

# OpenManage Integration for VMware vCenter

バージョン 5.1

ユーザーズガイド

## メモ、注意、警告

 **メモ:** 製品を使いやすくするための重要な情報を説明しています。

 **注意:** ハードウェアの損傷やデータの損失の可能性を示し、その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。

© 2010 - 2020 Dell Inc. またはその関連会社。Dell、EMC、およびその他の商標は、Dell Inc. またはその子会社の商標です。その他の商標は、それぞれの所有者の商標である場合があります。

<b>1 はじめに</b> .....	<b>10</b>
本リリースの新機能.....	10
OpenManage Integration for VMware vCenter の機能.....	10
<b>2 管理コンソールについて</b> .....	<b>12</b>
新しい vCenter サーバーの登録.....	12
非管理者アカウントを使用した vCenter サーバーの登録.....	13
Administrator 以外のユーザーに必要な権限.....	13
既存の役割へのデルの権限の割り当て.....	14
登録済み vCenter サーバーの SSL 証明書のアップデート.....	14
vCenter ログイン認証情報の変更.....	15
OpenManage Integration for VMware vCenter の登録解除.....	15
OMIVV 管理コンソールへのライセンスのアップロード.....	15
OMIVV アプライアンスの管理.....	16
グローバル アラートの設定.....	22
OMIVV VM コンソールについて.....	23
<b>3 ダッシュボードを使用したホストとシャーシの監視</b> .....	<b>31</b>
<b>4 ホスト認証情報プロファイルを使用したホストの管理</b> .....	<b>33</b>
ホスト認証情報プロファイル.....	33
ホスト認証情報プロファイルの作成.....	33
ホスト認証情報プロファイルの編集.....	34
ホスト認証情報プロファイルの表示.....	35
ホスト認証情報プロファイルのテスト.....	36
ホスト認証情報プロファイルの削除.....	36
<b>5 シャーシ認証情報プロファイルを使用したシャーシの管理</b> .....	<b>37</b>
シャーシ認証情報プロファイル.....	37
シャーシ認証情報プロファイルの作成.....	37
シャーシ認証情報プロファイルの編集.....	38
シャーシ認証情報プロファイルの表示.....	39
シャーシ認証情報プロファイルのテスト.....	39
シャーシ認証情報プロファイルの削除.....	39
<b>6 リポジトリ プロファイルを使用したファームウェアおよびドライバー リポジトリの管理</b> .....	<b>40</b>
リポジトリプロファイル.....	40
リポジトリ プロファイルの作成.....	40
リポジトリ プロファイルの編集.....	41
Dell デフォルト カタログの編集またはカスタマイズ.....	41
検証済み MX スタック カタログの編集.....	42
リポジトリの場所と同期.....	42
リポジトリ プロファイルの表示.....	42
リポジトリ プロファイルの削除.....	43

<b>7 クラスタプロフィールを使用したベースライン構成の取得</b> .....	<b>44</b>
クラスタプロフィール.....	44
クラスタプロフィールの作成.....	44
クラスタプロフィールの編集.....	45
クラスタプロフィールの表示.....	45
クラスタプロフィールのアップデート.....	46
クラスタプロフィールの削除.....	46
<b>8 導入</b> .....	<b>47</b>
ベアメタルサーバーの表示.....	47
デバイス検知.....	48
自動検出.....	48
自動検出の前提条件.....	48
iDRAC の管理者アカウントを有効または無効にする.....	49
PowerEdge サーバーでの自動検出の手動設定.....	49
ベアメタルサーバーの手動検出.....	49
ベアメタルサーバーの取り外し.....	50
ベアメタルサーバーの更新.....	50
iDRAC ライセンスの購入または更新.....	50
導入.....	50
システムプロフィールの導入 (ハードウェアの設定).....	51
ISO プロファイル (ESXi インストール) の導入.....	51
システムプロフィールと ISO プロファイルの導入.....	53
2 つの NIC を使用してホストを導入するための前提条件.....	53
VLAN サポート.....	53
展開ジョブのタイミング.....	54
システムプロフィール.....	54
システムプロフィールの作成.....	55
システムプロフィールの編集.....	56
システムプロフィールの表示.....	57
システムプロフィールの削除.....	57
ISO プロファイル.....	57
ISO プロファイルの作成.....	57
ISO プロファイルの編集.....	58
ISO プロファイルの表示.....	58
ISO プロファイルの削除.....	58
カスタム Dell EMC ISO イメージのダウンロード.....	58
<b>9 対応性</b> .....	<b>59</b>
管理対応性.....	59
非対応ホストの表示.....	59
非対応ホストの修正.....	60
iDRAC ライセンスの対応性の修正.....	61
OEM サーバのサポート.....	61
設定コンプライアンス.....	62
設定コンプライアンスの表示.....	62
ドリフトレポートの表示.....	62

<b>10 ジョブの管理</b> .....	<b>64</b>
展開ジョブ.....	64
シャーシ ファームウェア アップデート ジョブ.....	64
ホスト ファームウェア アップデート ジョブ.....	65
システムロックダウンモードジョブ.....	66
ドリフト検出ジョブ.....	66
ホスト インベントリー ジョブの表示.....	67
インベントリー ジョブの実行.....	67
ホスト インベントリー ジョブの変更.....	68
シャーシ インベントリー ジョブの表示.....	68
シャーシのインベントリー ジョブの実行.....	69
ホスト保証の表示.....	69
ホスト保証ジョブの変更.....	69
シャーシ保証の表示.....	70
<b>11 ログの管理</b> .....	<b>71</b>
ログ履歴の表示.....	71
<b>12 OMIVV アプライアンス設定の管理</b> .....	<b>72</b>
複数アプライアンスの管理.....	72
保証期限通知の設定.....	72
アプライアンスの最新バージョン通知の設定.....	72
展開用の資格情報の設定.....	73
ハードウェアコンポーネントの冗長性の正常性—Proactive HA.....	73
Proactive HA のイベント.....	73
ラック サーバーおよびタワー サーバーの Proactive HA の設定.....	75
クラスターでの Proactive HA の有効化.....	75
正常性のオーバーライド重大度のアップデート通知.....	76
初期設定.....	76
初期設定ステータスの表示.....	77
ファームウェア アップデート設定.....	77
ライセンス情報の表示.....	78
OpenManage Integration for VMware vCenter ( OMIVV ) のライセンス.....	78
ソフトウェア ライセンスの購入.....	79
サポート情報へのアクセス.....	79
トラブルシューティング バンドルの作成およびダウンロード.....	79
iDRAC のリセット.....	80
<b>13 vCenter 設定の管理</b> .....	<b>81</b>
イベントおよびアラームについて.....	81
イベントとアラームの設定.....	82
シャーシ イベントの表示.....	82
シャーシ アラームの表示.....	82
アラームおよびイベントの設定の表示.....	83
仮想化関連のイベント.....	83
データ取得スケジュールの管理.....	90
インベントリー ジョブのスケジュール.....	90
保証取得ジョブのスケジュール.....	90

<b>14 シャーシ管理.....</b>	<b>91</b>
Dell EMC シャーシ情報の表示.....	91
シャーシ インベントリー情報の表示.....	91
シャーシのハードウェアインベントリー情報の表示.....	91
ファームウェア インベントリー情報の表示.....	94
管理コントローラー情報の表示.....	94
ストレージ インベントリー情報の表示.....	95
保証情報の表示.....	96
シャーシに関連するホストの表示.....	96
関連するシャーシ情報の表示.....	96
PowerEdge MX シャーシの管理.....	97
統合シャーシ管理 IP を使用したシャーシおよびホストの管理.....	97
PowerEdge MX シャーシの追加.....	98
Mx シャーシ ファームウェアのアップデート.....	98
<b>15 ホストの管理.....</b>	<b>100</b>
OMIVV ホストの表示.....	100
単一ホストの監視.....	100
ホスト サマリー情報の表示.....	100
OMIVV ホスト情報の表示.....	102
クラスターおよびデータセンターでのホスト監視.....	107
ファームウェアアップデート.....	112
vSAN ホストのファームウェアとドライバーのアップデート.....	113
vSAN クラスターのファームウェアとドライバーのアップデート.....	115
vSphere ホストのファームウェアのアップデート.....	117
vSphere クラスターのファームウェアのアップデート.....	119
同じファームウェア コンポーネント タイプのアップデート.....	120
vSphere Lifecycle Manager の概要.....	121
Dell EMC 管理コンソールでの vSphere Lifecycle Manager ステータスの表示.....	122
Dell EMC 管理コンソールでの vSphere Lifecycle Manager の登録.....	122
Dell EMC 管理コンソールでの vSphere Lifecycle Manager の登録解除.....	122
vSphere Lifecycle Manager を使用したクラスターの管理.....	122
vSphere Lifecycle Manager のユーザー インターフェイスでの OMIVV のファームウェア アドオン プロ バイダーとしての使用.....	123
クラスターコンプライアンス ステータスの表示.....	123
クラスターコンプライアンスの問題の修正.....	124
ハードウェア互換性チェック.....	124
修復の事前チェックの実行.....	124
vSphere Lifecycle Manager でのクラスター修復.....	125
vSphere Lifecycle Manager の vSphere オートメーション API での OMIVV をファームウェアのアドオン プロバイダーとしての使用.....	125
点滅式インジケーター ライトの設定.....	128
システムロックダウンモードの設定.....	129
<b>16 セキュリティの役割および許可.....</b>	<b>130</b>
データ整合性.....	130
アクセス制御認証、承諾、および役割.....	130
Dell 操作役割.....	130
Dell インフラストラクチャ導入役割.....	131

特権について.....	131
<b>17 よくあるお問い合わせ (FAQ) .....</b>	<b>133</b>
よくあるお問い合わせ (FAQ) .....	133
非対応 vSphere ホストの場合、iDRAC のライセンス タイプと説明が正しく表示されない.....	133
Dell プロバイダーが正常性アップデート プロバイダーとして表示されない.....	133
無効または不明な iDRAC IP が原因でホストインベントリまたはテスト接続が失敗します。.....	133
非準拠 vSphere ホストを修正 ウィザードを実行しているときに、特定のホストのステータスが不明と表示されます.....	134
OMIVV アプライアンスの登録中に割り当てられるデルの権限は OMIVV の登録を解除した後、削除されません.....	134
VMware 認証局 (VMCA) によるエラーコード 2000000 を解決する方法.....	134
管理コンソールで、アプライアンスを工場出荷時設定にリセットした後、リポジトリパスのアップデートがデフォルトに設定されない.....	135
OMIVV で DNS 設定を変更した後、vCenter HTML-5 クライアントで Web 通信エラーが発生したらどうすればよいですか.....	135
ファームウェア ページで一部のファームウェアのインストール日が 12-31-1969 と表示される.....	135
vCenter にプラグインを登録できても、HTML-5 クライアントに OpenManage Integration アイコンが表示されない.....	135
アプライアンスの IP と DNS 設定が DHCP 値で上書きされると、なぜ、アプライアンスの再起動後に DNS 構成設定が元の設定に戻るのですか？.....	135
ファームウェア アップデートを実行すると、「ファームウェア リポジトリ ファイルが存在しないか、無効になっています」というエラー メッセージが表示される場合がある.....	136
OMIVV を使用しての、ファームウェアバージョン 13.5.2 の Intel ネットワークカードのアップデートはサポートされていない.....	136
OMIVV を使用して Intel ネットワークカードを 14.5 または 15.0 から 16.x にアップデートすると、DUP からのステージング要件によってアップデートが失敗する.....	136
管理ポータルに、アップデートリポジトリの場所に到達できないと表示される理由.....	136
1対多のファームウェアアップデートを実行したときに、システムがメンテナンスモードに移行しない理由.....	137
一部の電源装置のステータスが重要に変更されても、シャーシのグローバル正常性は正常のままになっている.....	137
システム概要 ページのプロセッサビューで、プロセッサのバージョンが「該当なし」と表示されます..	137
OMIVV は、リンクモードで vCenter をサポートしますか.....	137
OMIVV ではどのようなポート設定が必要ですか。.....	137
認証情報が新たに変更されたユーザーを含むシステム プロファイルを iDRAC ユーザー リストに正常に適用した後、ベアメタル検出に使用する同じユーザーのパスワードが変更されない.....	139
vCenter ホストおよびクラスタページにリストされる新しい iDRAC バージョンの詳細を表示できません .....	139
ロックダウンモードを有効にした状態で、OMIVV で ESXi をサポートすることができますか.....	139
ロックダウン モードを使用しようとすると失敗する.....	139
サーバで ESXi の導入が失敗する.....	139
自動検出されたシステムで、導入ウィザードでモデル情報が表示されない.....	139
ESXi ISO で NFS 共有がセットアップされているが、共有の場所をマウントするときのエラーで失敗する.....	140
vCenter から OMIVV アプライアンスを強制的に削除する方法を教えてください.....	140
今すぐバックアップ画面にパスワードを入力するとエラーメッセージが表示されます.....	140
ファームウェアアップデートに失敗した場合は、どうすればよいでしょうか.....	140
vCenter の登録に失敗した場合の対処方法.....	140
ホスト認証情報 プロファイルの認証情報テスト中、パフォーマンスが遅くなる、または応答しなくなる .....	141
OMIVV は VMware vCenter Server アプライアンスをサポートしていますか.....	141

サーバーが CSIOR ステータス「不明」で、「非対応」と表示される場合がある.....	141
次回の再起動時にファームアップデートを適用するオプションでファームウェアアップデートを行 ってシステムを再起動したにも関わらず、ファームウェアのレベルがアップデートされません.....	141
vCenter ツリーからホストを削除した後も、引き続きシャーシにそのホストが表示されます.....	142
OMIVV のバックアップと復元の後、アラーム設定が復元されない.....	142
NPAR がターゲット ノード上で有効で、システム プロファイルで無効の場合、OS の導入が失敗する	142
使用可能な OMIVV アプライアンスのバージョンが現在のバージョンよりも古い場合、誤った情報 が表示される.....	142
第 12 世代以降のベアメタル サーバーを追加しようとする時 267027 例外がスローされる.....	142
導入時に、システム プロファイルの適用が iDRAC エラーにより失敗する.....	142
プロキシがドメインユーザー認証で設定されている場合、OMIVV RPM のアップグレードが失敗する	143
FX シャーシに PCIe カードを搭載しているシステムプロファイルを適用できません.....	143
ドリフト検出で FX シャーシに PCIe カードを備えるモジュラーサーバが非対応と表示される.....	143
選択した NIC の MAC アドレスを iDRAC が入力しない場合に、PowerEdge サーバ上に OS を導入で きない.....	143
ESXi 6.5U1 を持つホストのホスト認証情報プロファイルの作成時に、ホストのサービス タグが選択 したホストのページに表示されない.....	143
以前の OMIVV バージョンから最新の OMIVV バージョンにバックアップして復元した後に Dell EMC アイコンが表示されない.....	144
OMIVV を使用して iDRAC ファームウェア バージョンをアップグレードまたはダウングレードする と、ファームウェア アップデートが成功していても、OMIVV ではジョブが失敗したと示される 場合がある.....	144
クラスタレベルでシステムロックダウンモードを設定すると、「クラスタの下にあるホストに正常 なインベントリが含まれていません」というメッセージが時々表示される.....	144
OMIVV アプライアンスの RPM アップグレード後、ログの複数のエントリが vCenter の最新タスク に表示される場合がある.....	145
vCenter の登録後、OMIVV の Dell EMC ロゴが VMware のホーム ページに表示されない.....	145
バックアップおよび復元後、非対応の第 11 世代 PowerEdge サーバーが OMIVV インベントリに保 持される.....	145
OMIVV アプライアンスをアップグレードした後、Flex クライアントから vCenter を起動できない.....	145
OMIVV にネットワーク アダプターを追加または削除するときに、既存の NIC が OMIVV コンソール から消える.....	145
2 番目の NIC を追加または削除した後、[ ネットワーク設定 ] ページに 3 つの NIC が表示される.....	146
以前のバージョンでステータスが [ 不明 ] になっていたサーバーが、OMIVV の最新バージョンへの バックアップおよび復元後に [ ベアメタル サーバー ] ページに表示されない.....	146
OS の導入後、OMIVV が vCenter への ESXi ホストの追加に失敗したか、ホスト プロファイルの追 加に失敗したか、ホストのメンテナンス モードの開始に失敗した.....	146
iDRAC IP に到達できないときに、iDRAC ライセンスのステータスが [ 対応性の管理 ] ページに [ 対 応 ] と表示される.....	146
OMIVV で OS を正常に導入した後、ESXi ホストが切断されるか、応答しない状態になる.....	147
OMIVV のネットワーク インターフェイス カード ( NIC ) が ESXi ホスト ネットワークに接続されて いない場合、導入ジョブがタイムアウトする.....	147
特定のホストで保証ジョブが実行されない.....	147
バックアップおよび復元の実行後に Proactive HA の初期化が実行されない.....	147
Firefox ブラウザーの環境で、OMIVV ページに無効なセッション、タイムアウト例外、または 200 万件のエラーが表示される.....	147
vCenter の最近のタスク ペインでは、一部の OMIVV タスク通知の詳細列が表示されない.....	148
vCenter 6.5 U2 を使用している場合、OMIVV のすべてのページに 2000002 エラーが表示されるこ とがある.....	148
RPM アップグレードの実行後、または以前の OMIVV バージョンからそれ以降の OMIVV バージョン へのバックアップおよび復元を実行した後、OMIVV のすべてのページに 2000002 エラーが表示 される.....	148

OMIVV が vCenter の登録解除を完了するまでに長時間かかる場合がある.....	148
ベアメタル展開の問題.....	148
新しく購入したシステムでの自動検出の有効化.....	149
<b>付録 A: システム固有属性.....</b>	<b>150</b>
<b>付録 B: 追加情報.....</b>	<b>153</b>
<b>付録 C: カスタマイズ属性.....</b>	<b>154</b>
<b>付録 D: コンポーネントとベースラインのバージョン比較表.....</b>	<b>155</b>
<b>付録 E: 応答コード.....</b>	<b>157</b>

## はじめに

VMware vCenter は、IT 管理者が VMware vSphere ESX/ESXi ホストを管理、監視する際の中心的な役割を果たすコンソールです。OpenManage Integration for VMware vCenter ( OMIVV ) は、vSphere 環境で Dell EMC サーバー インフラストラクチャの管理/監視関連タスクを合理化することで、データセンター管理の複雑さを軽減できます。

## 本リリースの新機能

OpenManage Integration for VMware vCenter 5.1 のこのリリースでは、次の機能を提供しています。

- ・ vSphere 7.0 のサポート
- ・ vSphere Lifecycle Manager を使用したファームウェア管理のサポート
- ・ XR2 および R7525 PowerEdge サーバーのサポート

## OpenManage Integration for VMware vCenter の機能

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

表 1. OMIVV の機能

機能	説明
インベントリ	<p>インベントリ機能では、次の項目が提供されます。</p> <ul style="list-style-type: none"> <li>・ PowerEdge サーバーの詳細( メモリー容量、メモリーの種類、NIC、PSU、プロセッサ、RAC など )</li> <li>・ サーバー、クラスター、およびデータセンターレベルの保証情報</li> <li>・ シャーシの詳細( シャーシ管理コントローラー( CMC )または管理モジュールの情報、シャーシの電源、KVM の状態、ファンや温度の詳細、保証情報、スイッチ、サーバー、およびストレージの詳細など )。</li> <li>・ マルチシャーシ管理( MCM )構成で MX シャーシの関係をサポート。</li> <li>・ MX シャーシ MCM 構成のファブリック情報</li> <li>・ MX シャーシの QuickSync ハードウェア情報</li> </ul>
監視およびアラートの送信	<p>監視とアラートには、次のような機能が含まれています。</p> <ul style="list-style-type: none"> <li>・ 主要なハードウェア障害を検知し、仮想化を認識した動作を実行する。たとえば、メンテナンスモードで作業負荷の移行やホストを設置、など。</li> <li>・ サーバやシャーシの問題を診断するための、インベントリやイベント、アラームなどの情報を提供する。</li> <li>・ VMware Proactive HA 機能のサポート。</li> </ul>
ファームウェアアップデート	<p>クラスター対応サーバーのファームウェア アップデートでは次の処理が行われます。</p> <ul style="list-style-type: none"> <li>・ サポートされているサーバを最新バージョンの BIOS とファームウェアにアップデートする。</li> </ul> <p>vSphere Lifecycle Manager とともに OMIVV を使用して、ファームウェアのアップデートを実行することもできます( vCenter 7.0 以降に適用されます )。</p>

機能	説明
クラスターのドリフト検出	<ul style="list-style-type: none"> <li>クラスターに対するファームウェアのコンプライアンス</li> <li>vSAN クラスターに対するドライバーのコンプライアンス</li> <li>ハードウェア コンプライアンス</li> </ul> <p><b>① メモ:</b> ハードウェアのコンプライアンスは、シャーシ認証情報プロファイルを使用して管理されているホストではサポートされません。</p>
ドライバのアップデート	vSAN クラスターに対するドライバのアップデート。
導入	<p>展開には次が含まれます。</p> <ul style="list-style-type: none"> <li>システム プロファイルを作成して展開します。</li> <li>PXE ではなく VMware vCenter を使用して、ベアメタル サーバーにオペレーティングシステムをリモートで展開します。</li> </ul>
サービス情報	デルの保証データベースから Dell EMC サーバーおよび関連するシャーシの保証情報を取得して、オンラインで簡単に保証をアップグレードできるようにする。
セキュリティの役割および許可	<p>セキュリティの役割および許可には次の機能があります。</p> <ul style="list-style-type: none"> <li>標準の vCenter 認証、規則、および許可との統合。</li> <li>iDRAC9 ベース サーバーでの iDRAC ロックダウン モードのサポート。iDRAC9 ベース サーバーのリストについては、「互換性マトリックス」を参照してください。</li> </ul>
OEM サーバのサポート	<p>次の OMIVV の機能がサポートされています。</p> <ul style="list-style-type: none"> <li>インベントリ</li> <li>監視およびアラートの送信</li> <li>ファームウェアアップデート</li> <li>導入</li> <li>サービス情報</li> <li>セキュリティの役割および許可</li> </ul>
Mx シャーシ ファームウェアのアップデート	MX シャーシの管理モジュール ファームウェア アップデート オプションがあります。

**① メモ:** OMIVV 5.0 以降では、VMware vSphere Client (HTML-5) のみがサポートされ、vSphere Web Client (FLEX) はサポートされません。

## 管理コンソールについて

OpenManage Integration for VMware vCenter とその仮想環境は、次の 2 つの管理ポータルのいずれかを使用して管理できます。

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

### 新しい vCenter サーバーの登録

アカウントには、サーバーを作成するために必要な権限が必要です。必要な権限の詳細については、「[Administrator 以外のユーザーに必要な権限](#)」を参照してください。

OMIVV アプライアンスは、OMIVV のインストール後に登録できます。OMIVV は、管理者ユーザー アカウント、または vCenter を操作するのに必要な権限を持つ管理者以外のユーザー アカウントを使用します。単一の OMIVV アプライアンス インスタンスは、15 台の vCenter サーバーおよび最大 2000 の ESXi ホストをサポートできます。

新規 vCenter サーバーを登録するには、次の手順を実行します。

1. <https://<アプライアンスIP/ホスト名/>> に移動します。
2. [ **vCenter 登録** ] ページの右ペインで、[ **新規 vCenter サーバーの登録** ] をクリックします。  
[ **新規 vCenter サーバーの登録** ] ページが表示されます。
3. [ **新規 vCenter の登録** ] ダイアログ ボックスの [ **vCenter 名** ] で、次のタスクを実行します。
  - a) [ **vCenter Server IP またはホスト名** ] ボックスに vCenter IP アドレスまたはホストの FQDN を入力します。  
Dell EMC では、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ています。すべての登録において、vCenter のホスト名は DNS サーバーで正しく解決される必要があります。次に、DNS サーバを使用する際のベストプラクティスを示します。
    - ・ DNS に正しく登録されている OMIVV アプライアンスを展開する場合は、静的 IP アドレスとホスト名を割り当てます。静的 IP アドレスを割り当てると、システムが再起動しても、OMIVV アプライアンスの IP アドレスは変わりません。
    - ・ OMIVV のホスト名情報が、DNS サーバーの前方ルックアップゾーンと逆引きルックアップゾーンの両方にあることを確認します。
  - b) [ **説明** ] ボックスに、説明を入力します ( オプション ) 。
4. **vCenter ユーザーアカウント** で、次の手順を実行します
  - a) [ **vCenter ユーザー名** ] ボックスに、管理者のユーザー名または必要な権限のある管理者以外のユーザー名を入力します。
  - b) [ **パスワード** ] ボックスにパスワードを入力します。
  - c) [ **パスワードの確認** ] ボックスにパスワードを再度入力します。
  - d) [ **vSphere Lifecycle Manager の登録** ] 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。
5. **登録** をクリックします。

vCenter サーバーを登録した後は、OMIVV が vCenter プラグインとして登録され、「Dell EMC OpenManage Integration」アイコンが vSphere WebClient に表示されます。この WebClient から OMIVV 機能にアクセスできます。

**① 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。

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 はデルの権限のみを持っているとします。ユーザー Y は vCenter にログインでき、OMIVV からファームウェアアップデートタスクをトリガできます。ファームウェアのアップデートタスクの実行中に、OMIVV はユーザー X の権限を使用して、ホストをメンテナンスモードにするか再起動します。

**① メモ:** カスタマイズした証明書署名要求 ( CSR ) を OMIVV にアップロードする必要がある場合、vCenter の登録前に、必ず新しい証明書をアップロードしてください。vCenter 登録後に新しいカスタム証明書をアップロードすると、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。

# 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、「[セキュリティの役割および許可](#)」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。

## 登録済み vCenter サーバーの SSL 証明書のアップデート

OpenManage Integration for VMware vCenter は、OpenSSL API と 2,048 ビットキー長の RSA 暗号化標準を使用して、証明書署名要求 (CSR) を生成します。

OMIVV によって生成された CSR は、信頼された認証局からデジタル署名付き証明書を取得します。OMIVV は、Web サーバーで SSL を有効にし、デジタル証明書を使用したセキュアな通信を行います。

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

1. `https://<アプライアンスIP>/ホスト名/<` に移動します。

2. 左ペインで、**VCENTER** の登録をクリックします。  
登録済み vCenter サーバーが作業中のペインに表示されます。
3. vCenter サーバー IP またはホスト名の証明書を更新するには、[ **アップデート** ] をクリックします。

## vCenter ログイン認証情報の変更

vCenter ログイン認証情報は、管理権限を持つユーザー、または必要な権限を持つ非管理者ユーザーが変更できます。

クラスターで Proactive HA 機能が有効になっている場合は、関連付けられているユーザーを変更しないでください。別の vCenter ユーザーの登録を変更すると、Proactive HA 機能が中断されます。資格情報に変更が必要な場合は、古い資格情報の登録を解除し、新しい資格情報を使用して登録します。



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て、[ **ログイン** ] をクリックします。
3. 左ペインで、**VCENTER** の登録をクリックします。  
登録済み vCenter サーバーが作業中のペインに表示されます。
4. [ **ユーザーアカウントの変更** ] ウィンドウを開くには、[ **資格情報** ] で、登録済み vCenter 用の [ **変更** ] をクリックします。
5. 誤った認証情報を入力すると、メッセージが表示されます。有効な vCenter ユーザー名、パスワードを入力し、パスワードを再入力して確認します。
6. パスワードを変更するには、[ **適用** ] をクリックします。アップデートをキャンセルするには、[ **キャンセル** ] をクリックします。

## OpenManage Integration for VMware vCenter の登録解除

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


クラスターで Proactive HA を有効にしたことがある場合は、Proactive HA がクラスター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。

## 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

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。

## OMIVV アプライアンスの管理

OMIVV アプライアンスの管理により、OpenManage Integration for VMware vCenter のネットワーク、NTP および HTTPS 情報を管理できます。これによって、管理者は次の操作ができます。

- ・ OMIVV アプライアンスを再起動します。「[OMIVV アプライアンスの再起動](#)」を参照してください。
- ・ OMIVV アプライアンスのアップデートとアップデート リポジトリの場所の設定。参照先 [OMIVV アプライアンスとリポジトリ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。「[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。
- ・ 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。
- ・ トラブルシューティング バンドルの生成とダウンロード。「[トラブルシューティング バンドルの生成とダウンロード](#)」を参照してください。
- ・ HTTP プロキシの設定。「[HTTP プロキシの設定](#)」を参照してください。
- ・ ネットワーク タイム プロトコル サーバーの設定。「[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。
- ・ 展開モードの設定。「[展開モードの設定](#)」を参照してください。
- ・ 拡張モニタリングについては、「[拡張モニタリング](#)」を参照してください。
- ・ 証明書署名要求 (CSR) の生成。「[証明書署名要求 \(CSR\) の生成](#)」を参照してください。
- ・ HTTPS 証明書のアップロード。「[HTTPS 証明書のアップロード](#)」を参照してください。
- ・ グローバル アラートの設定。「[グローバル アラートの設定](#)」を参照してください。

## アプライアンス管理へのアクセス

OpenManage Integration for VMware vCenter で次の手順を実行し、管理ポータルを使用して [ アプライアンス管理 ] 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. アプライアンス管理セクションを設定するには、左側のペインで **アプライアンス管理** をクリックします。


## OMIVV アプライアンスの再起動

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

## OMIVV アプライアンスとリポジトリ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。「[HTTP プロキシの設定](#)」を参照してください。
- ・ **リポジトリバスのアップデート** 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。「 <a href="#">RPMを使用したOMIVVアプライアンスのアップグレード</a> 」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。「 <a href="#">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</a> 」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。

- 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。

## OMIVV アップグレード オプション

### バックアップおよび復元

OMIVV 4.3以降から最新バージョンにバックアップおよび復元を実行できます (vCenter 6.5以降で)。


### RPM アップグレード

OMIVV 5.0以降から最新バージョンにRPM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

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。

- [ [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。「[HTTPプロキシの設定](#)」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。


- 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。

- 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。
- 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。
- [ [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。
- 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、「[」を参照してください。『インストール ガイド』の「インストールの検証」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、『[非対応ホストの修正](#)』の「[」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。

## 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 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。

- [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。
- [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。
- 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。
- 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、「」を参照してください。インストール ガイドの「インストールの検証」トピック

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。

- [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。
- [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。

## トラブルシューティング バンドルの生成とダウンロード

トラブルシューティング バンドルを生成するには、管理者ポータルにログインしていることを確認してください。

トラブルシューティング バンドルには、問題の解決やテクニカル サポートへの送信に役立つ OMIVV のログ情報が含まれています。

- [アプライアンスの管理] ページで、[トラブルシューティング バンドルの生成] をクリックします。
- [トラブルシューティング バンドルのダウンロード] をクリックします。

## HTTP プロキシの設定

- [アプライアンス管理] ページで、[HTTP プロキシ設定] にスクロールダウンし、[編集] をクリックします。
- 有効** を選択して HTTP プロキシ設定の使用を有効にします。
- プロキシサーバアドレス** に、プロキシサーバのアドレスを入力します。
- プロキシサーバポート** に、プロキシサーバのポートを入力します。
- プロキシ資格情報を使用するには **はい** を選択します。
- プロキシ資格情報を使用している場合は、**ユーザー名** にユーザー名を入力します。
- パスワード** にパスワードを入力します。
- 適用** をクリックします。

## ネットワーク タイム プロトコル (NTP) サーバーのセットアップ

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。

- 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。
- 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。
- 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。

## 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。メモリー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 2. 展開モードのシステム要件

展開モード	ホストの数	CPU の数	メモリー (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せん。

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。

- [ **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。
- 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。
- [ **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。
- 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に必要な 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。
- 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

- 管理コンソールにログインします。
- 展開モードを必要なレベルに変更します。
- 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。
- OMIVV アプライアンスの電源を入れます。

## 展開モードのアップグレード

- デル管理ポータルにログインする前に、ブラウザのキャッシュをクリアします。
- OMIVV アプライアンスの電源を入れます。
- 管理コンソールにログインします。
- 展開モードを必要なレベルに変更します。

## 拡張モニタリング

vRealize Operations Manager 用 OpenManage Management Pack をサポートする場合は、拡張モニタリングが有効になっていることを確認します。拡張モニタリングは、「中規模」導入モードで実行することをお勧めします。

vRealize Operations Manager 用 OpenManage Management Pack で SNMP アラートをサポートする場合は、SNMP トラップモニタリングが有効になっていることを確認します。これで、ユーザーはサーバやシャーシの稼働状態をリアルタイムでモニタリングできるようになります。

1. <https://<アプライアンスIP/ホスト名/>>に移動します。
2. 左ペインで **アプライアンス管理** をクリックします。
3. [ **アプライアンス管理** ] ページで、[ **拡張モニタリング** ] までスクロール ダウンします。
4. 拡張モニタリング設定を編集するには、[ **編集** ] をクリックします。
5. 編集モードで、拡張モニタリングと SNMP トラップ モニタリングを有効または無効にして、[ **適用** ] をクリックします。

