロードすることができます。

OMIVV をダウンロードするには、次の手順を実行します。

1. **https://www.dell.com/support** にアクセスします。
2. 次のいずれかの手順を実行します。
   - Dell EMC PowerEdge サーバのサービスタグを入力し、検索を選択します。
   - **すべての製品の参照** > **サーバ** > **PowerEdge** を選択します。
3. PowerEdge サーバの適切なモデルを選択します。
4. サーバのサポートページで、**ドライバおよびダウンロード** を選択します。
5. [ **オペレーティング システム** ] のリストから、適切なバージョンの VMware ESXi を選択します。
6. **カテゴリ**リストから、**システム管理**を選択します。
   OMIVV のサポートされているバージョンが表示されます。
7. [ **ダウンロード** ] をクリックするか、チェックボックスをオンにしてソフトウェアをダウンロード リストに追加します。

# vSphere Client ( HTML-5 ) を使用した OMIVV OVF の導入

製品の.zip ファイル ( *DellEMC_OpenManage_Integration_<バージョン番号>.<ビルド番号>.zip* ) をサポート Web サイトからダウンロードして解凍していることを確認します。

**メモ: 次のタスクは、vSphere Client ( HTML-5 ) を使用している場合にのみ推奨のタスクです。Web Client の使用時は、手順が異なる場合があります。**

1. OMIVV をダウンロードした場所に移動し、**DellEMC_OpenManage_Integration.exe** をダブル クリックしてファイルを解凍します。

   exe ファイルを取り出して実行できるクライアント オペレーティング システムのバージョンは、Windows 7 SP1 以降です。

   exe ファイルを取り出して実行できるサーバー オペレーティング システムのバージョンは、Windows 2008 R2 以降です。
2. **EULA** に同意して、.ovf ファイルを保存します。
3. アプライアンスをアップロードする VMware vSphere ホストへのアクセスが可能な場所に、.ovf ファイルをコピーまたは移動します。
4. [ **VMware vSphere Client ( HTML-5 )** ] を開始します。
5. [ **VMware vSphere Client** ] からホストを選択し、メイン メニューで **[ アクション ]** > **[ OVF テンプレートの展開 ]** をクリックします。

   **ホスト** を右クリックして **OVF テンプレートの展開** を選択することもできます。

   **OVF テンプレートの導入ウィザード** が表示されます。
6. [ **OVF テンプレートの選択** ] ウィンドウで、次の手順を実行します。
   a) インターネットから OVF パッケージをダウンロードする場合、[ **URL** ] を選択します。
   b) ローカル システムから OVF パッケージを選択する場合は、[ **ローカル ファイル** ] を選択して、[ **ファイルの選択** ] をクリックします。
   c) ファイルを選択します ( .mf、.ovf、.vmdk )。
   d) [ **次へ** ] をクリックします。

[ **名前とフォルダーの選択** ] ウィンドウが表示されます。

**メモ: OVF パッケージがネットワーク共有に保存されている場合、インストールには 10 ~ 30 分かかります。迅速にインストールするため、ローカルドライブで OVF をホストすることをお勧めします。**

7. [ **名前とフォルダーの選択** ] ウィンドウで、次の手順を実行します。
   a) [ **仮想マシン名** ] フィールドに、テンプレートの名前を入力します。この名前には 80 文字まで使用できます。
   b) [ **仮想マシンの場所の選択** ] リストで、テンプレートを導入する場所を選択します。
   c) [ **次へ** ] をクリックします。
   [ **コンピューティング リソースの選択** ] ウィンドウが表示されます。
8. [ **コンピューティング リソースの選択** ] リストから、転送先のコンピューティング リソースを選択し、[ **次へ** ] をクリックします。

   操作を続行するには、転送先のコンピューティング リソースを選択する必要があります。互換性チェックが実行されて、転送先のコンピューティング リソースが選択されているかが検証されます。

   **詳細の表示** ウィンドウでは、次の情報が表示されます。

   - [ **発行元** ] — 発行元のデータ
   - [ **ダウンロード サイズ** ] — OVF テンプレートのサイズ ( GB 単位 )
   - [ **ディスクのサイズ** ] — シックおよびシン プロビジョニングに関する情報
9. **次へ** をクリックします。
   **ストレージの選択** 画面が表示されます。
10. [ **ストレージの選択** ] ウィンドウで、次の手順を実行します。
    a) [ **仮想ディスク フォーマットの選択** ] ドロップダウン リストで、次のいずれかの形式を選択します。

       - シックプロビジョニング ( Lazy Zeroed )
       - シック プロビジョニング ( Eager Zeroed )
       - シンプロビジョニング

       シック プロビジョニング ( Eager Zeroed ) を選択することをお勧めします。
    b) [ **VM ストレージ ポリシー** ] ドロップダウン リストからポリシーを選択します。
    c) [ **次へ** ] をクリックします。
    [ **ネットワークの選択** ] ウィンドウに、ソースおよび宛先ネットワークの詳細が表示されます。
11. [ **ネットワークの選択** ] ウィンドウで、各ソース ネットワークの宛先ネットワークを選択し、[ **次へ** ] をクリックします。

    vSphere 環境での Dell EMC サーバーの管理において OMIVV は、vSphere ネットワーク ( vCenter と ESXi 管理ネットワーク ) と、アウトオブバンド ネットワーク ( iDRAC、CMC、Dell EMC OpenManage Enterprise Modular ( OME-Modular )) の両方へのアクセスを必要とします。

    vSphere ネットワークとアウトオブバンド ネットワークが別のネットワークとして維持されている環境の場合、OMIVV は両方のネットワークへのアクセスを必要とします。そうした場合、OMIVV アプライアンスの設定は 2 つのネットワーク アダプターで行う必要があります。帯域外ネットワークへのアクセスが vSphere ネットワークを使用して可能な場合は、OMIVV アプライアンス用のネットワーク アダプターを設定しないでください。2 つのネットワーク アダプター設定の詳細については、「2 つのネットワーク インターフェイス コントローラー ( NIC ) を用いた OMIVV アプライアンスの設定」を参照してください。

    - アウトオブバンド ネットワーク : iDRAC、CMC、OME-Modular が接続されている管理ネットワークです。
    - vSphere ネットワーク : ESXi ホスト、vCenter、および PSC が接続されている管理ネットワークです。
12. **完了準備** ウィンドウで、OVF 展開タスクに使用するために選択したオプションを確認し、**終了** をクリックします。
    導入ジョブが実行され、ジョブの進捗状況を追跡できる場所に完了ステータスが表示されます。
13. VM の電源を入れます。

    **メモ: OVF の導入後、OMIVV を登録する前に、日付と時刻を設定しておく必要があります。**

# 証明書署名要求 ( CSR ) の生成

OMIVV を vCenter に登録する前に、必ず CSR をアップロードしてください。

新しい CSR を生成すると、以前生成された 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。

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。
   新規の要求が生成されると、以前の CSR によって作成された証明書はアプライアンスにアップロードできなくなりますというメッセージが表示されます。要求を続けるには、[ **続行** ] をクリックします。
2. 要求を続行する場合は、[ **証明書署名要求の生成** ] ダイアログ ボックスに、共通名、組織名、市区町村名、都道府県名、国、および E メール アドレスを入力します。**続行** をクリックします。

3. [ **ダウンロード** ] をクリックして、アクセス可能な場所に生成された CSR を保存します。

# HTTPS 証明書のアップロード

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。

HTTPS 証明書は、OMIVV アプライアンスとホスト システム間のセキュアな通信に使用することができます。このタイプのセキュアな通信を設定するには、CSR 証明書を署名責任者に送信してから、管理者コンソールを使用してその CSR をアップロードします。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。

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. 証明書をアップロードするには、[ **参照** ] > [ **アップロード** ] の順にクリックします。
   ステータスを確認するには、登録済み vCenter の vSphere Client で [ **イベント コンソール** ] に移動します。

証明書のアップロード中に OMIVV 管理コンソールは最大 3 分間応答しなくなります。HTTPS 証明書のアップロード タスクが完了したら、ブラウザー セッションを閉じ、新しいブラウザー セッションで管理者ポータルにアクセスします。

# デフォルト HTTPS 証明書の復元

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。

証明書の復元中に OMIVV 管理コンソールは最大 3 分間応答しなくなります。デフォルト HTTPS 証明書の復元タスクが完了したら、ブラウザー セッションを閉じ、新しいブラウザー セッションで管理者ポータルにアクセスします。

# 展開モードの設定

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 アプライアンスに十分なメモリー リソースを確保するようにしてください。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。

必要な展開モードごとに次のシステム要件を満たすには、OMIVV を搭載している VM には以下に示すリソースを割り当てるようにしてください。

**表 14. 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 ) | 最小構成のストレージ |
|---|---|---|---|---|
| 小 | 最大 250 台 | 2 | 8 | 95 GB |
| 中 | 最高 500 台 | 4 | 16 | 95 GB |
| 大 | 最大 1000 台 | 8 | 32 | 95 GB |
| 特大モード | 最大 2,000 台 | 12 | 32 | 95 GB |

**メモ: MX シャーシ ファームウェアのアップデート機能は、中規模、大規模、および特大の展開モードでのみサポートされます。**

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。

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**、**中**、**大**、**特大**などの展開モードの構成値が表示されます。デフォルトでは、モードは**小**に設定されています。
2. 環境に基づいて展開モードを編集するには、[ **編集** ] をクリックします。
3. [ **編集** ] モードで、前提条件を満たしていることを確認し、必要な展開モードを選択します。
4. **適用** をクリックします。
   割り当てられた CPU とメモリーが、設定された展開モードで必要な CPU とメモリーに対して検証されます。
   - 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、変更内容を確定すると、展開モード更新のために、アプライアンスが再起動されます。

**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 ページでは 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 アプライアンスを終了し、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. 展開モードを必要な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 リソースを必要な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。

# 新しい vCenter サーバーの登録

1. サポートされているブラウザから、**管理コンソール** を開きます。
   [ **管理コンソール** ] を開くには、Web ブラウザーを起動し、「`https://`**<アプライアンス IP またはアプライアンス ホスト名または FQDN>**」と入力します。
   IP アドレスは、アプライアンス VM の IP アドレスであり、ESXi ホストの IP アドレスではありません。管理コンソールは、コンソールの上部に示されている URL を使用してアクセスできます。
   例：`https://10.210.126.120` または `https://myesxihost`
   この URL では大文字と小文字は区別されません。

