# OpenManage Integration for VMware vCenter バージョン 4.2

Web Client の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。



2018 - 04

Rev. A00

# 目次

# 1

# はじめに

本ガイドでは、PowerEdge サーバで使用するための OpenManage Integration for VMware vCenter（OMIVV）のインストールおよび設定の手順をステップバイステップで説明します。OMIVV のインストール完了後の、インベントリ管理、監視とアラート、ファームウェアアップデート、保証管理など、管理上のあらゆる側面の詳細については、**Dell.com/support/manuals** 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 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 EMC 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 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 http://www.dell.com/support/licensing の 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、www.dell.com/support/incidentsonline/in/en/indhs1/email/order-support 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。

# ホストおよび vCenter サーバのライセンス要件

ホストと vCenter のライセンス要件は次のとおりです。

- OMIVV で管理する Dell EMC サーバの数量に対応した 1 つのライセンスを購入できます。ライセンスは、ホストを接続プロファイルに追加した後でなければ使用できません。ライセンスは特定の 1 つのサーバに関連付けられていません。
- OMIVV の 1 つのインスタンスで、vCenter サーバの最大 10 のインスタンスをサポートします。vCenter サーバの特定の数量に対応した個別のライセンスはありません。

# 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 Locker 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。**

# ライセンスのアップロード後のオプション

## 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、注文の確認に関する電子メールがデルから届き、Dell Digital Locker（ http://www.dell.com/support/licensing ）から新しいライセンスファイルをダウンロードできます。ライセンスは .xml 形式です。ライセンスが .zip 形式の場合、ライセンスの XML ファイルを抽出してからアップロードします。

## ライセンスのスタッキング

OMIVV のバージョン 2.1 から、標準のライセンスを複数スタックすることが可能となりました。これにより、サポートされるホストの数をアップロードされているライセンスのホストの合計まで増加できます。評価ライセンスはスタックできません。スタックではサポートされる vCenter サーバの数を増やすことができず、複数のアプライアンスを使用する必要があります。

ライセンスのスタック機能には、いくつかの制限事項があります。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。アップロードした後にライセンスの有効期限が切れた場合、既存のホストの機能は続行しますが、新バージョンの OMIVV 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、デル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表示されます。

## 接続プロファイルへのホストの追加

接続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第 11 世代以降の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。

# 参照用の重要なメモ

- 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。
- vCenter 6.5 以降では、OMIVV アプライアンスは Flash 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。
- DNS サーバ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 5.5 の DNS 要件
  - vSphere 6.0 の DNS 要件

  - vSphere 6.5 および Platform Services Controller アプライアンスの 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、「展開モードのシステム要件」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、iDRAC Express または Enterprise 搭載サーバに対して全機能が対応している複数世代の Dell EMC サーバを完全にサポートしています。プラットフォーム要件の詳細については、Dell.com/support/manuals にある『*OpenManage Integration for VMware vCenter Release Notes*』（OpenManage Integration for VMware vCenter リリースノート）を参照してください。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）
- 第 11 世代およびそれ以前のサーバに対する OMSA サポートおよび ESXi バージョンのサポート（導入および管理の両方）
- OMIVV のサポートされているメモリと容量

OMIVV は、iDRAC / CMC システム管理ネットワークおよび vCenter 管理ネットワークの両方にアクセスできるマザーボード / ネットワークドーターカード上の LAN が必要です。

# 展開モードのシステム要件

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 1. 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 |
|---|---|---|---|---|
| 小規模 | 最大 250 台 | 2 | 8 | 44 GB |
| 中規模 | 最高 500 台 | 4 | 16 | 44 GB |
| 大 | 最大 1000 台 | 8 | 32 | 44 GB |

**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。**

# BIOS、iDRAC、Lifecycle Controller のバージョン

本項では、OpenManage Integration for VMware vCenter の機能を有効にするために必要な BIOS、iDRAC、および Lifecycle Controller のバージョンを示します。

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 2. PowerEdge 第 11 世代サーバ向けの BIOS**

| サーバー | 最小バージョン |
|---|---|
| PowerEdge R210 | 1.8.2 以降 |
| PowerEdge R210II | 1.3.1 以降 |
| PowerEdge R310 | 1.8.2 以降 |
| PowerEdge R410 | 1.9.0 以降 |
| PowerEdge R415 | 1.8.6 以降 |
| PowerEdge R510 | 1.9.0 以降 |
| PowerEdge R515 | 1.8.6 以降 |
| PowerEdge R610 | 6.1.0 以降 |
| PowerEdge R710 | 6.1.0 以降 |
| PowerEdge R710 | 6.1.0 以降 |
| PowerEdge R715 | 3.0.0 以降 |
| PowerEdge R810 | 2.5.0 以降 |
| PowerEdge R815 | 3.0.0 以降 |
| PowerEdge R910 | 2.5.0 以降 |
| PowerEdge M610 | 6.1.0 以降 |
| PowerEdge M610x | 6.1.0 以降 |
| PowerEdge M710HD | 5.0.1 以降 |
| PowerEdge M910 | 2.5.0 以降 |
| PowerEdge M915 | 2.6.0 以降 |
| PowerEdge T110 II | 1.8.2 以降 |
| PowerEdge T310 | 1.8.2 以降 |
| PowerEdge T410 | 1.9.0 以降 |
| PowerEdge T610 | 6.1.0 以降 |
| PowerEdge T710 | 6.1.0 以降 |

**表 3. PowerEdge 第 12 世代サーバ向けの BIOS**

| サーバー | 最小バージョン |
|---|---|
| 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 |

| サーバー | 最小バージョン |
|---|---|
| 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 4. PowerEdge 第 13 世代サーバ向けの BIOS**

| サーバー | 最小バージョン |
|---|---|
| R630 | 1.0.4 以降 |
| 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 5. PowerEdge 第 14 世代サーバ向けの BIOS**

| サーバー | 最小バージョン |
|---|---|
| R940 | 1.0.0 以降 |
| R740 | 1.0.0 以降 |
| R740xd | 1.0.0 以降 |
| R640 | 1.0.0 以降 |
| M640 | 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 |
| R7415 | 1.0.0 以降 |