## 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。

## グローバル アラートの設定

アラート管理では、すべての vCenter インスタンスを対象として、アラートを OMIVV に保存する方法をグローバルに設定できます。

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 **アラート管理** をクリックします。新規の vCenter アラート設定を入力するには、**編集** をクリックします。
4. 次のフィールドに数値を入力します。  
デフォルトでは、現在のアラート数が表示されます。
  - ・ **最大アラート数**
  - ・ **アラートの保持日数**
  - ・ **重複アラートのタイムアウト時間 ( 秒 )**
5. これらの設定を保存するには、[ **適用** ] をクリックします。

## OMIVV VM コンソールについて

OMIVV VM コンソールは仮想マシン上の vSphere クライアント内にあります。コンソールは管理コンソールと連動します。コンソールを使用して、次のタスクを実行できます。

- ・ ネットワークの設定構成
- ・ OMIVV アプライアンスのパスワードの変更
- ・ NTP の設定とローカル タイム ゾーンの設定
- ・ OMIVV アプライアンスを再起動します。
- ・ OMIVV アプライアンスの工場出荷時設定へのリセット
- ・ 読み取り専用の役割でのログイン
- ・ コンソールからログアウトする

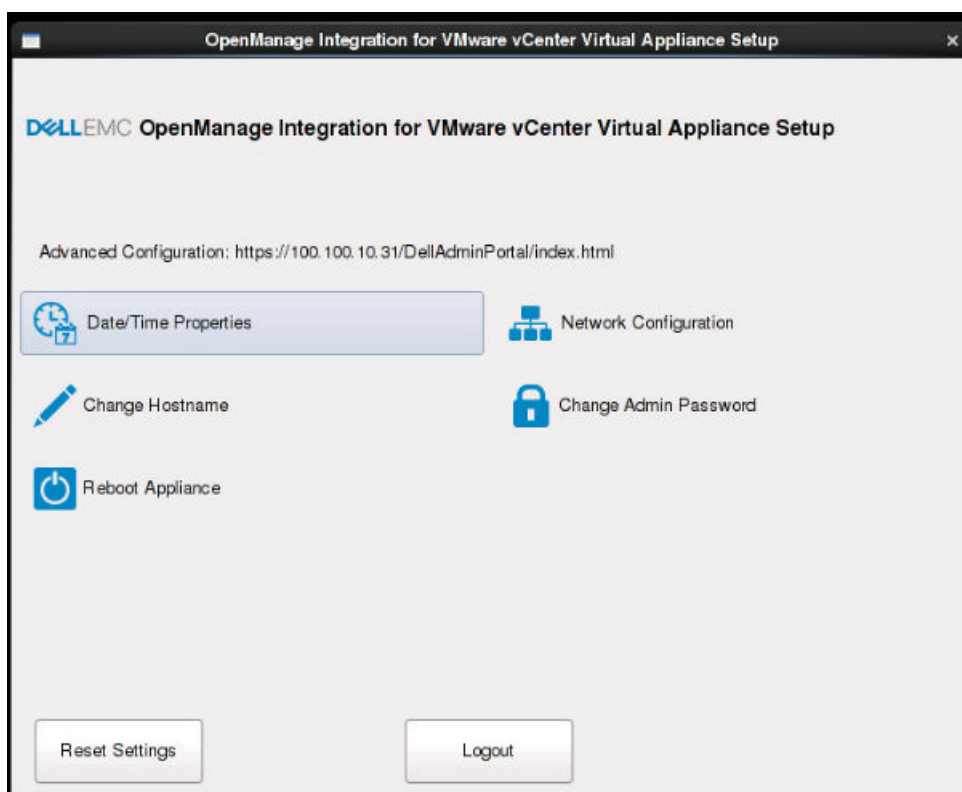
## OMIVV VM コンソールを開く

OMIVV VM コンソールを開くには、OMIVV アプライアンスの Web コンソールまたはリモート コンソールを起動します。

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

## 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、OpenManagement 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。

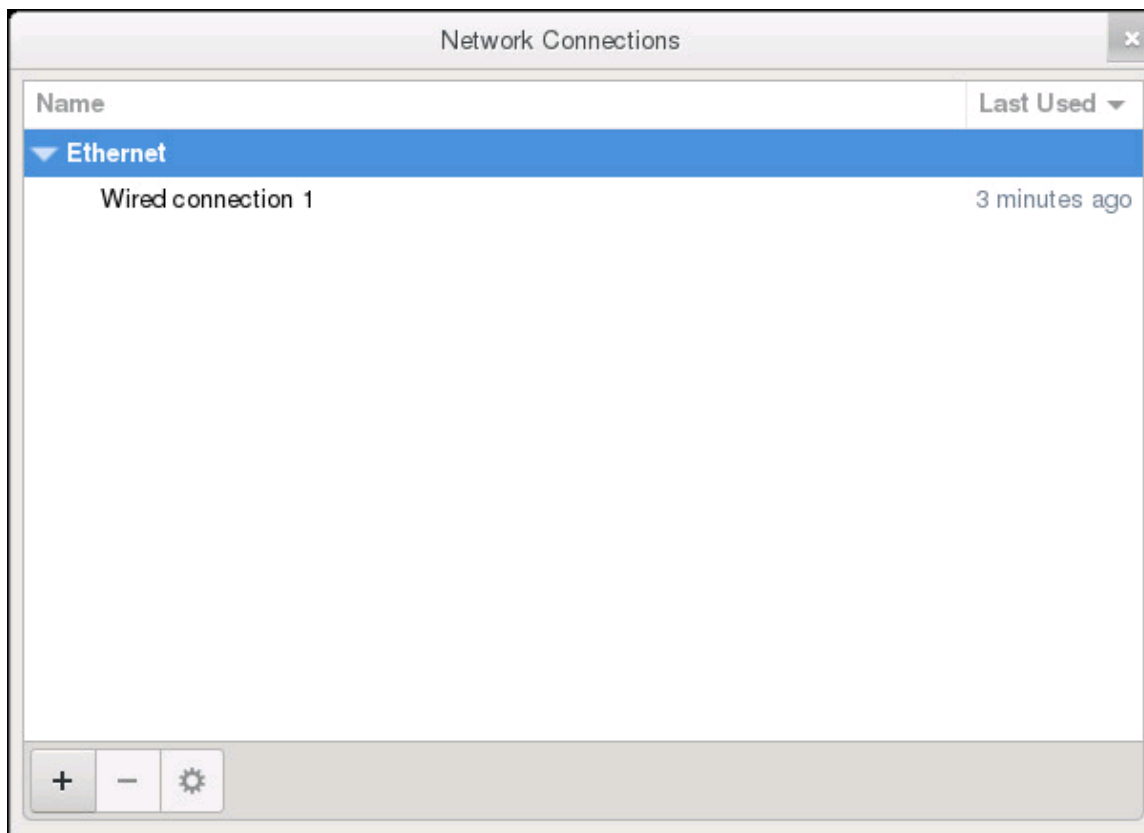
vSphere 環境での Dell EMC サーバーの管理において OMIVV は、vSphere ネットワーク (vCenter と ESXi 管理ネットワーク) と、アウトオブバンド ネットワーク (iDRAC、CMC、OME-Modular) の両方へのアクセスを必要とします。


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。

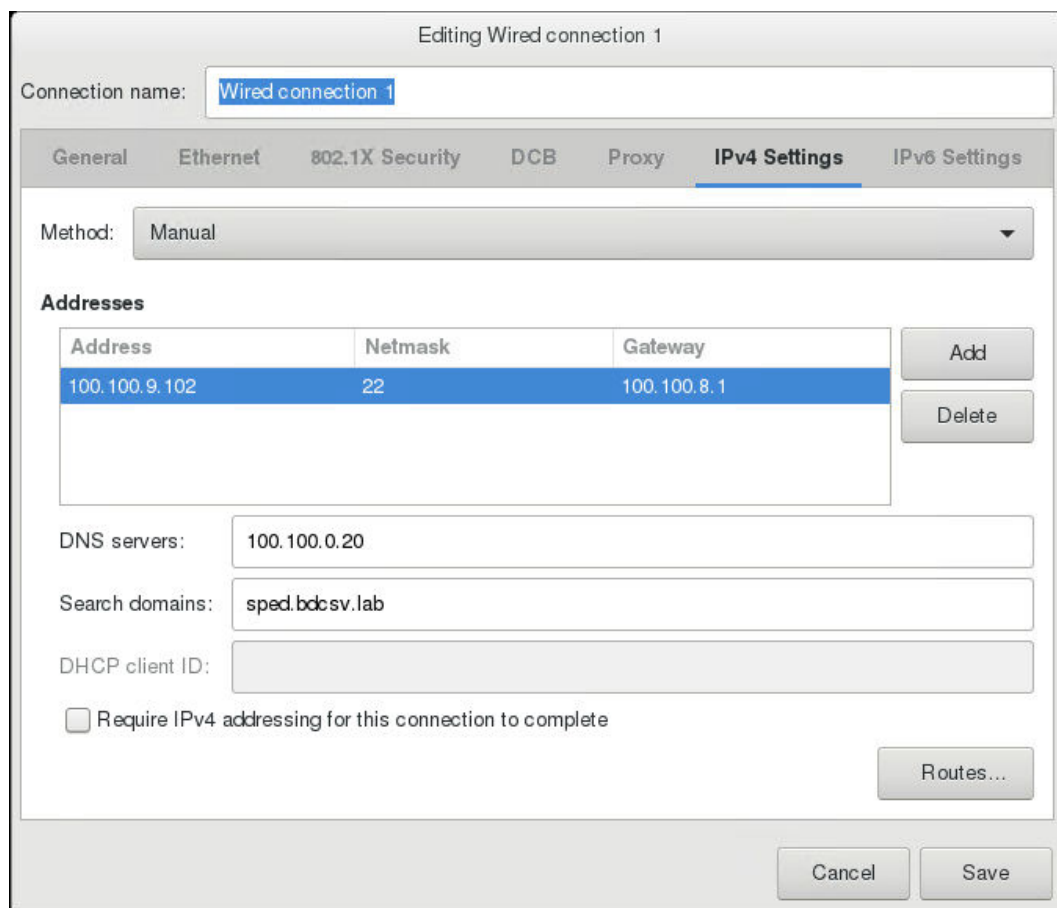
アウトオブバンド ネットワークへのアクセスが vSphere ネットワークを使用して行える場合、OMIVV アプライアンス用に 2 つのネットワーク アダプターを設定しないでください。2 つ目の NIC の設定の詳細については、「[2 つのネットワーク インターフェイス コントローラー \(NIC\) を用いた OMIVV アプライアンスの設定](#)」を参照してください。



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 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

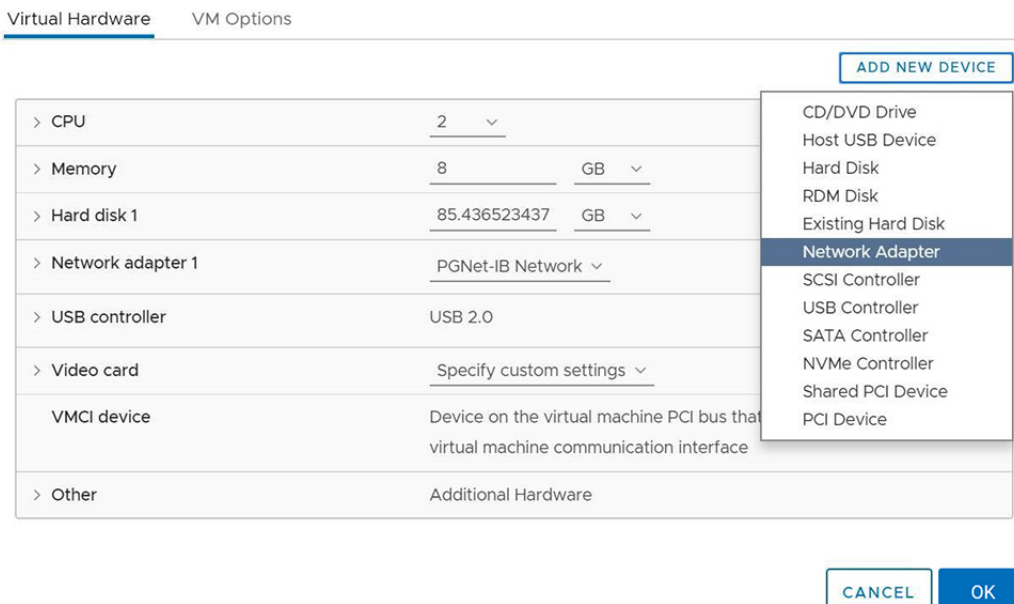
vSphere 環境での Dell EMC サーバーの管理において OMIVV は、vSphere ネットワーク (vCenter と ESXi 管理ネットワーク) と、アウトオブバンド ネットワーク (iDRAC、CMC、OME-Modular) の両方へのアクセスを必要とします。vSphere ネットワークとアウトオブバンド ネットワークが別のネットワークとして維持されている環境の場合、OMIVV は両方のネットワークへのアクセスを必要とします。そうした場合、OMIVV アプライアンスの設定は2つの NIC で行う必要があります。帯域外ネットワークへのアクセスが vSphere ネットワー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

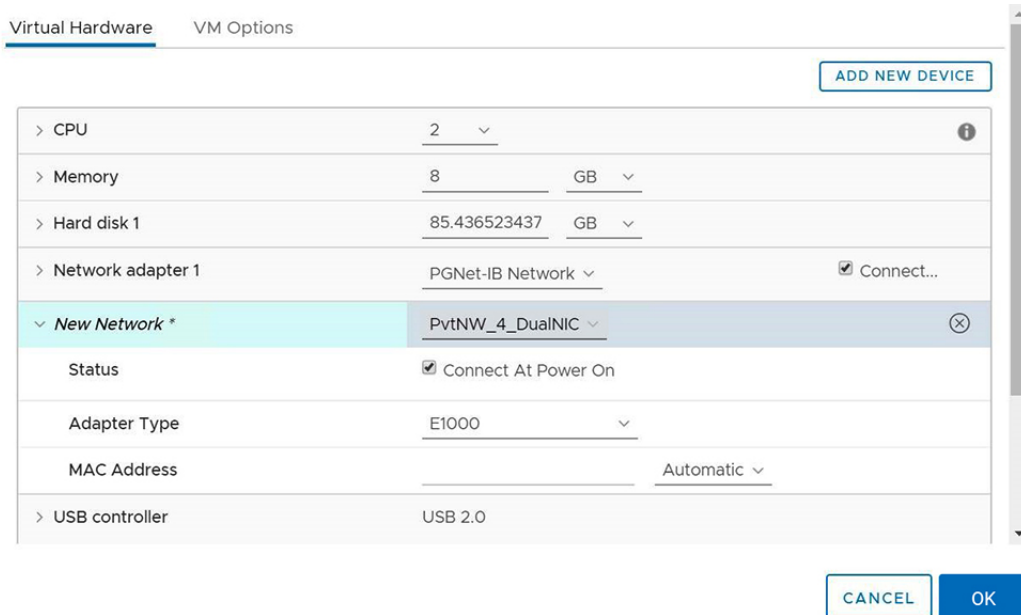
1. OMIVV アプライアンスの電源を切ります。

- 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。
- [ 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。

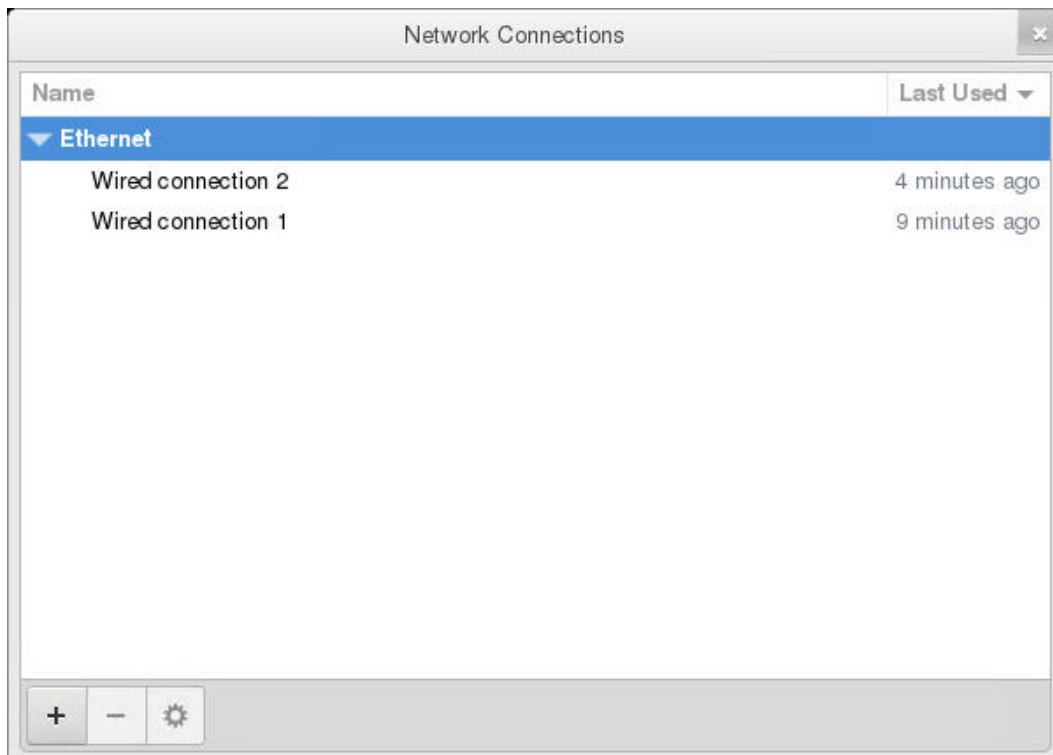



- NIC に適したネットワークを選択し、[ 電源投入時に接続する ] チェック ボックスを選択します。
- ドロップダウン メニューから [ VMXNET3 ] アダプタータイプを選択します。

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



- 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。
- [ 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。

Editing Wired connection 1

Connection name:

General   Ethernet   802.1X Security   DCB   Proxy   **IPv4 Settings**   IPv6 Settings

Method:

**Addresses**

Address	Netmask	Gateway
192.168.40.20	24	192.168.40.1

Add  
Delete

DNS servers:

Search domains:

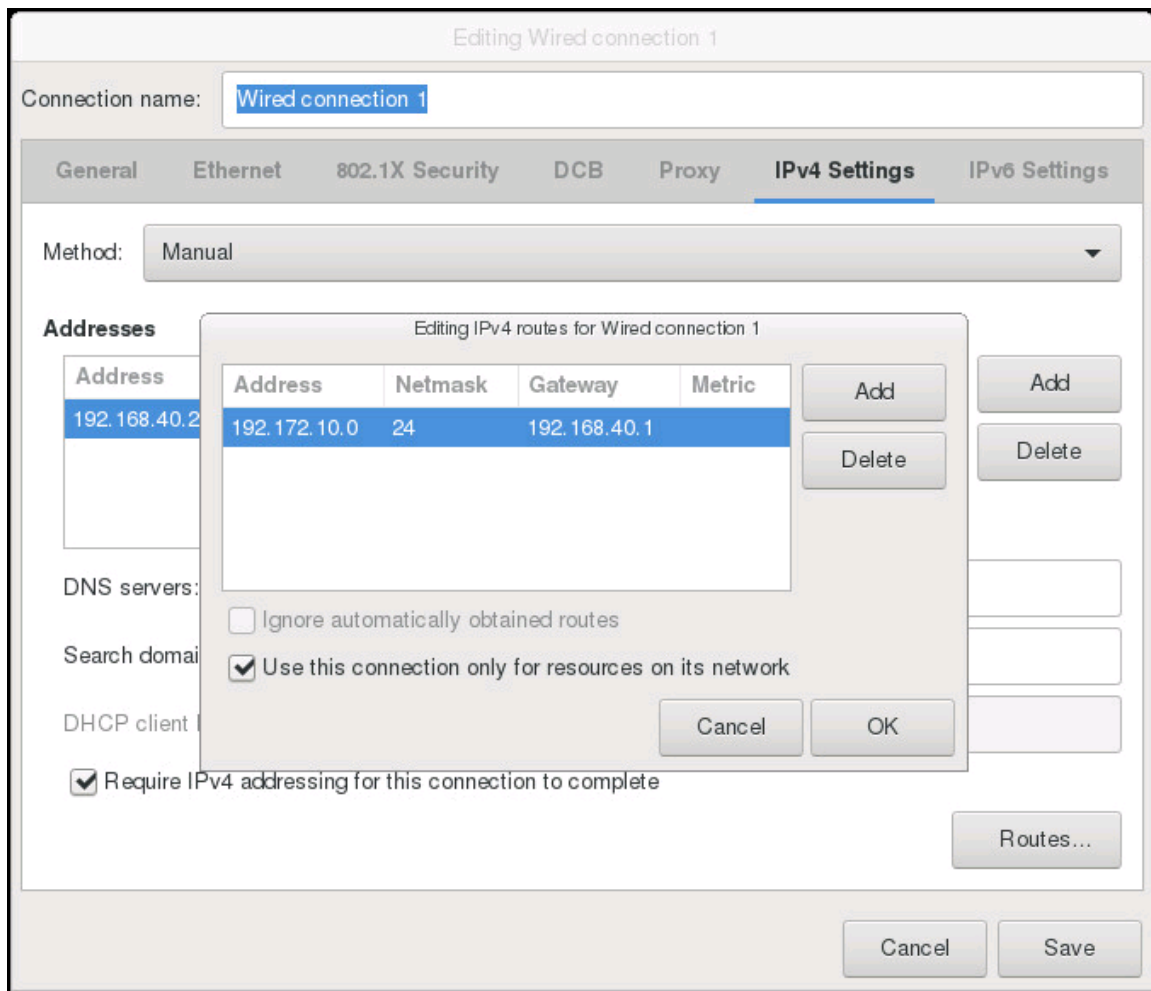
DHCP client ID:

Require IPv4 addressing for this connection to complete

Routes...

Cancel   Save

- 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。
- i** **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。
- i** **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ー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。

## 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。

## 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。

# ダッシュボードを使用したホストとシャーシの監視

ダッシュボードには次の項目が表示されます。

- ・ ホストとシャーシの正常性状態
- ・ ホストとシャーシの保証ステータス
- ・ ホストと vCenter のライセンス情報
- ・ ホストの設定コンプライアンス ステータス
- ・ OMIVV を使用してスケジュール設定されたジョブの状態
- ・ 展開可能なベアメタル サーバー
- ・ OMIVV 機能に関するクイック リファレンス

## 正常性

[ 正常性 ] セクションには、OMIVV で管理されるすべてのホストとシャーシの正常性が表示されます。ここに表示されるすべてのホストは、同じプラットフォーム サービス コントローラー ( PSC ) を使用して構成されます。

ホストおよびシャーシからの定期的な正常性メトリック タスクまたは SNMP イベントの完了後、各ホストおよびシャーシのステータスが更新されます。

次のリストでは、ホストとシャーシのさまざまな状態について説明しています。

- ・ **正常** — 正常な状態のホストとシャーシの数を表示します。
- ・ **警告** — 対応処置が必要だが、すぐにシステムに影響を与えないホストとシャーシの数を表示します。
- ・ **重要** — ホストまたはシャーシ内の1つ以上のコンポーネントに重大な問題があるホストとシャーシの数を表示します。これらは直ちに処置が必要です。
- ・ **不明** — 不明な状態のホストとシャーシの合計数を表示します。ホストまたはシャーシに到達できない、または正常性状態が不明の場合、ホストまたはシャーシには [ 不明 ] の状態が表示されます。

ホストの詳細情報を表示するには、[ ダッシュボード ] ページの [ 正常性 ] セクションで [ ホストの表示 ] をクリックします。

シャーシの詳細情報を表示するには、[ ダッシュボード ] ページの [ 正常性 ] セクションで [ シャーシの表示 ] をクリックします。

## 保証

この保証カテゴリーに表示されるホストの数は、PSC を使用して設定された vCenter サーバーに属するホストを示します。ホストとシャーシに関する保証情報を取得するには、[ 設定 ] ページで保証期限通知を有効にします。

[ 保証 ] セクションには、ホストとシャーシに関する次の情報が記載されています。

- ・ **正常** — 残りの保証日数が警告しきい値を超えているホストとシャーシの数を表示します。
- ・ **警告** — 残りの保証日数が警告しきい値を下回っているホストとシャーシの数を表示します。
- ・ **重要** — 残りの保証日数が重大しきい値を下回っているホストとシャーシの数を表示します。
- ・ **不明** — 保証が不明なホストとシャーシの数が表示されます。

## ライセンス

[ ライセンス ] セクションには、次の情報が表示されます。

- ・ 使用可能なホストおよび vCenter ライセンスの合計数
- ・ 使用中のホストおよび vCenter ライセンスの合計数。

ライセンスを購入するには、[ ダッシュボード ] ページの [ ライセンス ] セクションで [ ライセンスの購入 ] をクリックします。

# 導入準備

ベアメタル サーバーの数には、OMIVV を使用して検出された対応ベアメタル サーバーのみが表示されます。ベアメタル サーバーを導入するには、[ 導入 ] をクリックします。

# 設定コンプライアンス

[ 設定コンプライアンス ] セクションには、クラスター プロファイルに関連付けられているクラスターの一部であるホストが表示されます。ここに表示されるホストは、同じプラットフォーム サービスコントローラ (PSC) を使用して構成されます。ホストの設定コンプライアンスのステータスを表示するには、[ 対応性の表示 ] をクリックします。

# ジョブ

[ ジョブ ] セクションには、OMIVV を使用してスケジュールされたジョブが表示されます。過去7日間のジョブの詳細のみ表示されます。円グラフには、[ 成功 ]、[ 進行中 ]、[ 失敗 ]、[ スケジュール済み ]、および [ キャンセル済み ] ステータスのジョブの合計数が表示されます。ファイラーを使用して円グラフからジョブ ステータスを削除するには、ジョブ ステータスをクリックします。

次のジョブについて、さまざまなタイプのジョブを表示できるほか、[ 成功 ]、[ 進行中 ]、[ 失敗 ]、[ スケジュール済み ]、[ キャンセル済み ] のステータスにあるジョブの合計数を表示できます。

- ・ 展開ジョブ  
詳細については、次を参照してください：[展開ジョブ](#)
- ・ ホスト ファームウェア アップデート ジョブ  
詳細については、次を参照してください：[ホスト ファームウェア アップデート ジョブ](#)
- ・ シャーシ ファームウェア アップデート ジョブ  
詳細については、次を参照してください：[シャーシ ファームウェア アップデート ジョブ](#)
- ・ システム ロックダウン ジョブ  
詳細については、次を参照してください：[システムロックダウンモードジョブ](#)

すべてのジョブのステータスを表示するには、[ 表示 ] をクリックします。

# クイック リファレンス

このセクションでは、次の機能についてのクイック リファレンスを提供します。

- ・ 初期設定ウィザードの開始。参照先 [初期設定](#)
- ・ ホスト認証情報プロファイル。参照先 [ホスト認証情報プロファイル](#)
- ・ 管理対応性。参照先 [管理対応性](#)
- ・ シャーシ認証情報プロファイル。参照先 [シャーシ認証情報プロファイル](#)
- ・ クラスター プロファイル。参照先 [クラスタープロファイル](#)
- ・ 展開。参照先 [導入](#)

# ホスト認証情報プロファイルを使用したホストの管理

## ホスト認証情報プロファイル

ホスト認証情報プロファイルには、OMIVV がサーバーに接続する際に使用する iDRAC およびホストの認証情報が保存されます。OMIVV は、ホスト認証情報プロファイルに関連付けられているホストを管理します。単一のホスト認証情報プロファイルに複数のサーバーを関連付けることができます。

PowerEdge MX シャーシ ホストは、単一の統合シャーシ管理 IP を使用して管理できます。iDRAC IP が無効になっている PowerEdge MX シャーシに存在するホストは、シャーシ認証情報プロファイルを使用して管理する必要があります。シャーシ認証情報プロファイルを使用して PowerEdge MX シャーシを管理する方法については、「[シャーシ認証情報プロファイルの作成](#)」を参照してください。すべての OMIVV 機能を利用するために、ホスト認証情報プロファイルを使用して iDRAC IP で PowerEdge MX シャーシ ホストを管理することをお勧めします。

## 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使用を推奨す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。ESXi 6.7以降では、有効なパスワードの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。

- [ **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。
- [ **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。

- 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、ESXi 6.5 以降を実行中のホストの iDRAC IP を取得してから無効化します。

**メモ:** 有効な認証情報を入力した後で、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。

- [ **終了** ] をクリックします。

## ホスト認証情報プロファイルの編集

複数のホスト認証情報プロファイルの認証情報を一度に編集できます。

- [ **名前と認証情報** ] ページで、次の手順を行います。

- プロファイル名および説明を編集します。
- [ **iDRAC 資格情報** ] 領域で、iDRAC のローカル認証情報または AD 認証情報を編集します。
  - iDRAC のローカル認証情報を変更するには、次のタスクを実行します。
    - [ **ユーザー名** ] ボックスでユーザー名を変更します。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、[dell.com/support](https://dell.com/support) にある『iDRAC ユーザーズガイド』を参照してください。
    - パスワードを変更します。
    - 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** ] チェック ボックスを選択します。

- AD ですすでに設定および有効化されている iDRAC の認証情報を変更するには、[ **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** ] ボックスでユーザー名を変更します。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。ユーザー名の定義の詳細については、『*Microsoft Active Directory マニュアル*』を参照してください。
  - ・ パスワードを変更します。
  - ・ 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** ] チェック ボックスを選択します。
- c) [ **ホスト ルート** ] 領域で、ホストのローカル認証情報と 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変更するには、次のいずれかを実行します。
    - ・ 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。ESXi 6.7 以降では、有効なパスワードの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、[ **証明書チェックを有効にする** ] チェック ボックスを選択します。
  - ・ AD に対して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変更するには、[ **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** ] ボックスでユーザー名を変更します。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。
    - ・ パスワードを変更します。
    - ・ 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。
2. [ **次へ** ] をクリックします。  
[ **関連ホスト** ] ページが表示されます。
3. 関連ホスト リストにホストを追加または削除するには、[ **関連ホスト** ] ページで [ **ホストの追加** ] をクリックします。
- i** **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。
4. 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、[ **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。
- i** **メモ:** 有効な認証情報を入力した後で、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。
- テスト接続中、OMIVV は WBEM サービスを有効にし、ESXi 6.5 以降を実行中のホストの iDRAC IP を取得してから無効化します。
5. [ **終了** ] をクリックします。
- i** **メモ:** [ **変更日** ] と [ **最終変更者** ] フィールドには、ホスト認証情報プロファイルの vSphere Client インターフェイスを介して実行する変更が含まれます。OMIVV アプライアンスのそれぞれのホスト認証情報プロファイルに対して実行するすべての変更は、これら 2 個のフィールドには影響しません。

## ホスト認証情報プロファイルの表示

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。テーブルに、次の情報と共にすべてのホスト認証情報プロファイルが表示されます。
- ・ [ **プロファイル名** ]: ホスト認証情報プロファイルの名前
  - ・ [ **説明** ]: プロファイルの説明 ( 入力されている場合 )
  - ・ [ **vCenter** ]: 関連付けられている vCenter の FQDN、ホスト名、または IP アドレス
  - ・ [ **関連ホスト** ]: ホスト認証情報プロファイルに関連付けられているホスト。関連付けられているホストが複数ある場合、展開アイコンを使ってすべて表示します。
  - ・ [ **iDRAC 証明書チェック** ]: ホスト認証情報プロファイルの作成時に iDRAC 証明書が検証されているかどうかを示します。
  - ・ [ **ホスト ルート証明書チェック** ]: ホスト認証情報プロファイルの作成時にホスト ルート証明書が検証されているかどうかを示します。

- ・ [ **作成日** ]: ホスト認証情報プロファイルが作成された日付。
- ・ [ **変更日** ]: ホスト認証情報プロファイルが変更された日付。
- ・ [ **最終変更者** ]: ホスト認証情報プロファイルを変更したユーザーの詳細。

**i** **メモ:** PowerEdge MX ホストがシャーシ認証情報プロファイルを使用して管理されている場合、OMIVV はそれがシャーシ認証情報プロファイルに関連付けられていることを示します。詳細については、次を参照してください: [シャーシ認証情報プロファイルの表示](#)

2. ウィザードの列名の削除または追加を行うには、をクリックします。  
デフォルトでは、[ **変更日** ] 列および [ **最終変更日** ] 列は選択されていません。これらのカラムを選択するには、をクリックします。
3. ホスト認証情報プロファイルの情報をエクスポートするには  をクリックします。

## ホスト認証情報プロファイルのテスト

認証情報プロファイルのテスト機能を使用して、ホストおよび iDRAC の認証情報をテストできます。すべてのホストを選択することをお勧めします。

1. OMIVV ホーム ページで、ホストに関連付けられているホスト認証情報プロファイルを選択して [ **テスト** ] をクリックします。  
[ **ホスト認証情報プロファイルのテスト** ] ページが表示されます。
2. 関連付けられているホストをすべて選択して、[ **テストを開始** ] をクリックします。
  - a) テスト接続を中止するには、[ **テストの中止** ] をクリックします。  
iDRAC とホストの両方の認証情報について、テスト接続の結果が表示されます。