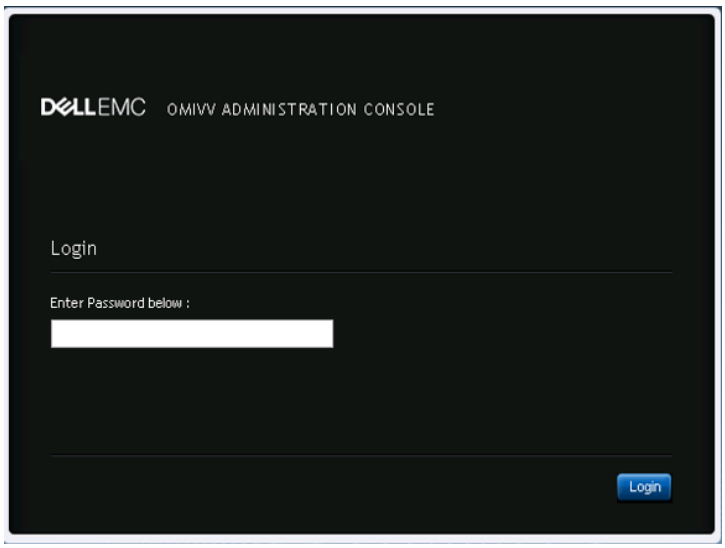



**図 1. 管理コンソール**

2. [ **OMIVV 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。

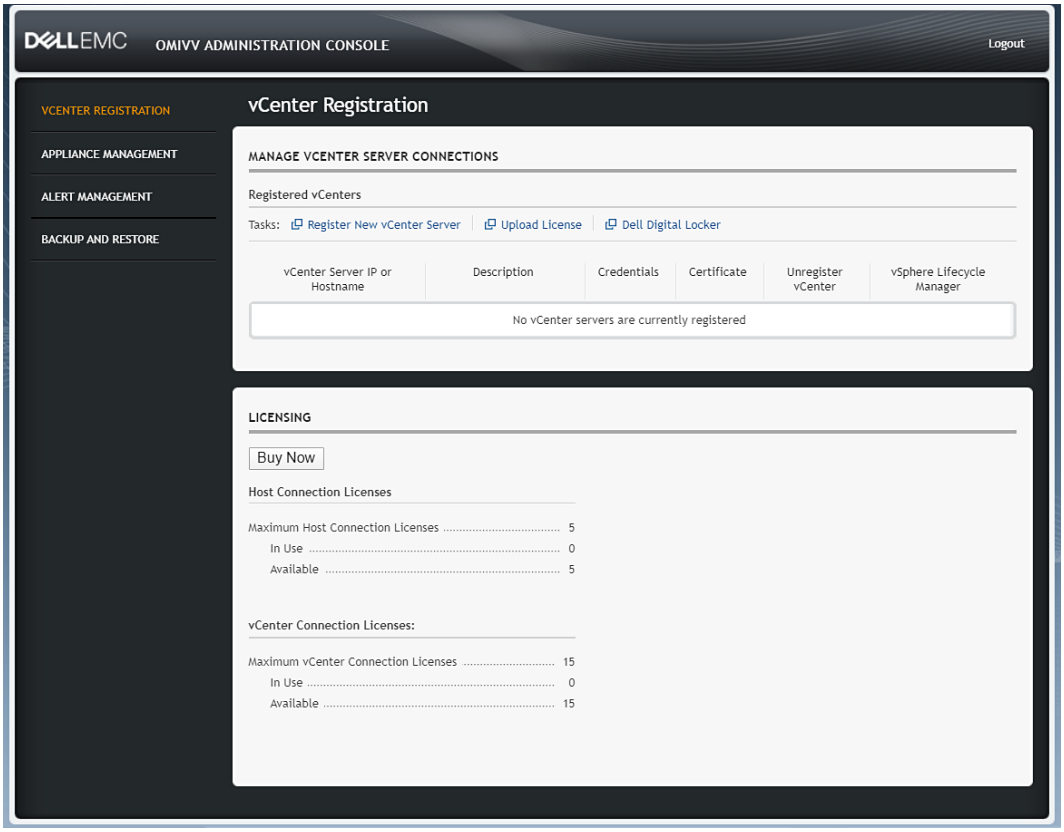



**図 2. vCenter の登録**

3. **vCenter 登録** ウィンドウで、**新規 vCenter サーバの登録** をクリックします。
4. **新規 vCenter サーバの登録** ウィンドウで、次のサブステップを実行します。
   a) [ **vCenter の名前** ] にある [ **vCenter サーバー IP またはホスト名** ] テキスト ボックスで、サーバー IP または FQDN を入力します。

   **メモ: 完全修飾ドメイン名 ( FQDN ) を使用して VMware vCenter で OMIVV を登録することをお勧めします。FQDN を使用して登録する際に、vCenter のホスト名が DNS サーバで正しく解決され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。説明はオプションです。
   c) [ **vCenter ユーザー アカウント** ] の [ **vCenter ユーザー名** ] に、管理者のユーザー名または、必要な権限を持つ管理者以外のユーザー名を入力します。

   **ユーザー名** に `domain\user`、`domain/user` または `user@domain` の形式で入力します。OMIVV では、vCenter の管理操作で Admin ユーザー アカウントまたは必要な権限を持つユーザーが使用されます。詳細については、「非管理者アカウントを使用した vCenter サーバーの登録」を参照してください。
   d) [ **パスワード** ] ボックスにパスワードを入力します。
   e) [ **パスワードの確認** ] にパスワードを再度入力します。
   f) [ **vSphere Lifecycle Manager の登録 ( vCenter 7.0 以降 )** ] チェック ボックスを選択します。[ **vSphere Lifecycle Manager の登録** ] チェック ボックスを選択すると、vCenter 7.0 以降から vSphere Lifecycle Manager の機能を使用できるようになります。

   vCenter の登録完了後、vSphere Lifecycle Manager のステータスを変更 ( 登録または登録解除 ) することができます。詳細については、「Dell EMC 管理コンソールでの vSphere Lifecycle Manager の登録」および「Dell EMC 管理コンソールでの vSphere Lifecycle Manager の登録解除」を参照してください。
5. **登録** をクリックします。

   OMIVV が登録されると、vSphere Client ( HTML-5 ) ホーム ページに [ OMIVV ] アイコンが表示されます。

   インストールを確認するには、「インストールの確認」を参照してください。

   **メモ: OpenManage Integration for VMware vCenter では、現在、リンク モードを使用することによって単一の vCenter インスタンスまたは複数の vCenter サーバーによる大規模な導入モードで最大 2000 のホストをサポートします。**
6. 次のいずれかの手順を実行します。
   - OMIVV の評価バージョンを使用している場合は、OMIVV アイコンが表示できます。

- 完全製品バージョンをお使いの場合は、**https://www.dell.com/support** の Dell Digital Locker からライセンス ファイルをダウンロードして、このライセンスを仮想アプライアンスにインポートできます。ライセンスファイルをインポートするには、**ライセンスのアップロード** をクリックします。ライセンスのアップロードの詳細については、「OMIVV 管理コンソールへのライセンスのアップロード」を参照してください。

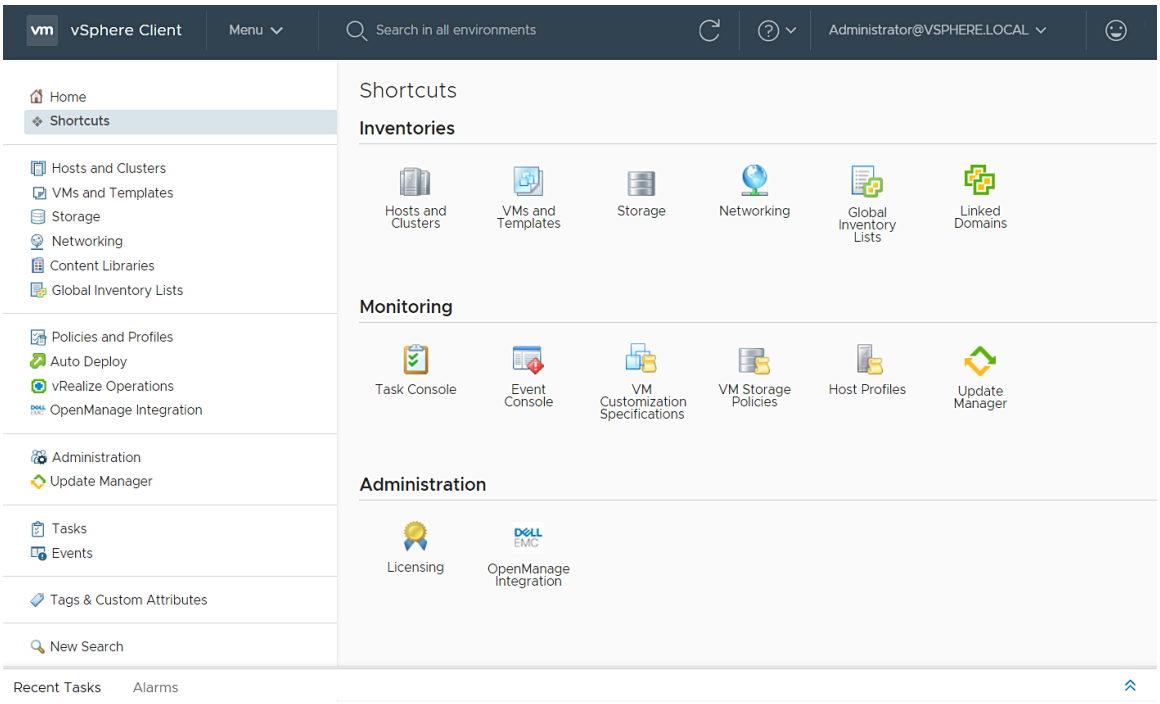



**図 3. vCenter に正常に追加された OpenManage Integration for VMware vCenter**

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、マシンをメンテナンスモードにするかホストを再起動します。

# OMIVV 管理コンソールへのライセンスのアップロード

自分のライセンスがダウンロード可能であることを、**https://www.dell.com/support** の Dell Digital Locker で確認します。複数のライセンスを注文した場合、各ライセンスが個別に有効化され、同時にはダウンロード可能にならない場合があります。他のライセンス アイテムのステータスは、**https://www.dell.com/support** の注文ステータスで確認できます。ライセンスファイルは .XML 形式で提供されます。

1. https://<*アプライアンス IP/ホスト名*/>に移動します。
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 サーバーが作業中の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 ファイルに変更や編集を加えた場合、ライセンス ファイル ( .XML ファイル ) は機能しなくなります。.XML ファイル ( ライセンス キー ) のダウンロードは、Dell Digital Locker を介して行えます。ライセンス キーをダウンロードできない場合は、https://www.dell.com/support の [ テクニカル サポートへのお問い合わせ ] ページに掲載されている、地域および製品ごとの Dell サポートの電話番号までお問い合わせください。**

# 非管理者アカウントを使用した vCenter サーバーの登録

vCenter の Administrator 資格情報があるか、またはデルの権限を持つ 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。

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。

1. 役割に必要な権限を持った役割を作成するか既存の役割を変更します。
   役割に必要な権限のリストの詳細については、「Administrator 以外のユーザーに必要な権限」を参照してください。
   役割を作成または変更し、vSphere Client（HTML-5）で権限を選択するために必要な手順については、VMware vSphere のマニュアルを参照してください
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。
   権限への役割の割り当ての詳細については、VMware vSphere のマニュアルを参照してください。
   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. 必要な権限のある Administrator 以外のユーザーにより vCenter サーバーを登録します。
4. 登録が完了したら、ステップ 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。「既存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 EMC 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、管理者以外のユーザーには次の権限が必要です。

管理者以外のユーザーが OMIVV で vCenter サーバーを登録する際に、次の権限が設定されていないと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
- 拡張権限
  - 登録の拡張権限
  - 登録解除の拡張権限
  - 更新の拡張権限
- グローバル
  - タスクのキャンセル
  - ログイベント
  - 設定
- 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
- ホスト
  - CIM
    - CIM インタラクション
- Host.Config
  - 詳細設定
  - 設定の変更
  - 接続
  - メンテナンス
  - ネットワークの設定
  - 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
  - クラスタの変更
- Lifecycle Manager：General Privileges
  - 読み取り

**メモ: vSphere Lifecycle Manager General Privileges は vCenter 7.0 以降にのみ適用されます。**

- 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
  - 作成
  - アップデート

**メモ: OMIVV の機能にアクセスするために、管理者以外のユーザーを使用して vCenter サーバーが登録されている場合、管理者以外のユーザーにはデルの権限が必要です。デルの特権を割り当てる方法の詳細については、「既存の役割へのデルの権限の割り当て」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

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。

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。

1. 管理者権限で vSphere Client ( HTML-5 ) にログインします。
2. vSphere Client ( HTML-5 ) で、[ **メニュー** ] を展開し、**[ 管理 ]** > **[ 役割 ]** の順にクリックします。
3. [ **役割プロバイダー** ] ドロップダウン リストから、vCenter サーバーを選択します。
4. [ **役割** ] リストから [ **デル操作** ] を選択し、[ **権限** ] をクリックします。
5. デルの権限を割り当てるには、編集アイコン ( ) をクリックします。
   [ **役割の編集** ] ページが表示されます。
6. 左ペインで [ **Dell** ] をクリックし、選択した役割に対して次のデルの権限を選択して [ **次へ** ] 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 内で使用可能な OMIVV 役割の詳細については、ユーザーズ ガイドの「セキュリティの役割および許可」トピックを参照してください。
7. 役割名を編集し、必要に応じて、選択した役割の説明を入力します。
8. **終了** をクリックします。
   ログ アウトして vCenter からログ インします。これで、必要な権限を持つユーザーが OMIVV 操作を実行できるようになります。

## 読み取り専用ユーザー役割

「読み取り専用」という弱い権限のユーザーがいます。診断目的のシェル アクセスができます。読み取り専用ユーザーには、いくつかのコマンドを実行するための限定的な特権があります。

# Dell EMC 管理コンソールでの vSphere Lifecycle Manager の登録

vCenter はバージョン 7.0 以降が必要です。

1. https://<*アプライアンス IP/ホスト名*/>に移動します。
2. [ **vCenter の登録** ] ページの [ **vSphere Lifecycle Manager** ] で、[ **登録** ] をクリックします。
   [ **vCenter Lifecycle Manager の登録** <*vCenter 名*> ] ダイアログ ボックスが表示されます。
3. [ **vSphere Lifecycle Manager の登録** ] をクリックします。

vSphere Lifecycle Manager の登録が正常に完了したことを示す確認メッセージが表示されます。

vSphere Lifecycle Manager を使用してクラスターを管理する方法の詳細については、**https://www.dell.com/support** にある『OMIVV ユーザーズ ガイド』を参照してください。