**表 6. 展開用の iDRAC および Lifecycle Controller**

| 世代 | バージョン | |
|---|---|---|
| | iDRAC | Lifecycle Controller |
| PowerEdge 第 11 世代サーバ | モジュラーには 3.35、ラックまたはタワーには 1.85 | 1.5.2 以降 |
| PowerEdge 第 12 世代サーバ | 1.00.0 以降 | 1.0.0.3017 以降 |
| PowerEdge 第 13 世代サーバ | 2.30.30.30 以降 | 2.30.30.30 以降 |
| PowerEdge 第 14 世代サーバ | 3.00.00.00 以降 | 3.00.00.00 以降 |

**表 7. クラウドサーバの BIOS と iDRAC の要件**

| モデル | BIOS | Lifecycle Controller 使用 iDRAC |
|---|---|---|
| C6320 | 1.0.2 | 2.30.30.30 以降 |
| C4130 | 1.0.2 | 2.30.30.30 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 |

# PowerEdge サーバーでサポートされる機能

次の機能は、OpenManage Integration for VMware vCenter によって管理されているホスト上でサポートされるものです。

**表 8. PowerEdge サーバーでサポートされる機能**

| リソース | プラットフォーム | | |
|---|---|---|---|
| | 第 11 世代 | 第 12/13 世代 | 第 14 世代 |
| ハードウェアインベントリ | はい | はい | はい |
| イベントとアラーム | はい ( SNMP v1 のみ ) | 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* | はい | はい | はい |
| BIOS / ファームウェアアップデート** | はい | はい | はい |
| Proactive HA*** | いいえ | はい | はい |
| 保証情報 | はい | はい | はい |
| ホスト準拠 | はい | はい | はい |
| ベアメタルサーバの自動 / 手動検出 | はい | はい | はい |
| ベアメタル準拠 | はい | はい | はい |
| ハードウェア構成 | はい | はい | はい |
| ベアメタルハイパーバイザー展開 | はい | はい | はい |
| サーバー LED の点滅 | はい | はい | はい |
| SEL ログの表示 / クリア | はい | はい | はい |
| iDRAC のリンクと起動 | はい | はい | はい |
| iDRAC のリセット | はい | はい | はい |
| システムロックダウンモード | いいえ | いいえ | はい |
| システムプロファイル | いいえ | いいえ | はい |
| クラスタプロファイル | いいえ | はい**** | はい |

*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。

***Proactive HA 機能は、ESXi 6.0 以降を搭載する vCenter 6.5 以降にのみ適用されます。また、Proactive HA 機能は、PSU 内蔵型のサーバおよびクラウドサーバモデルではサポートされません。

****クラスタプロファイルでは、構成ドリフトはサポートされていません。

# 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 9. 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 |
|---|---|---|---|
| SNMP アラート | はい | はい | はい |
| ハードウェアインベントリ | はい | はい | はい |
| CMS のリンクと起動 | はい | はい | はい |
| ライセンス情報 | 該当なし | はい | はい |
| 保証情報 | はい | はい | はい |
| 正常性レポート | はい | はい | はい |

# プロビジョニングされたストレージに必要な容量

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 44 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。

# ソフトウェア要件

vSphere 環境が仮想アプライアンス、ポートアクセス、およびリスニングポートの要件を完全に満たすことを確認します。

**VMware vSphere Web Client の要件**

- vCenter 5.5 以降に対応
- vCenter からの Web Client サービスが必要（ vSphere Desktop Client はサポートされません ）。

具体的なソフトウェア要件については、Dell.com/support/manuals にある『*OpenManage Integration for VMware vCenter* 互換性マトリックス』を参照してください。

# OpenManage Integration for VMware vCenter 要件

## 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 バージョンサポート | サーバの世代 | | | |
|---|---|---|---|---|
| | 第 11 世代 | 第 12 世代 | 第 13 世代 | 第 14 世代 |
| v5.0 | はい | はい | いいえ | いいえ |
| v5.0 U1 | はい | はい | いいえ | いいえ |
| v5.0 U2 | はい | はい | いいえ | いいえ |

| ESXi バージョンサポート | サーバの世代 | | | |
|---|---|---|---|---|
| | 第 11 世代 | 第 12 世代 | 第 13 世代 | 第 14 世代 |
| v5.0 U3 | はい | はい | いいえ | いいえ |
| v5.1 | はい | はい | いいえ | いいえ |
| v5.1 U1 | はい | はい | いいえ | いいえ |
| v5.1 U2 | はい | はい | はい | いいえ |
| v5.1 U3 | はい | はい | はい ( M830、FC830、FC430 を除く ) | いいえ |
| v5.5 | はい | はい | いいえ | いいえ |
| v5.5 U1 | はい | はい | いいえ | いいえ |
| v5.5 U2 | はい | はい | はい | いいえ |
| v5.5 U3 | はい | はい | はい | いいえ |
| v6.0 | はい | はい | はい | いいえ |
| v6.0 U1 | はい | はい | はい | いいえ |
| v6.0 U2 | はい | はい | はい | いいえ |
| v6.0 U3 | はい | はい | はい | はい |
| v6.5 | いいえ | はい | はい | いいえ |
| v6.5 U1 | いいえ | はい | はい | はい |
| v6.7 | いいえ | はい | はい | はい |

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 11. サポートされている vCenter サーババージョン**

| vCenter バージョン | Web クライアントサポート |
|---|---|
| v6.0 U2 | はい |
| v6.0 U3 | はい |
| v6.5 | はい |
| v6.5 U1 | はい |
| v6.7 | はい |

**メモ: vCenter サーバを登録する方法の詳細については、Dell.com/support/manuals で提供されている『*OpenManage Integration for VMware vCenter Version 4.2 Web Client Install Guide*』( OpenManage Integration for VMware vCenter バージョン 4.2 Web クライアントインストールガイド ) を参照してください。**

OpenManage Integration for VMware vCenter バージョン 4.2 は、VMware vRealize Operations Manager ( vROPS ) バージョン 1.1 および 1.2 をサポートします。

# ポート情報

## 仮想アプライアンスと管理ノード

OMIVV で **非対応 vSphere ホストの修正** ウィザードの 準拠ホストの修正 リンクを使用して OMSA エージェントを導入する場合、OMIVV では次のアクションを実行します。