## ホスト認証情報プロファイルの削除

インベントリ、保証、または展開ジョブが実行中の場合は、ホストに関連付けられているホスト認証情報プロファイルを削除しないでください。

OMIVV では、削除したホスト認証情報プロファイルの一部であるホストについては、それらのホストが別のホスト認証情報プロファイルに追加されるまで管理しません。

1. [ **ホスト認証情報プロファイル** ] ページでプロファイルを選択して [ **削除** ] をクリックします。
2. 確認を促すプロンプトが表示されたら、[ **削除** ] をクリックします。  
選択したプロファイルが、ホスト認証情報プロファイルのリストから削除されます。

# シャーシ認証情報プロファイルを使用したシャーシの管理

## シャーシ認証情報プロファイル

シャーシ認証情報プロファイルには、OMIVV がシャーシとの通信に使用するシャーシ認証情報が保存されます。OMIVV は、シャーシ認証情報プロファイルに関連付けられているシャーシを管理および監視します。単一のシャーシ認証情報プロファイルに複数のシャーシを割り当てることができます。

PowerEdge MX シャーシ ホストは、単一の統合シャーシ管理 IP を使用して管理できます。iDRAC IP が無効になっている PowerEdge MX シャーシに存在するホストは、シャーシ認証情報プロファイルを使用して管理する必要があります。すべての OMIVV 機能を利用するために、ホスト認証情報プロファイルを使用して iDRAC IP で PowerEdge MX シャーシ ホストを管理することをお勧めします。MX シャーシの管理の詳細については、「[PowerEdge MX シャーシの管理](#)」を参照してください。

## シャーシ認証情報プロファイルの作成

- ・ シャーシ資格情報プロファイルを作成するには、次の権限が必要です。
    - ・ M1000e、VRTX、および FX2 シャーシ：SNMP トラップ送信先の読み取りと設定
    - ・ PowerEdge MX シャーシ：管理者
  - ・ 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。
    - ・ CMC または OME モジュールは、AD ベースの認証用に設定されています。
1. OMIVV ホーム ページで、[ 対応性と導入 ] > [ シャーシ認証情報プロファイル ] > [ 新規プロファイルを作成 ] をクリックします。
  2. ウィザードの [ シャーシ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。
  3. [ 名前と認証情報 ] ページで、次の手順を行います。
    - a) プロファイル名と説明を入力します。説明はオプションです。
    - b) [ 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 Chassis Management Controller (CMC) または OpenManage Enterprise-Modular (OME-Modular) へのログインに通常使用されるものです。
    - c) パスワード テキストボックスにパスワードを入力します。
    - d) [ 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一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。
  4. [ シャーシの選択 ] ページで [ IP/ホスト名 ] 列の横にあるチェック ボックスを使用して、個々のシャーシまたは複数のシャーシを選択し、[ OK ] をクリックします。
 

選択したシャーシが [ 関連付けられたシャーシ ] ページに表示されます。関連するシャーシ リストからシャーシを追加または削除するには、[ シャーシの追加 ] をクリックします。

選択したシャーシがすでにシャーシ認証情報プロファイルに関連付けられている場合、次のメッセージが表示されます。「別のプロファイルに現在関連付けられているシャーシを選択すると、そのシャーシ認証情報プロファイルからそのシャーシが削除されます。シャーシに関連付けられていないシャーシ認証情報プロファイルは削除されます。」

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。

テスト接続は、選択したシャーシに対して自動的に実行されます。

テスト接続は、次のタイミングで自動的に実行されます。

- ・ シャーシを初めて選択した後。
- ・ 資格情報を変更したとき
- ・ シャーシを新たに選択したとき

[ **テスト結果** ] セクションに、テスト結果が [ **合格** ] または [ **不合格** ] と表示されます。シャーシ接続を手動でテストするには、シャーシを選択して、[ **テストの開始** ] をクリックします。

MCM グループで構成された PowerEdge MX シャーシの場合、リード シャーシを使用して、すべてのリードおよびメンバー シャーシを管理することをお勧めします。メンバー シャーシのテスト接続操作が失敗し、テスト結果のステータスが不合格と表示されます。リード シャーシの IP リンクが表示されます。リード シャーシの IP リンクをクリックして、MCM グループ全体を検出します。

**i** **メモ:** 追加した PowerEdge MX シャーシに関連付けられている登録済みの vCenter にホストが存在しない場合、シャーシのテスト接続は失敗します。

**i** **メモ:** 正常に検証されたシャーシのみがシャーシ認証情報プロファイルに関連付けられます。

5. **終了** をクリックします。

ウィザードのタスクを完了するには、検証が成功したシャーシが少なくとも1台はあることを確認してください。

PowerEdge MX シャーシを追加するには、[PowerEdge MX シャーシの追加](#)を参照してください。

## シャーシ認証情報プロファイルの編集

1. OMIVV ホーム ページで、[ **対応性と導入** ] > [ **シャーシ認証情報プロファイル** ] をクリックします。

2. [ **シャーシ認証情報プロファイル** ] ページで [ **編集** ] をクリックします。

3. [ **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編集します。説明はオプションです。

b) [ **ユーザー名** ] テキストボックスで、管理者権限のあるユーザー名を変更します。これはシャーシ管理コントローラー ( CMC ) または OpenManage Enterprise-Modular ( OME-Modular ) へのログインに通常使用されるものです。

c) [ **パスワード** ] テキスト ボックスでパスワードを変更します。

d) [ **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一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。

4. [ **シャーシの選択** ] ページで [ **IP/ホスト名** ] 列の横にあるチェック ボックスを使用して、シャーシを選択または削除し、[ **OK** ] をクリックします。

選択したシャーシが [ **関連付けられたシャーシ** ] ページに表示されます。関連するシャーシ リストからシャーシを追加または削除するには、[ **シャーシの追加** ] をクリックします。

選択したシャーシがすでにホスト認証情報プロファイルに関連付けられている場合、次のメッセージが表示されます。「別のプロファイルに現在関連付けられているシャーシを選択すると、そのシャーシ認証情報プロファイルからそのシャーシが削除されます。シャーシに関連付けられていないシャーシ認証情報プロファイルは削除されます。」

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。

テスト接続は、選択したシャーシに対して自動的に実行されます。

テスト接続は、次のタイミングで自動的に実行されます。

- ・ シャーシを初めて選択した後
- ・ 資格情報を変更したとき
- ・ シャーシを新たに選択したとき

[ **テスト結果** ] セクションに、テスト結果が [ **合格** ] または [ **不合格** ] と表示されます。シャーシ接続を手動でテストするには、シャーシを選択して、[ **テストの開始** ] をクリックします。

MCM グループで構成された PowerEdge MX シャーシの場合、リード シャーシを使用して、すべてのリードおよびメンバー シャーシを管理することをお勧めします。メンバー シャーシのテスト接続操作が失敗し、テスト結果のステータスが不合格と表示されます。リード シャーシの IP リンクが表示されます。リード シャーシの IP リンクをクリックして、MCM グループ全体を検出します。

**i** **メモ:** 追加した PowerEdge MX シャーシに関連付けられている登録済みの vCenter にホストが存在しない場合、シャーシのテスト接続は失敗します。

**i** **メモ:** 正常に検証されたシャーシのみがシャーシ認証情報プロファイルに関連付けられます。

5. **終了** をクリックします。

ウィザードのタスクを完了するには、検証が成功したシャーシが少なくとも1台はあることを確認してください。

PowerEdge MX シャーシを追加するには、「[PowerEdge MX シャーシの追加](#)」を参照してください。

# シャーシ認証情報プロファイルの表示

1つまたは複数のシャーシ認証情報プロファイルを作成した後、[シャーシ認証情報プロファイル] ページでシャーシおよび関連付けられたシャーシを表示できます。

1. OMIVV ホーム ページで、[対応性と導入] > [シャーシ認証情報プロファイル] をクリックします。

テーブルには、すべてのシャーシ認証情報プロファイルと次の情報が表示されます。

- ・ [プロファイル名]: シャーシ認証情報プロファイルの名前
- ・ [説明]: プロファイルの説明。
- ・ [シャーシ IP/ホスト名]: シャーシ IP またはホスト名のリンク

マルチシャーシ管理 (MCM) グループには、リード シャーシ () とメンバー シャーシ () が階層で表示されます。


**メモ:** MCM 構成の PowerEdge MX シャーシの場合、OMIVV はリード シャーシのみを使用してすべてのリード シャーシとメンバー シャーシを管理します。すべてのリードとメンバーは、リード シャーシが関連付けられている同じシャーシ認証情報プロファイルに関連付けられます。

IPv4 が無効にされている MCM グループ内のメンバー シャーシの場合、リードの IPv4 アドレスが、括弧内にメンバー シャーシのサービス タグと一緒に表示されます。

- ・ [シャーシ サービス タグ]: シャーシに割り当てられた固有の識別子。
- ・ [変更日]: シャーシ認証情報プロファイルが変更された日付。

2. 関連するホストについての次の情報が、下のグリッドに表示されます。

- ・ プロファイル名
- ・ 関連ホスト
- ・ サービスタグ
- ・ シャーシ IP/ホスト名
- ・ シャーシサービスタグ

3. シャーシ認証情報プロファイル情報をエクスポートするには、 をクリックします。

# シャーシ認証情報プロファイルのテスト

シャーシのテスト認証情報プロファイル機能を使用して、シャーシ認証情報プロファイルに関連付けられているシャーシの認証情報をテストできます。すべてのシャーシを選択することをお勧めします。

1. OMIVV ホーム ページで、[対応性と導入] > [シャーシ認証情報プロファイル] をクリックします。
2. シャーシ認証情報プロファイルを選択して、[テスト] をクリックします。
3. [シャーシ認証情報プロファイルのテスト] ページで関連付けられたシャーシを選択し、[テストを開始] をクリックします。
  - a) テスト接続を中止するには、[テストの中止] をクリックします。テストの結果が [テスト結果] 列に表示されます。

# シャーシ認証情報プロファイルの削除

シャーシ認証情報プロファイルを削除する前に、シャーシ インスタンスが OMIVV の登録された他の vCenter の一部ではないことを確認してください。

削除したシャーシ認証情報プロファイルに関連付けられているシャーシについては、他のシャーシ認証情報プロファイルに追加されない限り、OMIVV は当該のシャーシを監視しません。

1. OMIVV ホーム ページで、[対応性と導入] > [シャーシ認証情報プロファイル] > [削除] の順にクリックします。
2. 削除するシャーシ認証情報プロファイルを選択します。
3. 確認を促すプロンプトが表示されたら、[削除] をクリックします。

シャーシ認証情報プロファイルに関連付けられているすべてのシャーシが削除されるか、別のプロファイルに移動される場合、削除の確認メッセージが表示され、シャーシ認証情報プロファイルに関連付けられているシャーシが存在しないため、そのプロファイルが削除されることが示されます。シャーシ認証情報プロファイルを削除するには、削除の確認メッセージで [OK] をクリックします。

# リポジトリ プロファイルを使用したファームウェアおよびドライバー リポジトリの管理

## リポジトリ プロファイル

リポジトリ プロファイルを使用すると、ドライバーまたはファームウェア リポジトリを作成および管理できます。

ファームウェアおよびドライバー リポジトリ プロファイルを使用して、次の操作を実行できます。

- ・ ホストのファームウェアのアップデート
- ・ vSAN クラスターの一部であるホストのドライバーのアップデート。
- ・ クラスター プロファイルの作成とクラスターのベースライン化。

デフォルトの OMIVV ファームウェア カタログは次のとおりです。

- ・ **[ Dell EMC デフォルト カタログ ]**: Dell EMC オンライン カタログを使用して最新のファームウェア情報を取得する、工場で作成されたファームウェア リポジトリ プロファイルです。アプライアンスがインターネットに接続されていない場合は、ローカル CIFS、NFS、HTTP、または HTTPS ベースの共有を指すようにこのリポジトリを変更します。このカタログの変更の詳細については「[Dell デフォルト カタログの編集またはカスタマイズ](#)」を参照してください。

クラスター プロファイルに関連付けられていない vSphere ホストのファームウェアをアップデートするには、Dell EMC デフォルト カタログをデフォルト カタログとして選択できます。

- ・ **[ 検証済み MX スタック カタログ ]**: Dell EMC オンライン カタログを使用して、MX シャーシおよびその対応するスレッドの検証済みのファームウェア情報を取得する、工場で作成されたファームウェア リポジトリ プロファイルです。このカタログの変更の詳細については「[検証済み MX スタック カタログの編集](#)」を参照してください。検証済み MX スタック カタログの詳細については、[MX7000 ファームウェア アップデートのサイト](#)で入手可能なテクニカル ホワイトペーパーを参照してください。

**① メモ: Dell EMC のデフォルト カタログと検証済み MX スタック カタログ リポジトリ プロファイルを vSAN クラスターのベースラインとして使用することはできません。**

## リポジトリ プロファイルの作成

1. OMIVV ホーム ページで、**[ 対応性と導入 ]** > **[ プロファイル ]** > **[ リポジトリ プロファイル ]** の順にクリックします。
2. ウィザードの **[ リポジトリ プロファイル ]** 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。
3. **[ プロファイル名と説明 ]** ページで、プロファイル名と説明を入力します。**[ 説明 ]** フィールドはオプションであり、入力できる文字数は 255 文字までです。
4. **[ 次へ ]** をクリックします。  
**[ プロファイル設定 ]** ページが表示されます。
5. **[ プロファイル設定 ]** ページで、**[ ファームウェア ]** または **[ ドライバー ]** を選択します。

ドライバー リポジトリ プロファイルには以下が適用されます。

- ・ ドライバ リポジトリ プロファイルには、最大で 10 個のドライバを保存できます。ファイルがそれ以上存在する場合、ドライバはランダムに選択されます。
  - ・ オフライン ドライバ バンドル (.zip ファイル) のみが使用されます。
  - ・ オフライン ドライバ バンドル (.zip ファイル) をダウンロードして抽出し、共有の場所のフルパスを入力して共有の場所に保存します。OMIVV アプライアンスの内部にカタログが自動的に作成されます。ドライバー バンドルは、次の場所で入手できます。 <https://my.vmware.com/web/vmware/downloads>
  - ・ OMIVV には、CIFS または NFS への書き込みアクセスが必要になります。
  - ・ サブフォルダー内のファイルは無視されます。
  - ・ サイズが 10 MB を超えるファイルは無視されます。
  - ・ ドライバ リポジトリは vSAN クラスターにのみ適用されます。
6. **[ リポジトリ共有場所 ]** 領域で次のタスクを実行します。
    - a) リポジトリの共有の場所 (NFS または CIFS) を入力します。
    - b) CIFS の場合は、認証情報を入力します。

OMIVV は、サーバー 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:** ドライバー リポジトリに使用される **SMB 1.0 共有** の場合は、ディレクトリーパスの末尾にファイルセパレーターを追加します。

- [ **テストを開始** ] をクリックして、カタログパスと認証情報を検証します。  
リポジトリプロファイルの作成を続行するには、この検証プロセスを完了する必要があります。  
テスト接続の結果が表示されます。
- [ **次へ** ] をクリックします。  
[ **リポジトリの場所と同期** ] ページが表示されます。
- [ **次へ** ] をクリックします。  
サマリページが表示され、リポジトリプロファイルについての情報が示されます。
- 終了** をクリックします。  
カタログの作成後に、ダウンロードおよび解析が実行され、リポジトリプロファイルのホームページにステータスが表示されます。  
クラスタープロファイルの作成中、およびファームウェアのアップデート中は、正常に解析されたリポジトリプロファイルを使用できます。

## リポジトリプロファイルの編集

- OMIVV ホーム ページで、[ **対応性と導入** ] > [ **リポジトリプロファイル** ] > [ **編集** ] の順にクリックします。
- [ **プロファイル名と説明** ] ページで、プロファイル名と説明を編集して [ **次へ** ] をクリックします。
- [ **プロファイル設定** ] ページで、[ **ファームウェア** ] または [ **ドライバー** ] を選択します。  
ドライバーリポジトリプロファイルには以下が適用されます。
  - ドライバリポジトリプロファイルには、最大で 10 個のドライバを保存できます。ファイルがそれ以上存在する場合、ドライバはランダムに選択されます。
  - オフラインドライバーバンドル (.zip ファイル) のみが使用されます。
  - オフラインドライバーバンドル (.zip ファイル) をダウンロードして抽出し、共有の場所のフルパスを入力して共有の場所に保存します。OMIVV アプライアンスの内部にカタログが自動的に作成されます。ドライバーバンドルは、次の場所で入手できます。 <https://my.vmware.com/web/vmware/downloads>
  - OMIVV には、CIFS または NFS への書き込みアクセスが必要になります。
  - サブフォルダー内のファイルは無視されます。
  - サイズが 10 MB を超えるファイルは無視されます。
  - ドライバーリポジトリは vSAN クラスタにのみ適用されます。
- [ **リポジトリ共有場所** ] 領域で次のタスクを実行します。
  - リポジトリの共有の場所 (NFS または CIFS) を入力します。
  - CIFS の場合は、認証情報を入力します。

**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。
- [ **テストを開始** ] をクリックして、カタログパスと認証情報を検証します。  
処理を続行するには、この検証が必須です。  
テスト接続の結果が表示されます。
- [ **次へ** ] をクリックします。  
[ **リポジトリの場所と同期** ] ページが表示されます。
- [ **リポジトリの場所と同期** ] ページで、[ **リポジトリの場所と同期** ] チェックボックスを選択して [ **次へ** ] をクリックします。  
プロファイル名の更新または情報の確認のみを行うには、OMIVV でカタログが変更されないように、[ **リポジトリの場所と同期** ] チェックボックスはクリアしてください。リポジトリの場所と同期に関する詳細については、「**リポジトリの場所と同期**」を参照してください。
- [ **サマリ** ] ページでプロファイルの情報を確認してから、[ **終了** ] をクリックします。

## Dell デフォルトカタログの編集またはカスタマイズ

- [ **リポジトリプロファイル** ] ページで [ **デル デフォルトカタログ** ] を選択します。
- [ **プロファイル名と説明** ] ページでプロファイルの説明を編集してから、[ **次へ** ] をクリックします。

- [ **リポジトリの場所の指定** ] セクションで、次のいずれかを選択します。
  - ・ **Dell デフォルト オンライン** - リポジトリ プロファイルは **Dell オンライン** ( <https://downloads.dell.com/catalog/Catalog.gz> ) に設定されます。OMIVV は、カタログやアップデート パッケージのソースとして Dell EMC オンラインを使用します。
  - ・ **カスタム オンライン** - OMIVV は、カタログやアップデート パッケージのソースとして **カスタム オンライン** ( HTTP または HTTPS 共有 ) を使用します。Server Update Utility ( SUU ) を使用してカスタム リポジトリを作成する場合は、カタログの署名ファイル ( `catalog.xml.gz.sign` ) がカタログ ファイル フォルダーに存在することを確認してください。
  - ・ **共有ネットワーク フォルダー** - OMIVV は、カタログやアップデート パッケージのソースとして共有ネットワーク フォルダー ( CIFS または NFS ) を使用します。
    - a) [ **カスタム オンライン** ] を選択した場合は、カタログのオンライン パスを入力します。
    - b) [ **共有ネットワーク フォルダー** ] を選択した場合は、カタログファイルの場所 ( NFS または CIFS ) を入力します。
- [ **テストを開始** ] をクリックして、カタログ パスと認証情報を検証します。テスト接続の結果が表示されます。
- [ **リポジトリの場所と同期** ] ページで、[ **リポジトリの場所と同期** ] チェック ボックスを選択して [ **次へ** ] をクリックします。

プロファイル名の更新または情報の確認のみを行うには、OMIVV でカタログが変更されないように、[ **リポジトリの場所と同期** ] チェック ボックスはクリアしてください。リポジトリの場所との同期に関する詳細については、「[リポジトリの場所と同期](#)」を参照してください。
- [ **サマリー** ] ページでプロファイルの情報を確認してから、[ **終了** ] をクリックします。

## 検証済み MX スタック カタログの編集

- [ **リポジトリ プロファイル** ] ページで、[ **検証済み MX スタック カタログ** ] を選択して [ **編集** ] をクリックします。
- 次の情報のみを編集できます。
  - a) カタログの説明。
  - b) [ **リポジトリの場所と同期** ] チェック ボックス。

プロファイル名の更新または情報の確認のみを行うには、OMIVV でカタログが変更されないように、[ **リポジトリの場所と同期** ] チェック ボックスはクリアしてください。リポジトリの場所との同期に関する詳細については、「[リポジトリの場所と同期](#)」を参照してください。



## リポジトリの場所と同期

Dell デフォルト カタログおよび検証済み MX スタック リポジトリ プロファイルは、24 時間ごとまたは再起動のたびに自動的に変更をチェックしてアップデートします。

オフライン カタログをアップデートするには、次の手順を実行します。

- Dell EMC Repository Manager ( DRM ) または Server Update Utility ( SUU ) を使用して、オフライン ストア ( CIFS または NFS ) のカタログを更新します。ドライバーの場合は、ドライバー バンドルを置き換えます。
- リポジトリ プロファイルを編集し、[ **リポジトリの場所と同期** ] チェック ボックスを選択して、参照する OMIVV の変更をキャプチャします。このプロセスには数分かかります。
- 設定コンプライアンス ペースラインでファームウェアをアップデートするには、それぞれのクラスター プロファイルを編集して保存します。

## リポジトリ プロファイルの表示

- OMIVV ホーム ページで、[ **対応性と導入** ] > [ **リポジトリ プロファイル** ] をクリックします。テーブルには、すべてのリポジトリ プロファイルと次の情報が表示されます。
  - ・ [ **プロファイル名** ]: リポジトリ プロファイルの名前
  - ・ [ **説明** ]: プロファイルの説明
  - ・ [ **タイプ** ]: リポジトリのタイプ ( ファームウェアまたはドライバー )
  - ・ [ **共有パス** ]: NFS、CIFS、HTTP、または HTTPS のパス
  - ・ [ **最後に正常にアップデートされた時間** ]: リポジトリ プロファイルがアップデートされた日付と時刻。
  - ・ [ **最終更新ステータス** ]: カタログのダウンロードおよび解析ステータス
- ウィザードの列名の削除または追加を行うには、 をクリックします。
- リポジトリ プロファイル情報をエクスポートするには、 をクリックします。

# リポジトリ プロファイルの削除

リポジトリ プロファイルを削除する前に、関連するクラスター プロファイルからリポジトリ プロファイルの関連付けを解除していることを確認します。

1. [リポジトリ プロファイル] ページでリポジトリ プロファイルを選択して、[削除] をクリックします。
2. [削除の確認] ダイアログ ボックスで、[削除] をクリックします。

# クラスター プロファイルを使用したベースライン構成の取得

## クラスタプロファイル

クラスター プロファイルを使用すると、設定ベースライン（ハードウェア設定、ファームウェア、またはドライバーのバージョン）を取得し、設定ベースラインに対するドリフトを特定することによってクラスターの必要な状態を維持できます。

クラスター プロファイルを作成するには、システム プロファイル、ファームウェア リポジトリ プロファイル、ドライバー リポジトリ プロファイル、またはその組み合わせのいずれかのプロファイルがあることを確認します。ベースライン化されるクラスターには、同種のサーバー（同じモデル、同じハードウェア構成、および同じファームウェア レベル）を使用することをお勧めします。

- ・ クラスター プロファイルの作成後、ファームウェアおよびドライバー リポジトリ プロファイルをクラスター プロファイルの作成に使用される前に解析する必要があります。
- ・ クラスター プロファイルの作成後に、関連ファームウェアおよびドライバー リポジトリの最新スナップショットがベースライン用に作成されます。元のリポジトリを変更すると、その変更を反映するためにクラスター プロファイルの再度のアップデートが必要になります。そうしないと、元のリポジトリ上で行われたアップデートが、クラスター プロファイルのスナップショットに反映されません。
- ・ クラスター プロファイルが作成されると、ドリフト検出ジョブがトリガーされます。
- ・ クラスターが、クラスター プロファイルに関連付けられると、以前のクラスター プロファイルの関連付けは上書きされます（存在する場合）。
- ・ 複数のスタンドアロン vCenter が OMIVV に登録されている場合、vCenter ごとに個別のクラスター プロファイルを作成することを推奨します。
- ・ ドライバーのベースラインは vSAN クラスターでのみサポートされます。

**①メモ:** OMIVV の外部にインストールされたドライバーは、ベースライン用とは見なされません。

## クラスター プロファイルの作成

次の点を確認します。

- ・ システム プロファイル、ファームウェア リポジトリ プロファイル、ドライバー リポジトリ プロファイルのいずれかのプロファイル、またはその組み合わせがあること。
- ・ クラスターが vCenter 内に存在すること。

1. OMIVV ホーム ページで、[ 対応性と導入 ] > [ プロファイル ] > [ クラスター プロファイル ] > [ 新規プロファイルを作成 ] の順にクリックします。
2. ウィザードの [ クラスター プロファイル ] ページに表示される手順を読み、[ 開始 ] をクリックします。
3. [ プロファイル名と説明 ] ページにプロファイル名と説明を入力して、[ 次へ ] をクリックします。プロファイル名は最大 200 文字を使用できます。説明は最大 400 文字を使用できます。
4. [ プロファイルの関連付け ] ページで、次のいずれかのプロファイルまたはその組み合わせを選択します。
  - ・ システム プロファイル - システム プロファイルを選択すると、クラスター内のサーバーの設定ベースラインが設定されます。システム プロファイルのタイプが [ 基本 ] または [ 詳細設定 ] である場合、システム プロファイル名は、Basic\_<システム プロファイル名>、Advanced\_<システム プロファイル名> の形式で表示されます。
  - ・ ファームウェア リポジトリ プロファイル - ファームウェア リポジトリを選択すると、クラスター内のサーバーのファームウェアまたは BIOS ベースラインが作成されます。オンライン リポジトリは vSAN クラスターのベースラインではサポートされていません。
  - ・ ドライバー リポジトリ プロファイル - ドライバー リポジトリを選択すると、クラスター内のサーバーのドライバー ベースラインが作成されます。一度に最大 10 個のドライバーをベースラインに関連付けることができます。ドライバーのベースラインは vSAN クラスターでのみサポートされます。
5. [ 次へ ] をクリックします。[ クラスターの関連付け ] ページが表示されます。

6. [ クラスターの関連付け ] ページで、次のタスクを実行します。
    - a) 登録済み vCenter サーバーのインスタンスを選択します。
    - b) クラスターを関連付けるには [ 参照 ] をクリックします。
    - c) ベースライン化するクラスターを選択します。
    - d) [ OK ] をクリックします。  
選択したクラスターが [ クラスターの関連付け ] ページに表示されます。
    - e) [ 次へ ] をクリックします。
  7. [ ドリフト検出のスケジュール ] ページで、日時を選択し、[ 次へ ] をクリックします。  
サマリ ページが表示され、クラスタプロファイルに関する情報が示されます。
  8. 終了 をクリックします。  
クラスタープロファイルが保存された直後にドリフト検出ジョブが実行され、その後、スケジュールされた時間にも実行されます。[ ジョブ ] ページでジョブ完了ステータスを表示します。
- メモ:** クラスターのクラスタープロファイルを作成した後に OMIVV で管理されるノードの数が変更された場合、コレクション サイズはその後のドリフト検出ジョブ中に自動的に更新されます。

## クラスタープロファイルの編集

クラスタプロファイルを編集するとベースラインが変わり、対応性レベルの再計算が発生する可能性があります。

関連するドライバーリポジトリ、ファームウェアリポジトリ、またはシステムプロファイルが変更され、クラスタープロファイルの最新の変更を使用する場合は、クラスタープロファイルを選択して [ 編集 ] をクリックし、ウィザードで [ 次へ ] をクリックしてから、[ 終了 ] をクリックします。



1. OMIVV ホーム ページで、[ 対応性と導入 ] > [ プロファイル ] > [ クラスタープロファイル ] の順にクリックします。
2. クラスタープロファイルを選択して、[ 編集 ] をクリックします。
3. [ プロファイル名と説明 ] ページに説明を編集し、[ 次へ ] をクリックします。
4. [ プロファイルの関連付け ] ページで、プロファイルの組み合わせを変更できます。
5. [ クラスターの関連付け ] ページで、vCenter インスタンスおよび関連クラスターを変更できます。
6. [ ドリフト検出のスケジュール ] ページで、ドリフト検出スケジュールを変更できます。
7. [ サマリー ] ページの更新された情報を確認し、[ 終了 ] をクリックします。  
クラスタープロファイルが保存された直後にドリフト検出ジョブが実行され、その後、スケジュールされた時間にも実行されます。

## クラスタープロファイルの表示

1. OMIVV ページで、[ 対応性と導入 ] > [ プロファイル ] > [ クラスタープロファイル ] をクリックします。  
テーブルに、すべてのクラスタープロファイルとともに次の情報が表示されます。
  - ・ [ プロファイル名 ]: クラスタープロファイルの名前です。
  - ・ [ 説明 ]: プロファイルの説明
  - ・ [ 関連付けられたシステムプロファイル ]: [ 基本 ] および [ 詳細設定 ] システムプロファイルタイプに関連付けられたシステムプロファイル名です。システムプロファイル名は、Basic\_<システムプロファイル名>、Advanced\_<システムプロファイル名>の形式で表示されます。
  - ・ [ 関連付けられたファームウェアリポジトリプロファイル ]: 関連付けられたファームウェアリポジトリプロファイル名です。
  - ・ [ 関連付けられたドライバーリポジトリプロファイル ]: 関連付けられたドライバーリポジトリプロファイル名です。

**メモ:** シャーシ認証情報プロファイルを使用して管理されている PowerEdge MX ホストの場合、設定ドリフトは計算されません。

  - ・ [ vCenter ]: クラスタープロファイルに関連付けられている vCenter インスタンスです。
  - ・ [ 最後に正常にアップデートされた時間 ]: クラスタープロファイルがアップデートされた日付と時刻です。

**メモ:** 関連付けられたリポジトリプロファイル (ファームウェアまたはドライバー)、またはシステムプロファイルが変更されると、プロファイル名とともに警告マークが表示されます。リポジトリまたはシステムプロファイルを変更してベースラインの変更をアップデートした後、クラスタープロファイルをアップデートする必要があります。クラスタープロファイルのアップデートの詳細は、「[クラスタープロファイルのアップデート](#)」を参照してください。
2. ウィザードの列名の削除または追加を行うには、 をクリックします。
3. クラスタープロファイルの情報をエクスポートするには、 をクリックします。

## クラスター プロファイルのアップデート

リポジトリ プロファイル (ファームウェアまたはドライバー) およびシステム プロファイルをアップデートすると、[クラスター プロファイル] ページのプロファイル名に警告シンボルが表示されます。プロファイルをアップデートすると、vSphere Lifecycle Manager のクラスター プロファイルとファームウェア コンプライアンス ステータスに関連するクラスターの設定コンプライアンスに影響する場合があります。プロファイルのアップデート機能を使用して、クラスター プロファイルをアップデートまたは再ベースライン化することができます。

1. OMIVV ホーム ページで、[ **対応性と導入** ] > [ **プロファイル** ] > [ **クラスター プロファイル** ] の順にクリックします。
2. プロファイル名に警告シンボルがあるクラスター プロファイルを選択します。
3. [ **プロファイルのアップデート** ] をクリックします。
4. 関連するプロファイルを最新の状態にアップデートするには、[ **OK** ] をクリックします。  
プロファイルをアップデートすると、ベースラインを元に戻すことはできません。  
クラスター プロファイルがアップデートされたリポジトリ プロファイルまたはシステム プロファイルと同期され、警告マークが消えます。

## クラスター プロファイルの削除

1. OMIVV ホーム ページで、[ **対応性と導入** ] > [ **プロファイル** ] > [ **クラスター プロファイル** ] の順にクリックします。
2. 任意のクラスター プロファイルを選択して、[ **削除** ] をクリックします。
3. [ **削除の確認** ] ダイアログ ボックスで、[ **削除** ] をクリックします。  
クラスター プロファイルが削除される場合は、対応するドリフト検出ジョブも削除されます。

システム プロファイルと ISO プロファイルを導入するには、サーバーが導入ウィザードに表示されることを確認し、すべてのサーバーが次の要件に沿っていることを確認します。

- ・ 『OpenManage Integration for VMware vCenter 互換性マトリックス』に記載されている特定のハードウェア サポート情報を満たす。
- ・ iDRAC ファームウェアおよび BIOS の対応最小バージョンを満たす。具体的なハードウェアサポート情報については、『OpenManage Integration for VMware vCenter 互換性マトリックス』を参照してください。
- ・ IDSDM のストレージ仕様を満たす。IDSDM のストレージ仕様を把握するには、VMware のマニュアルを参照してください。OMIVV で OS を導入する前に、BIOS から IDSDM を有効にします。OMIVV では、IDSDM、ローカル ハードドライブ、BOSS への導入が可能です。
- ・ vCenter、OMIVV、iDRAC がそれぞれ異なるネットワークに接続されている場合、vCenter、OMIVV、および iDRAC のネットワーク間にルートがあることを確認します。これは、OMIVV アプライアンスが 2 つのネットワーク アダプターで設定されていない場合にのみ適用されます。
- ・ 再起動時にシステムインベントリを収集 (CSIOR) が有効になっていることを確認します。自動/手動検出を開始する前に、各日に最新のデータが取得されるようにするために、サーバーでハード再起動を実行してください。
- ・ ベアメタル サーバーの自動検出を行うには、自動検出またはハンドシェイク オプションが工場出荷時に事前設定された Dell EMC サーバーを注文します。サーバでこのオプションが事前設定されていない場合、手動で OMIVV IP アドレスを入力するか、この情報を提供するようローカルネットワークを設定する必要があります。
- ・ ハードウェアの設定に OMIVV を使用しない場合は、OS の導入前に、次の条件が満たされていることを確認します。
  - ・ 仮想化テクノロジー (VT) フラグを BIOS で有効にしている。
  - ・ 仮想ドライブ、IDSDM、および BOSS が最初の起動ディスクに設定されている。
- ・ ハードウェア設定に OMIVV を使用する場合は、BIOS 設定がシステム プロファイルの一部でなくても VT の BIOS 設定が自動的に有効化されることを確認します。ターゲット システムで仮想ドライブが構成されていない場合は、Express または Clone RAID 設定が必要になります。
- ・ すべての Dell EMC ドライバーを含むカスタム ESXi イメージが、導入で使用可能なことを確認します。正しいイメージは、[dell.com/support](#) の [ **ドライバー & ダウンロード** ] ページで見つけることができます。カスタム イメージは、導入プロセス中に OMIVV がアクセスできる CIFS または NFS 共有の場所に保存します。本リリース向けの対応 ESXi バージョンの最新リストは、『OpenManage Integration for VMware vCenter 互換性マトリックス』を参照してください。カスタム Dell EMC ISO イメージをダウンロードするには、「[カスタム Dell EMC ISO イメージのダウンロード](#)」を参照してください。