# Dell EMC 管理コンソールでの vSphere Lifecycle Manager の登録解除

vCenter はバージョン 7.0 以降が必要です。

1. https://<*アプライアンス IP/ホスト名*/>に移動します。
2. [ **vCenter の登録** ] ページの [ **vSphere Lifecycle Manager** ] で、[ **登録解除** ] をクリックします。
   [ **vCenter Lifecycle Manager の登録解除** <*vCenter 名*> ] ダイアログ ボックスが表示されます。
3. [ **登録解除** ] をクリックします。
   vSphere Lifecycle Manager が登録されます。vSphere Lifecycle Manager の登録解除が正常に完了したことを示す確認メッセージが表示されます。

   vSphere Lifecycle Manager を使用してクラスターを管理する方法の詳細については、**https://www.dell.com/support** にある『OMIVV ユーザーズ ガイド』を参照してください。

# インストールの確認

次の手順で OMIVV のインストールが正常に行われたことを検証します。

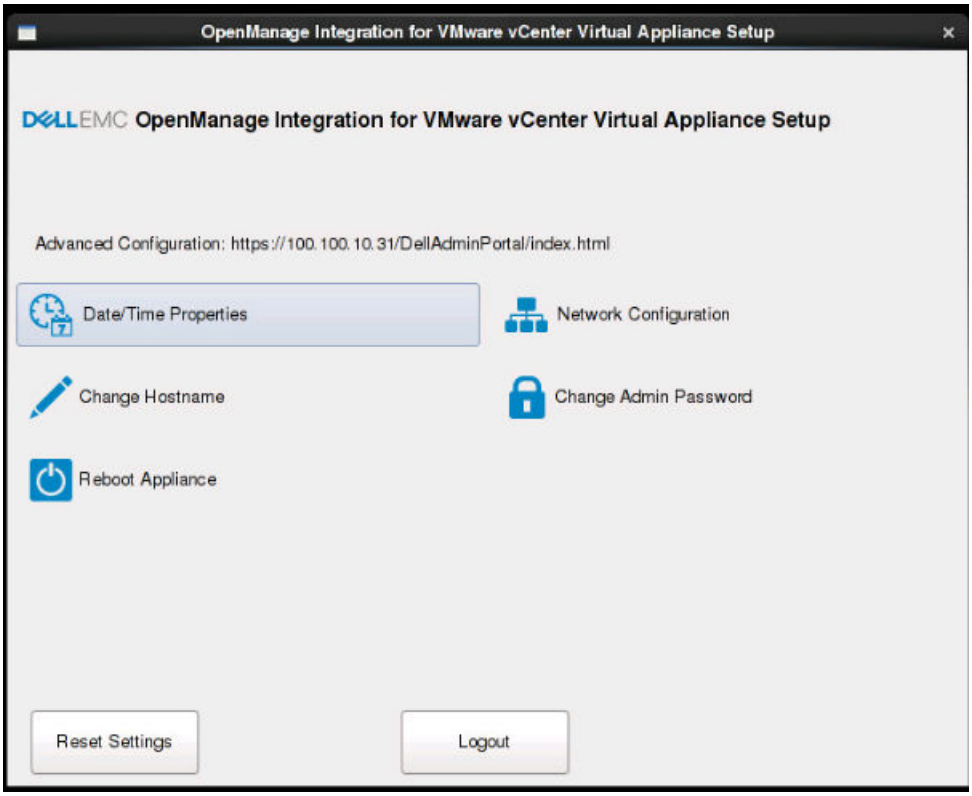
1. vSphere Client のウィンドウをすべて閉じて、新しい vSphere Client ( HTML-5 ) を開始します。
2. vCenter Server から、仮想アプライアンス IP アドレスまたはホスト名宛てに PING コマンドの実行を試行して、vCenter が OMIVV と通信できることを確認します。
3. vSphere Client で、 **メニュー**を展開し、**管理** > **ソリューション** > **Client Plug-ins** の順にクリックします。

   **Plug-In Management** または **Client Plug-Ins** ページのアクセス制限の詳細については、VMware のマニュアルを参照してください。
4. [ Client Plug-ins ] ページでバージョンを確認し、OMIVV がインストールされており有効になっていることを確認します。
   OMIVV が有効になっていない場合は、しばらく待ってから、vCenter からログ アウトしてログ インします。
5. [ OMIVV ] アイコンが vSphere Client ( HTML-5 ) 内に表示されることを確認するには、vSphere Client で [ **メニュー** ] を開きます。
   [ OpenManage Integration ] アイコンが表示されます。

# OMIVV アプライアンスの設定

1. VM の電源を入れます。
2. 右ペインで、[ **Web コンソールの起動** ] をクリックします。
3. 管理者としてログインします ( デフォルトのユーザー名は `admin` です )。
4. 初めてログインする場合は、画面の指示に従ってパスワードを設定します ( 管理者または読み取り専用ユーザー )。

   **メモ: 管理者パスワードを忘れた場合、OpenManage Integration for VMware vCenter アプライアンスからリカバリすることはできません。**
5. 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。




**メモ: OMIVV アプライアンスがネットワーク（DHCP）から IP アドレスを取得できない場合、0.0.0.0 が IP アドレスとして表示されます。この問題を解決するには、静的 IP を手動で設定する必要があります。**

a) [ **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** ] チェック ボックスを選択します。[ **ネットワーク上で日付と時間の同期化** ] チェック ボックスは、NTP が管理者ポータルを使用して正常に設定された後にのみ有効になります。NTP 設定の詳細については、「ネットワーク タイム プロトコル（NTP）サーバーのセットアップ」を参照してください。

b) [ **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。

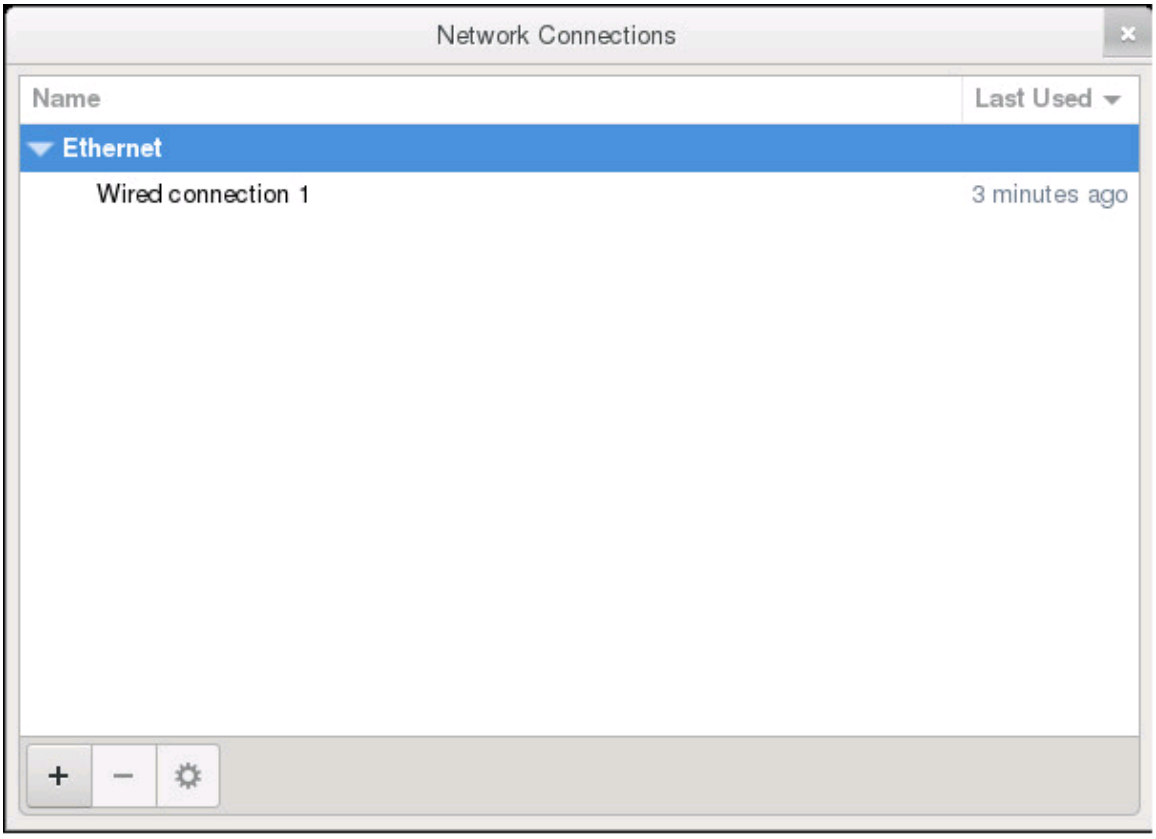
6. OMIVV アプライアンスのネットワークを設定するには、[ **ネットワークの設定** ] をクリックします。

   vSphere 環境での Dell EMC サーバーの管理において OMIVV は、vSphere ネットワーク（vCenter と ESXi 管理ネットワーク）と、アウトオブバンド ネットワーク（iDRAC、CMC、OME-Modular）の両方へのアクセスを必要とします。

   vSphere ネットワークとアウトオブバンド ネットワークが別のネットワークとして維持されている環境の場合、OMIVV は両方のネットワークへのアクセスを必要とします。そうした場合、OMIVV アプライアンスの設定は 2 つのネットワーク アダプターで行う必要があります。この両方のネットワークは、初期設定の一部として設定することをお勧めします。

   アウトオブバンド ネットワークへのアクセスが vSphere ネットワークを使用して行える場合、OMIVV アプライアンス用に 2 つのネットワーク アダプターを設定しないでください。2 つ目の NIC の設定の詳細については、「2 つのネットワーク インターフェイス コントローラー（NIC）を用いた OMIVV アプライアンスの設定」を参照してください。

7. [ **有線接続 1** ] を選択し、[  ] をクリックします。



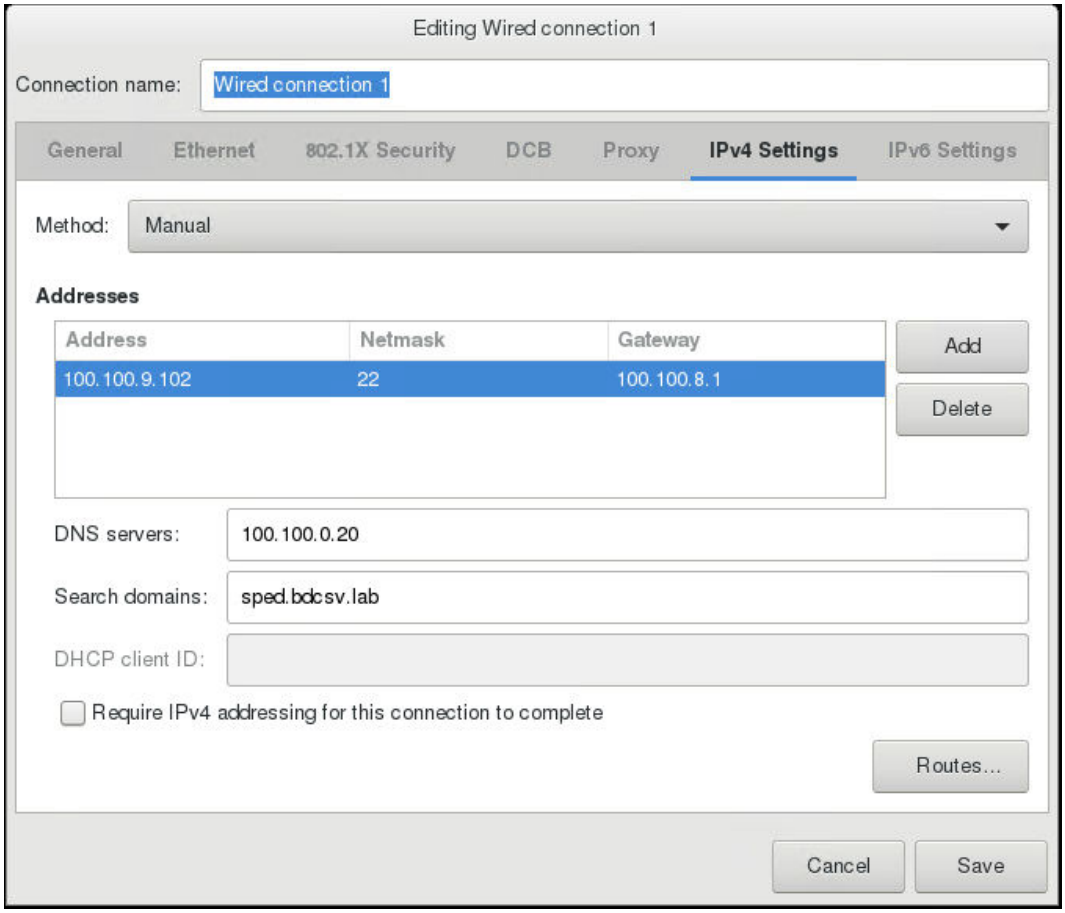

a) [ **IPv4 設定** ] タブをクリックし、[ **方法** ] ドロップダウン リストから [ **手動** ] を選択し、[ **追加** ] をクリックします。