- HTTP クライアントサービスを開始する
- ポート 8080 を有効にする
- ESXi 5.0 以降で OMSA VIB をダウンロードしてインストールするためのポートを利用できるようにする

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。

**表 12. 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。 |
| 69 | TFTP | UDP | なし | 出力 | OMIVV アプライアンスから TFTP サーバへ | TFTP クライアント | ファームウェアが古くなった 11G サーバのファームウェアアップデートに使用。 |
| 80 | HTTP | 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。 |
| 80 | HTTP | TCP | なし | 入力 | ESXi サーバから OMIVV アプライアンスへ | HTTP サーバ | 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 OS 導入フローで使用。 |
| 162 | SNMP エージェント | UDP | なし | 入力 | iDRAC/ESXi 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。 |
| 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。vCenter Web クライアントおよび Dell 管理ポータルで使用。 |
| 443 | WSMAN | TCP | 128 ビット | 入力 / 出力 | OMIVV アプライアンスと iDRAC/OMSA 間 | iDRAC/OMSA 通信 | 管理対象ノードの管理および監視に使用する iDRAC、OMSA、および CMC 通信。 |
| 445 | 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。 |
| 4433 | 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。 |

| 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 |
|---|---|---|---|---|---|---|---|
| 2049 | 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 OS 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 | 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 OS 導入のフローで使用。 |
| 11620 | SNMP エージェント | UDP | なし | 入力 | iDRAC から OMIVV アプライアンスへ | SNMP エージェント ( サーバー ) | 管理対象ノードの管理および監視に使用する iDRAC、OMSA、および CMC 通信。 |
| 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 13. 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、11620 | 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 ( OMSA ) へ | iDRAC/OMSA 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。 |
| 8080 | HTTP | TCP | 128 ビット | 出力 | ESXi から OMIVV アプライアンスへ | HTTP サーバ ( OMSA VIB をダウンロードし、非準拠 vSphere ホストを修正 ) | ESXi による OMSA / ドライバ VIB のダウンロードに使用。 |

**表 14. 管理対象ノード ( iDRAC/CMC )**

| 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 |
|---|---|---|---|---|---|---|---|
| 443 | WSMAN/HTTPS | TCP | 128 ビット | 入力 | OMIVV アプライアンスから iDRAC/CMC へ | iDRAC 通信 | 管理ステーションへの情報提供に使用。iDRAC および CMC からこのポートを開く必要あり。 |
| 4433 | HTTPS | TCP | 128 ビット | 出力 | iDRAC から OMIVV アプライアンスへ | 自動検出 | 管理ステーションでの iDRAC ( 管理対象ノード ) の自動検出用。 |

| 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 |
|---|---|---|---|---|---|---|---|
| 2049 | NFS | UDP | なし | 入力 / 出力 | iDRAC と OMIVV 間 | パブリック共有 | OMIVV アプライアンスによって公開された NFS パブリック共有に iDRAC がアクセスするために使用。OS 導入およびファームウェアアップデートに使用。<br><br>OMIVV から iDRAC 設定にアクセスするために使用。導入フローで使用。 |
| 4001 ~ 4004 | NFS | UDP | なし | 入力 / 出力 | iDRAC と OMIVV 間 | パブリック共有 | OMIVV アプライアンスによって公開された NFS パブリック共有に iDRAC がアクセスするために使用。OS 導入およびファームウェアアップデートに使用。<br><br>OMIVV から iDRAC 設定にアクセスするために使用。導入フローで使用。 |
| 69 | TFTP | UDP | 128 ビット | 入力 / 出力 | iDRAC と OMIVV 間 | トリビアルファイル転送 | 管理ステーションから iDRAC を正常に管理するために使用。 |

# 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のチェックリスト：

- vCenter サーバにアクセスするための OMIVV のユーザー名とパスワードがあることを確認します。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 パスワードを持っているか、ホストでの管理者権限がある Active Directory の資格情報を持っていることを確認します。
- iDRAC での管理権限がある、iDRAC Express または Enterprise に関連付けられたユーザー名およびパスワードを持っているかどうかを確認します。
- vCenter サーバが実行中か確認します。
- OMIVV のインストールディレクトリの場所を決定します。
- VMware vSphere 環境が仮想アプライアンス、ポートアクセス、およびリスニングポートの要件を確かに満たしていることを確認します。また、必要に応じて、クライアントシステムに Adobe Flash Player をインストールします。サポートされている Flash Player のバージョンについては、『*OpenManage Integration for VMware vCenter* 互換性マトリックス』を参照してください。

**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。中断またはシャットダウンは、仮想アプライアンスの全体的な機能に影響を与えます。**

**メモ: ESXi 5.5 以降に導入された場合、OMIVV で VMware ツールは実行中（旧式）として表示されます。OMIVV アプライアンスの導入が正常に完了した後であれば、いつでも必要に応じて VMware ツールをアップグレードできます。**

**メモ: OMIVV と vCenter サーバは同じネットワーク上に配置することをお勧めします。**

**メモ: OMIVV アプライアンスのネットワークは、iDRAC、ホスト、および vCenter にアクセスできる必要があります。**

# OMIVV のインストール、設定、およびアップグレード

**前提条件**
ハードウェア要件が満たされており、必要な VMware vCenter ソフトウェアが実行中であることを確認します。

**このタスクについて**
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。

**手順**

1 デルのサポートウェブサイト（**Dell.com/support**）から、ファイル *DellEMC_OpenManage_Integration_*<バージョン番号>.<ビルド番号>*.zip* をダウンロードします。

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 ウェブクライアントを使用して、OMIVV アプライアンスを含む Open Virtualization Format（OVF）ファイルを展開します。「OMIVV OVF の導入」を参照してください。

4 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、「ライセンスのアップロード」を参照してください。

5 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。「Registering OMIVV and importing the license file」（OMIVV の登録とライセンスファイルのインポート）を参照してください。

6 アプライアンスを設定するには、**初期設定ウィザード** を完了します。「設定ウィザードを使用した設定タスク」を参照してください。

# vSphere Web Client を使用した OMIVV OVF の導入

**前提条件**

製品の .zip ファイル（*Dell_OpenManage_Integration_*<バージョン番号>.<ビルド番号>*.zip*）をデルの 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。