## ベアメタル サーバーの表示

[ ベアメタル サーバー ] ページでは、次の操作を実行できます。

- ・ 自動検出と手動検出を使用して検出されたベアメタル サーバーを表示します。
 

[ サービス タグ ], [ モデル名 ], [ iDRAC Ip ], [ サーバー ステータス ], [ システム ロックダウン モード ], [ 対応状態 ], および [ iDRAC ライセンスのステータス ] などの情報が表示されます。

ベアメタル サーバーのステータスには以下があります。

  - ・ **未設定** - サーバーが OMIVV に追加され、設定待ちです。
  - ・ **設定済み** — サーバーは、正しいオペレーティング システム導入に必要なすべてのハードウェア情報で設定されています。
  - ・ **隔離** — サーバーが OMIVV アクションから除外されているため、サーバーはオペレーティング システム導入やファームウェア アップデートなどのタスクを実行できません。
- ・ ベアメタル サーバーの対応状態を表示します。
 

ベアメタル サーバーは、次の場合に非対応です。

  - ・ サポートされているサーバではない。
  - ・ サポートされている iDRAC ライセンスがない ( iDRAC Express が最小要件です )。
  - ・ iDRAC、BIOS、または LC のサポートされているバージョンがインストールされていない。
  - ・ LOM または NIC が存在しない。
  - ・ システムロックダウンモードがオンになります。
- ・ 対応の問題に関する詳細を表示するには、下部の水平ペインで [ **詳細** ] をクリックします。

[ [ベアメタル サーバー](#) ] ページで、次のタスクも実行できます。

- ・ [ベアメタル サーバーの手動検出](#)
- ・ [ベアメタル サーバーの取り外し](#)
- ・ [システム プロファイルと ISO プロファイルの導入](#)
- ・ [ベアメタル サーバーの更新](#)
- ・ [iDRAC ライセンスの購入または更新](#)

## デバイス検知

検出とは、サポートされているベアメタルサーバを追加するプロセスです。サーバーが検出されたら、これをシステム プロファイルおよび ISO プロファイルの導入に使用できます。サポートされているサーバーのリストについては、『[OpenManage Integration for VMware vCenter 互換性マトリックス](#)』を参照してください。

前提条件：

- ・ ベアメタルサーバの iDRAC から OMIVV 仮想マシンへのネットワーク接続が必要です。
- ・ OMIVV では、既存のオペレーティングシステムを持つホストを検出せず、その代わりに、vCenter に追加してください。ホストはホスト認証情報プロファイルに追加します。
- ・ SD カードにオペレーティングシステムを導入し、第 12 世代および第 13 世代の PowerEdge サーバーのシステム プロファイル機能を使用するには、iDRAC 2.50.50.50 以降がインストールされていることを確認してください。

## 自動検出

自動検出は、ベアメタルサーバを追加するプロセスです。サーバーが検出されたら、これをオペレーティングシステムおよびハードウェアの導入に使用します。自動検出は、OMIVV を使用してベアメタルサーバーを手動で検出する必要を排除する iDRAC 機能です。

## 自動検出の前提条件

PowerEdge ベアメタル サーバーの検出を行う前に、OMIVV がインストールされていることを確認してください。ベアメタルサーバのブルで検出することができるのは、iDRAC Express または iDRAC Enterprise を搭載した PowerEdge サーバです。Dell EMC ベアメタル サーバーの iDRAC から OMIVV アプライアンスへのネットワーク接続があることを確認します。

**メモ:** OMIVV を使用して既存のオペレーティングシステムを持つホストを検出ししないでください。代わりに、オペレーティングシステムをホスト認証情報プロファイルに追加してください。

自動検出を機能させるには、次の条件を満たしている必要があります。

- ・ 電源 - 必ずサーバをコンセントに接続してください。サーバーの電源を入れる必要はありません。
- ・ ネットワーク接続: サーバーの iDRAC がネットワークに接続され、プロビジョニングサーバーとポート 4433 経由で通信していることを確認します。プロビジョニングサーバーの IP アドレスは、DHCP サーバーを使用して取得するか、iDRAC 設定ユーティリティを使用して手動で指定することができます。
- ・ 追加のネットワーク設定: DNS 名を解決するには、DHCP 設定で DNS サーバーアドレスの取得を有効にします。
- ・ プロビジョニングサービスの場所: iDRAC に対してプロビジョニングサービスサーバーの IP アドレスまたはホスト名が既知であることを確認します。「[プロビジョニングサービスの場所](#)」を参照してください。
- ・ アカウントアクセス無効: 管理者権限を持つ iDRAC アカウントがある場合は、まず iDRAC ウェブコンソールからそれらを無効にします。自動検出が正常に完了すると、[ [設定](#) ] ページに入力された展開用の認証情報を使用して管理 iDRAC アカウントが再度有効化されます。展開用の認証情報の詳細については、「[展開用の資格情報の設定](#)」を参照してください。
- ・ 自動検出有効: 自動検出処理が開始できるように、サーバーの iDRAC で自動検出が有効にされていることを確認します。詳細については、次を参照してください: [iDRAC の管理者アカウントを有効または無効にする](#)

## プロビジョニングサービスの場所

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

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

プロビジョニングサービスの値が iDRAC 設定ユーティリティーで手動で指定されていない場合、iDRAC は DHCP スコープ オプションの値を使用しようとします。DHCP スコープオプションが存在しない場合、iDRAC は DNS からのサービスレコードの値を使用しようとします。

DHCP スコープオプションと DNS サービスレコードの設定方法の詳細については、<https://www.dell.com/support> で『Dell 自動検出 ネットワークセットアップ仕様』を参照してください。

## iDRAC の管理者アカウントを有効または無効にする

自動検出をセットアップする前に、管理者アクセス権のない iDRAC アカウントを除くすべての iDRAC アカウントを無効にします。自動検出後、ルート アカウント以外のすべてのアカウントを有効にできます。

**メモ:** 管理者権限を無効にする前に、iDRAC で非管理者ユーザー アカウントを作成することをお勧めします。

1. ブラウザで、**iDRAC IP アドレス**を入力します。
2. **Integrated Dell Remote Access Controller GUI** にログインします。
3. 次のうちのいずれか1つを実行してください。
  - ・ iDRAC7: 左ペインで、**iDRAC 設定** > **ユーザー認証** > **ユーザー** タブを順に選択します。
  - ・ iDRAC8: 左ペインで、**iDRAC 設定** > **ユーザー認証** > **ユーザー** タブを順に選択します。
  - ・ iDRAC9 の場合: [**iDRAC 設定**] > [**ユーザー**] > [**ローカル ユーザー**] の順に移動します。
4. [**ローカル ユーザー**] タブで、ルート以外の管理者アカウントを探します。
5. アカウントを無効にするには、ユーザー ID の下で **ID** を選択します。
6. [**次へ**] をクリックします。
7. **ユーザー設定** ページの **一般** の下で、**ユーザーを有効にする** チェックボックスのチェックを外します。
8. **適用** をクリックします。
9. 各管理者アカウントを再度有効にするには、自動検出を正しくセットアップした後でステップ 1~8 を繰り返しますが、ここでは [**ユーザーを有効にする**] チェックボックスを選択して [**適用**] をクリックします。

## PowerEdge サーバーでの自動検出の手動設定

iDRAC アドレスがあることを確認します。

Dell EMC にサーバを注文し、プロビジョニングサーバの IP アドレスを入力した後、サーバで自動検出機能を有効にするように依頼できます。プロビジョニングサーバの IP アドレスは OMIVV の IP アドレスである必要があります。Dell EMC からサーバを受け取り、iDRAC をマウントしてケーブルを接続してから電源をオンにすると、サーバが自動検出され、[**ベアメタル サーバー**] ページにリストされます。

**メモ:** 自動検出されたサーバについては、[**設定**] > [**アプライアンス設定**] > [**展開認証情報**] で提供される認証情報が**管理者認証情報**として設定され、オペレーティングシステムの導入が完了するまでサーバとの通信に使用されます。オペレーティングシステムの導入が正しく完了すると、関連付けられている**ホスト認証情報プロファイル**で提供される iDRAC 認証情報が設定されます。

ターゲット マシンで自動検出を手動で有効にするには、第 12 世代以降の PowerEdge サーバーに対して以下の手順を実行します。

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

## ベアメタル サーバーの手動検出

iDRAC の Administrator 権限があることを確認してください。

自動検出プロセスを使用して追加されていないベアメタル サーバーを手動で追加することができます。追加されると、サーバは [**ベアメタル サーバー**] ページのサーバのリストに表示されます。

1. OMIVV ホーム ページで、[ 対応性と導入 ] > [ 導入 ] > [ 検出 ] の順にクリックします。  
サーバの追加 ダイアログボックスが表示されます。
2. サーバの追加 ダイアログボックスで、以下を行います。
  - a) [ iDRAC IP アドレス ] ボックスに iDRAC IPv4 アドレスを入力します。
  - b) iDRAC 認証情報を入力します。
3. [ OK ] をクリックします。  
サーバの追加には数分かかることがあります。

検出操作が進行中の場合は、[ サーバの追加 ] ページを閉じることができます。検出プロセスはバックグラウンドで続行されます。検出されたサーバが [ ベアメタル サーバ ] ページに表示されます。手動検出のタイムアウト値は 15 分に設定されています。

ベアメタル サーバの詳細情報を表示するには、サーバを選択します。ライセンスの有効期限、BIOS バージョン、システム ロックダウン モードなどの情報は、ページの一番下の水平ペインに表示されます。


## ベアメタル サーバの取り外し

自動検出または手動で追加されたサーバは、手動で取り外すことができます。

1. OMIVV ホーム ページで、[ 対応性と導入 ] > [ 導入 ] > [ 削除 ] の順にクリックします。
2. 任意のベアメタル サーバを選択し、[ OK ] をクリックします。

## ベアメタル サーバの更新

更新操作では、iDRAC に接続して、基本インベントリを収集することによって、ベアメタル サーバを再検出します。

 **メモ:**「設定済み」ベアメタル サーバで更新操作を実行すると、更新操作によってサーバが再検出されるため、サーバのステータスが「設定なし」状態に変わります。

1. OMIVV ホーム ページで、[ 対応性と導入 ] > [ 導入 ] > [ 更新 ] の順にクリックします。
2. [ ベアメタル サーバの更新 ] ページでサーバを選択し、[ OK ] をクリックします。  
ベアメタルサーバのデータの更新には、数分かかる場合があります。操作の進行中に [ ベアメタル サーバの更新 ] ページを閉じることができ、再検出プロセスはバックグラウンドで続行されます。再検出されたサーバが [ ベアメタル サーバ ] ページに表示されます。

## iDRAC ライセンスの購入または更新

対応する iDRAC ライセンスがない場合、ベアメタル サーバのステータスに非対応が表示されます。表には、iDRAC ライセンスのステータスが表示されます。iDRAC ライセンスの詳細情報を表示する非対応ベアメタル サーバを選択します。

1. iDRAC ライセンスを更新するには、OMIVV ホーム ページで、[ 対応性と導入 ] > [ 導入 ] の順にクリックします。
2. iDRAC ライセンスが非対応であるベアメタル サーバを選択し、[ iDRAC ライセンスの更新/購入 ] をクリックします。
3. Dell Digital Locker にログインし、新しい iDRAC ライセンスにアップデートまたは購入します。
4. iDRAC ライセンスのインストール後、[ 更新 ] をクリックします。

## 導入

システム プロファイルと ISO プロファイルを導入する前に、次が使用可能であることを確認します。

- ・ ホスト認証情報プロファイル

ホスト認証情報プロファイルを作成するには、[ 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。

- ・ ベアメタル サーバ

ベアメタル サーバを検出するには、[ 検出 ] をクリックします。ベアメタル サーバ検出の詳細に関しては、「[ベアメタル サーバの手動検出](#)」を参照してください。

- ・ システムプロファイル

システム プロファイルを作成するには、[ 作成 ] をクリックします。システム プロファイル作成の詳細については、「[システムプロファイルの作成](#)」を参照してください。

- ・ ISO プロファイル

ISO プロファイルを作成するには、[作成] をクリックします。ISO プロファイル作成の詳細については、「[ISO プロファイルの作成](#)」を参照してください。

[システム プロファイルと ISO プロファイルの導入] ウィザードを使用して、次の操作を実行できます。

- ・ システム プロファイルの導入  
詳細については、次を参照してください：[システム プロファイルの導入 \(ハードウェアの設定\)](#)
- ・ ISO プロファイルの導入  
詳細については、次を参照してください：[ISO プロファイル \(ESXi インストール\) の導入](#)
- ・ システム プロファイルと ISO プロファイルの導入  
詳細については、次を参照してください：[システム プロファイルと ISO プロファイルの導入](#)

導入ウィザードを起動するには、[対応性と導入] > [導入] > [導入] の順に移動します。

## システム プロファイルの導入 (ハードウェアの設定)

1. 導入ウィザードの [システム プロファイルと ISO プロファイル導入チェックリスト] ページで導入チェックリストを確認し、[開始] をクリックします。  
導入は、対応ベアメタル サーバー上でのみ実行できます。詳細については、次を参照してください：[ベアメタル サーバーの表示](#)
2. [サーバーの選択] ページで、1つ以上のサーバーを選択します。  
[導入オプションの選択] ページが表示されます。
3. [導入オプションの選択] ページで、[システム プロファイル (ハードウェアの設定)] を選択します。
4. [システム プロファイル] ドロップダウン メニューから、適切なシステム プロファイルを選択し、[次へ] をクリックします。  
基本および詳細システム プロファイル タイプの場合、システム プロファイル名は Basic\_<システム プロファイル名>、Advanced\_<システム プロファイル名>の形式で表示されます。  
[設定プレビュー] ページが表示されます。[設定プレビュー] では、選択したサーバー上のサーバー設定プロファイルのインポート操作 (成功または失敗) についてプレビューできます。
5. iDRAC でプレビュージョブを作成するには、[設定プレビュー] ページで iDRAC IP を選択し、[プレビュー] をクリックします。  
設定プレビューは、オプションのタスクです。  
システム プロファイルのプレビュー操作が完了するまでに数分かかる場合があります。比較ステータスが [結果] 列に表示されます。  
比較結果は次のとおりです。
  - ・ 完了 - プレビュージョブは正常に実行されました。比較結果の詳細については、[詳細] 列の [詳細の表示] をクリックしてください。
  - ・ 未完了 - プレビュージョブが iDRAC で正常に実行されていません。iDRAC がアクセス可能であることを確認し、必要に応じて iDRAC のリセットを実行します。ジョブの詳細については、OMIVV ログおよび iDRAC コンソールのログを参照してください。
6. [展開ジョブのスケジュール設定] ページで、次の手順を実行します。
  - a) 展開ジョブ名および説明を入力します。[説明] フィールドはオプションです。
  - b) すぐに展開ジョブを実行するには、[今すぐ実行] をクリックします。
  - c) ジョブを後で実行するようにスケジュールするには、[後でスケジュールを設定] をクリックして、日付と時刻を選択します。
  - d) [ジョブの送信後にジョブ ページに移動] チェック ボックスを選択します。  
ジョブの状態は [ジョブ] ページで追跡することができます。詳細については、次を参照してください：[展開ジョブ](#)
7. 終了 をクリックします。

## ISO プロファイル (ESXi インストール) の導入

導入は、対応ベアメタル サーバー上でのみ実行できます。詳細については、次を参照してください：[ベアメタル サーバーの表示](#)

1. 導入ウィザードの [システム プロファイルと ISO プロファイル導入チェックリスト] ページで導入チェックリストを確認し、[開始] をクリックします。
2. [サーバーの選択] ページで、1つ以上のサーバーを選択します。  
[導入オプションの選択] ページが表示されます。
3. [導入オプションの選択] ページで、[ISO プロファイル (ESXi インストール)] を選択します。
4. [vCenter 名] ドロップダウン メニューから、vCenter のインスタンスを選択します。

5. vCenter 宛先コンテナを選択するには、[ 参照 ] をクリックし、オペレーティングシステムを導入する適切なデータセンターまたはクラスターを選択します。
6. [ ISO プロファイル ] ドロップダウンメニューで、適切な ISO プロファイルを選択します。
7. [ インストール ターゲット ] で次のいずれかを選択します。

- ・ [ **最初の起動ディスク** ]: ハードドライブ、ソリッドステートドライブ (SSD)、RAID コントローラーによって作成された仮想ドライブでオペレーティングシステムを導入します。
- ・ [ **内蔵デュアル SD モジュール (IDSDM)** ]: IDSDM にオペレーティングシステムを導入します。選択されたサーバの少なくとも1台で IDSDM が使用できる場合は、内蔵デュアル SD モジュール オプションが有効になっています。使用できない場合は、[ **最初の起動ディスク** ] オプションのみが使用できます。
- ・ 選択したサーバの中に IDSDM または BOSS モジュールに対応していないサーバがある場合、または導入中に IDSDM または BOSS がサーバにインストールされない場合は、それらのサーバでの導入操作はスキップされます。サーバの最初の起動ディスクにオペレーティングシステムを導入するには、[ **ハイパーバイザーを使用可能な内蔵デュアル SD モジュールのないサーバの最初のハードディスクに導入する** ] チェックボックスを選択します。

**① メモ:** 最初の起動ディスクのインストールターゲットは、BIOS ハードドライブシーケンスまたは UEFI ブートシーケンスの最初のエントリーと同じではありません。このオプションは、ESXi の pre-OS 環境で認識された最初のディスクにオペレーティングシステムを導入します。したがって、[ **最初の起動ディスク** ] オプションを選択するときは、[ **ハードディスクフェイルオーバー** ] または [ **起動順序再試行** ] オプションが有効になっていることを確認します。

- ・ [ **BOSS** ]: BOSS カード上にオペレーティングシステムを導入します。選択されたサーバの少なくとも1台で BOSS が使用できる場合は、BOSS オプションが有効になっています。使用できない場合は、[ **最初の起動ディスク** ] オプションのみが使用できます。

OMIVV を使用して BOSS コントローラーにオペレーティングシステムを導入する場合は、システムプロファイルが BOSS の VD 構成と一緒に参照サーバからキャプチャーされていて、ターゲットサーバに同様の構成を持つ BOSS があることを確認します。VD の作成の詳細については、[www.dell.com/support](http://www.dell.com/support) にある『Dell EMC Boot Optimized Server Storage-S1 ユーザーガイド』を参照してください。

8. [ **ホスト認証情報プロファイルの選択** ] ページで、次のタスクを実行します。
  - a. すべてのホストに同じホスト認証情報プロファイルを使用するには、[ はい ] をクリックして、ドロップダウンメニューからホスト認証情報プロファイルを選択します。
  - b. サーバごとに個別のホスト認証情報プロファイルを選択するには、[ いいえ ] をクリックして、ドロップダウンメニューからホスト認証情報プロファイルを選択します。

**① メモ:** ホスト認証情報プロファイルで iDRAC または ESXi の AD 認証情報が使用されている場合、これらのプロファイルはオペレーティングシステム導入では考慮されません。

**① メモ:** ホスト認証情報プロファイルでは、ベアメタルの検出に使用するユーザーを関連付けることをお勧めします。関連付けないと、検出されたユーザーはオペレーティングシステムの導入後に iDRAC で無効になります。

9. [ **ネットワークの設定構成** ] ページで、次のタスクを実行します。
  - a) サーバの完全修飾ホスト名 (FQDN) を入力します。ホスト名の完全修飾ドメイン名は必須です。FQDN での *localhost* の使用はサポートされていません。FQDN はホストを vCenter に追加する場合に使用します。IP アドレスを FQDN に解決する DNS の記録を作成します。DNS サーバが逆引き要求に対応するように設定します。展開ジョブを実行するスケジュールを作成する前に、DHCP 予約および DNS ホスト名が設定および検証されている必要があります。

**① メモ:** vCenter が FQDN を使用して OMIVV に登録されている場合は、ESXi ホストが DNS 解決により FQDN を解決できることを確認します。
  - b) 管理ネットワークに使用する NIC を選択します。NIC が接続状態であることを確認します。

**① メモ:** OMIVV へのネットワーク接続に基づいて、管理 NIC を選択するようにしてください。[ **すべてのサーバに設定を適用** ] オプションは、管理 NIC の選択には適用されません。
  - c) vCenter へのアクセス権を持つ OMIVV ネットワークインスタンスを選択します。詳細については、次を参照してください: [2つのNICを使用してホストを導入するための前提条件](#)
  - d) 次のいずれかのネットワークングオプションを選択します。

- ・ 静的ネットワークの場合は、優先 DNS サーバ、代替 DNS サーバ、IP アドレス、サブネットマスク、およびデフォルトゲートウェイを入力します。
- ・ [ **VLAN を使用** ]: VLAN ID を指定すると、導入中にオペレーティングシステムの管理インターフェイスに適用され、すべてのトラフィックに VLAN ID でタグ付けされます。サーバ識別では、導入されたサーバに新しい名前とネットワーク ID が割り当てられます。詳細については、次を参照してください: [VLAN サポート](#)
- ・ [ **DHCP を使用** ]: ホストを vCenter に追加する際に、DHCP によって割り当てられた IP アドレスが使用されます。DHCP を使用する場合、選択された NIC MAC アドレスには IP 予約を使うことをお勧めします。

10. [ **展開ジョブのスケジュール設定** ] ページで、次の手順を実行します。

- a) 展開ジョブ名および説明を入力します。
- b) すぐに展開ジョブを実行するには、[ **今すぐ実行** ] をクリックします。
- c) ジョブを後で実行するようにスケジュールするには、[ **後でスケジュールを設定** ] をクリックして、日付と時刻を選択します。
- d) [ **ジョブの送信後にジョブ ページに移動** ] チェック ボックスを選択します。  
ジョブの状態は [ **ジョブ** ] ページで追跡することができます。詳細については、次を参照してください：[展開ジョブ](#)

11. **終了** をクリックします。

**メモ:** ベアメタル サーバーでオペレーティング システム導入を実行した後、OMIVV はすべての iDRAC ジョブをクリアします。

## システム プロファイルと ISO プロファイルの導入

導入は、対応ベアメタル サーバー上でのみ実行できます。詳細については、「[ベアメタル サーバーの表示](#)」を参照してください。

1. 導入ウィザードの [ **システム プロファイルと ISO プロファイル導入チェックリスト** ] ページで導入チェックリストを確認し、[ **開始** ] をクリックします。
2. [ **サーバーの選択** ] ページで、1つ以上のサーバーを選択します。  
[ **導入オプションの選択** ] ページが表示されます。
3. [ **導入オプションの選択** ] ページで、[ **システム プロファイル (ハードウェアの設定)** ] および [ **ISO プロファイル (ESXi インストール)** ] を選択します。
4. [ **vCenter 名** ] ドロップダウン メニューから、vCenter のインスタンスを選択します。
5. vCenter 宛先コンテナを選択するには、[ **参照** ] をクリックし、オペレーティング システムを導入する適切なデータ センターまたはクラスターを選択します。
6. 選択したクラスターに関連付けられているクラスター プロファイルに関連付けられているシステム プロファイルを使用するには、[ **確認** ] をクリックします。
  - ・ 他のシステム プロファイルを選択するには、[ **別を選択** ] をクリックします。設定コンプライアンスのドリフトを回避するため、クラスターに関連付けられているシステム プロファイルを選択することをお勧めします。
7. [ **ISO プロファイル** ] ドロップダウン メニューから、適切な ISO プロファイルを選択し、[ **次へ** ] をクリックします。
8. iDRAC でプレビュージョブを作成するには、[ **設定プレビュー** ] ページで iDRAC IP を選択し、[ **プレビュー** ] をクリックします。設定プレビューは、オプションのタスクです。  
システム プロファイルのプレビュー操作が完了するまでに数分かかる場合があります。比較ステータスが [ **結果** ] 列に表示されます。

比較結果は次のとおりです。

- ・ 完了 - プレビュージョブは正常に実行されました。比較結果の詳細については、[ **詳細** ] 列の [ **詳細の表示** ] をクリックしてください。
  - ・ 未完了 - プレビュージョブが iDRAC で正常に実行されていません。iDRAC がアクセス可能であることを確認し、必要に応じて iDRAC のリセットを実行します。ジョブの詳細については、OMIVV ログおよび iDRAC コンソールのログを参照してください。
9. 「**ISO プロファイル (ESXi インストール) の導入**」トピックにリストされているタスク 7~10 を完了します。

## 2つの NIC を使用してホストを導入するための前提条件

2つの NIC の導入の前提条件は、次のとおりです。

- ・ ホストは、同じネットワークまたは2つの異なるネットワークに iDRAC および vCenter 管理 NIC を持つことができます。
- ・ ISO イメージは任意のネットワークに保存できます。
- ・ OS 導入ウィザードには両方の OMIVV ネットワークが表示されます。環境に適した正しい vCenter ネットワークと OMIVV ネットワークを選択していることを確認してください。

## VLAN サポート

OMIVV は、ルーダブル VLAN へのオペレーティング システム導入をサポートしており、導入ウィザードで VLAN サポートを設定できます。導入ウィザードのこの部分には、VLAN ID を使用して VLAN を指定するオプションがあります。VLAN ID を指定すると、導入中にオペレーティング システムの管理インターフェイスに適用され、すべてのトラフィックに VLAN ID でタグ付けできます。

導入中に指定する VLAN は、OMIVV アプライアンスおよび vCenter サーバーの両方と通信できることを確認してください。これらの宛先の一方または両方と通信できない VLAN へのオペレーティング システムの導入は、導入失敗の原因になります。

1回の展開ジョブで複数のベアメタル サーバーを選択し、同じ VLAN ID をすべてのサーバーに適用する場合は、導入ウィザードのサーバー識別の箇所で、[ すべてのサーバーに設定を適用 ] を使用します。このオプションを使用すると、その展開ジョブに含まれるすべてのサーバーに同じ VLAN ID およびその他のネットワーク設定を適用できます。

① **メモ:** OMIVV へのネットワーク接続に基づいて、管理 NIC を選択するようにしてください。[ すべてのサーバーに設定を適用 ] オプションは、管理 NIC の選択には適用されません。

## 展開ジョブのタイミング

システム プロファイルと ISO プロファイルの導入には、複数の要因により、完了まで30分から数時間かかる場合があります。展開ジョブを開始する場合は、提供されたガイドラインにしたがって、展開時間を計画することを推奨します。システム プロファイルと ISO プロファイルの導入にかかる時間は、展開タイプ、複雑性、同時に実行される展開ジョブ数などによって異なります。展開ジョブは、総合的な展開ジョブの時間を短縮するため、最大5台の並列サーバーによるバッチ処理で実行されます。並列ジョブの正確な数は使用可能なリソースによって異なります。

次の表には、平均値が表示されています。値は、サーバーの構成、サーバーの世代、導入予定のベアメタル サーバーの数などの要因によって異なる場合があります。

表 3. 単一サーバーのおおよその展開時間

展開タイプ	展開ごとのおおよその時間
ISO プロファイルのみ	30 ~ 130
システムプロファイルのみ	5 ~ 6 分
システム プロファイルと ISO プロファイル	30 ~ 60 分

## 展開シーケンス中のサーバー ステータス

自動または手動で検出されたサーバーは、データ センターにとって新しいサーバーか、未完了の展開ジョブがスケジュールされているかなどを特定しやすくするため、いくつかの状態に分類されます。管理者はこれらのステータスを使用して、ハードウェア構成ステータスを確認できます。

表 4. 展開シーケンス中のサーバ状態

サーバの状態	説明
未設定	サーバーが OMIVV に追加され、設定待ちです。
設定済み	サーバーは、正しいオペレーティング システム展開に必要なすべてのハードウェア情報で設定されています。

## システム プロファイル

システム プロファイルには、iDRAC、BIOS、RAID、イベント フィルター、FC、NIC のコンポーネントレベルの設定と構成が記録されます。これらの設定は、ベアメタル サーバーへオペレーティング システムを展開する際に他の同一サーバーに適用できます。クラスタ プロファイルでシステム プロファイルを使用して、設定のベースラインを維持することができます。

### 前提条件

システム プロファイルを作成または編集する前に、次を確認してください。

- ・ CSIOR 機能は、参照サーバーで有効になっています。iDRAC から返されたデータが最新の状態になるように、CSIOR を有効にした後で参照サーバーを再起動する必要があります。
- ・ OMIVV で、vCenter が管理する各参照ホスに対してインベントリー操作が正常に実行されている。
- ・ ベアメタル サーバーに必要な BIOS およびファームウェアの最小バージョンがインストールされている。詳細に関しては、サポート サイトで入手可能な『OMIVV 互換性マトリックス』を参照してください。
- ・ 参照サーバーとターゲット サーバーは同種です (モデル、ハードウェア構成、ファームウェア レベルが同じということ)。
- ・ ハードウェア (FC、NIC、および RAID コントローラーなど) は、参照サーバーとターゲット サーバーの同一のスロットに存在します。
- ・ デフォルトの選択内容に属性を追加または除外する前に、属性名の上にマウスカーソルを合わせて属性の詳細を確認してください。
- ・ iDRAC の検出に使用される iDRAC ユーザーは、システム プロファイルで iDRAC ユーザーを設定するときに選択されます。

**i** **メモ:** ベアメタルの検出に使用される、iDRAC ユーザーにリンクされている属性をクリアしないでください。クリアすると、システム プロファイルの展開ジョブが失敗します。

- ・ iDRAC の検出に使用される iDRAC ユーザーのユーザー名は変更しないでください。変更すると、iDRAC の接続問題が発生し、属性が適用されずにシステム プロファイルの展開ジョブが失敗します。

システム プロファイルを作成する前に、必要に応じて参照サーバーの属性と値を設定し、それらを必要なすべてのターゲット サーバーに適用することをお勧めします。

プロファイルの適用中に、システム プロファイルが正確なインスタンス (FQDD) を検索します。このプロファイルは、同一のラック サーバーでは正常に動作しますが、モジュラー サーバーでは若干の制限があります。たとえば、FC640 では、1つのモジュラー サーバーから作成されたシステム プロファイルは、NIC レベルの制限によって、同じ FX シャーシ内の他のモジュラー サーバー上に適用できません。この場合、シャーシの各スロットからリファレンス システム プロファイルを用意して、このシステム プロファイルを、対応するスロットのみに対し、シャーシ全体に適用することをお勧めします。

**i** **メモ:** システム プロファイルは起動オプションの有効化/無効化をサポートしていません。

**i** **メモ:**

- ・ システム プロファイルを使用している間は、**Enterprise** ライセンスによるシステム プロファイルのエクスポートと **Express** ライセンスによるサーバーでの同じシステム プロファイルのインポートは失敗します。
- ・ **iDRAC9** ファームウェア **3.00.00.00** の **Express** ライセンスを使用してシステム プロファイルをインポートすることはできません。 **Enterprise** ライセンスを持っている必要があります。

## システム プロファイルの作成

Google Chrome を使用してシステム プロファイルを作成または編集することをお勧めします。

1. OMIVV ホーム ページで、[ **対応性と導入** ] > [ **プロファイル** ] > [ **システム プロファイル** ] > [ **新規プロファイルを作成** ] の順にクリックします。
  2. [ **システム プロファイルの作成** ] ページに表示された手順を読み、[ **開始** ] をクリックします。
  3. [ **名前と説明** ] ページで、次の手順を行います。
    - a) プロファイル名と説明を入力します。[ **説明** ] フィールドはオプション フィールドです。
    - b) 次のシステム プロファイル タイプのいずれかを選択します。
      - ・ 基本 - iDRAC、BIOS、RAID、NIC、FC の最小限の属性セットを表示します。
      - ・ 詳細設定 - iDRAC、BIOS、RAID、NIC、FC、EventFilters のすべての属性を表示します。
  4. [ **参照サーバー** ] ページでホストまたはベアメタルのいずれかである参照サーバーを選択するには、[ **選択** ] をクリックします。次のいずれかの理由により、サーバーの選択が無効になっている可能性があります。
    - ・ サーバーが非対応ホストまたは非対応ベアメタル サーバーである。
    - ・ 展開ジョブがスケジュールされているか、サーバーで実行されている。
    - ・ サーバーがシャーシ認証情報プロファイルを使用して管理されている。
- [ **抽出確認** ] ダイアログ ボックスが表示されます。
5. 参照サーバーからシステム設定を抽出するには、[ **OK** ] をクリックします。参照サーバーからのシステム設定の抽出には、数分かかる場合があります。
  6. 参照サーバーの詳細を確認し、[ **次へ** ] をクリックします。
    - ・ [ **参照サーバーの選択** ] ページで参照サーバーを変更するには、[ **参照** ] をクリックします。参照サーバーがベアメタル タイプの場合は、その iDRAC IP のみが表示されます。参照サーバー自体がホスト サーバーの場合は、iDRAC とホスト ( FQDN ) IP の両方が表示されます。