**メモ: [ 自動 ( DHCP ) ] を選択した場合は、OMIVV アプライアンスが、次回の再起動時に DHCP サーバーから自動的に IP を受信するので、IP アドレスを入力しないでください。**

b) 有効な IP、ネットマスク ( Classless Inter-Domain Routing ( CIDR ) 形式 )、およびゲートウェイ情報を入力します。
[ **ネットマスク** ] ボックスに IP アドレスを入力すると、それぞれの CIDR 形式に自動的に変換されます。

c) [ **DNS サーバー** ] および [ **検索ドメイン** ] ボックスに、それぞれ検索対象の DNS サーバー IP およびドメインを入力します。

d) [ **この接続を完了するには IPV4 アドレス設定が必要です** ] チェック ボックスを選択し、[ **保存** ] をクリックします。




**メモ:**

**OMIVV アプライアンスを静的 IP で設定した後に、OMIVV ターミナル ユーティリティー ページがすぐに更新されず、アップデートされた IP が表示されないことがあります。この問題を解決するには、OMIVV ターミナル ユーティリティーを終了してから、再度ログインします。**

8. OMIVV アプライアンスのホスト名を変更するには、[ **ホスト名の変更** ] をクリックします。
   a) 有効なホスト名を入力して [ **ホスト名のアップデート** ] をクリックします。

   **メモ: OMIVV アプライアンスに登録済みの vCenter がある場合は、すべての vCenter インスタンスを登録解除して再登録します。詳細については、インストール ガイドの「登録解除と再登録の管理」を参照してください。**
9. アプライアンスを再起動します。

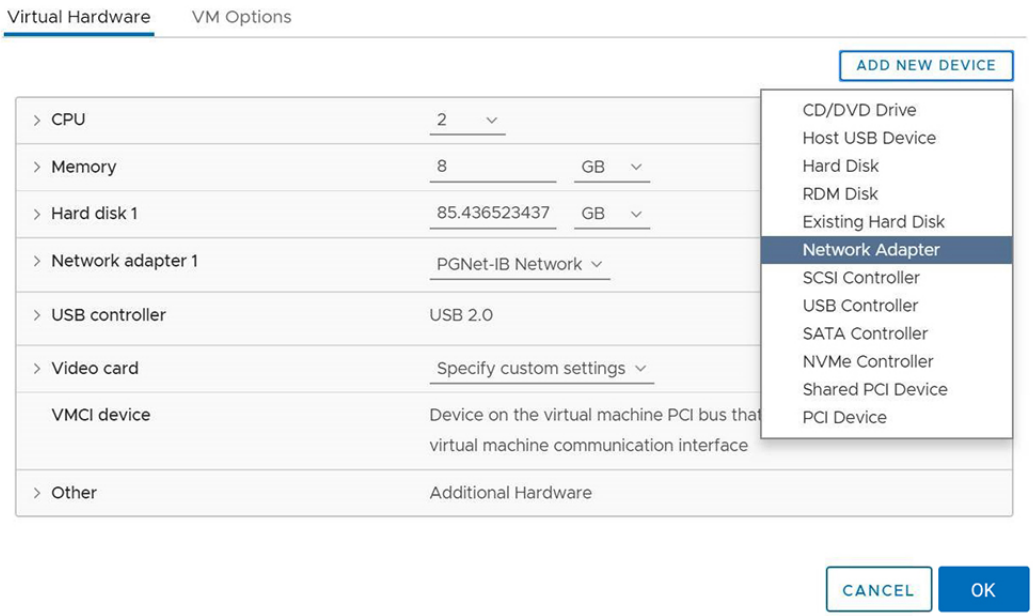
# 2 つのネットワーク インターフェイス コントローラー ( NIC ) を用いた OMIVV アプライアンスの設定

vSphere 環境での Dell EMC サーバーの管理において OMIVV は、vSphere ネットワーク ( vCenter と ESXi 管理ネットワーク ) と、アウトオブバンド ネットワーク ( iDRAC、CMC、OME-Modular ) の両方へのアクセスを必要とします。vSphere ネットワークとアウトオブバンド ネットワークが別のネットワークとして維持されている環境の場合、OMIVV は両方のネットワークへのアクセスを必要とします。そうした場合、OMIVV アプライアンスの設定は 2 つの NIC で行う必要があります。帯域外ネットワークへのアクセスが vSphere ネットワークを使用して可能な場合は、OMIVV アプライアンス用に 2 つの NIC を設定しないでください。

アウトオブバンド ネットワークと vSphere ネットワークの両方について、次の情報が準備されていることを確認します。

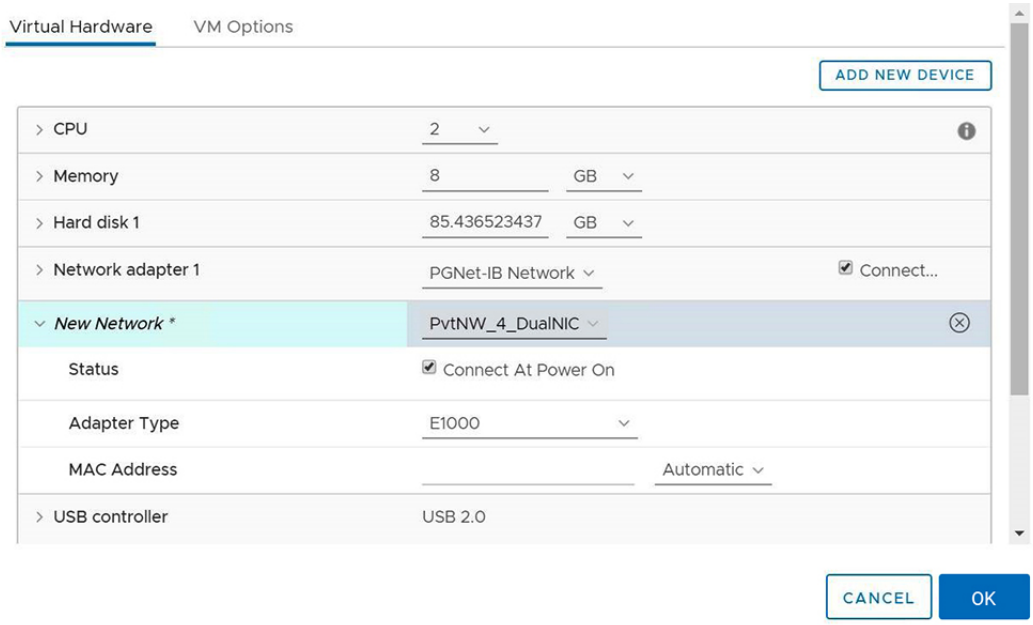
- アプライアンスの IP アドレス、ネットマスク ( CIDR 形式 )、およびゲートウェイ ( 静的な場合 )
- デフォルト ゲートウェイ : インターネットに接続された 1 つのネットワークにのみデフォルト ゲートウェイを設定する必要があります。vSphere ネットワークをデフォルト ゲートウェイとして使用することが推奨されます。
- ルーティング要件 ( ネットワーク IP、ネットマスク、およびゲートウェイ ): 直接またはデフォルト ゲートウェイを介してアクセスできないその他の外部ネットワークの場合は、静的ルートを設定します。
- DNS 要件 : OMIVV は、1 つのネットワークに対してのみ DNS 設定をサポートします。DNS 設定の詳細については、このトピックの手順 9 ( b ) を参照してください。

1. OMIVV アプライアンスの電源を切ります。
2. vSphere Client ( HTML-5 ) を使用して VM 設定を編集し、追加のネットワーク アダプターを登録します。VM 設定を編集するには、VM を右クリックして [ **設定の編集** ] をクリックします。
3. [ **新しいデバイスの追加** ] をクリックし、[ **ネットワーク アダプター** ] を選択します。



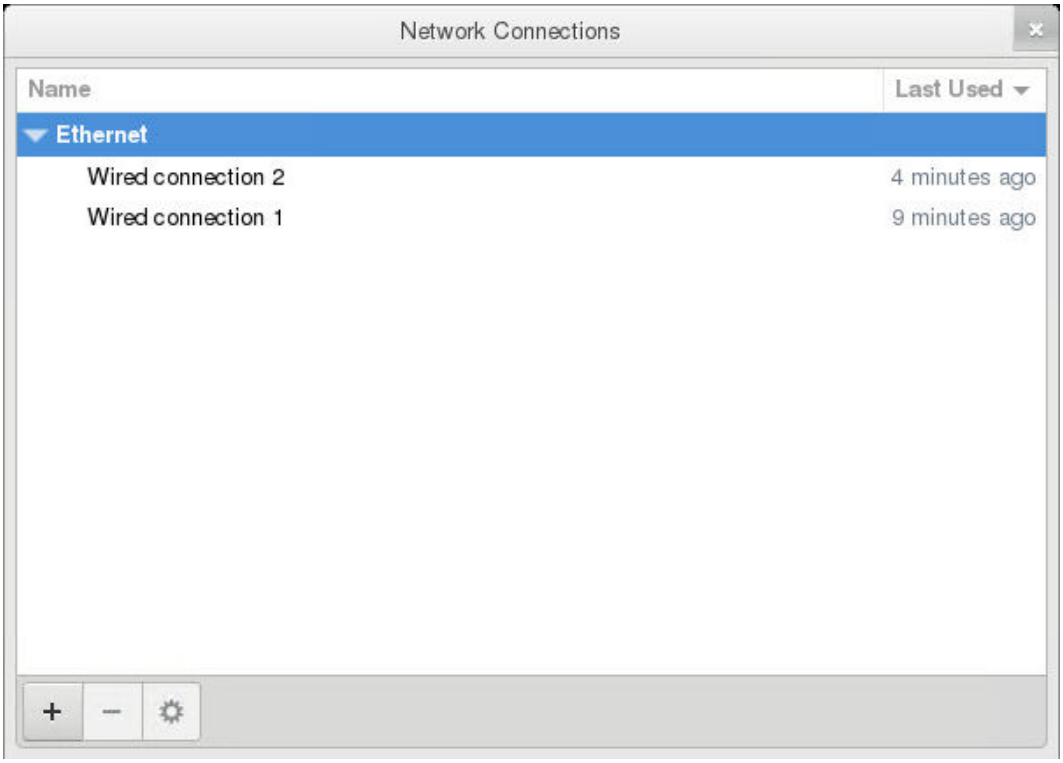

a) NIC に適したネットワークを選択し、[ **電源投入時に接続する** ] チェック ボックスを選択します。
b) ドロップダウン メニューから [ **VMXNET3** ] アダプター タイプを選択します。

**メモ: OMIVV は、VMXNET3 タイプの NIC をサポートしています。**




4. OMIVV アプライアンスの電源を入れます。管理者としてログインして ( デフォルトのユーザー名は Admin )、**Enter** を押します。
5. [ **OpenManage Integration for VMware vCenter の仮想アプライアンスのセットアップ** ] ユーティリティーで、[ **ネットワーク設定** ] を選択します。