**手順**

1 ダウンロードして解凍した OMIVV 仮想ディスクの場所を検索し、**Dell_OpenManage_Integration.exe** を実行します。

exe ファイルの取得と実行をサポートするクライアント OS のバージョンは、Windows 7 SP1 以降です。

exe ファイルの取得と実行をサポートするサーバ OS のバージョンは、Windows 2008 R2 以降です。

2 **EULA** に同意し、.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 Web Client** を開始します。

5 **VMware vSphere Web 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 **ソースの選択** ウィンドウで、次のサブタスクを実行します。

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、**参照** をクリックします。

**メモ: OVF パッケージがネットワーク共有上にある場合、インストールプロセスに 10 ~ 30 分かかる場合があります。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 **次へ** をクリックします。

**詳細の表示** ウィンドウでは、次の情報が表示されます。

- **プロダクト**— OVF テンプレートの名前が表示されます。
- **バージョン**— OVF テンプレートのバージョンが表示されます。
- **ベンダー**— ベンダー名が表示されます。
- **発行者**— 発行者の詳細が表示されます。
- **ダウンロードサイズ**— OVF テンプレートの実際のサイズ（ギガバイト単位）が表示されます。
- **ディスクのサイズ**— シックおよびシンプロビジョニングの詳細が表示されます。
- **説明**— コメントがここに表示されます。

8 **次へ** をクリックします。

**名前とフォルダの選択** ウィンドウが表示されます。

9 **名前とフォルダの選択** ウィンドウで、次のサブステップを実行します。

a **名前** 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 **フォルダまたはデータセンターの選択** リストで、テンプレートを展開する場所を選択します。

10 **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。

11 **ストレージの選択** ウィンドウで、次のサブステップを実行します。

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。

12 **次へ** をクリックします。

ソースおよび宛先ネットワークについての詳細を含む **ネットワークのセットアップ** ウィンドウが表示されます。

13 **ネットワークのセットアップ** ウィンドウで、**次へ** をクリックします。

**メモ: OMIVV アプライアンスと vCenter サーバは同じネットワーク上に配置することをお勧めします。**

14 **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。

展開ジョブが実行され、ジョブの進捗状況を追跡できる完了ステータスウィンドウが表示されます。

# 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 を認証局に送り、管理コンソールを使用してその結果の証明書を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 アップロードをキャンセルするには、**キャンセル** をクリックします。

**メモ: お使いのアプライアンスのカスタム証明書をアップロードする必要がある場合、必ず、vCenter 登録を行う前に新しい証明書をアップロードします。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、Web クライアントに通信エラーが表示されます。この問題を解決するには、アプライアンスを vCenter からいったん登録解除し、その後、再登録します。**

# 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。

# Administrator 以外のユーザーによる 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 管理者以外のユーザーが 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 Web Client 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 Web Client での権限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。

**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。**

以上で、必要な権限のある Administrator 以外の vCenter サーバ ユーザーが、vCenter の登録および/または vCenter の登録解除、資格情報の変更、資格情報のアップデートが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 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。「vSphere Web Client 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 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、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
- 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

**メモ: VMware vCenter 6.5 を使用している、または vCenter 6.5 以降にアップグレードしている場合は、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
- 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
  - 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

  **メモ: VMware vCenter 6.5 を使用している、または vCenter 6.5 以降にアップグレードしている場合、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
    - 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

    **メモ: vCenter 6.5 を使用している、または vCenter 6.5 以降にアップグレードしている場合、クラスタの変更権限が割り当てられていることを確認します。**
- 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
  - タスクの作成
  - タスクの更新

# 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

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、または Administrator として vCenter サーバの登録を行う方法については、「OpenManage Integration for VMware vCenter の登録とライセンスファイルのインポート」の手順 5 ~ 9 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 の左パネルで、**管理** → **役割** をクリックします。

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、 をクリックします。

5 **権限** をクリックして **Dell** を展開し、選択した役割に対して次のデル権限を選択して、**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、「」Dell.com/support/manuals にある『*OpenManage Integration for VMware vCenter User's Guide*』( OpenManage Integration for VMware vCenter ユーザーガイド ) の「セキュリティの役割および許可」を参照してください。

許可と役割への変更は直ちに反映されます。これで、必要な権限を持つユーザーは、OpenManage Integration for VMware vCenter の操作を実行することができます。

**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。**

**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。**

# OpenManage Integration for VMware vCenter の登録とライセンスファイルのインポート

**前提条件**

ライセンスがダウンロード可能であることを、http://www.dell.com/support/licensing 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、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。

**メモ: お使いのアプライアンスのカスタム証明書をアップロードする必要がある場合、必ず、vCenter 登録を行う前に新しい証明書をアップロードします。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、Web クライアントに通信エラーが表示されます。この問題を解決するには、アプライアンスを vCenter からいったん登録解除し、その後、再登録します。**

**手順**

1 vSphere Web Client から **ホーム** > **ホストとクラスタ** を選択し、左パネルで先ほど展開した OMIVV を探して、**仮想マシンの電源をオンにする** をクリックします。