[ **プロファイル設定** ] ページが表示されます。

7. [ **プロファイル設定** ] ページには、参照サーバーの設定に基づいて、iDRAC、BIOS、RAID、NIC、CNA、FCoE、EvenFilters などのコンポーネントのプロファイル設定を表示または変更することができます。デフォルトでは、プラットフォーム固有の属性や読み取り専用属性はリストされません。プラットフォーム固有属性の詳細については、「**システム固有属性**」を参照してください。

**i** **メモ:** システム プロファイルでは、**擬似属性**が表示されません。詳細については、「**サーバー設定 XML ファイル**」を参照してください。

デフォルトで選択されている属性以外の属性を選択する前に、属性、依存関係、およびその他の詳細の性質を確認します。

デフォルトで選択されている属性以外の属性を選択すると、次のメッセージが表示されます。

これらの属性は、他の依存属性に影響を与える可能性があります。また、本質的に破壊的な属性であり、サーバー ID を分解したり、ターゲットサーバーのセキュリティに影響を与えたりする可能性もあります。

**メモ:** 第 12 世代と第 13 世代の PowerEdge サーバーでは、一部の属性が OMIVV で依存関係を正しくマップしない可能性があります。たとえば、[システム BIOS 設定] でシステム プロファイルが [カスタム] に設定されていない限り、BIOS のメモリー動作電圧コンポーネントは読み取り専用です。

- a) 各コンポーネントを展開して、[インスタンス]、[属性名]、[値]、[破壊的]、[依存関係]、および [グループ] などの設定オプションを表示します。

依存関係テキストが使用できない場合は、空のフィールドが表示されます。

**メモ:** [検索] フィールドを使用して、[値] を除くすべての列で固有データをフィルターできます。

- b) 赤い感嘆符が付いた属性の値の設定は必須です。このオプションは、ユーザー名の有効な iDRAC 対応ユーザーのみが使用できます。

8. [次へ] をクリックします。

[サマリー] ページに、プロファイルの詳細と、システム構成の属性統計に関する情報が表示されます。

属性の合計数、有効な属性の合計数、および破壊的属性の合計数が属性統計の下に表示されます。

9. 終了 をクリックします。

保存されたプロファイルが [システム プロファイル] ページに表示されます。

OMIVV が機能するためにシステム プロファイルの一部の属性が上書きされます。カスタマイズされた属性の詳細については、「[カスタマイズ属性](#)」を参照してください。システム プロファイル設定テンプレート、属性、およびワークフローの詳細については、「[追加情報](#)」を参照してください。

## システム プロファイルの編集

Google Chrome を使用してシステム プロファイルを作成または編集することをお勧めします。

1. [システム プロファイルの作成] ページでシステム プロファイルを選択して、[編集] をクリックします。

2. [名前と説明] ページで、プロファイル名と説明を変更します。説明はオプションです。

**メモ:** 基本または詳細設定システム プロファイルの作成後、プロファイルを変更することはできません。

3. [参照サーバー] ページでホストまたはベアメタルのいずれかである参照サーバーを変更するには、[選択] をクリックします。

次のいずれかの理由により、サーバーの選択が無効になっている可能性があります。

- ・ サーバーが非対応ホストまたはベアメタルサーバーである。
- ・ 展開ジョブがスケジュールされているか、サーバーで実行されている。
- ・ サーバーがシャーシ認証情報プロファイルを使用して管理されている。

[抽出確認] ダイアログ ボックスが表示されます。

4. 参照サーバーからシステム設定を抽出するには、[OK] をクリックします。

参照サーバーからのシステム設定の抽出には、数分かかる場合があります。

5. 参照サーバーの詳細を確認し、[次へ] をクリックします。

- ・ [参照サーバーの選択] ページで参照サーバーを変更するには、[参照] をクリックします。参照サーバーがベアメタルタイプの場合は、その iDRAC IP のみが表示されます。参照サーバー自体がホストサーバーの場合は、iDRAC とホスト (FQDN) IP の両方が表示されます。

[プロファイル設定] ページが表示されます。

6. [プロファイル設定] ページには、参照サーバーの設定に基づいて、iDRAC、BIOS、RAID、NIC、CNA、FCoE、EvenFilters などのコンポーネントのプロファイル設定を表示または変更することができます。デフォルトでは、プラットフォーム固有の属性や読み取り専用属性はリストされません。プラットフォーム固有属性の詳細については、「[システム固有属性](#)」を参照してください。

一部の属性を変更しようとする、次の警告メッセージが表示されます。

これらの属性は、他の依存属性に影響を与える可能性があります。また、本質的に破壊的な属性であり、サーバー ID を分解したり、ターゲットサーバーのセキュリティに影響を与えたりする可能性もあります。



**メモ:** システム プロファイルの編集後、ベアメタルサーバーの検出に使用されている iDRAC ユーザーのパスワードが変更された場合、アップデートされたパスワードは無視され、ベアメタルサーバーの検出に使用されるパスワードに置き換えられます。

- a) 各コンポーネントを展開して、インスタンス、属性名、値、破壊的、依存関係、およびグループなどの設定オプションを表示します。

依存関係テキストが使用できない場合は、空のフィールドが表示されます。

- b) 赤い感嘆符が付いた属性の値の設定は必須です。このオプションは、ユーザー名の有効な iDRAC 対応ユーザーのみが使用できます。
7. [次へ] をクリックします。  
[サマリー] ページに、プロファイルの詳細と、システム構成の属性統計に関する情報が表示されます。  
属性の合計数、有効な属性の合計数、および破壊的属性の合計数が属性統計の下に表示されます。
8. 終了 をクリックします。  
保存されたプロファイルが [システム プロファイル] ページに表示されます。  
OMIVV が機能するためにシステム プロファイルの一部の属性が上書きされます。カスタマイズされた属性の詳細については、「[カスタマイズ属性](#)」を参照してください。システム プロファイル設定テンプレート、属性、およびワークフローの詳細については、「[追加情報](#)」を参照してください。

## システムプロファイルの表示

- OMIVV ホーム ページで、[対応性と導入] > [システム プロファイル] の順にクリックします。  
テーブルに、すべてのシステム プロファイルとともに次の情報が表示されます。
  - [プロファイル名]: システム プロファイルの名前です。
  - [説明]: プロファイルの説明
  - [参照サーバー]: システム設定の詳細の抽出元になった iDRAC IP
  - [サーバー モデル]: 参照サーバーのモデル名です。
- ウィザードの列名の削除または追加を行うには、 をクリックします。
- システム プロファイルの情報をエクスポートするには、 をクリックします。

## システムプロファイルの削除

実行中の展開タスクの一部であるシステムプロファイルを削除すると、削除ジョブが失敗する原因になる可能性があります。


- [システム プロファイル] ページでシステム プロファイルを選択して、[削除] をクリックします。
- [削除の確認] ダイアログ ボックスで、[削除] をクリックします。

## ISO プロファイル

ISO プロファイルには、NFS または CIFS フォルダーに保存された Dell EMC カスタマイズ ESXi ISO イメージ ファイルへのフォルダーパスが含まれています。ISO プロファイルは導入ウィザードで使用されます。

## ISO プロファイルの作成



ISO プロファイルでは、NFS または CIFS 上の Dell EMC カスタマイズ ISO ファイルの場所を指定する必要があります。

- OMIVV ホーム ページで、[対応性と導入] > [プロファイル] > [ISO プロファイル] > [新規プロファイルを作成] の順にクリックします。
- ウィザードの [ISO プロファイル] ページに表示された手順を読み、[開始] をクリックします。
- [プロファイル名と説明] ページで、プロファイル名と説明を入力します。[説明] フィールドはオプションです。
- [インストール元 (ISO)] ボックスで、ISO ファイルの場所 (NFS または CIFS) を入力します。  
 **メモ:** OMIVV は、サーバー 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。
  - CIFS を使用する場合は、認証情報を入力します。
- [ESXi バージョン] ドロップダウン リストで、ESXi のバージョンを選択します。  
適切なインストール起動スクリプトが使用されるように、正しい ESXi バージョンを選択してください。誤った ESXi バージョンを選択すると、導入に失敗する可能性があります。
- [テストを開始] をクリックして、ISO ファイル パスにアクセスできるかどうかと認証情報を検証します。  
テストの結果が表示されます。
- 終了 をクリックします。

## ISO プロファイルの編集

1. OMIVV ホーム ページで、[ 対応性と導入 ] > [ プロファイル ] > [ ISO プロファイル ] の順にクリックします。
2. ISO プロファイルを選択し、[ 編集 ] をクリックします。
3. [ プロファイル名と説明 ] ページで、プロファイル名と説明を編集します。[ 説明 ] フィールドはオプションです。
4. [ インストール元 ( ISO ) ] ボックスで、ISO ファイルの場所 ( NFS または CIFS ) を変更します。
  - ① **メモ:** OMIVV は、サーバー 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。
    - a) CIFS を使用する場合は、認証情報を入力します。
5. [ ESXi バージョン ] ドロップダウンリストで、ESXi のバージョンを選択します。  
適切なインストール起動スクリプトが使用されるように、正しい ESXi バージョンを選択してください。誤った ESXi バージョン  
を選択すると、導入に失敗する可能性があります。
6. [ テストを開始 ] をクリックして、ISO ファイル パスと認証を検証します。  
テストの結果が表示されます。
7. **終了** をクリックします。

## ISO プロファイルの表示

1. OMIVV ホーム ページで、[ 対応性と導入 ] > [ ISO プロファイル ] の順にクリックします。  
テーブルに、すべての ISO プロファイルとともに次の情報が表示されます。
  - ・ [ プロファイル名 ]: プロファイルの名前
  - ・ [ 説明 ]: プロファイルの説明
  - ・ [ インストール元 ]: ISO ファイルの場所 ( NFS または CIFS )
  - ・ [ ESXi ベース バージョン ]: ESXi のベース バージョン
2. ウィザードの列名の削除または追加を行うには、 をクリックします。
3. ISO プロファイル情報をエクスポートするには、 をクリックします。

## ISO プロファイルの削除

実行中の導入タスクの一部となっている ISO プロファイルを削除すると、導入タスクが失敗する可能性があります。

1. OMIVV ホーム ページで、[ 対応性と導入 ] > [ プロファイル ] > [ ISO プロファイル ] の順に選択します。
2. ISO プロファイルを選択し、[ 削除 ] をクリックします。
3. [ 確認 ] ダイアログ ボックスで、[ 削除 ] をクリックします。

## カスタム Dell EMC ISO イメージのダウンロード

展開に必要なすべての Dell EMC ドライバーを含むカスタム ESXi イメージです。

1. ブラウザーを開いて、support.dell.com にアクセスします。
2. **すべての製品の参照** > **サーバー** > **PowerEdge** の順にクリックします。
3. PowerEdge サーバモデルをクリックします。
4. サーバモデルのドライバーおよびダウンロードページをクリックします。
5. オペレーティング システムドロップダウン リストから、ESXi バージョンを選択します。
6. カテゴリドロップダウン メニューからエンタープライズ ソリューションを選択します。
7. エンタープライズ ソリューションリストで、必要な ISO バージョンを選択し、**ダウンロード** をクリックします。

## 管理対応性

OMIVV でホストを表示および管理するには、それぞれのホストが特定の条件を満たしている必要があります。ホストが対応性基準を満たしていない場合、OMIVV でこのホストは管理および監視されません。OMIVV には、ホストの非対応に関する詳細が表示され、該当する場合は非対応箇所を修正できます。

ホストは次の場合に非対応になります。

- ・ ホストがホスト認証情報プロファイルに関連付けられていない。
- ・ 再起動時のシステム インベントリー収集 (CSIOR) 機能が無効化されている、または実行されたことがないので手動の再起動が必要。
  - ① **メモ:** ホストがシャーシを使用して管理されている場合、CSIOR のステータスは判別されません。
- ・ ホストの SNMP トラップ送信先が、OMIVV アプライアンスの IP アドレスに設定されていません。SNMP トラップ送信先の設定でエラーが発生した場合、ホスト認証情報プロファイルで指定されている iDRAC またはホストの認証情報が無効である可能性があります。または、iDRAC に空きスロットがないか、iDRAC ロックダウン モードがオンになっています (iDRAC9 ベース サーバーのみ)。iDRAC9 ベース サーバーのリストについては、「互換性マトリックス」を参照してください。
- ・ OMIVV が、ESXi 6.5 以降を実行しているホスト上の WBEM サービスの有効化に失敗する。
- ・ iDRAC ファームウェアのバージョンが 2.50.50.50 より前である。iDRAC バージョン 2.50.50.50 以降は、システム プロファイル機能を使用する場合にのみ必要です。
- ・ iDRAC ライセンスに互換性がありません (iDRAC Express が最小要件です)。互換性のある iDRAC ライセンスがないサーバーは、ファームウェアの監視およびアップデートには使用できません。

**△ 注意:** 非対応であっても、ロックダウン モードのホストは対応性テストに表示されません。こうしたホストの対応性レベルは手動でチェックしてください。手動でチェックを行うと、メッセージが表示されます。このメッセージは無視してください。表示されないのは対応状態が確認できないためです。これらのシステムの対応状況は手動で確認してください。このようなシナリオでは、警告メッセージが表示されます。

[管理対応性] ページでは、次のタスクを実行できます。

- ・ 対応性の修正。詳細については、次を参照してください：[非対応ホストの修正](#)
- ・ インベントリーの実行。ホスト認証情報プロファイルに関連付けられたホストのいずれかの iDRAC の対応状態が「非対応」または「不明」の場合には、[インベントリージョブを実行] リンクがアクティブになります。
- ・ iDRAC ライセンスの更新。詳細については、「[iDRAC ライセンスの対応性の修正](#)」を参照してください。
- ・ OEM ホストの追加。OEM ホストの追加に関する詳細については、「[OEM ホストの追加](#)」を参照してください。

## 非対応ホストの表示

1. OMIVV ホーム ページで、[対応性と導入] > [管理対応性] の順にクリックします。

テーブルに、すべての非対応ホストと次の情報が表示されます。

- ・ [ホスト]: ホストの FQDN または IP アドレス
- ・ [モデル]: サーバーのモデル名。
- ・ [認証情報プロファイル]: ホスト認証情報プロファイルの名前
- ・ [CSIOR ステータス]: CSIOR のステータス ([オン] または [オフ])。CSIOR ステータスは、シャーシを使用して管理されているホストでは [判別不能] と表示されます。
- ・ [SNMP トラップ ステータス]: SNMP トラップのステータス ([設定済み] または [未設定])
- ・ [ハイパーバイザー]: ハイパーバイザーの名前とバージョン。
- ・ [WBEM ステータス]: WBEM のステータス ([対応] または [非対応])。CSIOR ステータスは、シャーシを使用して管理されているホストでは [該当なし] と表示されます。
- ・ [iDRAC ファームウェア バージョン]: iDRAC のファームウェアのバージョン。
- ・ [iDRAC ライセンス ステータス]: iDRAC ライセンスのステータス ([対応] または [非対応])

- メモ:** PowerEdge MX ホストがシャーシ認証情報プロファイルを使用して管理されている場合、[ 対応性の管理 ] ページでは iDRAC ファームウェア バージョンは [ 該当なし ] と表示されます。これは、iDRAC ファームウェアの対応性が iDRAC9 ベース サーバーには適用できないためです。iDRAC9 ベース サーバーのリストについては、「互換性マトリックス」を参照してください。

## 非対応ホストの修正

ホストは次の場合に非対応になります。

- ホストがホスト認証情報プロファイルに関連付けられていない。
- 再起動時のシステム インベントリ収集 (CSIOR) 機能が無効化されている、または実行されたことがないので手動の再起動が必要。
- メモ:** ホストがシャーシを使用して管理されている場合、CSIOR のステータスは判別されません。
- ホストの SNMP トラップ送信先が、OMIVV アプライアンスの IP アドレスに設定されていません。SNMP トラップ送信先の設定でエラーが発生した場合、ホスト認証情報プロファイルで指定されている iDRAC またはホストの認証情報が無効である可能性があります。または、iDRAC に空きスロットがないか、iDRAC ロックダウン モードがオンになっています (iDRAC9 ベース サーバーのみ)。iDRAC9 ベース サーバーのリストについては、「互換性マトリックス」を参照してください。
- OMIVV が、ESXi 6.5 以降を実行しているホスト上の WBEM サービスの有効化に失敗する。
- iDRAC ファームウェアのバージョンが 2.50.50.50 より前である。iDRAC バージョン 2.50.50.50 以降は、システム プロファイル機能を使用する場合にのみ必要です。
- iDRAC ライセンスに互換性がありません (iDRAC Express が最小要件です)。互換性のある iDRAC ライセンスがないサーバーは、ファームウェアの監視およびアップデートには使用できません。

- OMIVV ホーム ページで、[ 対応性と導入 ] > [ 管理対応性 ] の順にクリックします。
- 非対応ホストを選択し、[ 対応性を修正 ] をクリックします。
- ウィザードの [ ようこそ ] ページに表示された手順を読み、[ 開始 ] をクリックします。
- [ ホストの選択 ] ページで非対応ホストを1つ以上選択して、[ 次へ ] をクリックします。

- ホストがホスト認証情報プロファイルに関連付けられていない場合は、次の警告メッセージが表示されます。

ホスト認証情報プロファイルに割り当てられていないホストが選択されています。OMIVV が対応性チェックを実行できるようにするには、これらのホストをホスト認証情報プロファイルに追加する必要があります。

ホスト認証情報プロファイルに割り当てられていないホストを除外するには、[ 続行 ] をクリックします。

[ ホスト認証情報プロファイル ] ページにホストを追加するには、[ キャンセル ] をクリックし、ホスト認証情報プロファイル ページに移動します。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。

iDRAC IPv4 が無効になっている MX シャーシに存在するホストは、シャーシ認証情報プロファイルを使用して管理する必要があります。これらのホストをシャーシ認証情報プロファイルに関連付けるには、[ Dell EMC シャーシ ] ページの [ MX シャーシの追加 ] を使用してシャーシを追加し、そのシャーシをシャーシ認証情報プロファイルに関連付ける必要があります。

iDRAC ファームウェアおよび BIOS バージョンをアップデートするには、次の手順を実行します。

- [ iDRAC ファームウェアと BIOS バージョンのアップデート ] ページで、ファームウェアのバージョンをアップデートするホストを1つ以上選択します。
- [ 次へ ] をクリックします。
- [ ホストの再起動 ] ページで、再起動の必要がある ESXi ホストを確認します。
- ホストを自動でメンテナンス モードにして、必要に応じて再起動するには、チェック ボックスを選択して [ 次へ ] をクリックします。
- [ サマリー ] ページでアクションの結果の概要を確認し、[ 終了 ] をクリックします。

CSIOR をオンにするには、次の手順を実行します。

- [ ホストの選択 ] ページで非対応ホストを1つ以上選択して、[ 次へ ] をクリックします。
- [ CSIOR をオンにする ] ページで、CSIOR をオンにするホストを1つ以上選択して [ 次へ ] をクリックします。
- [ サマリー ] ページでアクションの結果の概要を確認し、[ 終了 ] をクリックします。

ホスト認証情報プロファイルに有効な情報を提供して iDRAC またはホスト認証情報を修正するか、iDRAC のトラップ宛先で最初の4つのスロットのいずれかを使用可能にするか、または iDRAC でシステム ロックダウン モードを無効にすると、ウィザードは SNMP トラップ送信先ステータスを [ 設定済み ] に設定します。

- メモ:** システム ロックダウン モードは iDRAC9 ベースのサーバーのみに適用されます。

WBEM 非対応ホストが存在する場合は、WBEM サービスの有効化に失敗する原因となるそれらのホストの状態を手動で修正してください。エラー状態は、ユーザー ログに表示することで修正ができます。OMIVV を有効にし、インベントリー中にこれらのホストに対して WBEM サービスを有効にします。

## iDRAC ライセンスの対応性の修正

互換性のある iDRAC ライセンスは、ホストの対応性基準の 1 つです。ホストに互換性のある iDRAC ライセンスがない場合、それらのホストは [ 管理対応性 ] ページで非対応ホストとしてリストされます。任意の非対応ホストをクリックすると、iDRAC の有効期限、ライセンス タイプ、ライセンスの説明などの詳細が表示されます。ホスト認証情報プロファイルに関連付けられたホストのいずれかの iDRAC の対応状態が [ 非対応 ] または [ 不明 ] の場合には、[ インベントリーを **実行** ] リンクがアクティブになります。

1. iDRAC ライセンスの対応を修正するには、OMIVV ホーム ページで、[ 対応性と導入 ] > [ 対応性 ] > [ 管理対応性 ] の順にクリックします。
2. iDRAC ライセンスが非対応であるホストを選択し、[ **iDRAC ライセンスの更新** ] をクリックします。
3. Dell Digital Locker にログインし、新しい iDRAC ライセンスにアップデートまたは購入します。  
iDRAC ライセンスのインストール後、ホスト用にインベントリージョブを実行し、インベントリージョブが正常に完了した後で、このページに戻ります。

## OEM サーバのサポート

OEM サーバは、PowerEdge サーバと同様の機能やポートフォリオを提供する Dell EMC パートナーが提供しています。

- ・ OMIVV 4.3 以降では、OEM ラック サーバがサポートされています。
- ・ **OEM ホストの追加** ウィザードを使用して、OEM サーバをオンボーディングします。OEM ホストの追加に関する詳細については、「**OEM ホストの追加**」を参照してください。
  - ① **メモ:** WBEM サービスが OEM ホストですでに有効になっていて、vCenter に追加されている場合は、デフォルトで OMIVV が OMIVV 管理対象リストにこれらの OEM サーバを追加します。ホストをホスト認証情報プロファイルに関連付けて、これらのサーバを管理します。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。
- ・ オンボーディング後、すべてのホスト管理プロセスは、Dell EMC PowerEdge サーバの管理方法と同様になります。
- ・ ベアメタルおよび展開機能は、iDRAC を使用して OEM サーバでもサポートされています。

## OEM ホストの追加

OMIVV は、Dell EMC PowerEdge サーバに加えて、ブランド変更済みサーバおよび非ブランド化済みサーバもサポートします。OEM の詳細については、<https://www.dellemc.com> を参照してください。

WBEM サービスが既に有効になっている場合は、OMIVV がホストの iDRAC の接続方法を決定します。接続可能な場合は、OMIVV がホストを管理下リストに追加します。OMIVV が決定できない場合は、**OEM ホストの追加** ウィザードでホストを手動で選択して、ホストを OMIVV 管理下リストに追加する必要があります。

WBEM サービスが無効になっているか、iDRAC に到達できない場合は、**OEM ホストの追加** ウィザードを使用して、ホストを OMIVV 管理リストに追加します。

1. OMIVV ホーム ページで、[ 対応性と導入 ] > [ 対応性 ] > [ 管理対応性 ] > [ **OEM ホストの追加** ] の順にクリックします。
2. [ **OEM ホストの追加** ] ウィンドウで、[ vCenter インスタンス ] ドロップダウン リストから vCenter のインスタンスを選択します。
3. [ **ホスト認証情報プロファイル** ] ドロップダウン リストから、適切なホスト認証情報プロファイルを選択します。
4. 関連付けられているホストを追加または削除するには、[ **ホストの追加** ] をクリックします。  
ホストの **選択** ウィンドウが表示されます。
5. ホストの **選択** ウィンドウで、ホストを選択して **はい** をクリックします。

① **メモ:** OMIVV によって管理されていないホストのみが、ホストの **選択** ウィンドウに表示されます。

OMIVV は接続を自動的にテストし、テスト接続の結果が [ **OEM ホストの追加** ] ウィンドウに表示されます。

[ **iDRAC テスト** ] および [ **ホスト テスト** ] 列に [ **iDRAC 認証情報** ] および [ **ホスト認証情報** ] に対するテスト接続結果が表示されます。

すべてのテスト接続を中止するには、[ **テストの中止** ] をクリックします。

6. [ **OK** ] をクリックします。  
選択したホストが選択したホスト認証情報プロファイルに追加され、インベントリーがトリガーされます。

# 設定コンプライアンス

[設定コンプライアンス] ページには、クラスター プロファイルに関連付けられたすべてのクラスターのドリフト検出に基づく、コンプライアンスの状態が表示されます。複数の vCenter サーバーがある PSC 環境では、設定コンプライアンス ページに、同じアプライアンスに登録された同じ PSC に属するすべての vCenter からすべてのクラスターが一覧表示されます。

- ・ ハードウェア設定コンプライアンス - クラスター プロファイルで使用されるシステム プロファイルと関連するホスト (クラスターの一部) の間の、属性のドリフトが表示されます。
- ・ ファームウェアコンプライアンス - クラスター プロファイルで使用されるファームウェア リポジトリ プロファイルと関連するホスト (クラスターの一部) の間の、ファームウェア バージョンのドリフトが表示されます。
- ・ ドライバーコンプライアンス - クラスター プロファイルで使用されるドライバー リポジトリ プロファイルと関連する vSAN ホスト (クラスター プロファイルの一部) の間の、ドライバー バージョンドリフトが表示されます。

## 設定コンプライアンスの表示

1. OMIVV ホームページで、[対応性と導入] > [対応性] > [設定コンプライアンス] の順に選択します。  
表に、クラスター プロファイル、システム プロファイル、ファームウェア リポジトリ プロファイル、およびドライバー リポジトリ プロファイルが関連付けられたクラスターが表示されます。

基本および詳細システム プロファイル タイプの場合、システム プロファイル名は Basic\_<システム プロファイル名>、Advanced\_<システム プロファイル名>の形式で表示されます。

2. [設定コンプライアンス] ページで、クラスターを選択します。  
設定コンプライアンス情報と対応状態が表示されます。

[設定コンプライアンス] セクションには、次の情報が表示されます。

- ・ [クラスター名]: クラスターの名前
- ・ [対応状態]: 対応性の状態 (対応または非対応) を表示します。クラスター内のいずれかのホストが非対応である場合、状態は非対応と表示されます。
- ・ [ホスト数]: クラスター内に存在するホストの総数
- ・ [スケジュール]: 次のドリフト検出ジョブがスケジュールされている日時。
- ・ [最終ドリフト検出時間]: 最後のドリフト検出ジョブが完了した日時。

[対応状態] セクションには、ハードウェア、ファームウェア、およびドライバー コンポーネントの対応状態が表示されます。対応状態には、以下があります。

- ・ **対応**: 関連付けられているハードウェア、ファームウェア、およびドライバー コンポーネントに対応しているホストの数が表示されます。
- ・ **非対応**: 関連付けられたハードウェア、ファームウェア、およびドライバー コンポーネントに非対応のホストの数が表示されます。
- ・ **該当なし**: 該当しないホストの数が表示されます。

ハードウェアドリフトは、シャシ認証情報プロファイルを使用して管理されているホストには適用されません。

ドライバードリフトは、vSphere クラスターの一部であるホストには適用されません。

クラスター プロファイルがオンライン カタログを使用して作成されている場合、ファームウェアの対応性は vSAN クラスターには適用されません。

3. ドリフトの詳細を表示するには、[ドリフトレポートの表示] をクリックします。このリンクは、非対応クラスターに対してのみ有効になります。ドリフトレポートの表示の詳細については、「[ドリフトレポートの表示](#)」を参照してください。

## ドリフトレポートの表示

[設定コンプライアンス レポート] ページには、ハードウェア、ファームウェア、およびドライバー コンポーネントのドリフトの詳細が表示されます。

ドリフト検出ジョブのステータスは [サマリー] セクションに表示されます。

ハードウェアの場合:

- ・ ホスト名または IP - ホスト IP またはホスト名です。
- ・ サービス タグ - ホストのサービス タグです。
- ・ ドリフト ステータス - ドリフトのステータス (非対応または失敗) です。
- ・ インスタンス - ハードウェアコンポーネントの名前です。

- ・ グループ - 属性のグループ名です。
- ・ 属性名 - 属性の名前です。
- ・ 現在の値 - ホスト内の属性の現在の値です。
- ・ ベースライン値 - ベースラインの値です。
- ・ ドリフトタイプ/エラー - 非対応の理由です。ドリフトタイプの詳細については、「[コンポーネントとベースラインのバージョン比較表](#)」を参照してください。

**メモ:** ドリフト検出ジョブは、ホストまたは iDRAC に到達できない場合にのみ失敗します。ホストまたは iDRAC のインベントリが正常に行われると、ドリフト検出ジョブは成功と表示されます。その他のドリフト検出ジョブの失敗理由を確認するには、ドリフトレポートの [ドリフトタイプ/エラー] 列を参照してください。

ファームウェアおよびドライバーの場合：

- ・ ホスト名または IP - ホスト IP またはホスト名です。
- ・ サービス タグ - ホストのサービス タグです。
- ・ ドリフト ステータス - ドリフトのステータスです。
- ・ コンポーネント名 - コンポーネントの名前です。
- ・ 現在の値 - ホスト内の属性の現在の値です。
- ・ ベースライン値 - ベースラインの値です。
- ・ ドリフトタイプ/エラー - 非対応の理由です。ドリフトタイプの詳細については、「[コンポーネントとベースラインのバージョン比較表](#)」を参照してください。
- ・ 重要度 (ファームウェアの場合) - 指定コンポーネントのバージョンアップデートの重要度レベルです。
- ・ 推奨 (ドライバー用) - ドライバーコンポーネントの推奨アップデートを示します。

**メモ:** 利用可能なファームウェアバージョンが複数ある場合、対応性の比較には常に最新のファームウェアバージョンが使用されます。



フィルターオプションを使用すると、ドリフトステータスごとにドリフトの詳細を表示できます。

**メモ:** 5.x では、32 ビット版ファームウェアバンドルはサポートされていません。クラスタープロファイルが 4.x バージョンの 32 ビット版ファームウェアバンドルに関連付けられている場合、バックアップを実行して 4.x から 5.x に復元すると、ドリフトステータスが [失敗] と表示されます。クラスタープロファイルを含む 64 ビット版ファームウェアバンドルを使用して、ドリフト検出ジョブを再実行します。

**メモ:** OMIVV と vSphere Lifecycle Manager のドリフトレポートに不整合がある場合があります。これは、vSphere Lifecycle Manager が常に実況のドリフトレポートを表示し、OMIVV はスケジュールされた日時に基づいてドリフトレポートを表示するためです。ドリフトレポートが一致していない場合は、[ドリフト検出ジョブ] ページでドリフト検出ジョブをオンデマンドで実行します。

## 展開ジョブ




展開タスクが完了したら、[展開ジョブ] ページで展開ジョブのステータスを追跡できます。

- OMIVV ホーム ページで、[ジョブ] > [展開ジョブ] の順にクリックします。  
テーブルに、次の情報と共にすべての展開ジョブが表示されます。
  - [名前]: 展開ジョブ名
  - [説明]: ジョブの説明
  - [スケジュールされた時刻]: ジョブがスケジュールされた日時。
  - [ステータス]: 展開ジョブのステータス。
  - [コレクション サイズ]: 展開ジョブにおけるサーバーの台数。
  - [進捗状況サマリー]: 展開ジョブの進捗状況の詳細。
- 展開ジョブにおけるサーバーの詳細を表示するには、展開ジョブを選択します。  
次の情報が下部のペインに表示されます。
  - サービスタグ
  - iDRAC IP
  - ステータス
  - 警告
  - 詳細
  - 開始日時
  - 終了日時
  - 詳細
  - 展開ジョブの詳細を表示するには、ジョブを選択し、[詳細] 列の上でポインタを留めます。
  - システム プロファイル ベースのジョブの失敗の詳細については、[詳細] をクリックしてください。  
次の情報が表示されます。
    - コンポーネントの FQDD
    - 属性の値
    - 古い値
    - 新しい値
    - エラーに関するメッセージとメッセージ ID (いくつかのタイプのエラーには表示されません)
 [システム プロファイルの適用 - エラーの詳細] ウィンドウの [属性名] の下に表示されるいくつかの属性は、[詳細] をクリックしたときに表示されるシステム プロファイルの属性名と同じではありません。
- 展開ジョブを停止するには、 をクリックします。
- 展開ジョブをバージするには、 をクリックし、[日付とジョブステータスより古い] を選択して、[適用] をクリックします。  
その後、選択したジョブが [展開ジョブ] ページからクリアされます。

## シャーシ ファームウェア アップデート ジョブ




シャーシのファームウェア アップデート タスクが完了すると、[シャーシ ファームウェア アップデート ジョブ] ページでファームウェア アップデート ジョブのステータスを表示できるようになります。