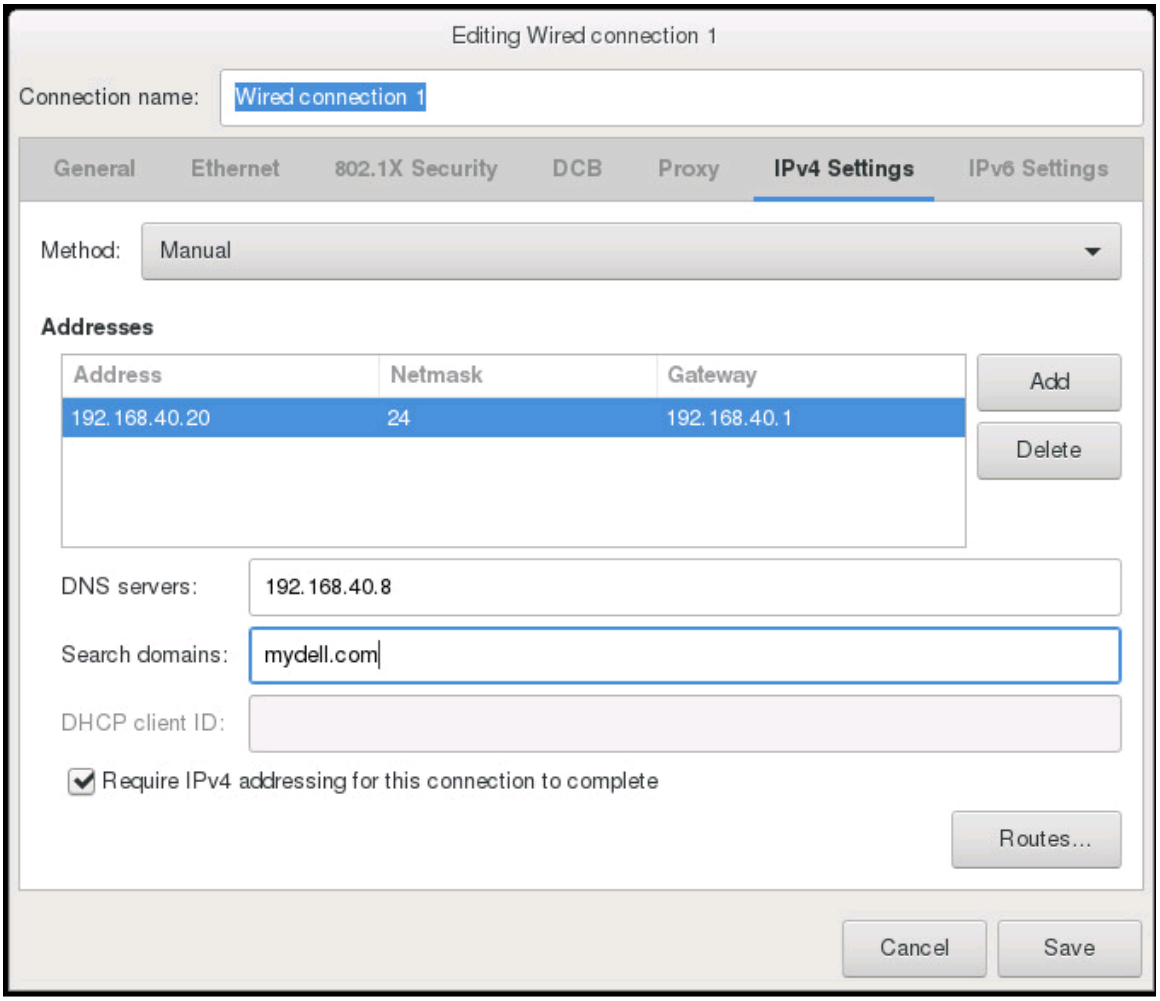
[ **ネットワーク接続** ] ページに 2 つの NIC が表示されます。




**警告: 新しいネットワーク インターフェイスの追加に「+」を使用しないでください。NIC を追加するには、vSphere の設定の編集を使用する必要があります。**

6. 設定する NIC を選択し、  をクリックします。
7. 正しい NIC を識別するには、[ **Ethernet** ] タブに表示されている MAC ID を使用して、vSphere Client ( HTML-5 ) に表示されている MAC ID と比較します。

   [ **Ethernet** ] タブに表示されているデフォルトの MAC アドレスを変更しないようにしてください。
8. [ **全般** ] タブをクリックし、[ **使用可能なときはこのネットワークに自動的に接続する** ] チェック ボックスを選択します。
9. [ **IPv4 設定** ] タブをクリックし、次の手順を実行します。




a) [ **方法** ] ドロップダウン リストから [ **手動** ] または [ **自動 ( DHCP )**] を選択します。

b) [ **手動** ] 方式を選択した場合は、[ **追加** ] をクリックして、有効な IP アドレス、ネットマスク ( CIDR 形式 )、およびゲートウェイの詳細を入力します。DNS サーバーの優先度 ( プライマリーおよびセカンダリー DNS エントリー ) を制御する場合は、静的 IP の使用をお勧めします。

通常、vCenter や ESXi ホストなどのデータ センターの vSphere 要素は、ホスト名または FQDN を使用して管理されます。iDRAC、CMC、および OME-Modular は、IP アドレスを使用して管理されます。この場合は、vSphere ネットワークに対してのみ DNS 設定を行うことを推奨します。

vSphere ネットワークと iDRAC 管理ネットワークの両方がホスト名または FQDN を使用して管理されている場合、両方のネットワークのホスト名または FQDN を解決するように DNS サーバーを設定する必要があります。詳細については、CentOS のマニュアルを参照してください。

**メモ: 最後に設定された DNS サーバーは、DNS が設定されているネットワークに関係なくプライマリ DNS になります。**

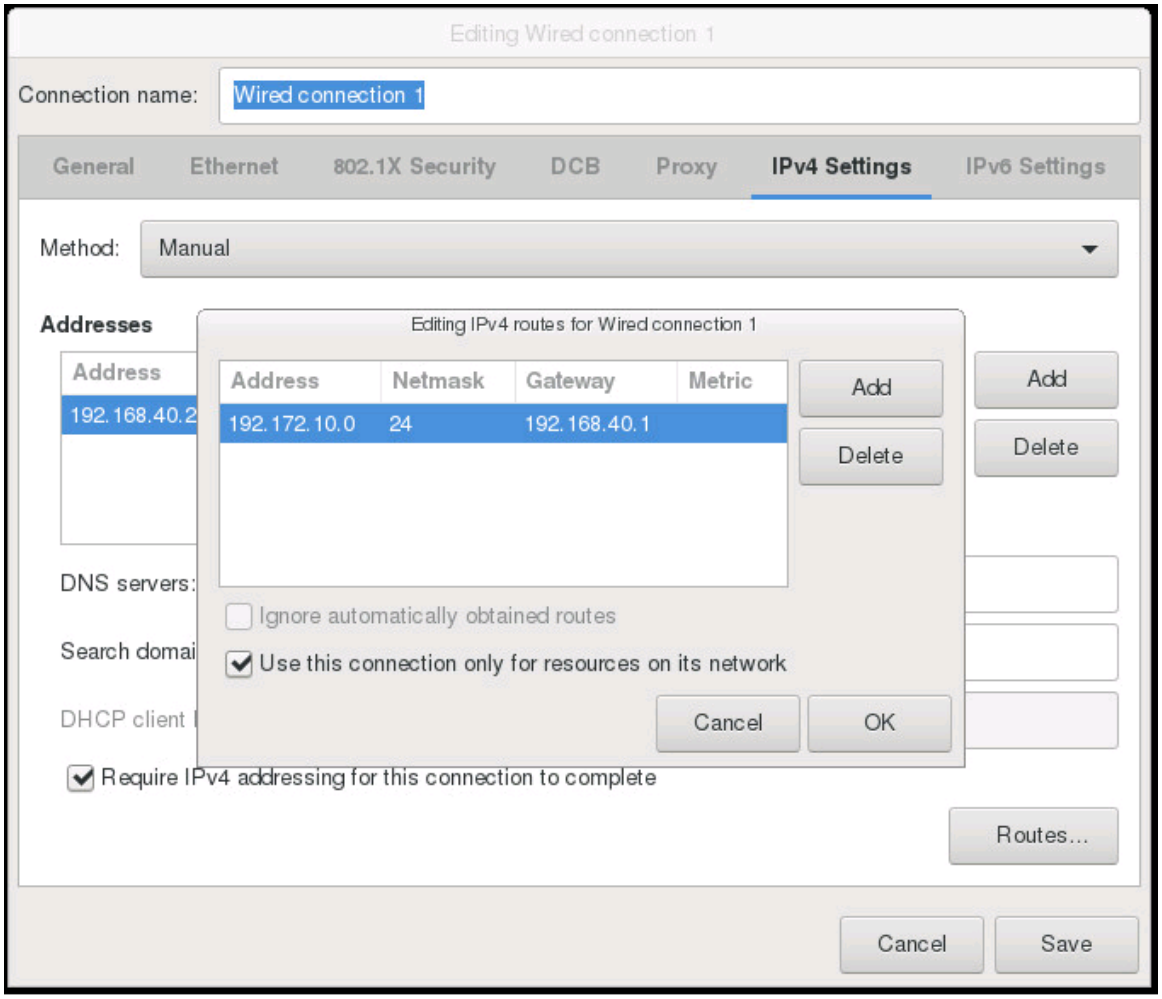
c) [ **DNS サーバー** ] および [ **検索ドメイン** ] ボックスにそれぞれ、検索対象の DNS サーバー IP およびドメインを入力します。

d) [ **この接続を完了するには IPV4 アドレス設定が必要です** ] チェック ボックスを選択し、[ **保存** ] をクリックします。

e) このネットワークをデフォルトのネットワーク ( ゲートウェイ ) として使用しない場合、[ **ルート** ] をクリックし、[ **この接続をそのネットワーク上のリソースに対してのみ使用する** ] チェック ボックスを選択します。

**メモ: 複数のネットワークをデフォルト ゲートウェイとして追加すると、ネットワークの問題が発生し、OMIVV の機能が影響を受ける可能性があります。**

f) 既知のゲートウェイを使用して外部ネットワークにアクセスする場合、同じページで [ **追加** ] をクリックし、ネットワーク IP アドレス、ネットマスク ( CIDR 形式 )、およびゲートウェイの詳細を追加します。




通常、デフォルト ゲートウェイとして設定したネットワークでは、ゲートウェイが到達性を提供できるため、手動でルートを設定する必要はありません。ただし、デフォルト ゲートウェイが設定されていないネットワーク ([ **この接続をそのネットワーク上のリソースに対してのみ使用する** ] チェック ボックスが選択されている場合 ) では、手動ルート設定が必要な場合があります。このネットワークが外部ネットワークに到達するようにデフォルト ゲートウェイが設定されていないため、手動ルーティング設定が必要です。

**メモ: ルーティング設定が正しくないと、ネットワーク インターフェイスの応答が突然停止することがあります。必ずルーティング エントリを適切に設定してください。**

g) [ **OK** ] をクリックします。

10. [ **保存** ] をクリックします。別の NIC を設定するには、タスク 6 ~ 10 を繰り返します。
11. [ **OpenManage Integration for VMware vCenter の仮想アプライアンスのセットアップ** ] ユーティリティーに移動し、[ **アプライアンス再起動** ] をクリックします。ネットワーク設定は、OMIVV アプライアンスの再起動後にのみ完了します。

    アプライアンスが正常に再起動されると、NIC は設定どおりに動作し始めます。NIC のステータスを表示するには、**読み取り専用**ユーザーとしてログインし、`ifconfig`、`ping`、および `route -n` コマンドを実行します。

# OMIVV アプライアンスのパスワードの変更

vSphere Client の OMIVV 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。

1. OMIVV Web コンソールを開きます。
2. [ **OpenManage Integration for VMware vCenter の仮想アプライアンスのセットアップ** ] ユーティリティーで、[ **管理者パスワードの変更** ] をクリックします。
3. [ **現在のパスワード** ] テキスト ボックスに現在の管理パスワードを入力します。

   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. [ **新規パスワード** ] テキスト ボックスに新しいパスワードを入力します。
5. [ **新規パスワードの確認** ] テキスト ボックスに新しいパスワードを再度入力します。

6. [ **管理パスワードの変更** ] をクリックします。

# ネットワーク タイム プロトコル ( NTP ) の構成およびローカル タイム ゾーンの設定

1. OMIVV Web コンソールを開きます。
2. [ **OpenManage Integration for VMware vCenter の仮想アプライアンスのセットアップ** ] ユーティリティーで、[ **日付と時刻のプロパティ** ] をクリックします。

   NTP の詳細を管理コンソールに入力したことを確認します。詳細については、次を参照してください：ネットワーク タイム プロトコル ( NTP ) サーバーのセットアップ
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. 別の NTP サーバーの IP/ホスト名を追加するには ( 必要な場合 )、[ **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。

## ネットワーク タイム プロトコル ( NTP ) サーバーのセットアップ

NTP を用いて、OMIVV アプライアンスのクロックを NTP サーバーのものに同期させることができます。

1. 管理コンソールの [ **アプライアンス管理** ] ページにある [ **NTP 設定** ] 領域で、[ **編集** ] をクリックします。
2. **有効** を選択します。優先サーバーおよびセカンダリ NTP サーバーのホスト名または IP アドレスを入力し、[ **適用** ] をクリックします。
3. NTP の設定後、ターミナル コンソールを起動して [ **ネットワーク上で日付と時間の同期化** ] チェック ボックスを選択します。

**メモ: OMIVV のクロックが NTP サーバーと同期するまでには数分かかります。**

**メモ: OMIVV 管理ポータルで情報のロードに時間がかかる場合、NTP の設定が正しいこと、および NTP サーバーに OMIVV 仮想マシンからアクセスできることを確認してください。**

# OMIVV アプライアンスのホスト名の変更

1. [ **OpenManage Integration for VMware vCenter の仮想アプライアンスのセットアップ** ] ユーティリティーで、[ **ホスト名の変更** ] をクリックします。