展開中に **展開後に電源をオン**を選択した場合、展開が完了したら VM の電源を自動的にオンになります。

2 **管理コンソール** を実行するには、メインの **VMware vCenter** ウィンドウで **コンソール** タブをクリックします。

3 OMIVV を完全に起動するよう許可し、**Admin** ( デフォルトは Admin ) としてユーザー名を入力して、**Enter** を押します。

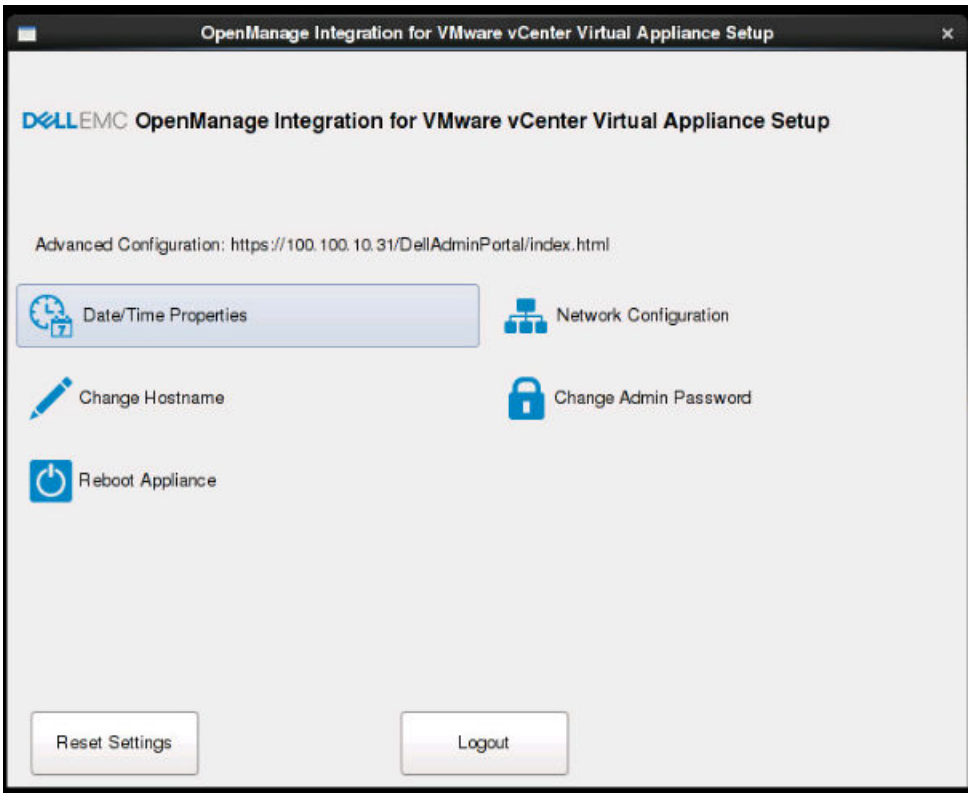
4 新しい Admin パスワードを入力します。新しい Admin パスワードが、インタフェースに表示されるパスワードの複雑性規則に準拠していることを確認します。**Enter** を押します。

5 以前に提供されたパスワードを再入力し、**Enter** を押します。

**Enter** を押して、OMIVV アプライアンスでネットワークおよびタイムゾーン情報を設定します。

6 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。

**図 1. コンソールタブ**




7 **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** ボックスが表示されます。

8 有効な NTP サーバの詳細を、vCenter の同期先に追加します。

9 **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。

10 OMIVV アプライアンスに静的 IP を設定するには、**ネットワーク設定** をクリックします。またはステップ 17 に進んでください。

11 **Auto eth0** を選択し、**編集** をクリックします。

12 **IPv4 設定** タブを選択し、**方法** ドロップダウンで **手動** を選択します。

13 **追加** をクリックして、有効な IP、ネットマスク、およびゲートウェイ情報を追加します。

14 **DNS サーバ** フィールドで、DNS サーバの詳細情報を入力します。

15 **適用** をクリックします。

16 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。

17 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: ホスト名および NTP サーバの変更後は、システムが再起動されたことを確認します。**

**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。**

管理コンソールを開く前に、iDRAC、DRM でのサーバのプロビジョニングなど、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。

18 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、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 URL **https://<アプライアンスの IP / ホスト名>** を指定します。

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。

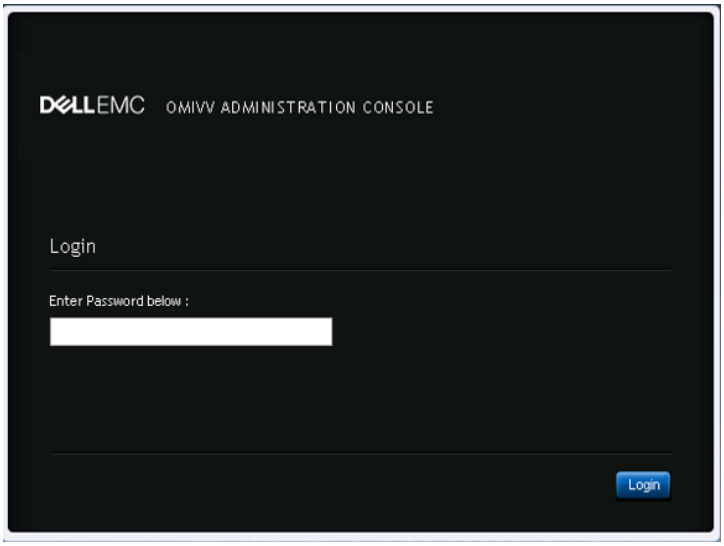



**図 2. 管理コンソール**

19 **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。

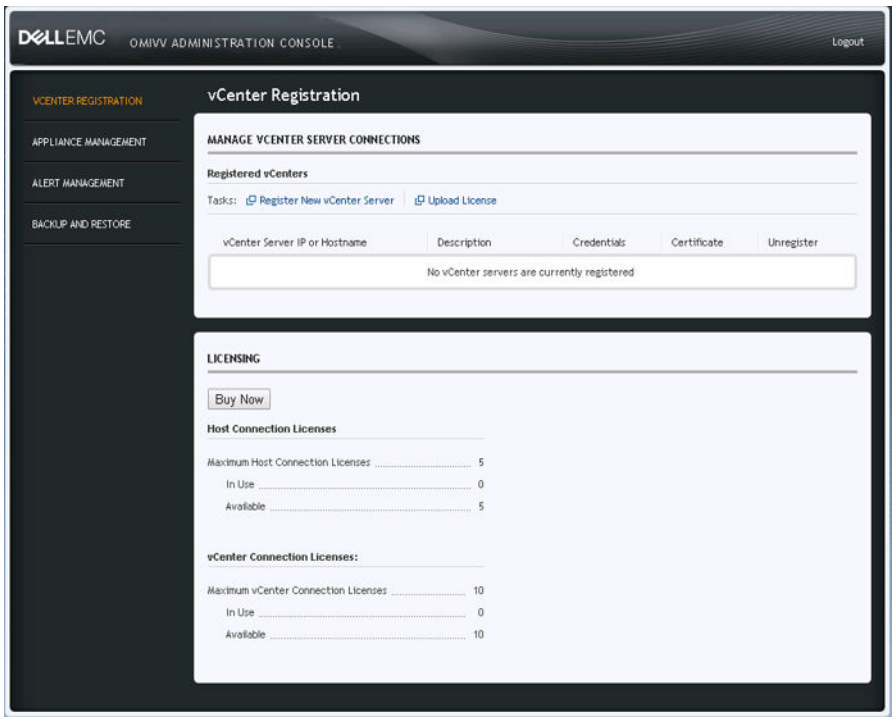



**図 3. 管理コンソールから開いた vCenter 登録 ウィンドウ**

20 **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。

21 **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** で、**vCenter サーバ IP またはホスト名** テキストボックスにサーバ IP またはホスト名を入力した後で、**説明** テキストボックスに詳細を入力します。