- OMIVV ホーム ページで、[ジョブ] > [ファームウェア アップデート] > [シャーシ ファームウェア アップデート] の順にクリックします。
- 最新のログ情報を表示するには、更新アイコンをクリックします。  
テーブルに、すべてのシャーシ ファームウェア アップデート ジョブとともに次の情報が表示されます。
  - ステータス - ファームウェア アップデート ジョブのステータス
  - スケジュールされた時刻 - ファームウェア アップデート ジョブがスケジュールされた時刻

- ・ **名前** - ジョブの名前
  - ・ **説明** - ファームウェア アップデート ジョブの説明
  - ・ **vCenter** - vCenter の名前
  - ・ **コレクション サイズ** - ファームウェア アップデート ジョブに含まれるシャーシの数  
シャーシの合計数には、リード シャーシとスタンダアロン シャーシのみが含まれます。メンバー シャーシは参加しません。
  - ・ **進捗状況サマリー** - ファームウェア アップデート ジョブの進捗状況詳細
3. 特定のジョブに関する詳細情報を表示するには、そのジョブを選択します。  
次の情報が下部のグリッドに表示されます。
- ・ **シャーシ サービス タグ** - シャーシのサービス タグ
  - ・ **ステータス** - ジョブのステータス
  - ・ **開始時刻** - ファームウェア アップデート ジョブの開始時刻
  - ・ **終了時刻** - ファームウェア アップデート ジョブの終了時刻
4. 実行中ではないスケジュール済みファームウェア アップデートを停止するには、停止するジョブを選択し、 をクリックします。
-  **警告:** すでに **MX** シャーシに送信済みのファームウェア アップデート ジョブを停止した場合、ホストではそのファームウェアがそのままアップデートされる可能性があります。**OMIVV** は、ジョブをキャンセル済みとして報告します。
5. 以前のファームウェア アップデート ジョブまたはスケジュール済みファームウェア アップデートをページするには、 をクリックします。  
ファームウェア アップデート ジョブのページ ダイアログボックスが表示されます。ページできるのは、キャンセルされたジョブ、成功したジョブ、または失敗したジョブのみで、スケジュール済みジョブやアクティブなジョブはページできません。
6. [ファームウェア アップデート ジョブのページ] ダイアログボックスで [日付とジョブ ステータスより古い] を選択し、[OK] をクリックします。  
選択したジョブが [シャーシ ファームウェア アップデート] ジョブリストからクリアされます。

## ホスト ファームウェア アップデート ジョブ


シャーシ ファームウェア アップデート タスクが完了すると、[ホスト ファームウェア アップデート ジョブ] ページでファームウェア アップデート ジョブのステータスを表示できます。

1. OMIVV ホーム ページで、[ジョブ] > [ファームウェア アップデート] > [ホスト ファームウェア アップデート] の順にクリックします。
2. 最新のログ情報を表示するには、更新アイコンをクリックします。  
テーブルに、すべてのホスト ファームウェア アップデート ジョブとともに次の情報が表示されます。
- ・ **ステータス** - ファームウェア アップデート ジョブのステータス
  - ・ **スケジュールされた時刻** - ファームウェア アップデート ジョブがスケジュールされた時刻
  - ・ **名前** - ジョブの名前
  - ・ **説明** - ファームウェア アップデート ジョブの説明
  - ・ **vCenter** - vCenter の名前
  - ・ **コレクション サイズ** - ファームウェア アップデート ジョブにおけるサーバーの台数
  - ・ **進捗状況サマリー** - ファームウェア アップデート ジョブの進捗状況詳細
3. 特定のジョブに関する詳細情報を表示するには、そのジョブを選択します。  
次の情報が下部のグリッドに表示されます。
- ・ **ホスト名** - ホストのサービス タグ
  - ・ **ステータス** - ジョブのステータス
  - ・ **開始時刻** - ファームウェア アップデート ジョブの開始時刻
  - ・ **終了時刻** - ファームウェア アップデート ジョブの終了時刻
-  **メモ:** ファームウェア アップデート ジョブが複数の **Dell** アップデート パッケージでスケジュールされている場合、**OMIVV** は、選択されたアップデート パッケージの一部のダウンロードに失敗しても、正常にダウンロードされたパッケージのアップデートは続行します。[ジョブ] ページには、正常にダウンロードされたパッケージのステータスが表示されます。
4. 実行中ではないスケジュール済みファームウェア アップデートを停止するには、停止するジョブを選択し、 をクリックします。
-  **警告:** すでに **iDRAC** に送信済みのファームウェア アップデート ジョブを停止した場合、ホストではそのファームウェアがそのままアップデートされる可能性があります。**OMIVV** は、ジョブをキャンセル済みとして報告します。

5. 以前のファームウェア アップデート ジョブまたはスケジュール済みファームウェア アップデートをページするには、 をクリックします。  
ファームウェアアップデートジョブのページ ダイアログボックスが表示されます。ページできるのは、キャンセルされたジョブ、成功したジョブ、または失敗したジョブのみで、スケジュール済みジョブやアクティブなジョブはページできません。
6. [ファームウェア アップデート ジョブのページ] ダイアログボックスで [日付とジョブステータスより古い] を選択し、[OK] をクリックします。  
選択したジョブが [ホスト ファームウェア アップデート] ジョブ リストからクリアされます。


## システムロックダウンモードジョブ

システム ロックダウン モードの設定は、iDRAC9 ベースのサーバーに対してのみサポートされています。この設定をオンにするとファームウェアアップデートなどのシステム構成がロックされます。この設定は、システムが誤って変更されないようにするためのものです。管理対象のホストのシステムロックダウンモードは、OMIVV アプライアンス、または iDRAC コンソールを使用してオンまたはオフにすることができます。OMIVV バージョン 4.1以降から、サーバで iDRAC のロックダウンモードを設定および監視することができます。また、ロックダウンモードを有効にするには、iDRAC にエンタープライズライセンスが必要です。

 **メモ:** シャーシ認証情報プロファイルを使用して管理されるホストのシステム ロックダウン モードをユーザーが変更することはできません。


システム ロックダウン設定の完了後、ロックダウン モードの最新の状態を [システム ロックダウン モード ジョブ] ページで確認できます。

1. OMIVV ホーム ページで、[ジョブ] > [システム ロックダウン モード] の順にクリックします。  
テーブルに、すべてのシステム ロックダウン モード ジョブとともに次の情報が表示されます。
  - ・ **名前** - システム ロックダウン モードのジョブ名
  - ・ [説明]: ジョブの説明
  - ・ **スケジュール時刻** - システム ロックダウン モード ジョブがスケジュールされた日付と時刻です。
  - ・ **vCenter** - vCenter の名前
  - ・ **ステータス** - システム ロックダウン モード ジョブのステータス
  - ・ **コレクション サイズ** - システム ロックダウン モード ジョブに含まれるサーバーの数
  - ・ **進捗状況サマリー** - システム ロックダウン モード ジョブの進捗状況詳細
2. システム ロックダウン モード ジョブに含まれるサーバーの詳細を表示するには、任意のシステム ロックダウン モード ジョブを選択します。  
次の情報が下部のグリッドに表示されます。
  - ・ **サービスタグ**
  - ・ **iDRAC IP**
  - ・ **ホスト名**
  - ・ **ステータス**
  - ・ **詳細**
  - ・ **開始日時**
  - ・ **終了日時**


システム ロックダウン モード ジョブの詳細を表示するには、ジョブを選択して、ポインタを [詳細] 列の上で停止させます。
3. システム ロックダウン モード ジョブをページするには、 をクリックし、[日付とジョブステータスより古い] を選択して、[適用] をクリックします。  
選択したジョブが [システム ロックダウン モード] ジョブ ページからクリアされます。

## ドリフト検出ジョブ

ドリフト検出ジョブを実行すると、検証済みのベースラインと、ハードウェア構成やファームウェアとドライバのバージョンなどのサーバ設定との比較が行われます。

 **メモ:** ドリフト検出ジョブは、ホストまたは iDRAC に到達できない場合にのみ失敗します。ホストまたは iDRAC が正常にインベントリされると、ドリフト検出ジョブが正常に実行され、ドリフトレポートでドリフトの詳細を表示できます。ドリフトレポートの詳細については、「[ドリフトレポートの表示](#)」を参照してください。

1. OMIVV ホーム ページで、[ジョブ] > [ドリフト検出] の順にクリックします。  
テーブルに、すべてのドリフト検出ジョブとともに次の情報が表示されます。
  - ・ **名前** - ドリフト検出ジョブの名前
  - ・ **最終実行** - 最後のドリフト検出ジョブを実行した日付と時刻です。

- ・ **次の実行** - 次のドリフト検出ジョブがスケジュールされている日時です。
  - ・ **ステータス** - ドリフト検出ジョブのステータス
  - ・ **コレクション サイズ** - ドリフト検出ジョブにおけるサーバーの台数
  - ・ **進捗状況サマリー** - ドリフト検出ジョブの進捗状況詳細
- 更新された [ドリフト検出ジョブの詳細] を表示するには、[更新] をクリックします。
  - ドリフト検出ジョブ内のサーバーの詳細情報を表示するには、ドリフト検出ジョブを選択します。次の情報が表示されます。
    - ・ サービスタグ
    - ・ iDRAC IP
    - ・ ホスト名
    - ・ クラスタ
    - ・ vCenter
    - ・ ステータス
    - ・ 開始日時
    - ・ 終了日時
  - ドリフト検出ジョブをオンデマンドで実行するには、 をクリックします。  
ベースラインのクラスターでは、ホスト認証情報プロファイルまたはシャーシ認証情報プロファイルにホストを追加すると、新たに追加されたホスト上でドリフト検出ジョブが自動的に実行されます。

## ホスト インベントリー ジョブの表示

[ホスト インベントリー] ページには、ホスト認証情報プロファイルに関連付けられたホストで実行された最新のインベントリー ジョブに関する情報が表示されます。


- OMIVV ホーム ページで、[ジョブ] > [インベントリー] > [ホスト インベントリー] の順にクリックします。
- vCenter を選択すると、関連付けられているホスト インベントリー ジョブの情報がすべて表示されます。
  - ・ **vCenter** - vCenter の FQDN または IP アドレスです。
  - ・ **ホスト合格** — インベントリーが正常に行われたホストの数です
  - ・ **最終インベントリー** — 最後のインベントリーの実行日時です
  - ・ **次のインベントリー** — 次のインベントリーがスケジュールされている日時です

下側のペインには、関連付けられているホストの詳細が表示されます。

- ・ **ホスト** - ホストの FQDN または IP アドレスです。
- ・ **ステータス** - ホストのインベントリー ステータスを表示します。次のステータスがあります。
  - ・ 成功
  - ・ 失敗
  - ・ 進行中
- ・ **継続時間 (MM:SS)** - インベントリー ジョブの継続時間 (分および秒) です。
- ・ **開始日時** — インベントリー ジョブが開始された日付と時刻です
- ・ **終了日時** - インベントリー ジョブが完了した日付と時刻です。

## インベントリー ジョブの実行

初期設定が完了すると、ホスト認証情報プロファイルに追加されたすべてのホストについて、自動的にインベントリーが開始されます。

- インベントリーをオンデマンドで実行するには、[ジョブ] > [インベントリー] > [ホスト インベントリー] の順にクリックします。
- [今すぐ実行] () をクリックします。
- インベントリージョブのステータスを見るには、**更新** をクリックします。  
インベントリージョブの完了後、[OMIVV ホスト情報] ページのホスト情報を表示することができます。
- OMIVV ホスト情報を表示するには、[メニュー] を展開し、[ホストとクラスター] を選択します。
- 左ペインで、任意のホストを選択します。
- 右ペインで [モニター] を選択し、[OMIVV ホスト情報] を展開します。  
次の情報が表示されます。
  - ・ ハードウェアインベントリ

- ・ 保管時
- ・ ファームウェア
- ・ 電源モニタ
- ・ 保証
- ・ システムイベントログ

シャーシ認証情報プロファイルを使用してホストを管理している場合、ファームウェア インベントリ データに、Lifecycle Controller やソフトウェア RAID などのいくつかの追加コンポーネントが表示されます。

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

7. [サマリー] ページの [OMIVV ホスト情報] セクションで、次のアクションを実行することもできます。

- ・ Remote Access Console (iDRAC) の起動
- ・ 点滅式サーバー LED インジケーター
- ・ システムロックダウンモードの設定



ホストがシャーシを使用して管理されている場合、システムロックダウンモードの設定はサポートされません。

- ・ ファームウェア ウィザードの実行

## ホスト インベントリ ジョブの変更

ホストをホスト認証情報プロファイルに関連付けた後、ホストのインベントリ情報が最新であることを確認するために、インベントリを定期的にスケジュールする必要があります。インベントリ ジョブには、ホストで実行されているインベントリ ジョブのステータスが表示されます。

インベントリ スケジュールは、[設定] > [データ取得スケジュール] > [インベントリの取得] ページでも変更できます。

1. [ジョブ] ページで vCenter インスタンスを選択し、 をクリックします。  
[インベントリ データの取得] ダイアログ ボックスが表示されます。
2. [インベントリ データ] セクションで、次の手順を実行します。
  - a) [インベントリ 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。
  - b) インベントリ データの取得日時を選択し、[適用] をクリックします。
  - c) 設定をリセットするには、[クリア] をクリックします。
  - d) インベントリ ジョブを今すぐ実行するには、[ジョブ] ページで、 をクリックします。

**i** **メモ:** iDRAC Express または Enterprise ライセンスを持たないサーバーでは、iDRAC のライセンス アップグレードが必要のため、インベントリが失敗します。

**i** **メモ:** モジュラーホストのインベントリを実行すると、対応するシャーシが自動的に検出されます。シャーシがシャーシ認証資格プロファイルの一部である場合、シャーシ インベントリはホスト インベントリ後に自動的に実行されます。

## シャーシ インベントリ ジョブの表示

[シャーシ インベントリ] ページには、シャーシ認証情報プロファイルに関連付けられたシャーシで実行された最新のインベントリ ジョブに関する情報が表示されます。


1. OMIVV ホーム ページで [ジョブ] > [インベントリ] > [シャーシ インベントリ] をクリックします。
2. シャーシ インベントリ情報を表示するには、シャーシを選択します。
  - ・ シャーシ IP/ホスト名: シャーシの IP アドレス
  - ・ サービス タグ - シャーシのサービス タグを表示します。サービス タグは、サポートとメンテナンスのためにメーカーが提供する一意の識別子です。
  - ・ ステータス - シャーシのステータス
  - ・ 継続時間 (MM:SS) - ジョブの継続時間 (分と秒)
  - ・ 開始日時 - インベントリ ジョブが開始された日付と時刻です。
  - ・ 終了日時 - インベントリ ジョブが完了した日付と時刻です。

MCM グループでは、インベントリはリードシャーシでのみ実行されます。インベントリ情報では、リードとメンバシャーシの両方に関するデータを参照できます。

**i** **メモ:** PowerEdge サーバー C6320P、C6320、C4130、C6420 では、シャーシ インベントリ ジョブはサポートされません。

- メモ:** MX シャーシブレードサーバは、ESXi 6.5U2 以降のバージョンでのみサポートされます。それ以前のバージョンの ESXi がこれらのホスに導入されている場合、インベントリジョブは OMIVV で失敗します。

## シャーシのインベントリジョブの実行


1. OMIVV ホーム ページで、[ **ジョブ** ] > [ **シャーシ インベントリ** ] の順にクリックします。
2. シャーシを選択し、[ **今すぐ実行** ] (  ) をクリックします。  
シャーシ インベントリが完了したら、[ **ホストとシャーシ** ] > [ **シャーシ** ] ページでシャーシ情報を表示できます。
3. シャーシ情報を表示するには、[ **シャーシ** ] ページでシャーシを選択し、[ **表示** ] をクリックします。

**メモ:** インベントリ時に、トラップの送信先およびアラートポリシーが MCM グループのリードシャーシ上で OMIVV によって設定されます。

**メモ:** ホストがシャーシを使用して管理されている場合、シャーシインベントリを実行すると、ホストのホストインベントリもトリガされます。また、ホスト インベントリを実行すると、シャーシ インベントリがトリガーされます。


## ホスト保証の表示

保証ジョブは、すべてのシステムに関する保証情報を [www.dell.com/support](http://www.dell.com/support) から取得するスケジュールされたタスクです。保証情報を抽出するには、OMIVV アプライアンスがインターネットと接続している必要があります。ネットワークの設定によっては、インターネットに接続して保証情報を取得するために、OMIVV でプロキシ情報が必要になる可能性があります。プロキシの詳細は、管理コンソールで更新できます。

1. OMIVV ホーム ページで、[ **ジョブ** ] > [ **保証** ] > [ **ホスト保証** ] の順にクリックします。
2. vCenter を選択すると、関連付けられているホストの情報が表示されます。
  - ・ **vCenter** - vCenter のリスト
  - ・ [ **ホスト合格** ] — 合格した vCenter ホストの数
  - ・ [ **前の保証** ]: 最後の保証ジョブを実行した日付と時刻が表示されます。
  - ・ [ **次の保証** ]: 次回の保証ジョブを実行する日付と時刻が表示されます。下側のペインには、関連付けられているホストの情報が表示されます。
  - ・ **ホスト** - ホストの IP アドレス
  - ・ **ステータス** - 保証ジョブのステータス。次のオプションがあります。
    - ・ 成功
    - ・ 失敗
    - ・ 進行中
    - ・ スケジュール済み
  - ・ **継続時間 (MM:SS)** - 保証ジョブの継続時間 (MM:SS 単位)
  - ・ **開始日時** — 保証ジョブが開始された日付と時刻
  - ・ **終了日時** — 保証ジョブが終了した時刻
3. ホスト保証をオンデマンドで実行するには、[ **今すぐ実行** ] (  ) をクリックします。

## ホスト保証ジョブの変更

保証ジョブは最初、**初期設定ウィザード** で設定されます。保証ジョブ スケジュールは、[ **設定** ] > [ **データ取得スケジュール** ] > [ **保証の取得** ] ページで変更することもできます。

1. [ **ジョブ** ] ページで [ **保証** ] を展開し、[ **ホスト保証** ] を選択します。
2. vCenter を選択し、 をクリックします。
3. [ **保証データ** ] セクションで、次の手順を実行します。
  - a) [ **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。
  - b) 保証データの取得日時を選択し、[ **適用** ] をクリックします。
  - c) 設定をリセットするには、[ **クリア** ] をクリックします。

# シャーシ保証の表示

保証ジョブは、すべてのシステムに関する保証情報を Support.dell.com から取得するスケジュールされたタスクです。保証情報を抽出するには、OMIVV アプライアンスがインターネットと接続している必要があります。OMIVV アプライアンスがインターネットに接続されていることを確認します。ネットワークの設定によっては、インターネットに接続して保証情報を取得するために、OMIVV でプロキシ情報が必要になる可能性があります。プロキシの詳細は、管理コンソールで更新できます。


1. OMIVV ホーム ページで、[ **ジョブ** ] > [ **保証** ] > [ **シャーシ保証** ] の順にクリックします。

テーブルに、すべてのシャーシ保証ジョブ情報が表示されます。

- ・ **シャーシ IP/ホスト名** - ホスト IP アドレス
- ・ **サービス タグ** - シャーシのサービス タグ
- ・ **ステータス** - 保証ジョブのステータス。次のオプションがあります。
  - ・ 成功
  - ・ 失敗
  - ・ 進行中
  - ・ スケジュール済み
- ・ **継続時間 (MM:SS)** - 保証ジョブの継続時間 (MM:SS 単位)
- ・ **開始日時** - 保証ジョブが開始された日付と時刻です。
- ・ **終了日時** - 保証ジョブが終了した時刻です。

2. シャーシ保証ジョブをオンデマンドで実行するには、[ **今すぐ実行** ] (▶) をクリックします。

## ログ履歴の表示

1. [ **OpenManage Integration for VMware vCenter** ] ページで、すべてのログを表示するには、[ **ログ** ] をクリックします。  
OMIVV のログ取得プロセスでは、データベースからすべてのログが取得されます。ログ サイズによっては数秒かかる場合があります。
  - ・ ログ データをエクスポートするには、 をクリックします。
  - ・ グリッド内のデータを並べ替えるには、行のヘッダーをクリックします。
  - ・ ページ間を移動するには、前へアイコンと次へアイコンをクリックします。
  - ・ ログを更新するには、左上隅にある更新アイコンをクリックします。
2. ▼をクリックすると、次のカテゴリや日付範囲に基づいてログをフィルターできます。  
[ **カテゴリ** ]:
  - ・ **すべてのカテゴリ**
  - ・ **情報**
  - ・ **警告**
  - ・ **エラー**[ **日付** ]:
  - ・ **過去 1 週間**
  - ・ **過去 1 か月**
  - ・ **過去 1 年間**
  - ・ [ **カスタム範囲** ]: このオプションを選択した場合は、カレンダー アイコンをクリックして開始日と終了日を指定します。
3. 目的のカテゴリと日付を選択したら、[ **適用** ] をクリックします。  
選択したカテゴリまたは日付範囲に関連するログを表示できます。ログ データ テーブルには、一度に 1 ページ 100 個のログが表示されます。
4. フィルター処理されたデータをクリアするには、[ **フィルターのクリア** ] をクリックします。

## OMIVV アプライアンス設定の管理

[ 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。詳細については、次を参照してください：[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。詳細については、次を参照してください：[アプライアンスの最新バージョン通知の設定](#)
- ・ Proactive HA アラートの重大度のオーバーライド。詳細については、次を参照してください：[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。詳細については、次を参照してください：[初期設定](#)
- ・ イベントとアラームの設定および表示。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](#)
- ・ インベントリおよび保証のデータ取得スケジュールの設定または変更。詳細については、「[インベントリジョブのスケジュール](#)」および「[保証取得ジョブのスケジュール](#)」を参照してください。

### 複数アプライアンスの管理

複数の vCenter インスタンスが同じ PSC を共有し、OMIVV アプライアンスの複数のインスタンスで登録されている場合、アプライアンスの切り替えウィザードを使用して OMIVV の異なるインスタンスを切り替えることができます。

OMIVV の現在のインスタンスは、ホーム ページで確認できます。

1. [ **OMIVV** ] ホーム ページで、[ **変更** ] をクリックします。
  - ・ **IP/名前** - OMIVV アプライアンスの FQDN または IP
  - ・ **バージョン** - OMIVV アプライアンスの現在のバージョン
  - ・ **対応ステータス** - バージョンに基づいた OMIVV アプライアンスのステータス ([ **対応** ] または [ **非対応** ])
  - ・ **可用性ステータス** - OMIVV サービスが実行されているかどうかに基づいた OMIVV アプライアンスの可用性ステータス。[ **OK** ] または [ **エラー** ] が表示され、OMIVV の稼働状態を示します。
  - ・ **登録済み vCenter サーバー** - 登録済みの vCenter サーバー FQDN または IP
  - ・ **アクション** - アクション名 ([ **選択** ] または [ **選択済み** ])
2. [ **OMIVV アプライアンスの切り替え** ] ページで [ **選択** ] をクリックします。
3. 確定するには、[ **はい** ] をクリックします。  
アプライアンス IP の変更は、ホーム ページで確認できます。

### 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が必要な場合は、管理者ポータルでプロキシ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。

## ハードウェアコンポーネントの冗長性の正常性— Proactive HA

Proactive HA は、OMIVV で動作する vCenter 機能です。Proactive HA を有効にすると、この機能がホスト内でサポートされるコンポーネントの冗長性の正常性の低下に基づいてプロアクティブに対応することによりワークロードを保護します。

サポートされるホストコンポーネントの冗長性の正常性ステータスを評価した後で、OMIVV アプライアンスは、vCenter サーバに対して正常性ステータスの変更をアップデートします。サポートされるコンポーネント（電源装置、ファン、および iSDM）で利用できる冗長性の正常性ステータスは次の通りです。

- ・ 正常（情報）— コンポーネントが通常通りに動作しています。
- ・ 警告（中程度の劣化）— コンポーネントに重大ではないエラーが発生しています。中程度の劣化ステータスは、[イベント] ページの [タイプ] 列に、[警告] と表示されます。
- ・ 重要（深刻な劣化）— コンポーネントには重大な障害があります。

**メモ:** 正常性ステータスが **不明** の場合、Dell Inc プロバイダからの任意の Proactive HA の正常性のアップデートが利用できないことを示します。不明の正常性ステータスは次の場合に発生することがあります。

- ・ Proactive HA クラスタに追加されるすべてのホストは、OMIVV が適切な状態に初期化されるまでの数分間は、不明な状態のままとなる場合があります。
- ・ vCenter サーバを再起動すると、OMIVV が再度適切な状態に初期化されるまで、Proactive HA クラスタのホストが不明な状態となる場合があります。

OMIVV が、サポートされるコンポーネントの冗長性の正常性ステータスでの変更を検出した場合は（トラップまたはポーリング経由で）、コンポーネントの正常性のアップデート通知が vCenter サーバに送信されます。ポーリングは毎時間実行され、トラップの損失の可能性に対応するためのフェールセーフメカニズムとして使用できます。

**メモ:**

- ・ イベントを設定する際は、[すべてのイベントを掲載する] オプションをイベント掲載レベルとして選択することをお勧めします。イベント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。
- ・ Proactive HA は、電源、ファン、および iSDM の冗長性をサポートするプラットフォーム上でのみ使用できます。
- ・ Proactive HA 機能は、冗長性を設定できない PSU ではサポートされていません（たとえば、ケーブル接続式 PSU）。

## Proactive HA のイベント

Proactive HA の VMware でサポートされるコンポーネントに基づいて、vCenter による登録中に Dell Inc プロバイダによって次のイベントが登録されます。

表 5. Dell Proactive HA イベント

Dell Inc プロバイダのイベント	コンポーネントタイプ	説明
DellFanRedundancy	ファン	ファンの冗長性イベント
DellPowerRedundancy	電源装置ユニット ( PSU )	電源の冗長性イベント
DellIDSDMRedundancy	ストレージ	IDSDM の冗長性イベント <b>i</b> <b>メモ:</b> ホストが <b>Proactive HA 対応</b> のクラスターに追加されていて、IDSDM コンポーネントが存在する場合、iDRAC 設定で [ 内蔵 SD カードの冗長性 ] が「ミラー」に設定されていることを確認します。

Proactive HA が有効化されたホストでは、次のトラップが、コンポーネントの冗長性の正常性を判断するトリガーとして OMIVV によって使用されます。

表 6. Proactive HA のイベント

イベント名	説明	重大度
ファン情報	ファン情報	情報
ファン警告	ファン警告	警告
ファン障害	ファン障害です	重要
電源装置正常	電源装置が正常に戻りました	情報
電源装置警告	電源装置が警告を検出しました	警告
電源装置エラー	電源装置がエラーを検出しました	重要
電源装置がありません	電源装置がありません	重要
冗長性情報	冗長性情報	情報
冗長性低下	冗長性が低下しています	警告
冗長性喪失	冗長性が喪失しました	重要
内蔵デュアル SD モジュールの情報です	内蔵デュアル SD モジュール ( IDSDM ) の情報です	情報
内蔵デュアル SD モジュールの警告です	内蔵デュアル SD モジュールの警告です	警告
内蔵デュアル SD モジュールエラーです	内蔵デュアル SD モジュールエラーです	重要
内蔵デュアル SD モジュールが不在です	内蔵デュアル SD モジュールが不在です	重要
内蔵デュアル SD モジュールの冗長性情報です	内蔵デュアル SD モジュールの冗長性情報です	情報
内蔵デュアル SD モジュールの冗長性が劣化しています	内蔵デュアル SD モジュールの冗長性が劣化しています	警告
内蔵デュアル SD モジュールの冗長性が失われました	内蔵デュアル SD モジュールの冗長性が失われました	重要
シャーシイベント		
ファン情報	ファン情報	情報
ファン警告	ファン警告	警告
ファン障害	ファン障害です	重要
電源装置正常	電源装置が正常に戻りました	情報

イベント名	説明	重大度
電源装置警告	電源装置が警告を検出しました	警告
電源装置エラー	電源装置がエラーを検出しました	重要
冗長性情報	冗長性情報	情報
冗長性低下	冗長性が低下しています	警告
冗長性喪失	冗長性が喪失しました	重要

## ラック サーバーおよびタワー サーバーの Proactive HA の設定

すべてのホストが、サポート対象の3つのすべての冗長コンポーネント（電源装置、ファン、および iDRAC）の冗長性に対して設定されていることを確認します。

1. ホスト認証情報プロファイルを作成し、ホストをホスト認証情報プロファイルに関連付けます。「[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。
2. ホストインベントリが正常に完了したことを確認します。「[ホストインベントリジョブの表示](#)」を参照してください。
3. iDRAC での SNMP トラップ送信先が OMIVV アプライアンスの IP アドレスとして設定されていることを確認します。  
**① メモ:** ログ データから、Proactive HA クラスターのホストの可用性を確認します。
4. クラスターでの Proactive HA の有効化「[クラスターでの Proactive HA の有効化](#)」を参照してください。

## モジュラー型サーバーの Proactive HA の設定

モジュラーサーバ用に Proactive HA を設定する前に、次の条件が満たされていることを確認します。

- ・ すべてのホストが、サポート対象の3つのすべての冗長コンポーネント（電源装置、ファン、および iDRAC）の冗長性に対して正しく設定されています。
- ・ ホストおよびシャーシインベントリが正常に完了しています。

**① メモ:** シャーシ コンポーネント (PSU およびファン) の障害は関連付けられているすべてのサーバーに影響するため、Proactive HA クラスター内のすべてのモジュラー ホストを同じシャーシ内に配置しないようにすることを推奨します。

1. ホスト認証情報プロファイルを作成し、ホストをホスト認証情報プロファイルに関連付けます。「[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。
2. ホストインベントリが正常に完了したことを確認します。「[ホストインベントリジョブの表示](#)」を参照してください。  
**① メモ:** ログ データから、Proactive HA クラスターのホストの可用性を確認します。
3. 関連付けられているシャーシのシャーシ認証情報プロファイルを作成します。「[シャーシ認証情報プロファイルの作成](#)」を参照してください。
4. シャーシインベントリが正常に完了したことを確認します。「[シャーシインベントリジョブの表示](#)」を参照してください。
5. CMC または OME-Modular を起動し、シャーシのトラップ送信先が OMIVV アプライアンスの IP アドレスとして設定されていることを確認します。トラップの設定の詳細については、[dell.com/support](http://dell.com/support) から入手できる『CMC および OME-Modular ユーザーズ ガイド』を参照してください。
6. クラスターでの Proactive HA の有効化「[クラスターでの Proactive HA の有効化](#)」を参照してください。

## クラスターでの Proactive HA の有効化

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

- ・ vCenter コンソールに DRS が有効にされているクラスターが作成され、設定されています。クラスターで DRS を有効にするには、VMware のマニュアルを参照してください。
  - ・ クラスターの一部であるすべてのホストは、ホスト認証情報プロファイルの一部であり、正常にインベントリされる必要があります。
  - ・ モジュラー型サーバーの場合、対応するシャーシをシャーシ認証情報プロファイルに追加し、正常にインベントリする必要があります。
1. vSphere Client で [メニュー] を展開し、[ホストとクラスター] を選択します。  
すべてのホストとクラスターが左ペインに表示されます。

2. クラスターを選択し、右ペインで [ vSphere DRS ] > [ 編集 ] をクリックします。
3. [ vSphere DRS ] が選択されていない場合は選択します。
4. [ 設定 ] > [ vSphere の可用性 ] > [ Proactive HA ] > [ 編集 ] の順に選択します。  
[ クラスター設定の編集 ] ページが表示されます。
5. [ クラスター設定の編集 ] ページで、[ Proactive HA ] を選択します。
6. [ 障害と対応 ] セクションで、自動化レベルのドロップダウンメニューから [ 手動 ] または [ 自動化 ] を選択します。
7. 修正 に、重要度のステータスに基づいて、隔離モード、メンテナンスモード、または隔離とメンテナンスモードの両方の組み合わせを選択します。詳細については、VMware のマニュアルを参照してください。
8. [ プロバイダー ] をクリックし、クラスターのプロバイダーとして [ Dell Inc ] を選択します。
9. [ 保存 ] をクリックします。

クラスターで Proactive HA が有効にされると、OMIVV は Proactive HA の正常性と冗長性の状態を初期化し、vCenter に報告します。OMIVV からの正常性アップデート通知に基づいて、vCenter Server は、[ 修正 ] に選択された手動または自動アクションを実行します。


既存の重大度をオーバーライドするには、「[正常性のオーバーライド重大度のアップデート通知](#)」を参照してください。

## 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。


## 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、[非対応ホストの修正](#)」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。インベントリジョブのスケジュールの詳細については、「[インベントリジョブのスケジュール](#)」を参照してください。
- 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** ] > [ **インベントリの取得** ] または [ **ジョブ** ] > [ **インベントリ** ] > [ **ホストのインベントリ** ] 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 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。

## 初期設定ステータスの表示

初期設定ウィザード ページでは、次の操作を実行できます。

- ・ 初期設定ステータスの表示  
初期設定ステータスは、すべての vCenter がホスト認証情報プロファイル、イベントとアラーム、インベントリ、および保証ジョブで設定されている場合にのみ完了と表示されます。
- ・ 初期設定ウィザードを起動します。