   **メモ: OMIVV アプライアンスで登録された vCenter がある場合は、すべての vCenter インスタンスを登録解除し、再登録します。**
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 ホスト名がアップデートされ、メイン メニュー ページが表示されます。
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: iDRAC および Dell EMC Repository Manager ( DRM ) のプロビジョニング サーバーなど、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、必ず手動で更新するようにしてください。**

# OMIVV アプライアンスの再起動

1. OMIVV Web コンソールを開きます。
2. [ **OpenManage Integration for VMware vCenter の仮想アプライアンスのセットアップ** ] ユーティリティーで、[ **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。

# OMIVV アプライアンスの工場出荷時設定へのリセット

1. OMIVV Web コンソールを開きます。

2. [ **OpenManage Integration for VMware vCenter の仮想アプライアンスのセットアップ** ] ユーティリティーで、[ **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。
   [ **はい** ] をクリックすると、OMIVV アプライアンスが工場出荷時のデフォルト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削除されます。
   工場出荷状態へのリセットが完了したら、vCenter を OMIVV アプライアンスに再度登録します。

**メモ: OMIVV アプライアンスが工場出荷時のデフォルト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。これらの設定はリセットされません。**

# 登録済み vCenter バージョンのアップグレード後の OMIVV の再設定

登録済みの vCenter をアップグレードした後、次のタスクを実行します。

- 非管理者ユーザーの場合：
  1. 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。
     たとえば、vCenter 6.0 から vCenter 6.5 にアップグレードする場合は、追加の権限を割り当てます。
  2. 登録済み OMIVV アプライアンスを再起動します。
  3. 登録された vCenter が 7.0 以降の場合は、OMIVV 管理コンソールで vSphere Lifecycle Manager を有効にします。
- 管理者ユーザーの場合：
  1. 登録済み OMIVV アプライアンスを再起動します。
  2. 登録された vCenter が 7.0 以降の場合は、OMIVV 管理コンソールで vSphere Lifecycle Manager を有効にします。

# バックアップおよび復元の管理

管理コンソールを使用して、関連タスクのバックアップおよび復元を実行できます。

- 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
- 即時バックアップの実行
- バックアップからのデータベースの復元
- バックアップおよび復元設定のリセット

OMIVV 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。

1. `https:\\<`**アプライアンス** `IP|`**ホスト名**`>`に移動します。
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の場所 ( NFS および CIFS ) にバックアップして、後でそれに基づく復元を可能にします。このバックアップには、プロファイル、設定、およびホスト情報が含まれます。データの喪失に備えるため、自動バックアップをスケジュールすることを推奨します。

**メモ: NTP の設定は保存および復元されません。**

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、以下を行います。
   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。

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

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。

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 ジョブ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. **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場所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、[ **バックアップ設定の場所と暗号化パスワードを使用する** ] 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!、@、#、$、%、*などの特殊文字を使用できます。パスワードの作成には文字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

以前のバージョンから OMIVV を復元した場合：

- 第 11 世代サーバーはサポートされません。復元後は 12G 以降のサーバーのみが保持されます。
- ハードウェア プロファイルと導入テンプレートはサポートされません。導入は、システム プロファイルを使用して行うことをお勧めします。
- 11G サーバーでスケジュールされた導入タスクと、ハードウェア プロファイル ベースの導入テンプレートを使用した導入タスクはキャンセルされます。
- すべての 11G サーバーが認証情報プロファイルから削除され、使用されていたライセンスは放棄されます。
- リポジトリー プロファイルは 64 ビット バンドルのみを使用します。

**メモ: 4.x から 5.x へのバックアップと復元を実行すると、OMIVV は 5.x の 32 ビット ファームウェア バンドルをサポートしていないため、クラスター プロファイル名に対して警告記号が表示されます。クラスター プロファイルの最新の変更を使用するには、クラスター プロファイルを編集します。**

- 11G サーバーでスケジュールされたファームウェア アップデート ジョブはキャンセルされます。

復元の操作では、復元作業の完了後に OMIVV アプライアンスが再起動します。

1. [ **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。
2. [ **今すぐ復元** ] ダイアログ ボックスで、[ **ファイルの場所** ] にパスを入力し、バックアップの.gz ファイルを CIFS/NFS 形式で入力します。
3. 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!、@、#、$、%、*などの特殊文字を使用できます。
4. 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。インストールを確認するには、「インストールの確認」を参照してください。

復元が完了したら、管理者ポータルにログインする前に、ブラウザーを閉じてブラウザーのキャッシュをクリアします。

# バックアップおよび復元設定のリセット

設定のリセット機能は、設定を未設定の状態にリセットします。

1. [ **バックアップおよび復元設定** ] ページで、[ **設定のリセット** ] をクリックします。
2. [ **設定のリセット** ] ダイアログ ボックスで、[ **適用** ] をクリックします。
   アプライアンスが再起動します。

# OMIVV アプライアンスとリポジトリーの場所のアップデート

- すべてのデータが保護されていることを確認するには、OMIVV アプライアンスをアップデートする前に OMIVV 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。
- OMIVV アプライアンスで、利用可能なアップグレード メカニズムを表示し、RPM のアップグレードを実行するためには、インターネット接続が必要です。OMIVV アプライアンスがインターネットに接続されていることを確認します。プロキシ ネットワークが必要な場合は、環境ネットワーク設定に基づいてプロキシ設定を有効にして、プロキシのデータを入力します。ユーザーズ ガイドの「HTTP プロキシの設定」の項「」を参照してください。
- **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。
- 必ず、登録された vCenter Server へのすべての vSphere Client ( HTML-5 ) セッションからログ アウトしてください。
- 登録された vCenter Server 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 コントローラー ( 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。そうしない場合は、OMIVV インスタンスで一貫性のない情報が表示されることがあります。

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 OMIVV バージョンを確認します。

   使用可能な OMIVV アプライアンスのバージョンについては、該当する RPM および OVF の OMIVV アプライアンス アップグレード メカニズムが、チェック マーク ( ✔ ) とともに表示されます。

   アップグレード メカニズム タスクのいずれかを実行可能なアップグレード メカニズム オプションを次に示します。

| オプション | 説明 |
|---|---|
| 1 | チェック マークが RPM に表示された場合、既存のバージョンから使用可能な最新バージョンへ RPM によるアップグレードを実行できます。「RPM を使用した OMIVV アプライアンスのアップグレード」を参照してください。 |
| 2 | チェック マークが OVF に表示された場合、既存のバージョンから OMIVV データベースのバックアップを作成し、使用可能な最新バージョンのアプライアンスに復元します。「バックアップと復元を使用した OMIVV アプライアンスのアップグレード」を参照してください。 |
| 3 | チェック マークが RPM と OVF の両方に表示された場合、上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 によるアップグレードをお勧めします。 |

2. OMIVV 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。

# RPM を使用した OMIVV アプライアンスのアップグレード

アップグレード後のアプライアンスは、現在のバージョンよりも新しいバージョンになることを確認します。

1. [ **アプライアンス管理** ] ページで、ネットワーク設定に基づいてプロキシを有効にし、必要に応じてプロキシ設定データを入力します。「」を参照してください。

   使用可能な OMIVV アプライアンスのバージョンについては、該当する RPM および OVF の OMIVV アプライアンス アップグレード メカニズムが、チェック マーク ( ✔ ) とともに表示されます。
2. OMIVV のプラグインを既存のバージョンから利用可能な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。

- [ **リポジトリー パスのアップデート** ] で使用できる RPM を使用してアップグレードするには、[ **リポジトリー パスのアップデート** ] が次のパスに設定されていることを確認してください：https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/

  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 https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ にアップデートして [ **適用** ] をクリックします。

3. 利用可能な OMIVV アプライアンスのバージョンと、現在の OMIVV アプライアンスのバージョンを比較します。
4. OMIVV 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アウトされます。
6. Web ブラウザを閉じます。

   アプライアンスで RPM のアップグレードが完了したら、Dell 管理ポータルにログインする前に、必ずブラウザーのキャッシュをクリアします。

**メモ: アップグレード処理中、アプライアンスは 1 度か 2 度再起動します。**

**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。ブラウザーを開いて、「*https:\\<アプライアンス IP/ホスト名>*」リンクを入力し、[ アプライアンスのアップデート ] 領域に移動します。使用可能な OMIVV アプライアンスと現在の OMIVV 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。クラスタで Proactive HA を有効にしている場合は、OMIVV は、それらのクラスタの Dell Inc プロバイダを登録解除し、アップグレード後に Dell Inc プロバイダを再度登録します。Dell EMC ホストの正常性アップデートは、アップグレードが完了するまで使用できません。**

# バックアップと復元を使用した OMIVV アプライアンスのアップグレード

バックアップを実行した後およびバックアップ ファイルを復元する前に、OMIVV で管理されるクラスターまたはホストに対する変更や削除は行わないことをお勧めします。OMIVV によって管理されているクラスターまたはホストが変更または削除された場合は、復元後にそれらのクラスターおよびホストに関連付けられているプロファイル ( ホスト認証情報プロファイル、クラスター プロファイルなど ) を再設定します。

vCenter から OMIVV のプラグインの登録を解除しないでください。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 に登録されている Proactive HA クラスターの Dell Health Update Provider が削除されます。

OMIVV アプライアンスを旧バージョンから現在のバージョンにアップデートするには、次の手順を実行します。

1. 以前のリリースのデータをバックアップします。
2. vCenter から、旧 OMIVV アプライアンスの電源を切ります。
3. 新しい OpenManage Integration アプライアンスの OVF を展開します。
4. OpenManage Integration の新アプライアンスの電源を入れます。
5. 新しいアプライアンスのネットワークとタイム ゾーンを設定します。

   **メモ: 以前の OMIVV アプライアンスの識別情報 ( IP または FQDN ) は、新しい OMIVV アプライアンス用に保存しておくことを推奨します。**

   **メモ: 新しいアプライアンスの IP アドレスが古いアプライアンスの IP アドレスと異なる場合、Proactive HA 機能が正常に動作しない可能性があります。このようなシナリオでは、Dell EMC ホストが存在するクラスターごとに Proactive HA を無効にして有効にします。**
6. OMIVV アプライアンスにはデフォルト証明書が付属しています。お使いのアプライアンスでカスタム証明書が必要な場合、同じ証明書をアップデートします。「証明書署名要求 ( CSR ) の生成」および「HTTPS 証明書のアップロード」を参照してください。そうでない場合は、このステップをスキップしてください。
7. 新しい OMIVV アプライアンスにデータベースを復元します。「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。
8. アプライアンスを検証します。詳細については、「インストールの確認」を参照してください。『』の「」トピック
9. アップグレード後は、OMIVV プラグインで管理される全ホストでインベントリーを再度実行することを推奨します。

   アプライアンスの復元後、イベントおよびアラーム設定は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。

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、スケジュールされたジョブがすべて実行され続けます。

**メモ: 新しい OMIVV バージョン Y の識別情報（IP または FQDN）が OMIVV バージョン X から変更されている場合、新しいアプライアンスをポイントするように SNMP トラップのトラップ送信先を設定します。識別情報の変更を修正するには、当該ホスト上でインベントリーを実行します。ホスト上でインベントリーを実行中に、SNMP トラップが新しい IP を指定しない場合、そのホストは非準拠としてリストされます。ホスト対応問題の解決法については、『ユーザーズ ガイド』の「管理対応性」の項を参照してください。**

旧バージョンの OMIVV からアップデート バージョンへのバックアップ/復元を実行した後に、200000 メッセージが表示されるか、Dell EMC のロゴが表示されないか、または OMIVV UI が vCenter UI で反応しないという場合は、次の手順を実行します。

- vCenter Server で、vSphere Web Client（HTML-5）と vSphere Client（FLEX）の両方に対する vSphere Client サービスを再開します。
- 問題が解決しない場合は、
  - VMware vCenter Server アプライアンスの場合は、`/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity` に移動します。Windows vCenter の場合は、vCenter アプライアンスの `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` フォルダーに移動して、旧バージョンに対応する古いデータが存在することを確認します。

    古いデータの例としては、com.dell.plugin.OpenManage—com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX があります。
  - OMIVV の旧バージョンに対応するフォルダーを手動で削除し、vSphere Client（HTML-5）と Web Client（FLEX）の両方で vSphere Client サービスを再起動します。