説明はオプションです。

**メモ: OpenManage Integration for VMware vCenter を VMware vCenter に登録する際には、完全修飾ドメイン名（FQDN）の使用をお勧めします。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 **vCenter ユーザーアカウント** で、管理者のユーザー名または必要な権限のあるユーザー名を **vCenter ユーザー名** に入力します。

**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。

c **パスワード**にパスワードを入力します。

d **パスワードの 確認**にパスワード をもう一度入力します。

22 **登録** をクリックします。

**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 サーバによる大規模な導入モードで最大 1000 のホストをサポートします。**

23 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、Dell Digital Locker（http://www.dell.com/support/licensing ）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。

24 **ライセンスのアップロード** ウィンドウで **参照** をクリックしてライセンスファイルの参照先を指定し、**アップロード** をクリックしてライセンスファイルをインポートします。

**メモ: ライセンスファイルを変更または編集すると、ライセンスファイル（.XML ファイル）は無効になります。この場合、.XML ファイル（ライセンスキー）を Dell Digital Locker からダウンロードし直す必要があります。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。**

OMIVV が登録されると、Web クライアントのホームページの **管理** カテゴリの下に OMIVV アイコンが表示されます。

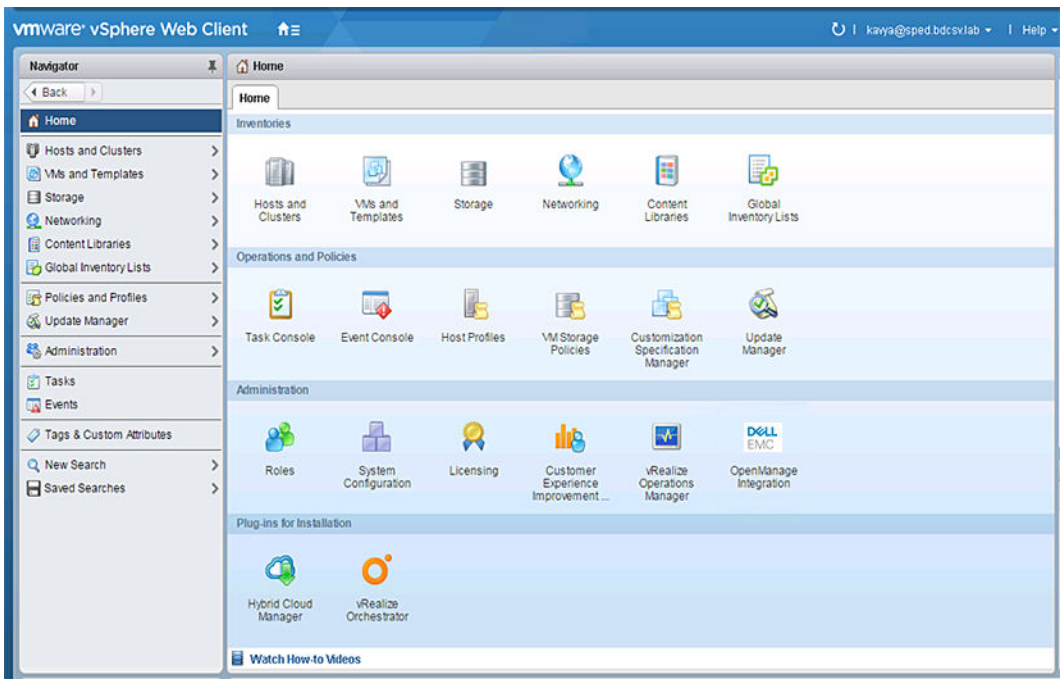



**図 4. OpenManage Integration for VMware vCenter が vCenter に正常に追加された**

**例**

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。

# 登録済み vCenter のアップグレード

非管理者ユーザーまたは管理者ユーザーの登録済み vCenter をアップグレードすることができます。vCenter 6.5 などの最新バージョンの vCenter サーバにアップグレードする場合は、登録済み vCenter のアップグレード前に、VMware のマニュアルを参照してください。登録済み vCenter のアップグレード後に、必要に応じて、次のオプションのいずれかの作業を実行します。

- 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。
  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。
  b 登録済み OMIVV アプライアンスを再起動します。
- 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。

# インストールの確認

**このタスクについて**
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。

**手順**

1 vSphere クライアントのウィンドウをすべて閉じ、新しい vSphere Web Client を開始します。
2 OMIVV アイコンが vSphere Web Client 内に表示されることを確認します。
3 vCenter Server から仮想アプライアンスの IP アドレスまたはホスト名宛てに ping コマンドを実行して、vCenter が OMIVV と通信可能であることを確認します。
4 vSphere ウェブクライアントで、**ホーム** > **管理** > **ソリューション** の順にクリックし、**Plug-In Management**（古いバージョンの vCenter）または **Client Plug-Ins**（新しいバージョン）をクリックします。
**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。
5 **Plug-In Management** または **Client Plug-Ins** ウィンドウで、OMIVV がインストールされ、有効化されていることを確認します。

# 以前のバージョンから 4.2 への移行

**このタスクについて**
以前のバージョンをアンインストールしてから v4.2 OVF を改めて導入し、その後、バックアップ / リストアの手順を使用して以前のバージョンからバージョン 4.2 にデータを移行します。
以前のバージョンから OMIVV バージョン 4.2 に移行するには、次の手順を実行します。

**手順**

1 以前のリリース（v4.x）のデータベースのバックアップを作成します。
バックパックの詳細については、**Dell.com/support/manuals** にある『*OpenManage Integration for VMware vCenter User's Guide*』（OpenManage Integration for VMware vCenter ユーザーズガイド）を参照してください。
2 vCenter から旧アプライアンスの電源を切ります。