## ファームウェア アップデート設定

[ **iDRAC ジョブをクリアして iDRAC をリセットする** ] チェックボックスを選択すると、ホスト上でファームウェアをアップデートする前に、[ **ジョブキュー** ] に存在するすべての iDRAC ジョブがクリアされ、iDRAC がリセットされます。

[ **iDRAC ジョブをクリアして iDRAC をリセットする** ] 設定は、以下を実行するときに使用されます。

- ・ OMIVV を使用したファームウェア アップデート  
OMIVV を使用してファームウェアをアップデートするときに、この設定はオーバーライドすることができます。ただし、設定をオーバーライドしても、[ **ファームウェア アップデート設定** ] ページで行った設定には影響しません。
- ・ vSphere Lifecycle Manager を使用したファームウェアの修復  
この設定は、ファームウェア修復の実行中は上書きできません。

1. [ **iDRAC ジョブをクリアして iDRAC をリセットする** ] チェックボックスを選択します。

2. [ **適用** ] をクリックします。

# ライセンス情報の表示

OMIVV ライセンスをアップロードすると、サポートされているホストと vCenter サーバーの数がこのタブに表示されます。

ソフトウェアライセンスを購入するには、[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。詳細については、「ソフトウェアライセンスの購入」を参照してください。

[ライセンス] ページに、次の情報が表示されます。

## ライセンスの種類 説明

- |               |  |
|---------------|--|
| ホストのライセンス     | <ul style="list-style-type: none"><li>使用可能なライセンス<br/>使用可能なライセンスの数を表示します</li><li>使用中のライセンス<br/>使用中のライセンス数を表示します</li></ul> |
| vCenter ライセンス | <ul style="list-style-type: none"><li>使用可能なライセンス<br/>使用可能なライセンスの数を表示します</li><li>使用中のライセンス<br/>使用中のライセンス数を表示します</li></ul> |

[ライセンス管理] セクションには、次のリンクが表示されます。

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

# 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。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。

1 つの XML キーのライセンス期間は、元の注文の販売日に基づいて計算されます。アップロードされた新しいライセンスは、以前の期限切れのライセンスに対して 90 日の猶予期間が終了した後、カウントに反映されます。

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:** 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せん。

## 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。

## サポート情報へのアクセス

表 7. サポート ページの情報

名前	説明
マニュアルのサポート	次のマニュアルのリンクを提供します。 <ul style="list-style-type: none"><li>・ PowerEdge サーバ</li><li>・ OMIVV のマニュアル</li><li>・ Lifecycle Controller 使用 iDRAC</li></ul>
管理コンソール	管理コンソールへのリンクを提供します。
一般的なヘルプ	Dell EMC サポート サイトへのリンクを提供します。
iDRAC のリセット	iDRAC が応答しないときに使用できる、iDRAC をリセットするためのリンクです。このリセットは、通常の iDRAC の再起動を実行します。iDRAC のリセットの詳細については、「 <a href="#">iDRAC のリセット</a> 」を参照してください。
テクニカルサポートに連絡する前に	Dell EMC サポート への連絡方法と正しい電話の転送についてのヒントが記載されています。
トラブルシューティング バンドル	トラブルシューティングバンドルを作成およびダウンロードするためのリンクを提供します。テクニカルサポートにお問い合わせの際は、このバンドルを提供または表示することができます。詳細については、「 <a href="#">トラブルシューティング バンドルの作成およびダウンロード</a> 」を参照してください。
Dell EMC 推奨	Dell EMC Repository Manager ( DRM ) サポート ページへのリンクを提供します。DRM はカスタム カタログを作成するために使用され、ファームウェアおよびドリフト検出のアップデートに使用できます。

## トラブルシューティング バンドルの作成およびダウンロード

トラブルシューティング バンドルを生成するには、管理者ポータルにログインしていることを確認してください。

トラブルシューティング バンドルには、問題の解決やテクニカル サポートへの送信に役立つ OMIVV アプライアンスのログ情報が含まれています。

1. [サポート] ページで、[トラブルシューティング バンドルの作成およびダウンロード] をクリックします。  
[トラブルシューティング バンドル] ダイアログボックスが表示されます。
2. [トラブルシューティング バンドル] ダイアログボックスで [作成] をクリックします。  
ログのサイズによっては、バンドルの作成に時間がかかる場合があります。
3. ファイルを保存するには、[ダウンロード] をクリックします。

## iDRAC のリセット

iDRAC をリセットすると、iDRAC は通常の再起動を実行します。iDRAC のリセット後、iDRAC は通常再起動されますが、ホストは再起動されません。リセット後、iDRAC は数分後に使用できます。iDRAC が OMIVV アプライアンスで応答しない場合にのみリセットします。

- ・ このリセット処置を適用できるホストは、少なくとも1回、インベントリー操作を行っているホスト認証情報プロファイルに含まれるホストに限ります。
- ・ ホストをメンテナンス モードに切り替えてから iDRAC をリセットすることをお勧めします。
- ・ iDRAC のリセット後、iDRAC が使用できなくなったり、応答が停止したりした場合は、iDRAC をハード リセットします。ハード リセットの詳細については、<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 の再起動中、次の状況が生じる場合があります。

- ・ OMIVV がホストの正常性ステータスを取得する間の通信遅延。
- ・ 現在 iDRAC に対して開かれているすべてのセッションが終了します。
- ・ iDRAC の DHCP アドレスの変更。iDRAC が IP アドレスの生成に DHCP を使用している場合、iDRAC IP アドレスが変わることがあります。この場合、ホストのインベントリー ジョブを再度実行して、インベントリー データで新規 iDRAC IP アドレスを取得します。

1. [ サポート ] ページで、[ **iDRAC のリセット** ] をクリックします。
2. [ **iDRAC のリセット** ] ページで、ホスト名または IP アドレスを入力します。
3. iDRAC のリセット プロセスを理解していることを確認するため、[ **iDRAC のリセットの効果について理解しています。選択したホストで iDRAC のリセットを続行します** ] を選択します。
4. [ **iDRAC のリセット** ] をクリックします。

## vCenter 設定の管理

### イベントおよびアラームについて

[設定] ページで、ホストおよびシャーシのイベントとアラームを有効にしたり、イベント掲載レベルを選択したり、デフォルトアラームを復元することができます。vCenter ごとにイベントとアラームを設定することも、すべての登録済み vCenter に対してイベントとアラームを設定することもできます。シャーシに対応するイベントとアラームは vCenter に関連付けられます。

次に 4 つのイベント掲載レベルを示します。

表 8. イベント掲載レベル

イベント	説明
イベントは掲載しない	OMIVV がイベントやアラートを関連付けられた vCenter に転送しないようにします。
すべてのイベントを掲載する	OMIVV が管理対象の Dell EMC ホストから受信する、非公式イベントも含めてすべてのイベントを、関連付けられた 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掲載する	重要または警告イベントのみを関連付けられた vCenter に掲載します。
仮想化関連の重要、および警告イベントのみを掲載する	ホストから受信する仮想化関連イベントのみを、関連 vCenter に掲載します。仮想化関連イベントとは、仮想マシンを実行しているホストにとって最も重要であるとデルが選定したイベントです。

イベントとアラームを設定する際に、重要なハードウェアアラームによって、OMIVV アプライアンスがホストシステムをメンテナンスモードに切り替えることがあります。場合によっては、仮想マシンを別のホストシステムに移行します。OMIVV は、管理対象ホストから受信したイベントを vCenter に転送し、それらのイベントのアラームを作成します。このアラームを使い、vCenter に対し、再起動、保守モードまたは移行などの措置を起動できます。

たとえば、電源が故障しアラームが生成された場合、その結果の措置としてマシンがメンテナンスモードになり、ワークロードがクラスター内の別のホストに移行されます。

クラスター外のホスト、または VMware Distributed Resource Scheduling (DRS) が起動されていないクラスターにあるホストでは、重要イベントのために仮想マシンはシャットダウンされる可能性があります。Dell アラームを有効にする前に DRS を有効にすることをお勧めします。詳細に関しては、VMware マニュアルを参照してください。

DRS はリソースプール全体の使用率を連続的に監視し、使用可能なリソースをビジネスニーズに従って各仮想マシンにインテリジェントに割り当てます。重要なハードウェアイベントの際に仮想マシンが自動的に移行されるようにするには、DRS と Dell アラームが設定されたクラスターを使用します。画面上のメッセージの詳細に記載されているのは、この vCenter インスタンスにある、影響を受ける可能性のあるクラスターです。イベントとアラームを有効化する前に、クラスターが影響を受けるかどうか確認してください。

初期設定のアラーム設定に戻すには、[アラームの復元] オプションを選択します。このオプションは、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オプションです。インストール以降に Dell EMC アラーム設定が変更された場合、[アラームの復元] で元に戻すことができます。

**メモ:** Dell イベントを受信するには、必要なイベントを iDRAC、CMC、および管理コントローラーで有効にします。

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

# 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。
  - ① **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。
  - ① **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。
  - ① **メモ:** BMC トラップにはメッセージ ID がいないため、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。
  - ① **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。

## シャーシ イベントの表示

1. vSphere Client で [ メニュー ] を展開し、[ ホストとクラスター ] を選択します。
2. 左ペインで、vCenter のインスタンスを選択します。
3. 右ペインで、[ モニター ] > [ タスクとイベント ] > [ イベント ] をクリックします。
4. 詳細を表示するには、特定のイベントを選択します。
  - ① **メモ:** MCM 構成の PowerEdge Mx シャーシの場合、イベントのソースはリード シャーシとして表示されます。ただし、メッセージの詳細には、識別のためにメンバー シャーシのサービス タグが表示されます。

## シャーシ アラームの表示

1. vSphere Client で [ メニュー ] を展開し、[ ホストとクラスター ] を選択します。
2. 左ペインで、vCenter のインスタンスを選択します。
3. 右ペインで、[ 監視 ] > [ 問題とアラーム ] > [ トリガーされたアラーム ] の順にクリックします。
4. [ トリガーされたアラーム ] で、アラーム名をクリックしてアラーム定義を表示します。

## アラームおよびイベントの設定の表示

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

1. OMIVV ホーム ページで、[ 設定 ] > [ イベントとアラーム ] をクリックします。

次の詳細が表示されます。

- ・ Dell EMC ホスト用の vCenter アラーム - [ 有効 ] または [ 無効 ] が表示されます。
- ・ イベント掲載レベル

2. イベントとアラームを設定します。「[イベントとアラームの設定](#)」を参照してください。

イベント掲載レベルを表示するには、「[イベントおよびアラームについて](#)」を参照してください。

## 仮想化関連のイベント

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

仮想化関連のイベントは、次の形式で表示されます。

デルメッセージ ID : <ID 番号>、メッセージ : <メッセージの説明>。

シャーシイベントは、次の形式で表示されます。

デルメッセージ : <メッセージの説明>、シャーシ名 : <シャーシ名>、シャーシサービスタグ : <シャーシサービスタグ>、シャーシの場所 : <シャーシの場所>

表 9. 仮想化イベント

イベント名	説明	重大度	推奨処置
Dell-電流センサーが警告値を検出しました	指定したシステムの電流センサーが警告しきい値を超えました	警告	処置は不要
Dell-電流センサーが障害値を検出しました	指定したシステムの電流センサーが障害しきい値を超えました	エラー	システムをメンテナンスモードにしてください
Dell-電流センサーが回復不可能な値を検知しました	指定したシステムの電流センサーが回復不可能なエラーを検出しました	エラー	処置は不要
Dell-冗長性回復	センサーが正常値に戻りました	情報	処置は不要
Dell-冗長性低下	指定したシステムの冗長性センサーが、冗長性ユニットのいずれかのコンポーネントで障害が発生したが、ユニットは引き続き冗長であることを検出しました	警告	処置は不要
Dell-冗長性喪失	指定したシステムの冗長性センサーが、冗長性ユニットのコンポーネントの1つが切断された、故障した、または存在しないことを検出しました	エラー	システムをメンテナンスモードにしてください
Dell-電源装置が正常に戻りました	センサーが正常値に戻りました	情報	処置は不要
Dell-電源装置が警告を検出しました	指定したシステムの電源装置センサー読み取り値が、ユーザー定義可能な警告しきい値を超えました	警告	処置は不要

イベント名	説明	重大度	推奨処置
Dell-電源装置が障害を検知しました	電源装置の接続が切断されているか、故障しました	エラー	システムをメンテナンスモードにしてください
Dell-電源装置センサーが回復不可能な値を検知しました	指定したシステムの電源装置センサーが、回復不可能なエラーを検知しました	エラー	処置は不要
Dell-メモリデバイスステータス警告	メモリデバイスの修正レートが許容値を超えました	警告	処置は不要
Dell-メモリデバイスエラー	メモリデバイスの修正レートが許容値を超えた、メモリスベアバンクがアクティブになった、またはマルチビットのECCエラーが発生しました	エラー	システムをメンテナンスモードにしてください
Dell-ファンエンクロージャがシステムに挿入されました	センサーが正常値に戻りました	情報	処置は不要
Dell-ファンエンクロージャがシステムから取り外されました	指定したシステムからファンエンクロージャが取り外されました	警告	処置は不要
Dell-ファンエンクロージャがシステムから長時間取り外されました	ユーザー定義可能な時間にわたって、指定したシステムからファンエンクロージャが取り外されたままになっています	エラー	処置は不要
Dell-ファンエンクロージャセンサーが回復不可能な値を検知しました	指定したシステムのファンエンクロージャセンサーが、回復不可能なエラーを検知しました	エラー	処置は不要
Dell-AC 電源が回復しました	センサーが正常値に戻りました	情報	処置は不要
Dell-AC 電源喪失警告	AC 電源コードが電源を失いましたが、これを警告として分類するだけの十分な冗長性があります	警告	処置は不要
Dell-AC 電源コードが電源を失いました	AC 電源コードが電源を失っており、冗長性不足のため、これをエラーとして分類する必要があります	エラー	処置は不要
Dell-プロセッサセンサーが正常値に戻りました	センサーが正常値に戻りました	情報	処置は不要
Dell-プロセッサセンサーが警告値を検知しました	指定したシステムのプロセッサセンサーがスロットル状態です	警告	処置は不要
Dell-プロセッサセンサーが障害値を検知しました	指定したシステムのプロセッサセンサーが無効になっているか、設定エラーがあるか、またはサーマルトリップが発生しました	エラー	処置は不要
Dell-プロセッサセンサーが回復不可能な値を検知しました	指定したシステムのプロセッサセンサーが故障しました。	エラー	処置は不要
Dell-デバイス設定エラーです	指定したシステムのプラグ可能デバイスで、設定エラーが検出されました	エラー	処置は不要
Dell-バッテリーセンサーが正常値に戻りました	センサーが正常値に戻りました	情報	処置は不要

イベント名	説明	重大度	推奨処置
Dell-バッテリーセンサーが警告値を検出しました	指定されたシステムのバッテリーセンサーが、バッテリーが予測不具合状態にあることを検出しました	警告	処置は不要
Dell-バッテリーセンサーが障害値を検出しました	指定したシステムのバッテリーセンサーが、バッテリーの故障を検出しました	エラー	処置は不要
Dell-バッテリーセンサーが回復不能な値を検知しました	指定したシステムのバッテリーセンサーが、バッテリーの故障を検出しました	エラー	処置の必要なし
Dell-サーマルシャットダウン保護が開始されました	このメッセージは、システムがエラーイベントによるサーマルシャットダウンに設定されたときに生成されます。温度センサー読み取り値がシステムで設定されたエラーしきい値を超えると、オペレーティングシステムがシャットダウンし、システムの電源がオフになります。このイベントは、システムからファンエンクロージャが長い時間取り外されている場合にも、特定のシステムで発生することがあります。	エラー	処置は不要
Dell-温度センサーが正常値に戻りました	センサーが正常値に戻りました	情報	処置は不要
Dell-温度センサーが警告値を検出しました	指定したシステムのバックプレーンボード、システム基板、CPU、またはドライブキャリア上の温度センサーが、警告しきい値を超えました	警告	処置は不要
Dell-温度センサーが障害値を検出しました	指定したシステムのバックプレーンボード、システム基板、またはドライブキャリア上の温度センサーが、障害しきい値を超えました	エラー	システムをメンテナンスモードにしてください
Dell-温度センサーが回復不能な値を検知しました	指定したシステムのバックプレーンボード、システム基板、またはドライブキャリアの温度センサーが、回復不可能なエラーを検出しました	エラー	処置は不要
Dell-ファンセンサーが正常値に戻りました	センサーが正常値に戻りました	情報	処置は不要
Dell-ファンセンサーが警告値を検出しました	ホスト <x> のファンセンサー読み取り値が、警告しきい値を超えました	警告	処置の必要なし
Dell-ファンセンサーが障害値を検出しました	指定したシステムのファンセンサーが、1つまたは複数のファンの障害を検出しました	エラー	システムをメンテナンスモードにしてください
Dell-ファンセンサーが回復不能な値を検知しました	ファンセンサーが回復不可能なエラーを検出しました	エラー	処置は不要
Dell-電圧センサーが正常値に戻りました	センサーが正常値に戻りました	情報	処置は不要

イベント名	説明	重大度	推奨処置
Dell-電圧センサーが警告値を検出しました	指定したシステムの電圧センサーが警告しきい値を超えました。	警告	処置は不要
Dell-電圧センサーが障害値を検出しました	指定したシステムの電圧センサーが障害しきい値を超えました	エラー	システムをメンテナンスモードにしてください
Dell-電圧センサーが回復不能な値を検知しました	指定したシステムの電圧センサーが回復不可能なエラーを検出しました	エラー	処置は不要
Dell-電流センサーが正常値に戻りました	センサーが正常値に戻りました	情報	処置は不要
Dell-ストレージ：ストレージ管理エラー	ストレージ管理がデバイス依存のエラー状態を検出しました	エラー	システムをメンテナンスモードにしてください
Dell-ストレージ：コントローラ警告	物理ディスクの一部が破損しています。	警告	処置は不要
Dell-ストレージ：コントローラ障害	物理ディスクの一部が破損しています。	エラー	システムをメンテナンスモードにしてください
Dell-ストレージ：チャネル障害	チャネル障害です	エラー	システムをメンテナンスモードにしてください
Dell-ストレージ：エンクロージャハードウェア情報	エンクロージャハードウェア情報です	情報	処置は不要
Dell-ストレージ：エンクロージャハードウェア警告	エンクロージャハードウェア警告です	警告	処置は不要
Dell-ストレージ：エンクロージャハードウェアエラー	エンクロージャハードウェアエラーです	エラー	システムをメンテナンスモードにしてください
Dell-ストレージ：アレイディスク障害	アレイディスク障害です	エラー	システムをメンテナンスモードにしてください
Dell-ストレージ：EMM 障害	EMM 障害です	エラー	システムをメンテナンスモードにしてください
Dell-ストレージ：電源装置障害	電源装置障害です	エラー	システムをメンテナンスモードにしてください
Dell-ストレージ：温度プローブ警告	物理ディスク温度プローブ警告で、低温すぎるか高温すぎます。	警告	処置は不要
Dell-ストレージ：温度プローブエラー	物理ディスク温度プローブエラーで、低温すぎるか高温すぎます。	エラー	システムをメンテナンスモードにしてください
Dell-ストレージ：ファン障害	ファン障害です	エラー	システムをメンテナンスモードにしてください
Dell-ストレージ：バッテリー警告	バッテリー警告です	警告	処置は不要
Dell-ストレージ：仮想ディスク劣化警告	仮想ディスクの劣化警告です	警告	処置は不要
Dell-ストレージ：仮想ディスク劣化障害	仮想ディスク劣化障害です。	エラー	システムをメンテナンスモードにしてください
Dell-ストレージ：温度プローブ情報	温度プローブ情報です。	情報	処置は不要
Dell-ストレージ：アレイディスク警告	アレイディスク警告です	警告	処置は不要

イベント名	説明	重大度	推奨処置
Dell-ストレージ：アレイディスク情報	アレイディスク情報です	情報	処置は不要
Dell-ストレージ：電源装置警告	電源装置警告です	警告	処置は不要
Dell-Fluid Cache ディスク障害	Fluid Cache ディスクの障害です	エラー	システムをメンテナンスモードにしてください
Dell-ケーブルの故障または重要なイベント	ケーブルの故障、または重要なイベントです	エラー	システムをメンテナンスモードにしてください
Dell-シャーシ管理コントローラが警告を検出しました	シャーシ管理コントローラが警告を検出しました	警告	処置は不要
Dell-シャーシ管理コントローラがエラーを検出しました	シャーシ管理コントローラがエラーを検出しました	エラー	システムをメンテナンスモードにしてください
Dell-I/O 仮想化の失敗または重要なイベント	I/O 仮想化の失敗または重要なイベントです	エラー	システムをメンテナンスモードにしてください
Dell-リンク状態警告	リンク状態に関する警告です	警告	処置は不要
Dell-リンク状態エラーまたは重要なイベント	リンク状態のエラーか、重要なイベントです	エラー	システムをメンテナンスモードにしてください
Dell-セキュリティ警告	セキュリティ警告です	警告	処置は不要
Dell-システム：ソフトウェア設定警告	システム：ソフトウェア設定の警告です	警告	処置は不要
Dell-システム：ソフトウェア設定エラー	システム：ソフトウェア設定に障害が発生しています	エラー	システムをメンテナンスモードにしてください
Dell-ストレージセキュリティ警告	ストレージセキュリティの警告です	警告	処置は不要
Dell-ストレージセキュリティエラーまたは重要なイベント	ストレージセキュリティのエラー、または重要なイベントです	エラー	システムをメンテナンスモードにしてください
Dell-ソフトウェアの変更アップデートに関する警告	ソフトウェアの変更アップデートに関する警告です	警告	処置は不要
Dell-シャーシ管理コントローラの監査に関する警告	シャーシ管理コントローラの監査に関する警告です	警告	処置は不要
Dell-シャーシ管理コントローラの監査エラーまたは重要なイベント	シャーシ管理コントローラの監査エラー、または重要なイベントです	エラー	システムをメンテナンスモードにしてください
Dell-PCI デバイスの監査に関する警告	PCI デバイスの監査に関する警告です	警告	処置は不要
Dell-電源装置の監査に関する警告	電源装置の監査の警告です	警告	処置は不要
Dell-電源装置の監査エラーまたは重要なイベント	電源装置の監査エラー、または重要なイベントです	エラー	システムをメンテナンスモードにしてください
Dell-消費電力の監査に関する警告	消費電力の監査の警告です	警告	処置は不要
Dell-消費電力の監査エラーまたは重要なイベント	消費電力の監査エラー、または重要なイベントです	エラー	システムをメンテナンスモードにしてください
Dell-セキュリティ設定に関する警告	セキュリティ設定に関する警告です	警告	処置は不要
Dell-設定：ソフトウェア設定に関する警告	設定：ソフトウェア設定に関する警告です	警告	処置は不要

イベント名	説明	重大度	推奨処置
Dell-設定：ソフトウェア設定エラー	設定：ソフトウェア設定に障害が発生しています	エラー	システムをメンテナンスモードにしてください
Dell-仮想ディスクパーティション障害	仮想ディスクのパーティションの障害です	エラー	システムをメンテナンスモードにしてください
Dell-仮想ディスクパーティション警告	仮想ディスクのパーティションに関する警告です	警告	処置は不要
<b>iDRAC イベント</b>			
<p><b>① メモ:</b> クラスタの一部である <b>Proactive HA</b> が有効化されたすべてのホストでは、次の仮想化されたイベントが <b>Proactive HA</b> イベントにマッピングされます。ただし、「ファンは冗長ではありません」および「電源装置が冗長ではありません」のイベントはマッピングされません。</p>			
ファンが冗長です	なし	情報	処置は不要
ファンの冗長性が失われました	1つまたは複数のファンが故障したか、取り外されたか、または追加のファンが必要になる構成の変更が発生しました	重要	故障したファンを取り外してから再度取り付けるか、追加のファンを取り付けます
ファンの冗長性が劣化しています	1つまたは複数のファンが故障したか、取り外されたか、または追加のファンが必要になる構成の変更が発生しました。	警告	故障したファンを取り外してから再度取り付けるか、追加のファンを取り付けます
ファンが冗長ではありません	1つまたは複数のファンが故障したか取り外された、または追加のファンが必要になる構成の変更が発生しました	情報	故障したファンを取り外してから再度取り付けるか、追加のファンを取り付けます
ファンが冗長ではありません。正常な動作を維持するためのリソースが不足しています	1つまたは複数のファンが故障したか取り外された、または追加のファンが必要になる構成の変更が発生しました	重要	故障したファンを取り外してから再度取り付けるか、追加のファンを取り付けます
電源装置は冗長です	なし	情報	処置は不要
電源装置の冗長性が失われました	電源装置の例外、電源装置のインベントリの変更、システム電源インベントリの変更などのため、現在の電源動作モードには冗長がありません。以前、システムは電源冗長モードで動作していました	重要	電源ユニットの障害が発生していないか、イベントログを確認します。システム構成と電力消費を確認します
電源装置の冗長性が劣化しています	電源装置の例外、電源装置のインベントリの変更、システム電源インベントリの変更などのため、現在の電源動作モードには冗長がありません。以前、システムは電源冗長モードで動作していました	警告	電源ユニットの障害が発生していないか、イベントログを確認します。システム構成と電力消費を確認します
電源装置が冗長ではありません	現在の電源装置構成は、冗長性を有効にするプラットフォーム要件を満たしていません。1台の電源装置に障害が発生すると、システムがシャットダウンするおそれがあります。	情報	意図した状態でない場合は、システム構成と電力消費を確認し、電源ユニットを正しい構成で取り付けます。電源ユニットのステータスにエラーがないか確認します
電源装置が非冗長です。正常な動作を維持するためのリソースが不足しています	システムの電源が切れるか、またはパフォーマンスが低下した状態で動作する可能性があります	重要	電源ユニットの障害が発生していないか、イベントログを確認します。システム構成と電力消費を確認し、電源ユニット

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

イベント名	説明	重大度	推奨処置
ファンが冗長ではありません。正常な動作を維持するためのリソースが不足しています	1つまたは複数のファンが故障したか取り外された、または追加のファンが必要になる構成の変更が発生しました	重要	故障したファンを取り外してから再度取り付けるか、追加のファンを取り付けます

## データ取得スケジュールの管理

### 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行う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。

- ① **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。
- ① **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ー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。

- 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。
- [ 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。
- 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。

- ① **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

- 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。
- 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が必要な場合は、管理者ポータルでプロキシ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、保証は自動的に実行されません。

- ① **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。

- 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。
- [ 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。
- 保証データの取得日時を選択し、[ 適用 ] をクリックします。

- ① **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。

## Dell EMC シャーシ情報の表示

OMIVV を使用して、検出およびインベントリされたシャーシ情報を表示できます。[ Dell EMC シャーシ ] ページには、OMIVV が管理するすべてのシャーシがリストされます。

1. OMIVV ホーム ページで、[ ホストとシャーシ ] > [ シャーシ ] > [ シャーシ リスト ] をクリックします。次の情報が表示されます。

- ・ **名前** - それぞれの Dell EMC シャーシの IP アドレスのリンクを表示します。
- ・ **IP アドレス/FQDN** - vCenter の IP アドレスまたは FQDN を表示します。
- ・ **サービス タグ** - シャーシのサービス タグを表示します。
- ・ **シャーシ URL** - シャーシ URL を表示します。
- ・ **モデル** - モデル名を表示します。
- ・ **役割** - MX シャーシのみに適用。シャーシの役割 ( リードまたはメンバー ) を表示します。
- ・ **最終インベントリ** - 最後のインベントリ情報を表示します。
- ・ **利用可能スロット** - シャーシの利用可能なスロットを表示します。
- ・ **プロファイル名** - シャーシが関連付けられているシャーシ認証情報プロファイル名を表示します。
- ・ **場所** - シャーシの場所を表示します。

インベントリを実行しない場合、[ 名前 ]、[ 最終インベントリ ]、[ 利用可能スロット ]、[ プロファイル名 ]、[ 場所 ]、およびシャーシ インベントリ情報は表示されません。

**メモ:** MCM 構成の PowerEdge MX シャーシでは、MCM インフラストラクチャ全体がリード シャーシを使用して管理されています。メンバー シャーシの IP と iDRAC IP を無効にするか、シャーシの役割を変更した場合は、既存のリード シャーシを削除して新しいリード シャーシの IP を再度追加してから、シャーシ認証情報プロファイルに関連付けることをお勧めします。

2. シャーシを選択すると、ファームウェア、ライセンス タイプ、および保証関連の情報が表示されます。インベントリを実行しない場合、[ 名前 ]、[ ファームウェア ]、[ ライセンス タイプ ]、および [ 保証 ] 情報は表示されません。

## シャーシ インベントリ情報の表示

1. [ Dell EMC シャーシ ] ページで、シャーシを選択するか、サービス タグをクリックします。
2. [ シャーシ情報 ] セクションで、[ 表示 ] をクリックします。  
[ 概要 ] ページには、シャーシの正常性、アクティブ エラー、シャーシのコンポーネント レベルの正常性状態、ハードウェア概要、およびシャーシの関係性 ( MX シャーシのみ ) が表示されます。

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

メインのペインには、シャーシの全般的な正常性が表示されます。有効な正常性インジケータは、[ 正常 ]、[ 警告 ]、[ 重要 ]、[ 不明 ] です。シャーシの正常性のグリッドビューには、各コンポーネントの正常性が表示されます。シャーシの正常性パラメータは、VRTX バージョン 1.0 以降、M1000e バージョン 4.4 以降のモデルに適用されます。M1000e ファームウェアの 4.3 より前のバージョンでは、正常性インジケータは、[ 正常 ] および [ 警告 ] または [ 重要 ] など、2 つのみが表示されます。

全般的な正常性は、正常性パラメータが最も少ないシャーシに基づいた正常性を示します。例えば、正常記号が 5 つ、警告記号が 1 つある場合には、全般的な正常性は警告として表示されます。

## シャーシのハードウェアインベントリ情報の表示


選択したシャーシのハードウェア インベントリについての情報を表示することができます。

1. OMIVV ホーム ページで、[ ホストとシャーシ ] > [ シャーシ ] > [ シャーシ リスト ] をクリックします。  
**Dell EMC シャーシ** ページが表示されます。
2. シャーシを選択し、[ サービス タグ ] リンクをクリックします。  
**概要** ページが表示されます。

3. [概要] ページで、[ハードウェア] をクリックします。

表 10. ハードウェアインベントリ情報

ハードウェアインベントリ：コンポーネント	OMIVV でのナビゲーション	情報
ファン	<ul style="list-style-type: none"> <li>[ Dell EMC シャーシ ] ページで、[ シャーシ ] &gt; [ シャーシ リスト ] の順にクリックし、サービス タグ リンク をクリック します。</li> <li>[ 概要 ] ページの左ペインで、[ ハードウェア ] を選択 します。</li> <li>右ペインで、[ ファン ] を展開 します。</li> </ul> <p>または</p> <ul style="list-style-type: none"> <li>[ 概要 ] ページで [ ファン ] を クリック します。</li> </ul>	<p>ファンに関する情報には、次のものがあります。</p> <ul style="list-style-type: none"> <li>名前</li> <li>存在</li> <li>識別子 (MX シャーシにのみ適用)</li> <li>電源状況</li> <li>読み取り値 (RPM)</li> <li>警告しきい値 (MX シャーシには適用されません)</li> <li>重要しきい値 (MX シャーシには適用されません)</li> </ul> <ul style="list-style-type: none"> <li>最小</li> <li>最大</li> <li>パルス幅変調 (MX シャーシのみ)</li> </ul> <p><b>i</b> <b>メモ:</b> PowerEdge MX シャーシでは、ファンがシャーシから取り外された場合でも、ファンの存在は「あり」と表示されます。ただし、ファンの正常性状態は、[ サマリー ] ページで [ 重要 ] と表示され、アクティブエラーも表示されます。</p>
電源装置	<ul style="list-style-type: none"> <li>[ Dell EMC シャーシ ] ページで、[ シャーシ ] &gt; [ シャーシ リスト ] の順にクリックし、サービス タグ リンク をクリック します。</li> <li>[ 概要 ] ページの左ペインで、[ ハードウェア ] を選択 します。</li> <li>右ペインで、[ 電源装置 ] を展開 します。</li> </ul> <p>または</p> <ul style="list-style-type: none"> <li>[ 概要 ] ページで [ 電源装置 ] を クリック します。</li> </ul>	<p>電源装置に関する情報には、次のものがあります。</p> <ul style="list-style-type: none"> <li>名前</li> <li>容量</li> <li>存在</li> <li>電源状況</li> <li>入力電圧 (PowerEdge MX シャーシのみ)</li> </ul>
温度センサー	<ul style="list-style-type: none"> <li>[ Dell EMC シャーシ ] ページで、[ シャーシ ] &gt; [ シャーシ リスト ] の順にクリックし、サービス タグ リンク をクリック します。</li> <li>[ 概要 ] ページの左ペインで、[ ハードウェア ] を選択 します。</li> <li>右ペインで、[ 温度センサー ] を展開 します。</li> </ul> <p>または</p> <ul style="list-style-type: none"> <li>[ 概要 ] ページで [ 温度センサー ] を クリック します。</li> </ul>	<p>温度センサーに関する情報には、次のものがあります。</p> <ul style="list-style-type: none"> <li>場所</li> <li>読み取り</li> <li>警告しきい値</li> <li>最大</li> <li>最小</li> <li>重要しきい値</li> <li>最大</li> <li>最小</li> </ul> <p><b>i</b> <b>メモ:</b> PowerEdge M1000e シャーシでは、シャーシ温度に関する情報が表示されます。他のシャーシでは、温度センサーについての情報がシャーシと関連するモジュラーサーバに対して表示されます。</p>
I/O モジュール	<ul style="list-style-type: none"> <li>[ Dell EMC シャーシ ] ページで、[ シャーシ ] &gt; [ シャーシ リスト ] の順にクリックし、サービス タグ リンク をクリック します。</li> </ul>	<p>I/O モジュールに関する情報には、次のものがあります。</p> <ul style="list-style-type: none"> <li>スロット / 場所</li> <li>存在</li> <li>名前</li> <li>ファブリック</li> </ul>