# OpenManage Integration for VMware vCenter の登録解除

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

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 の可用性 ]** の順に選択し、クラスターの [ **Proactive HA の障害と対応** ] 画面にアクセスして、[ **編集** ] をクリックします。[ **Proactive HA の障害と対応** ] 画面で Proactive HA を無効にするには、**Dell Inc** プロバイダーのチェック ボックスをオフにします。

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。

1. https://<*アプライアンス IP/ホスト名*/>に移動します。
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: OMIVV は複数の vCenter に関連付けることができるため、必ず正しい vCenter を選択してください。**
3. 選択した vCenter サーバー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: OMIVV の登録解除後、vSphere Client（HTML-5）からログアウトしてログインします。[ OMIVV ] アイコンがまだ表示されている場合は、vSphere Client（HTML-5）と Web クライアント（FLEX）の両方のクライアント サービスを再起動します。**

# 登録解除後の OMIVV の回復

## 登録解除した OMIVV の旧バージョンのリカバリー

以前のバージョンのデータベースに対するバックアップを取得した後で OMIVV プラグインの登録を解除した場合は、移行に進む前に次のステップを実行してください。

**メモ: プラグインの登録解除をすると、PHA クラスターの Dell 正常性アップデート プロバイダーおよび登録済みアラームへのカスタマイズはすべて削除されます。次の手順では、カスタマイズは復元されません。デフォルトの状態でアラームが再登録されます。**

**メモ: 以前の OMIVV アプライアンスの識別情報 ( IP または FQDN ) は、新しい OMIVV アプライアンス用に保存しておくことを推奨します。**

**メモ: 新しいアプライアンスの IP アドレスが古いアプライアンスの IP アドレスと異なる場合、Proactive HA 機能が正常に動作しない可能性があります。このようなシナリオでは、Dell ホストが存在するクラスターごとに PHA を無効にして有効にします。**

バックアップと復元を使用した OMIVV アプライアンスのアップグレードに記載されている 3~9 のタスクを実行します。

# 登録解除と再登録の管理

登録解除を実行する前に、バックアップを取っておくことをお勧めします。

**メモ: プラグインの登録解除をすると、PHA クラスターの Dell 正常性アップデート プロバイダーおよび登録済みアラームへのカスタマイズはすべて削除されます。次の手順では、カスタマイズは復元されません。デフォルトの状態でアラームが再登録されます。**

1. OMIVV のバックアップを取ります。
2. OMIVV から vCenter の登録を解除します。
3. 予定の設定変更を実行します。たとえば、ホスト名の変更、新しい設定の変更などです。
4. OMIVV アプライアンスを再起動します。
5. バックアップ ファイルを復元します。詳細については、次を参照してください : バックアップと復元を使用した OMIVV アプライアンスのアップグレード

# 3

# 初期設定ウィザードを使用した OMIVV アプライアンスの設定

OMIVV の基本インストールと vCenter の登録の完了後、vCenter で OMIVV を最初に起動すると、自動的に初期設定ウィザードが表示されます。

初期設定ウィザードの起動は、次の手順でも行うことができます。

- **[ 設定 ]** > **[ 初期設定ウィザード ]** > **[ 初期設定ウィザードの開始 ]**
- **[ ダッシュボード ]** > **[ クイック リファレンス ]** > **[ 初期設定ウィザードの開始 ]**

**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。**

**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、ブラウザーのキャッシュをクリアし、vSphere Client ( HTML-5 ) から一旦ログアウトして、ログインし直します。**

初期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。

- vCenter の選択
- ホスト認証情報プロファイルの作成詳細については、次を参照してください：ホスト認証情報プロファイルの作成
- イベントとアラームを設定します。詳細については、次を参照してください：イベントとアラームの設定
- インベントリジョブをスケジュールします。詳細については、次を参照してください：インベントリー ジョブのスケジュール
- 保証取得ジョブをスケジュールします。詳細については、次を参照してください：保証取得ジョブのスケジュール

**トピック：**

- 初期設定
- [ 設定 ] ページでの設定タスク

# 初期設定

OMIVV の基本インストールと vCenter の登録の完了後、vCenter で OMIVV を最初に起動すると、自動的に初期設定ウィザードが表示されます。

その後で初期設定ウィザードを起動させたい場合は、次の場所にアクセスしてください。

- **[ 設定 ]** > **[ 初期設定ウィザード ]** > **[ 初期設定ウィザードの開始 ]**
- **[ ダッシュボード ]** > **[ クイック リファレンス ]** > **[ 初期設定ウィザードの開始 ]**

1. [ **ようこそ** ] ページに表示された手順を確認し、[ **開始** ] をクリックします。
2. [ **vCenter の選択** ] ページにある [ **vCenter** ] ドロップダウン メニューで、特定の vCenter または [ **すべての登録済み vCentervCenter** ] を選択し、[ **次へ** ] をクリックします。

   **メモ: 同じ OMIVV アプライアンスに登録された同じ PSC に属する vCenter Server が複数ある場合、単一 vCenter Server の設定を選択すると、それぞれの vCenter の設定を始める前に手順 2 を繰り返す必要があります。**
3. [ **ホスト認証情報プロファイルの作成** ] ページで、[ **ホスト認証情報プロファイルの作成** ] をクリックします。
   ホスト認証情報プロファイル作成の詳細については、「ホスト認証情報プロファイルの作成」を参照してください。

   ホストがホスト認証情報プロファイルに追加されると、ホストの iDRAC の SNMP トラップ送信先として、OMIVV の IP アドレスが自動的に設定されます。OMIVV は WBEM サービスを有効にし、その後 ESXi 6.5 以降を実行しているホストの iDRAC IP を取得すると、これを無効化します。

   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。特定のホストに対する SNMP トラップ送信先の設定が失敗するか、特定のホストに対する WBEM サービスが失敗する場合、それらのホストは非対応としてリストされます。非対応とされた項目の表示と修正については、ユーザーズ ガイドの「管理対応性」の項を参照してください。
4. [ **追加設定** ] ページで、次の手順を実行します。
   a) インベントリジョブをスケジュールします。インベントリー ジョブのスケジュールの詳細については、「インベントリー ジョブのスケジュール」を参照してください。

b) 保証取得ジョブをスケジュールします。保証取得ジョブのスケジュールの詳細については、「保証取得ジョブのスケジュール」を参照してください。

インベントリー ジョブのスケジュールを変更する場合は、**[ 設定 ]** > **[ vCenter 設定 ]** > **[ データ取得スケジュール ]** > **[ インベントリーの取得 ]** または **[ ジョブ ]** > **[ インベントリー ]** > **[ ホストのインベントリー ]** の順に移動します。

保証取得ジョブのスケジュールを変更する場合は、**[ 設定 ]** > **[ vCenter 設定 ]** > **[ データ取得スケジュール ]** > **[ 保証の取得 ]** または **[ ジョブ ]** > **[ 保証 ]** の順に移動します。

c) イベントとアラームを設定します。イベントとアラームの設定の詳細については、「イベントとアラームの設定」を参照してください。

d) 個々の設定を適用するには、それぞれの [ **適用** ] ボタンを個別にクリックし、[ **次へ** ] をクリックします。

追加設定は、すべて有効にしておくことを強くお勧めします。適用されていない追加設定がある場合、すべての追加設定が必須であることを示すメッセージが表示されます。

5. [ **次の手順** ] ページに表示された指示を確認し、[ **終了** ] をクリックします。

ホストや関連クラスターでの設定変更の発生を詳細に監視できるため、OMIVV ホストを設定ベースラインに関連付けることをお勧めします。OMIVV によるホスト群の管理が正常に行われると、任意のクラスターに対して設定ベースラインの作成が可能になります。設定ベースラインを作成するには、次の手順を実行します。

- ファームウェアおよびドライバーのリポジトリー プロファイルの作成 — ベースライン化されたファームウェアとドライバーのバージョンの定義に役立ちます。
- システム プロファイルの作成 — ベースライン化されたハードウェア設定のホスト用の定義に役立ちます。
- クラスター プロファイルの作成 — ベースラインを正常に作成するために、クラスターの選択と、ファームウェア、ドライバー、ハードウェア設定の関連付けを行います。
- iDRAC IPv4 が無効になっている PowerEdge MX シャーシのホストの管理は、シャーシ認証情報プロファイルを使用して行う必要があります。

# ホスト認証情報プロファイルの作成

ホスト認証情報プロファイル作成用のライセンスの制限よりも多いホストを追加した場合、ホスト認証情報プロファイルを作成することはできません。

ホスト認証情報プロファイルで Active Directory ( AD ) 認証情報を使用する前に、次のことを確認してください。

- ユーザー アカウントが AD に存在している。
- iDRAC またはホストで AD ベースの認証が設定されている。

1. OMIVV ホーム ページで、**[ 対応性と導入 ]** > **[ ホスト認証情報プロファイル ]** の順にクリックします。
2. [ **ホスト認証情報プロファイル** ] ページで、[ **新規プロファイルを作成** ] をクリックします。
3. ウィザードの [ **ホスト認証情報プロファイル** ] ページで手順を読み、[ **開始** ] をクリックします。
4. [ **名前と認証情報** ] ページで、次の手順を行います。
   a) プロファイル名および説明を入力します。説明のフィールドはオプションです。
   b) [ **vCenter 名** ] リストで、ホスト認証情報プロファイルを作成する vCenter のインスタンスを選択します。
   c) [ **iDRAC 認証情報** ] 領域で、iDRAC ローカル認証情報または AD 認証情報を入力します。
      - iDRAC のローカル認証情報を入力するには、次のタスクを実行します。
        - [ **ユーザー名** ] ボックスにユーザー名を入力します。名前は 16 文字以内です。ユーザー名の定義の詳細については、**https://www.dell.com/support** にある『*iDRAC ユーザーズ ガイド*』を参照してください。
        - パスワードを入力します。ユーザー名とパスワードでの使用が推奨される文字の詳細については、**https://www.dell.com/support** にある『*iDRAC ユーザーズ ガイド*』を参照してください。
        - 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** ] チェック ボックスを選択します。
      - AD ですでに設定および有効化されている iDRAC の認証情報を入力するには、[ **Active Directory を使用する** ] チェック ボックスを選択します。

        **メモ: iDRAC アカウントでファームウェアのアップデートおよびオペレーティング システム ( OS ) の導入を行うには、管理者権限が必要です。**

        - [ **Active Directory ユーザー名** ] ボックスにユーザー名を入力します。ユーザー名は、`domain\username` または `username@domain` のいずれかの形式で入力してください。名前は 256 文字以内です。ユーザー名の制限については、*Microsoft Active Directory のマニュアル*を参照してください。
        - パスワードを入力します。

        AD の認証情報は、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。

- 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** ] チェック ボックスを選択します。

d) [ **ホスト ルート** ] 領域で、ホストのローカル認証情報または AD 認証情報を入力します。

- ESXi ホストのローカル認証情報を入力するには、次のタスクを実行します。
  - デフォルトのユーザー名は **root** です。これは編集できません。
  - 有効なパスワードを入力してください。vCenter 6.7 以降では、有効なパスワード入力は必須ではありません。
  - 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、[ **証明書チェックの有効化** ] チェック ボックスを選択します。
- AD ですでに設定および有効化されているホストの認証情報を入力するには、[ **Active Directory を使用する** ] チェック ボックスを選択します。
  - [ **Active Directory ユーザー名** ] ボックスにユーザー名を入力します。ユーザー名は、`domain\username` または `username@domain` のいずれかの形式で入力してください。名前は 256 文字以内です。ユーザー名の制限については、*Microsoft Active Directory のマニュアル*を参照してください。
  - パスワードを入力します。
  - 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、[ **証明書チェックの有効化** ] チェック ボックスを選択します。

**メモ: ESXi 6.5 U2 以降のバージョンを実行しているホストでは、誤ったホスト認証情報を入力した場合でも、OMIVV は iDRAC の情報を取得できます。**

5. [ **次へ** ] をクリックします。
   [ **ホストの選択** ] ページが表示されます。
6. [ **ホストの選択** ] ページで、ツリー ビューを展開してホストを選択し、[ **OK** ] をクリックします。
   - [ **ホストの追加** ] をクリックして、[ **関連ホスト** ] ページでホストを追加または削除します。

     **メモ: iDRAC IPv4 が無効になっている PowerEdge MX サーバーをホスト認証情報プロファイルに追加しないでください。これらのサーバーの管理は、シャーシ認証情報プロファイルを使用して行います。**

   選択したホストが [ **関連ホスト** ] ページに表示されます。
7. 接続をテストするには、1 台または複数のホストを選択し、次に [ **テストを開始** ] をクリックします。設定されているすべてのホストについて、接続をテストすることをお勧めします。
   テスト接続中、OMIVV は WBEM サービスを有効にし、その後 ESXi 6.5 以降を実行しているホストの iDRAC IP を取得すると、これを無効化します。