**メモ: 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。バックアップ後にプラグインの登録を解除した場合は、『*OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 4.2*』( vSphere Web Client バージョン 4.2 向け OpenManage Integration for VMware vCenter クイックインストールガイド ) で詳細を参照してください。**

3 新しい OpenManage Integration バージョン 4.2 OVF を導入します。

OVF の導入の詳細については、『*OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 4.2*』( vSphere Web Client バージョン 4.2 向け OpenManage Integration for VMware vCenter クイックインストールガイド )を参照してください。

4 OpenManage Integration バージョン 4.2 アプライアンスの電源を入れます。

5 OMIVV アプライアンスのネットワークおよびタイムゾーンを設定します。

新しい OpenManage Integration バージョン 4.2 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。ネットワークの詳細を設定するには、『*OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 4.2*』( vSphere Web Client バージョン 4.2 向け OpenManage Integration for VMware vCenter クイックインストールガイド ) を参照してください。

**メモ: OMIVV 4.2 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 新しい OMIVV アプライアンスにデータベースを復元します。

**メモ: クラスタで Proactive HA を有効にしている場合は、OMIVV がそれらのクラスタの Dell Inc プロバイダを登録解除し、復元後に Dell Inc プロバイダを再度登録します。そのため、Dell ホストの正常性アップデートは、復元が完了するまで使用できません。**

詳細については、Dell.com/support/manuals にある『*OpenManage Integration for VMware vCenter User's Guide*』( OpenManage Integration for VMware vCenter ユーザーズガイド ) の「**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 新しいライセンスファイルをアップロードします。

ライセンスの詳細については、『*OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 4.2*』( vSphere Web Client バージョン 4.2 向け OpenManage Integration for VMware vCenter クイックインストールガイド )を参照してください。

8 アプライアンスを検証します。

データベースの移行が正常に行われたことを確認するための、アプライアンスの検証の詳細については、『*OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 4.2*』( vSphere Web Client バージョン 4.2 向け OpenManage Integration for VMware vCenter クイックインストールガイド ) を参照してください。

9 すべてのホストで **インベントリ** を実行します。

**メモ:**

アップグレード後に、OMIVV で管理するすべてのホスト上でインベントリを実行することをお勧めします。詳細については、『*OpenManage Integration for VMware vCenter User's Guide*』( OpenManage Integration for VMware vCenter ユーザーズガイド ) の「**インベントリジョブの実行**」を参照してください。

新しい OMIVV バージョン 4.2 アプライアンスの IP アドレスが旧アプライアンスの IP アドレスから変更された場合、新しいアプライアンスをポイントするように SNMP トラップのトラップ送信先を設定します。第 12 世代以降のサーバの場合は、これらのホストでインベントリを実行することによって IP の変更が修正されます。以前のバージョンに準拠していた第 12 世代よりも前のホストでは、IP が変更されると非準拠として表示され、Dell EMC OpenManage Server Administrator ( OMSA ) を設定する必要があることが示されます。ホストの対応性の修正については、Dell.com/support/manuals にある『*OpenManage Integration for VMware vCenter User's Guide*』( OpenManage Integration for VMware vCenter ユーザーズガイド ) の「**vSphere ホストの対応性のレポートおよび修正**」を参照してください。

# 以前のバージョンの OMIVV の登録解除した後で OMIVV をリカバリする

**このタスクについて**

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: プラグインの登録を解除すると、プラグインによって登録されたアラームに実装されていたすべてのカスタマイズが削除されます。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。**

**手順**

1 「以前のバージョンから 4.2 への移行」のステップ 3 ~ 5 を実行します。

2 以前のプラグインで登録したときと同じ vCenter にプラグインを登録します。

3 移行を完了するには、「以前のバージョンから 4.2 への移行」のステップ 6 ~ 9 を実行します。

2

# 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。**

トピック：



## 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。
未設定の vCenter がある場合、またはお使いの環境へ vCenter を追加済みの場合、その特定の vCenter を選択します。vCenter 選択 ページで、設定する vCenter を 1 つでも複数でも選択できます。
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 OMIVV アプライアンスに登録された同じシングルサインオン（SSO）に属する vCenter サーバが複数ある場合、単一の vCenter サーバを設定するように選択すると、それぞれの vCenter の設定を始める前に手順 1 ~ 3 を繰り返す必要があります。**

# 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 EMC 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 EMC 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。**

**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、第 14 世代サーバでのシステム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 IP 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 **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。

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 の資格情報を検証します。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 サービスが無効にされている ESXi 6.5 以降を実行するすべてのホストに対するテスト接続が失敗します。このようなホストの場合は、それらのホストでインベントリを実行するときに WBEM サービスが自動的に有効になります。テスト接続には失敗しますが、接続プロファイルウィザードでアクションを完了し、ホストでインベントリを実行してから、接続プロファイルを再度テストすることが推奨されます。**

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。詳細については、本ガイドの「**接続プロファイルの変更**」を参照してください。Dell.com/support/manuals にある『*OpenManage Integration for VMware vCenter* ユーザーズガイド』の「**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。**

ホストが接続プロファイルに追加されると、OMIVV の IP アドレスがホストの iDRAC の SNMP トラップ送信先に自動的に設定され、OMIVV は、ESXi 6.5 ホストのウェブベースエンタープライズ管理 ( WBEM ) サービスを自動的に有効にします。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。SNMP トラップ送信先の再設定や WBEM サービスの有効化が必要な非対応ホストを表示するには、Dell.com/support/manuals にある『*OpenManage Integration for VMware vCenter* ユーザーズガイド』の「**vSphere ホストの対応性のレポートおよび修正**」を参照してください。

# 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、定期的なインベントリジョブをスケジュールすることをお勧めします。インベントリジョブは最小限のリソースしか消費しないので、ホストパフォーマンスを低下させません。**

**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プロファイルに追加されている場合、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、有効化がまだの場合は、**インベントリデータの取得を有効にする** を選択します。デフォルトでは、**インベントリデータの取得を有効にする** が有効になっています。