   **メモ: 有効な認証情報を入力している場合でも、ホストに対する接続のテスト操作が失敗し、無効な認証情報が入力されていることを示すメッセージが表示される場合があります。この問題は、ESXi がアクセスをブロックしている場合に発生します。誤った認証情報を使用して ESXi に複数回接続しようとすると、ESXi へのアクセスが 15 分間ブロックされます。15 分待ってから、もう一度操作してください。**

   - テスト接続プロセスを中止するには、[ **テストの中止** ] をクリックします。

   テスト接続の結果は、[ **テスト結果** ] セクションで確認できます。
8. [ **終了** ] をクリックします。

# インベントリー ジョブのスケジュール

OMIVV で最新のインベントリー データを表示するには、ホストまたはシャーシのインベントリー情報が最新であることを確認するために、インベントリー ジョブを定期的に実行するようスケジュールする必要があります。インベントリー ジョブは週単位で実行することをお勧めします。

**メモ: シャーシは OMIVV コンテキストで管理されます。シャーシ管理に vCenter のコンテキストがありません。スケジュールされたホスト インベントリーが完了すると、OMIVV を使用して管理されているすべてのシャーシのシャーシ インベントリーがトリガーされます。**

**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。**

1. OMIVV ホーム ページで、**[ 設定 ]** > **[ vCenter 設定 ]** > **[ データ取得スケジュール ]** > **[ インベントリーの取得 ]** の順にクリックします。
2. [ **インベントリー データ取得の有効化 ( 推奨 )** ] チェック ボックスを選択します。

複数の vCenter サーバーがある PSC 環境で、個々の vCenter のスケジュールが異なる場合に、[ **すべての登録済み vCenter** ] オプションを選択してインベントリー スケジュールをアップデートすると、インベントリー スケジュール設定ページにデフォルトのスケジュールが表示されます。

3. インベントリー データの取得日時を選択し、[ **適用** ] をクリックします。

**メモ: 複数の vCenter サーバーがある PSC 環境で、[ すべての登録済み vCenter ] のインベントリー スケジュールをアップデートすると、アップデートによって個々の vCenter インベントリー スケジュール設定が上書きされます。**

# 保証取得ジョブのスケジュール

1. ホストおよびシャーシでインベントリーが正常に実行されていることを確認します。
2. OMIVV の保証機能を使用するには、インターネット接続が必要です。お使いの環境でインターネットに接続するためにプロキシーが必要な場合は、管理者ポータルでプロキシー設定を構成してください。

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。サービス タグのみが送信され、デル オンラインでは保存されません。

複数の vCenter サーバーを持つ PSC 環境では、いずれかの vCenter で保証が実行されると、すべての vCenter でシャーシの保証が自動的に実行されます。ただし、シャーシ認証情報プロファイルに保証が追加されていない場合、保証は自動的には実行されません。

**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。**

1. OMIVV ホーム ページで、**[ 設定 ]** > **[ vCenter 設定 ]** > **[ データ取得スケジュール ]** > **[ 保証の取得 ]** の順にクリックします。
2. [ **保証データの取得を有効にする ( 推奨 )** ] チェック ボックスを選択します。
   複数の vCenter サーバーがある PSC 環境で、個々の vCenter のスケジュールが異なる場合に、[ **すべての登録済み vCenter** ] オプションを選択して保証スケジュールをアップデートすると、保証スケジュール設定ページにデフォルトのスケジュールが表示されます。
3. 保証データの取得日時を選択し、[ **適用** ] をクリックします。

**メモ: 複数の vCenter サーバーがある PSC 環境で、[ すべての登録済み vCenter ] の保証スケジュールをアップデートすると、アップデートによって個々の vCenter 保証スケジュール設定が上書きされます。**

# イベントとアラームの設定

サーバーからイベントを受信するには、SNMP トラップ送信先を iDRAC に設定します。OMIVV は、SNMP v1 および v2 アラートをサポートしています。

1. OMIVV ホーム ページで、**[ 設定 ]** > **[ vCenter 設定 ]** > **[ イベントとアラーム ]** をクリックします。
2. すべてのホストとそのシャーシのアラームを有効にするには、[ **すべてのホストとそのシャーシのアラームを有効にする** ] をクリックします。
   [ **Dell アラーム警告の有効化** ] ページには、Dell EMC アラームの有効化後に影響を受ける可能性のあるクラスターおよび非クラスター ホストが表示されます。

   **メモ: アラームが有効化されている Dell EMC ホストは、メンテナンス モードに入ることによって特定重要イベントの一部に対応します。必要に応じてアラームを変更できます。**

   **メモ: vCenter 6.7 U1 および 6.7 U2 では、編集オプションは失敗します。アラーム定義を編集する場合は、Web クライアント ( FLEX ) を使用することをお勧めします。**

   **メモ: BMC トラップにはメッセージ ID がないため、アラートにはこのような OMIVV の詳細情報は含まれません。**
3. 変更を受け入れるには、[ **続行** ] をクリックします。
   すべてのホストとそのシャーシについて、アラームが有効になります。
4. 以下のイベント掲載レベルのいずれかを選択します。
   - [ **イベントは掲載しない** ]: イベントやアラートを関連 vCenter に転送しません。
   - [ **すべてのイベントを掲載する** ]: 情報イベントを含むすべてのイベントと、管理対象ホストやシャーシから受信したイベントを関連 vCenter に掲載します。イベント掲載レベルとして [ すべてのイベントを掲載する ] オプションを選択することをお勧めします。
   - [ **重要および警告イベントのみを掲載する** ]: 重要および警告レベルのイベントのみを関連 vCenter に掲載します。

- [ **仮想化関連のイベントのみを掲載する** ]: ホストから受信した仮想化関連イベントを関連 vCenter に掲載します。仮想化関連のイベントは、VM を実行するホストにとって最も重要なイベントです。

5. 変更を保存するには、[ **適用** ] をクリックします。

   すべてのホストおよびそのシャーシで、デフォルトの vCenter アラーム設定を復元するには、[ **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。

   [ **アラームの復元** ] オプションは、製品のアンインストールと再インストールを行わずにデフォルトのアラーム設定を行うことができる便利な機能です。インストール以降に Dell EMC アラーム設定が変更されていた場合、[ **アラームの復元** ] オプションで元に戻すことができます。

   **メモ: アプライアンスの復元後、イベントおよびアラーム設定は有効化されていません。設定 タブから、イベントとアラーム 設定を再度有効化することができます。**

# [ 設定 ] ページでの設定タスク

[ **設定** ] ページでは、次のタスクを実行できます。

- 保証期限通知の設定
- アプライアンスの最新バージョン通知の設定
- 展開用の資格情報の設定
- 正常性のオーバーライド重大度のアップデート通知
- 初期設定

## 保証期限通知の設定

いずれかのホストの保証の有効期限が近づいている場合に通知を受けるには、保証期限通知を有効にします。

1. OMIVV ホーム ページで、**[ 設定 ]** > **[ 通知 ]** > **[ 保証期限通知 ]** の順にクリックします。
2. [ **ホストの保証期限通知を有効にする** ] を選択します。
3. 保証期限の何日前に通知するか選択します。
4. [ **適用** ] をクリックします。

## アプライアンスの最新バージョン通知の設定

OMIVV の最新バージョンの可用性に関する通知を取得するには、[ **最新バージョンの通知を有効化 ( 推奨 )** ] チェック ボックスを選択します。この確認は、週単位で行うことをお勧めします。OMIVV の最新のアプライアンス バージョンの通知機能を使用するには、インターネット接続が必要です。お使いの環境でインターネットに接続するためにプロキシーが必要な場合は、管理者ポータルでプロキシー設定を構成してください。

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。

1. OMIVV ホームページで、**[ 設定 ]** > **[ アプライアンス設定 ]** > **[ 通知 ]** > **[ 最新バージョンの通知 ]** とクリックします。
2. [ **最新バージョンの通知を有効化 ( 推奨 )** ] チェック ボックスを選択します。
3. アプライアンスの最新バージョンの通知を受信するには、日付と時間を選択します。
4. [ **適用** ] をクリックします。

## 展開用の資格情報の設定

OMIVV はプロビジョニング サーバとして機能します。展開用の認証情報を使用することで、自動検出プロセスで OMIVV プラグインをプロビジョニング サーバーとして使用する iDRAC と通信することができます。オペレーティング システムの展開が完了するまで、自動検出されたベアメタル サーバーとの安全な通信は、展開用の認証情報を用いて iDRAC 認証情報をセットアップすることで行えます。

オペレーティング システム展開プロセスが正常に完了すると、OMIVV はホスト認証情報プロファイルの指定に従って iDRAC の認証情報を変更します。展開用の認証情報を変更した場合、自動検出を使用して新たに検出されたすべてのシステムは、それ以降、新しい iDRAC 認証情報でプロビジョニングされます。ただし、展開用の認証情報を変更する前に検出されたサーバー上の認証情報は、この変更の影響を受けません。

1. OMIVV ホーム ページで、**[ 設定 ]** > **[ アプライアンス設定 ]** > **[ 展開認証情報 ]** の順にクリックします。

2. ユーザー名とパスワードを入力します。デフォルトのユーザー名は「**root**」で、パスワードは「**calvin**」です。
   iDRAC 対応の文字と iDRAC ローカル資格情報のみを入力していることを確認します。
3. [ **適用** ] をクリックします。

# 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 EMC ホストおよびそのコンポーネントの Dell Proactive HA イベントの既存の重大度をオーバーライドするように設定することができます。

以下は、各 Proactive HA イベントに適用される重大度レベルです。

- **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、Proactive HA コンポーネントの重大度をカスタマイズできません。**

1. OpenManage Integration for VMware vCenter で、**[ 設定 ]** > **[ Proactive HA の重大度のオーバーライド ]** の順にクリックします。
   データ グリッドに、サポートされているすべての Proactive HA イベントが表示されます。データ グリッド列には、イベント ID、イベントの説明、コンポーネントのタイプ、デフォルトの重大度、およびホストとそのコンポーネントの重大度をカスタマイズするためのオーバーライド重大度などの列が含まれています。
2. ホストまたはその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 リストから該当するステータスを選択します。
   このポリシーは、OMIVV で登録されているすべての vCenter サーバのすべての Proactive HA ホストに適用されます。
3. 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 2 を繰り返します。
4. 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、[ **適用** ] をクリックします。
   b) 重大度設定の上書きをキャンセルするには、[ **キャンセル** ] をクリックします。
   重大度設定の上書きをデフォルトにリセットするには、[ **デフォルトにリセット** ] をクリックします。

# A

# Dell EMC サポートサイトからのドキュメントへのアクセス

次のリンクを使用して、必要なドキュメントにアクセスします。

- Dell EMC エンタープライズシステム管理のマニュアル — **www.dell.com/SoftwareSecurityManuals**
- Dell EMC OpenManage マニュアル — **www.dell.com/OpenManageManuals**
- Dell EMC リモートエンタープライズシステム管理のマニュアル — **www.dell.com/esmmanuals**
- iDRAC マニュアル — **www.dell.com/idracmanuals**
- Dell EMC OpenManage Connections エンタープライズ システム管理のマニュアル — **www.dell.com/OMConnectionsEnterpriseSystemsManagement**
- Dell EMC Serviceability Tools マニュアル — **www.dell.com/ServiceabilityTools**
- 1. **www.support.dell.com** にアクセスします。
  2. **すべての製品を参照** をクリックします。
  3. **すべての製品** ページで **ソフトウェア** をクリックして、次の中から必要なリンクをクリックします。
     - **統計**
     - **クライアントシステム管理**
     - **エンタープライズアプリケーション**
     - **エンタープライズシステム管理**
     - **公共機関向けソリューション**
     - **ユーティリティ**
     - **メインフレーム**
     - **保守ツール**
     - **仮想化ソリューション**
     - **オペレーティングシステム**
     - **サポート**
  4. マニュアルを表示するには、該当する製品をクリックして、該当する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。

# B

# 関連マニュアル

このガイド以外にも、**https://www.dell.com/support** で他のガイドにアクセスできます。[ **すべての製品を参照** ] をクリックし、**[ ソフトウェア ]** > **[ 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 5.1** ] をクリックすると、次の文書にアクセスできます。

- *OpenManage Integration for VMware vCenter バージョン 5.1 ユーザーズ ガイド*
- *OpenManage Integration for VMware vCenter バージョン 5.1 リリース ノート*
- *OpenManage Integration for VMware vCenter バージョン 5.1 互換性マトリックス*

**https://www.dell.com/support** 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。

# C

# デルへのお問い合わせ

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

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

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