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。

入力時刻は現地時刻です。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、この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** タブでホストのインベントリスケジュールの詳細を変更できます。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「**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。

# 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。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 世代以降のホストでは、SNMP トラップ送信先を iDRAC で設定するようにします。第 12 世代より前のホストでは、トラップ送信先を OMSA で設定するようにします。

**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 EMC 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 EMC 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 EMC 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 EMC 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 EMC 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、イベントとアラーム 設定を再度有効化することができます。**

**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。**

5 **適用** をクリックします。

# SNMP トラップコミュニティ文字列の設定

1 **OpenManage Integration for VMware vCenter** の **管理** > **設定** タブの、**アプライアンスの設定** の下で、**OMSA SNMP トラップコミュニティ文字列**に対して をクリックします。
**OMSA SNMP トラップコミュニティ文字列の設定** ダイアログボックスが表示されます。デフォルトでは、「public」が SNMP トラップコミュニティ文字列に表示されます。

2 「public」を任意の文字列にカスタマイズして、**適用** をクリックします。

**メモ: 第 11 世代 PowerEdge サーバの SNMP トラップコミュニティ文字列設定は、OMIVV 経由で OMSA をインストールまたはアップグレードしているときに設定されます。**

# 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、**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** の下の 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。

- **Dell Online** - Dell（Ftp.dell.com）のファームウェアアップデートリポジトリを使用する場所にアクセスできます。OpenManage Integration for VMware vCenter は選択されたファームウェアアップデートを 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）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。**

**メモ: 最新バージョン（3.x）以降の DRM を使用していることを確認します。**

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: OMIVV は、サーバメッセージブロック（SMB）バージョン 1.0 および SMB バージョン 2.0 ベースの CIFS 共有のみをサポートします。**

**メモ: CIFS 共有を使用している場合は、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。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 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 60 ~ 90 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自動検出で検出されたベアメタルシステムと安全に通信するための、資格情報のセットアップを行うことができます。iDRAC と安全に通信を行うため、OMIVV は最初の検出時から展開プロセスの終了時まで、展開用の資格情報を使用します。OS 展開プロセスが正常に完了すると、OMIVV は接続プロファイルの指定に従って iDRAC の資格情報を変更します。展開用の資格情報を変更した場合、それ以降に新たに検出されたシステムはすべて、新しい資格情報でプロビジョニングされます。ただし、展開用の資格情報を変更する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として使用する iDRAC と通信することができます。**

**手順**

1 OpenManage Integration for VMware vCenter の **管理** > **設定** タブの **アプライアンスの設定** の下で、**展開資格情報** 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）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）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、PowerEdge 第 11 世代以前のサーバのみです。**

**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 EMC 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 EMC 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を有効または無効にできます。現在のアラートステータスは vCenter アラーム タブに表示されます。重要イベントは実際のまたは切迫したデータ喪失あるいはシステム異常を示します。警告イベントは必ずしも重大ではありませんが、将来の潜在的な問題を示す可能性があります。イベントおよびアラームは VMware Alarm Manager を使用して有効化することもできます。イベントは、ホストとクラスタ ビューの vCenter タスクとイベント タブに表示されます。サーバからイベントを受信するには、OMIVV を SNMP トラップ送信先として設定します。第 12 世代以降のホストでは、SNMP トラップ送信先は 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 EMC 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。第 12 世代より前のホストでは、OMIVV は SNMP v1 アラートをサポートしています。**

**メモ: Dell イベントを受信するには、アラームとイベントの両方を有効にします。**

**手順**

1 OpenManage Integration for VMware vCenter の **管理** > **設定** タブで、**vCenter 設定** の下にある **イベントおよびアラーム** を展開します。

現在の **Dell EMC 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 **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 EMC 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 EMC 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。

このステップは変更が有効になるまでに最大 1 分かかります。また、**Dell EMC 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、『*OpenManage Integration for VMware vCenter User's Guide*』( OpenManage Integration for VMware vCenter ユーザーガイド ) の「**イベント、アラーム、および正常性の監視**」セクション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、次の手順を実行します。
a **インベントリ / 保証データ** の下にある **インベントリ / 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 **インベントリ / 保証データの取得スケジュール** の下で、ジョブを実行する曜日を選択します。
c **インベントリ / 保証データの取得時間** テキストボックスで、このジョブの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。
d 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。

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。

# シャーシプロファイルの作成

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。

**関連するシャーシ** 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、 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。

# 3

# 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 Enterprise システム管理マニュアル — **Dell.com/SoftwareSecurityManuals**
- Dell EMC OpenManage マニュアル — **Dell.com/OpenManageManuals**
- Dell EMC 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 Dell EMC Lifecycle Controller マニュアル — **Dell.com/idracmanuals**
- Dell EMC OpenManage Connections エンタープライズシステム管理マニュアル — **Dell.com/OMConnectionsEnterpriseSystemsManagement**
- Dell EMC 保守ツールマニュアル — **Dell.com/ServiceabilityTools**
- a **Dell.com/Support/Home** に移動します。
  b **Choose from all products（すべての製品から選択）** をクリックします。
  c **All products（すべての製品）** セクションで **Software & Security（ソフトウェアおよびセキュリティ）** 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。
  - **Enterprise Systems Management（エンタープライズシステム管理）**
  - **Remote Enterprise Systems Management（リモートエンタープライズシステム管理）**
  - **Serviceability Tools（保守ツール）**
  - **Dell Client Command Suite（デルクライアントコマンドスイート）**
  - **Connections Client Systems Management（接続クライアントシステム管理）**

  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。

# 4

# 関連マニュアル

このガイド以外にも、Dell.com/support で他のガイドにアクセスできます。**すべての製品から選択** をクリックしてから、**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 4.2** 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 Version 4.2 Web Client User's Guide*』*( OpenManage Integration for VMware vCenter バージョン 4.2 Web Client ユーザーズガイド )*
- 『*OpenManage Integration for VMware vCenter Version 4.2 Release Notes*』*( OpenManage Integration for VMware vCenter 4.2 リリースノート )*
- 『*OpenManage Integration for VMware vCenter Version 4.2 Compatibility Matrix*』*( OpenManage Integration for VMware vCenter バージョン 4.2 互換性マトリックス )*

**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 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、各種の記事を参照できます。