ハードウェアインベントリ：コンポーネント	OMIVV でのナビゲーション	情報
	<ul style="list-style-type: none"> <li>・ [ 概要 ] ページの左ペインで、[ ハードウェア ] を選択します。</li> <li>・ 右ペインで、[ I/O モジュール ] を展開します。</li> </ul> <p>または</p> <ul style="list-style-type: none"> <li>・ [ 概要 ] ページで、[ I/O モジュール ] をクリックします。</li> </ul>	<ul style="list-style-type: none"> <li>・ サービスタグ</li> <li>・ 電源状態</li> <li>・ 役割</li> <li>・ ファームウェアバージョン</li> <li>・ ハードウェアバージョン</li> <li>・ IP アドレス</li> <li>・ サブネットマスク</li> <li>・ ゲートウェイ</li> <li>・ MAC アドレス</li> <li>・ DHCP が有効</li> </ul>
ファブリック ( PowerEdge MX シャーシのみ )	<ul style="list-style-type: none"> <li>・ [ Dell EMC シャーシ ] ページで、[ シャーシ ] &gt; [ シャーシ リスト ] の順にクリックし、サービスタグリンクをクリックします。</li> <li>・ [ 概要 ] ページの左ペインで、[ ハードウェア ] を選択します。</li> <li>・ 右ペインで、[ ファブリック ] を展開します。</li> </ul> <p>または</p> <ul style="list-style-type: none"> <li>・ [ 概要 ] ページで、[ ファブリック ] をクリックします。</li> </ul>	<p>ファブリック コンポーネントについての情報：</p> <ul style="list-style-type: none"> <li>・ 正常性</li> <li>・ ファブリック</li> <li>・ 説明</li> <li>・ スイッチ数</li> <li>・ コンピュート数</li> <li>・ アップリンク数</li> </ul> <p>ファブリックに関連付けられたスイッチを表示するには、ファブリックコンポーネントを選択すると、次の情報が下のグリッドに表示されます。</p> <ul style="list-style-type: none"> <li>・ スイッチ</li> <li>・ シャーシ</li> <li>・ スロット</li> <li>・ シャーシの役割</li> <li>・ スイッチのモデル</li> </ul>
PCIe	<ul style="list-style-type: none"> <li>・ [ Dell EMC シャーシ ] ページで、[ シャーシ ] &gt; [ シャーシ リスト ] の順にクリックし、サービスタグリンクをクリックします。</li> <li>・ [ 概要 ] ページの左ペインで、[ ハードウェア ] を選択します。</li> <li>・ 右ペインで、[ PCIe ] を展開します。</li> </ul> <p>または</p> <ul style="list-style-type: none"> <li>・ [ 概要 ] ページで、[ PCIe ] をクリックします。</li> </ul>	<p>PCIe に関する情報には、次のものがあります。</p> <ul style="list-style-type: none"> <li>・ PCIe スロット <ul style="list-style-type: none"> <li>・ スロット</li> <li>・ 名前</li> <li>・ 電源ステータス</li> <li>・ ファブリック</li> </ul> </li> <li>・ サーバスロット <ul style="list-style-type: none"> <li>・ 名前</li> <li>・ 番号</li> <li>・ スロットタイプ</li> <li>・ サーバマッピング</li> <li>・ 割り当てステータス</li> <li>・ スロットに割り当てられた電力</li> <li>・ PCI ID</li> <li>・ ベンダー ID</li> </ul> </li> </ul> <p> <b>メモ:</b> PCIe 情報を M 1000 e シャーシには適用されません。</p>
iKVM : PowerEdge M1000e のみ	<ul style="list-style-type: none"> <li>・ [ Dell EMC シャーシ ] ページで、[ シャーシ ] &gt; [ シャーシ リスト ] の順にクリックし、サービスタグリンクをクリックします。</li> <li>・ [ 概要 ] ページの左ペインで、[ ハードウェア ] を選択します。右</li> </ul>	<p>iKVM に関する情報には、次のものがあります。</p> <ul style="list-style-type: none"> <li>・ iKVM 名</li> <li>・ 存在</li> <li>・ ファームウェアバージョン</li> <li>・ フロントパネル USB/ ビデオが有効</li> <li>・ CMC CLI へのアクセスを許可</li> </ul>

ハードウェアインベントリ：コンポーネント	OMIVV でのナビゲーション	情報
	ペインで、[ iKVM ] を展開します。 または ・ [ 概要 ] ページで、[ iKVM ] をクリックします。	 <b>メモ:</b> シャーシに iKVM モジュールが含まれている場合にのみ iKVM タブが表示されています。

## ファームウェア インベントリ情報の表示

選択したシャーシについて、ファームウェア関連の情報を表示することができます。

1. OMIVV ホーム ページで、[ ホストとシャーシ ] > [ シャーシ ] > [ シャーシ リスト ] をクリックします。  
Dell EMC シャーシ ページが表示されます。
2. シャーシを選択し、[ サービス タグ ] リンクをクリックします。  
概要 ページが表示されます。
3. [ 概要 ] ページで、[ ファームウェア ] をクリックします。  
ファームウェアに関する次の情報が表示されます。
  - ・ コンポーネント
  - ・ 現在のバージョン

このページでは、OpenManage Enterprise モジュラーおよび CMC を起動することもできます。

## 管理コントローラー情報の表示

選択したシャーシについて、管理コントローラー関連の情報を表示することができます。

1. OMIVV ホーム ページで、[ ホストとシャーシ ] > [ シャーシ ] > [ シャーシ リスト ] をクリックします。  
Dell EMC シャーシ ページが表示されます。
2. シャーシを選択し、[ サービス タグ ] リンクをクリックします。  
概要 ページが表示されます。
3. [ 概要 ] ページで、[ 管理コントローラー ] をクリックします。  
管理コントローラーについて、次の情報が表示されます。
  - ・ 一般
    - ・ 名前
    - ・ ファームウェアバージョン
    - ・ 最終アップデート時刻
    - ・ シャーシの位置
    - ・ ハードウェアバージョン
  - ・ 共通ネットワーク
    - ・ DNS ドメイン名
    - ・ DNS に DHCP を使用
    - ・ MAC アドレス
    - ・ 冗長性モード
    - ・ ハードウェアバージョン
  - ・ IPv4 情報
    - ・ IPv4 が有効
    - ・ DHCP が有効
    - ・ IP アドレス
    - ・ サブネットマスク
    - ・ ゲートウェイ
    - ・ 優先 DNS サーバー
    - ・ 代替 DNS サーバー
  - ・ IPv6 情報

- ・ IPv6 が有効
- ・ DHCP が有効
- ・ IP アドレス
- ・ リンクのローカルアドレス
- ・ ゲートウェイ
- ・ 優先 DNS サーバー
- ・ 代替 DNS サーバー
- ・ ローカルアクセス設定
  - ・ Quick Sync ハードウェアあり
  - ・ LCD あり
  - ・ LED あり
  - ・ KVM 有効

**メモ:** MCM 構成の一部であるメンバー シャーシでは、ネットワーク関連情報の属性のいくつかは [ 管理コントローラー ] セクションに表示されません。

## ストレージ インベントリ情報の表示

選択したシャーシについて、ストレージ関連の情報を表示することができます。

1. OMIVV ホーム ページで、[ ホストとシャーシ ] > [ シャーシ ] > [ シャーシ リスト ] をクリックします。  
**Dell EMC** シャーシ ページが表示されます。
2. シャーシを選択し、[ サービス タグ ] リンクをクリックします。  
**概要** ページが表示されます。
3. [ **概要** ] ページで、[ **ストレージ** ] をクリックします。

ストレージに関して次の情報が表示されます。

- ・ 仮想ディスク
- ・ 物理ディスク
- ・ コントローラ
- ・ エンクロージャ
- ・ ホットスベア

MX シャーシでは、次の情報が表示されます。

- ・ スロット番号
- ・ スロット名
- ・ モデル
- ・ サービスタグ
- ・ ファームウェアバージョン
- ・ 資産タグ
- ・ 電源状況
- ・ 割り当てモード

MX シャーシの場合、ドライブに関する情報を表示するには、ストレージスレッドをクリックします。次のドライブ情報が下部のペインに表示されます。

- ・ 正常性
- ・ 状態
- ・ スロット
- ・ スロットの割り当て
- ・ ディスク名
- ・ 容量
- ・ バスプロトコル
- ・ メディア

PowerEdge MX シャーシ内のディスクに割り当てがない場合、スロットの割り当てには [ **該当なし** ] と表示されます。

M1000e シャーシでは、ストレージモジュールを使用する場合、次のストレージ詳細が、追加の情報なしでグリッドビューに表示されます。

- ・ 名前
- ・ モデル

- ・ サービスタグ
- ・ IP アドレス ( ストレージへのリンク )
- ・ ファブリック
- ・ グループ名
- ・ グループ IP アドレス ( ストレージ グループへのリンク )。

**i** **メモ:** ストレージでハイライト表示されたリンクをクリックすると、ビューの表にそれぞれのハイライトされた項目の詳細が表示されます。ビューの表で、各ラインの項目をクリックすると、それぞれのハイライトされた項目の追加の詳細が表示されます。

## 保証情報の表示

選択したシャーシについて、保証関連の情報を表示することができます。

1. OMIVV ホーム ページで、[ ホストとシャーシ ] > [ シャーシ ] > [ シャーシ リスト ] をクリックします。  
**Dell EMC** シャーシ ページが表示されます。
2. シャーシを選択し、[ サービス タグ ] リンクをクリックします。  
**概要** ページが表示されます。
3. [ **概要** ] ページで、[ **保証** ] をクリックします。

保証に関する情報には、次のものがあります。

- ・ プロバイダ
- ・ 説明
- ・ ステータス
- ・ 資格タイプ
- ・ 開始日
- ・ 終了日
- ・ 残日数
- ・ 最終更新日

**i** **メモ:** 保証ステータスを表示するには、保証ジョブを実行したことを確認します。「[保証取得ジョブのスケジュール](#)」を参照してください。

## シャーシに関連するホストの表示

選択したシャーシに関連するホストについての情報を表示することができます。

1. OMIVV ホーム ページで、[ ホストとシャーシ ] > [ シャーシ ] > [ シャーシ リスト ] をクリックします。  
**Dell EMC** シャーシ ページが表示されます。
2. シャーシを選択し、[ サービス タグ ] リンクをクリックします。  
**概要** ページが表示されます。
3. [ **概要** ] ページで、[ **関連ホスト** ] をクリックします。  
関連ホストについて、次の情報が表示されます。

- ・ ホスト名
- ・ サービスタグ
- ・ モデル
- ・ iDRAC IP
- ・ 場所
- ・ スロットの場所
- ・ 最新のインベントリ

4. ホストの詳細を表示するには、ホストを選択します。

## 関連するシャーシ情報の表示

[ シャーシの関係性 ] セクションでは、MCM モードで導入された MX シャーシ内のシャーシの関係性が表示されます。

**i** **メモ:** 関連シャーシ情報は、**MCM** グループで設定された **PowerEdge MX** シャーシにのみ適用されます。

1. OMIVV ホーム ページで、[ ホストとシャーシ ] > [ シャーシ ] > [ シャーシ リスト ] をクリックします。

Dell EMC シャーシ ページが表示されます。

2. シャーシを選択し、[ サービス タグ ] リンクをクリックします。  
概要 ページが表示されます。

[ 概要 ] ページの [ シャーシの関係性 ] セクションには、リードおよびメンバー シャーシに関連するすべてのシャーシ情報が表示されます。

## PowerEdge MX シャーシの管理

MX7000X シャーシの管理方法は、M1000e、VRTX、および FX2 などの他の Dell EMC シャーシの管理とは異なります。

管理モジュールと iDRAC 用のパブリック IP を持つスタンドアロンモードの MX シャーシを管理できます。また、1つのリードと複数メンバーに対応するマルチシャーシ管理 (MCM) モードで MX シャーシを設定することができます。

Dell EMC OpenManage Enterprise-Modular は、有線 MCM グループをサポートしています。有線タイプでは、シャーシは、管理モジュールの冗長ポートを介してダイジーチェーン接続されます。グループ作成用に選択したシャーシは、少なくとも1つのシャーシにダイジーチェーン接続される必要があります。シャーシ グループの作成に関する詳細については、[dell.com/support](http://dell.com/support) で『PowerEdge MX7000 向け Dell EMC OpenManage Enterprise-Modular ユーザーズガイド』を参照してください。

MX シャーシ内のサーバは2つの方法で管理できます。

1. **ホスト認証情報プロファイルを使用してサーバーを管理する**：すべての機能がサポートされる、サーバー管理に関する標準かつ推奨される方法です。この場合、シャーシは、MX ホストインベントリが完了した後にのみ検出されます。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。
2. **シャーシ認証情報プロファイルを使用してサーバーを管理する**：シャーシ認証情報プロファイルを使用したホストの管理を選択した場合、インベントリ、モニタリング、ファームウェア、ドライバーのアップデートなど、OMIVV 機能がサポートされます。シャーシ認証情報プロファイルを使用してシャーシおよびホストを管理する方法の詳細については、「[シャーシ認証情報プロファイルの作成](#)」を参照してください。

**メモ**: OMIVV は、バックアップ リード設定を使用した PowerEdge MX シャーシの管理をサポートしていません。

**メモ**: iDRAC の IPv4 アドレスが無効になっている場合は、シャーシ認証情報プロファイルを使用してサーバーを管理することができません。シャーシ認証情報プロファイルを使用してサーバーを管理する場合は、次の OMIVV 機能はサポートされません。

- iDRAC ロックダウンモード
- このサーバーを参照サーバーとして使用し、システム プロファイルをキャプチャーする機能
- OS 導入
- CSIOR ステータスの取得または更新
- サーバーの設定コンプライアンス
- いくつかのインベントリ関連情報

**メモ**: パブリック IPv4 iDRAC IP を持つホストは、シャーシ認証情報プロファイルを使用して管理することも可能です。ただし、上記に表示した機能が利用できないため、お勧めしません。

## 統合シャーシ管理 IP を使用したシャーシおよびホストの管理

認証情報プロファイルを使用して管理されているホストに対して iDRAC IPv4 が無効である場合は、ホストのインベントリは失敗し、シャーシが検出されません。このような場合、シャーシを手動で追加する必要があり、シャーシや関連するホストを管理するためには、シャーシ認証情報プロファイルに関連付ける必要があります。

統合シャーシ管理 IP を使用したホストの管理を選択した場合、インベントリ、モニタリング、ファームウェア、およびドライバのアップデートなどの OMIVV 機能がサポートされます。次に、統合シャーシ管理 IP を使用してホストとシャーシを管理するためのタスクの高度な説明を示します。

1. MX シャーシを追加します。

MX シャーシの追加の詳細については、「[PowerEdge MX シャーシの追加](#)」を参照してください。

2. シャーシ認証情報プロファイルを作成し、ホストを関連付けます。

シャーシ認証情報プロファイル作成の詳細については、「[シャーシ認証情報プロファイルの作成](#)」を参照してください。

3. シャーシ認証情報プロファイルを使用して管理されているシャーシとホストの両方のジョブを表示します。
4. シャーシとホストのインベントリを表示します。

ホストとシャーシのインベントリの詳細については、「[ホスト インベントリ ジョブの表示](#)」および「[シャーシ インベントリ ジョブの表示](#)」を参照してください。

5. シャーシを使用して管理されているホストでファームウェアのアップデートを実行します。  
ファームウェアアップデートの詳細については、「[ファームウェアアップデート](#)」を参照してください。

**i** **メモ:** ホストがシャーシを使用して管理されている場合、ベアメタルワークフローはサポートされません。

## PowerEdge MX シャーシの追加

有効な IPv4 iDRAC IP を持つホストはホスト認証情報プロファイルに追加することが可能です。ホストのインベントリー中に関連する MX シャーシが自動的に検出され、[ **Dell EMC シャーシ** ] ページ上に表示されます。

iDRAC IPv4 が無効なホストの場合は、ホストのインベントリーは失敗し、シャーシが検出されません。このような場合、MX シャーシを手動で追加する必要があり、シャーシや関連するホストを管理するためには、シャーシ認証情報プロファイルに関連付ける必要があります。

MX シャーシを手動で追加するには、次の手順を実行します。

1. **OMIVV** ホーム ページで、[ **ホストとシャーシ** ] > [ **シャーシ** ] をクリックします。
2. [ **Dell EMC シャーシ** ] ページで、[ **MX シャーシの追加** ] をクリックします。
3. 管理モジュールの IPv4 または FQDN またはホスト名を入力し、**OK** をクリックします。

入力した IP が OMIVV によって管理されている場合は、検証が行われます。

**i** **メモ:** ホスト名または FQDN を使用してシャーシを追加する前に、**DNS** で有効な前方ルックアップと逆引きルックアップのエントリが作成されていることを確認します。

**i** **メモ:** FQDN を入力すると、シャーシの URL が FQDN とともに表示されます。

シャーシが **Dell EMC シャーシ** ページに追加されます。

4. シャーシ認証情報プロファイルを作成すると、ホストはシャーシ認証情報プロファイルに関連付けられます。シャーシ認証情報プロファイル作成の詳細については、「[シャーシ認証情報プロファイルの作成](#)」を参照してください。

**i** **メモ:** MX シャーシ IP 以外の IP を入力した場合は、テスト接続は失敗し、無効のエントリが **Dell EMC シャーシ** ページに残ります。正常に検証されたシャーシのみがシャーシ認証情報プロファイルに関連付けられます。

**i** **メモ:** 追加された MX シャーシに関連付けられている、登録済みの vCenter にホストが存在しない場合、テスト接続に失敗します。

**i** **メモ:** MCM 構成で構成された PowerEdge MX シャーシの場合、リードとメンバーの資格情報が同じである必要があります。

## Mx シャーシ ファームウェアのアップデート

ファームウェア アップデートをスケジュールする前に、環境で次の条件が満たされていることを確認してください。

- ・ MX シャーシがシャーシ認証情報プロファイルの一部であり、正常にインベントリーされていることを確認します。
- ・ ホストのいずれかがファームウェアのアップデート中である場合、シャーシ ファームウェアをアップデートできません。

**i** **メモ:** MX シャーシ ファームウェアのアップデート機能を使用することで、管理モジュール ファームウェアのみをアップデートできます。

1. OMIVV ホーム ページで、[ **ホストとシャーシ** ] > [ **シャーシ** ] > [ **シャーシリスト** ] > [ **MX シャーシ ファームウェア アップデート** ] をクリックします。
2. ウィザードの [ **シャーシ ファームウェア アップデート** ] ページで手順を読み、[ **開始** ] をクリックします。
3. [ **MX シャーシ リスト** ] から、1つまたは複数の MX シャーシを選択し、[ **次へ** ] をクリックします。

環境内で次のいずれかの条件が満たされていない場合、シャーシは表示されません。

- ・ OMIVV からシャーシ ファームウェアのアップデートが進行中である。
- ・ シャーシのシャーシ認証情報プロファイルが作成されていない。
- ・ シャーシのインベントリーが正常に行われていない。

MCM 構成の PowerEdge Mx シャーシでは、リード シャーシのみを選択できます。メンバー シャーシが自動的に選択されます。

4. **アップデートソースの選択** ページで、次の手順を実行します。
  - a) 適切なファームウェア リポジトリ プロファイルをドロップダウン メニューから選択します。

- b) 選択したシャーシおよびファームウェア リポジトリ プロファイルに基づいて、識別されたシステム カテゴリから適切なバンドルを選択します。
5. [ **ファームウェア コンポーネントの選択** ] ページで、アップデートの必要があるファームウェア コンポーネントを選択して [ **次へ** ] をクリックします。
- カタログ内の使用可能なバージョンよりも古いバージョンのコンポーネント、または同じレベル (最新) のコンポーネントは選択できません。ダウングレード ステータスにリストされているコンポーネントを選択するには、[ **ファームウェア ダウングレードを許可する** ] をクリックします。
- MCM 構成に関連付けられた PowerEdge Mx シャーシでは、[ **ファームウェア ダウングレードを許可する** ] チェックボックスが選択されていない場合でも、ファームウェア バージョンをダウングレードできます。
- アップデートまたはダウングレードの対象としてメンバー シャーシのみを選択することはできません。リード シャーシを選択すると、自動的にメンバー シャーシが選択されます。
- すべてのページのすべてのファームウェア コンポーネントを選択するには、☰ をクリックします。
- すべてのページのすべてのファームウェア コンポーネントをクリアするには、✕ をクリックします。
6. [ **ジョブのスケジュール設定** ] ページで、次の手順を実行します。
- a) ファームウェア アップデート ジョブの名前と説明を入力します。[ **説明** ] フィールドはオプションです。
- ファームウェアアップデートのジョブの名前は必須です。ここでは、すでに使用されている名前は使用しないようにしてください。ファームウェアアップデートのジョブ名をパージすれば、そのジョブ名を再度使用できます。
- b) 適切なスケジュール オプションを選択して、アップデートを適用します。
7. [ **サマリーのレビュー** ] ページで、ファームウェア アップデートの詳細を確認し、[ **終了** ] をクリックします。

**表 11. 展開モードごとに同時実行される MX シャーシ ファームウェア アップデートの合計数**

展開モード	同時実行されるシャーシ ファームウェア アップデートの数
小	1
中	1
大	2
特大	2

## OMIVV ホストの表示

[ **OMIVV** ホスト ] ページでは、OMIVV で管理するすべてのホストを表示できます。

1. OMIVV ホーム ページで、[ ホストとシャーシ ] > [ ホスト ] の順にクリックします。
2. [ **OMIVV** ホスト ] タブに、次の情報が表示されます。
  - ・ [ **ホスト名** ] — ホストの IP アドレスが表示されます。ホストの情報を表示するには、ホストを選択します。
  - ・ [ **vCenter** ] — ホストの vCenter IP アドレスが表示されます。
  - ・ **クラスタ** — Dell EMC ホストがクラスタ内にある場合、クラスタ名が表示されます。
  - ・ [ **ホスト認証情報プロファイル** ] — ホスト認証情報プロファイルの名前が表示されます。

## 単一ホストの監視

OMIVV では、単一ホストの詳細情報を表示できます。[ **ホストとクラスタ** ] ページで OMIVV ホストをすべて表示できます。詳細を表示するには、特定の OMIVV 管理対象ホストを選択し、[ **監視** ] > [ **OMIVV** ホスト情報 ] の順に移動します。

## ホスト サマリー情報の表示

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

- ・ **OMIVV** ホストの正常性
- ・ **OMIVV** ホスト情報

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

1. OMIVV ホームページで、[ **メニュー** ] を展開し、[ **ホストとクラスタ** ] を選択します。
2. 左ペインで、特定のホストを選択します。
3. 右ペインで、[ **サマリー** ] をクリックします。
4. スクロールダウンすると、OMIVV の Server Management ポートレットが表示されます。  
[ **OMIVV** ホスト情報 ] および [ **OMIVV** ホストの正常性 ] セクションでは、次の情報を表示できます。

表 12. OMIVV ホスト情報

情報	説明
サービスタグ	サーバのサービスタグを表示します。この ID は、サポートに電話をする際に使用します。
モデル名	サーバーのモデル名を表示します。
耐障害性メモリ	BIOS 属性のステータスを表示します。BIOS 属性は、サーバの初回セットアップ中に BIOS で有効化され、サーバのメモリ動作モードを表示します。メモリ動作モード値を変更するときはシステムを再起動します。これは、耐障害性メモリー (FRM) オプションをサポートし、ESXi 5.5 以降のバージョンを実行する PowerEdge サーバーで適用されます。BIOS 属性の値は次の 4 つです。 <ul style="list-style-type: none"> <li>・ 有効かつ保護状態：この値は、システムがサポートされており、オペレーティングシステムのバージョンが ESXi 5.5 以降であり、BIOS のメモリ操作モードが FRM に設定されていることを示します。</li> </ul>

情報	説明
	<ul style="list-style-type: none"> <li>・ NUMA が有効かつ保護状態：この値は、システムがサポートされており、オペレーティングシステムのバージョンが ESXi 5.5 以降で、BIOS のメモリ動作モードが NUMA に設定されていることを示します。</li> <li>・ 有効かつ非保護状態：この値はオペレーティングシステムのバージョンが ESXi 5.5 未満のシステムをサポートすることを示しています。</li> <li>・ 無効：この値は、どのオペレーティングシステムのバージョンのシステムでもサポートし、BIOS のメモリ操作モードは FRM に設定されていないことを示します。</li> <li>・ ブランク：BIOS のメモリ操作モードがサポートされていない場合、FRM 属性が表示されません。</li> </ul>
システムロックダウンモード	iDRAC 8 以降のサーバー用の iDRAC ロックダウン モードのステータスを表示します。閉じられたロックは iDRAC ロックダウンモードがオンになっていることを示し、開かれたロックは iDRAC ロックダウンモードがオフになっていることを示します。
ID	<p>次が表示されます：</p> <ul style="list-style-type: none"> <li>・ ホスト名 — OMIVV 管理ホストの名前を表示します</li> <li>・ 電源状態 — 電源がオンかオフかが表示されます。</li> <li>・ iDRAC IP — iDRAC の IP アドレスが表示されます</li> <li>・ 管理 IP — 管理 IP アドレスが表示されます</li> <li>・ ホスト認証情報プロファイル — このホストのホスト認証情報プロファイル名を表示します</li> <li>・ モデル — Dell EMC サーバのモデルが表示されます</li> <li>・ サービス タグ — サーバーのサービス タグが表示されます。</li> <li>・ 資産タグ — 資産タグが表示されます</li> <li>・ 保証残日数 — 保証の残りの日数が表示されます</li> <li>・ 最終インベントリスキャン — 最終インベントリスキャンの日付と時刻が表示されます</li> </ul>
ハイパーバイザー & ファームウェア	<p>次が表示されます：</p> <ul style="list-style-type: none"> <li>・ ハイパーバイザー — ハイパーバイザーのバージョンが表示されます</li> <li>・ BIOS バージョン — BIOS バージョンが表示されます</li> <li>・ リモートアクセスカードバージョン — リモートアクセスカードバージョンが表示されます</li> </ul>
管理コンソール	Remote Access Console ( iDRAC ) を起動するためのリンクを表示します。
ホストアクション	さまざまな間隔で点滅するように、物理サーバを設定します。「 <a href="#">点滅式インジケータライトの設定</a> 」を参照してください。

表 13. OMIVV ホストの正常性

情報	説明
OMIVV ホストの正常性	コンポーネントの正常性は、すべての主要なホスト サーバーコンポーネントのステータスを図式で表したものです。サーバー グローバル ステータス、サーバー、電源装置、温度、電圧、プロセッサ、バッテリー、イントルージョン、ハードウェア ログ、電源管理、電源とメモリーがあります。シャーシの正常性パラメータは、VRTX バージョン 1.0 以降、M1000e バージョン 4.4 以降のモデルに適用されます。バージョン 4.3 より前のバージョンでは、2 つの正常性インジケータのみが表示され、それらは正常および警告または重大(逆三角形にオレンジ色の感嘆符)となります。全般的な正常性は、正常性パ

情報	説明
	<p>ラメーターが最も少ないシャーシに基づいた正常性を示します。以下のオプションがあります。</p> <ul style="list-style-type: none"> <li>・ 正常(緑色のチェックマーク) — コンポーネントは通常通りに動作中</li> <li>・ 警告(黄色の三角に感嘆符) — コンポーネントには重大でない不具合があります。</li> <li>・ 重要(赤い×印) — コンポーネントには重大な障害があります。</li> <li>・ 不明(疑問符) — コンポーネントステータスは不明です。</li> </ul>

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

**i** **メモ:** 電源モニタリング情報は、ケーブル接続された PSU またはモジュラーサーバーのホストでは使用できません。

## OMIVV ホスト情報の表示

[ **OMIVV ホスト情報** ] ページでは、OMIVV で管理するすべてのホストに関するハードウェア、ストレージ、ファームウェア、電源監視、保証、システム イベント ログ情報を表示できます。

1. OMIVV ホームページで、[ **メニュー** ] を展開し、[ **ホストとクラスター** ] を選択します。
2. 左ペインで、ホストを選択し、[ **モニター** ] > [ **OMIVV ホスト情報** ] の順にクリックします。

## ホストのハードウェア情報の表示

表 14. 単一ホストのハードウェア情報

ハードウェア：コンポーネント	情報
FRU	<ul style="list-style-type: none"> <li>・ <b>パーツ名</b> — FRU のパーツ名が表示されます。</li> <li>・ <b>パーツ番号</b> — FRU のパーツ番号が表示されます。</li> <li>・ <b>製造元</b> — 製造元の名前が表示されます</li> <li>・ <b>シリアル番号</b> — 製造元のシリアル番号が表示されます。</li> <li>・ <b>製造日</b> — 製造日が表示されます。</li> </ul>
プロセッサ	<ul style="list-style-type: none"> <li>・ <b>ソケット</b> — スロット番号が表示されます。</li> <li>・ <b>速度</b> — 現在の速度が表示されます。</li> <li>・ <b>ブランド</b> — プロセッサのブランドが表示されます。</li> <li>・ <b>バージョン</b> — プロセッサのバージョンが表示されます。</li> <li>・ <b>コア</b> — このプロセッサ内のコアの数が表示されます。</li> </ul>
電源装置	<ul style="list-style-type: none"> <li>・ <b>タイプ</b> — 電源装置のタイプが表示されます。電源装置には、次のタイプがあります。 <ul style="list-style-type: none"> <li>・ 不明</li> <li>・ リニア</li> <li>・ スイッチング</li> <li>・ BATTERY</li> <li>・ UPS</li> <li>・ コンバータ</li> <li>・ レギュレータ</li> <li>・ AC</li> <li>・ DC</li> <li>・ VRM</li> </ul> </li> <li>・ <b>場所</b> — スロット 1 など、電源装置の場所が表示されます。</li> <li>・ <b>出力(ワット)</b> — ワット単位で電力が表示されます。</li> </ul>
メモリ	<ul style="list-style-type: none"> <li>・ <b>メモリースロット</b> — 使用済み、合計、使用可能なメモリー数が表示されます</li> </ul>

ハードウェア：コンポーネント	情報
	<ul style="list-style-type: none"> <li>・ <b>メモリー容量</b> — インストール済みメモリー、総メモリー容量、および利用可能なメモリーが表示されます</li> <li>・ <b>スロット</b> — DIMM スロットが表示されます。</li> <li>・ <b>サイズ</b> — メモリー サイズが表示されます。</li> <li>・ <b>タイプ</b> — メモリーのタイプが表示されます。</li> </ul>
<b>NIC</b>	<ul style="list-style-type: none"> <li>・ <b>合計</b> — 使用可能なネットワーク インターフェイス カードの合計数が表示されます</li> <li>・ <b>名前</b> — NIC 名が表示されます。</li> <li>・ <b>製造元</b> — 製造元の名前のみが表示されます。</li> <li>・ <b>MAC アドレス</b> — NIC の MAC アドレスが表示されます。</li> </ul>
<b>PCI スロット</b>	<ul style="list-style-type: none"> <li>・ <b>PCI スロット</b> — 使用済み、合計、使用可能な PCI スロット数が表示されます</li> <li>・ <b>スロット</b> — スロットを表示します。</li> <li>・ <b>製造元</b> — PCI スロットのメーカー名が表示されます。</li> <li>・ <b>説明</b> — PCI デバイスの説明が表示されます。</li> <li>・ <b>タイプ</b> — PCI スロット タイプが表示されます。</li> <li>・ <b>幅</b> — データ バス幅が表示されます ( 該当する場合 ) 。</li> </ul>
<b>リモート アクセス デバイス</b>	<ul style="list-style-type: none"> <li>・ <b>IP アドレス</b> — リモート アクセス カードの IP アドレスが表示されます。 統合 IP アドレスを使用してホストを管理している場合、iDRAC IP はこのセクションに表示されません。</li> <li>・ <b>MAC アドレス</b> — リモート アクセス カードの MAC アドレスが表示されます。</li> <li>・ <b>RAC タイプ</b> — リモート アクセス カードのタイプが表示されます。</li> <li>・ <b>URL</b> — このホストに関連付けられた動作している iDRAC の URL が表示されます。</li> </ul>

## ホストのストレージ情報の表示

仮想ディスク、コントローラー、エンクロージャー、関連物理ディスク ( グローバル ホット スペアおよび専用ホット スペアとともに ) の数が表示されます。各ストレージ コンポーネントの詳細を表示するには、[ 表示 ] ドロップダウンメニューから特定のコンポーネントを選択します。

シャーシを使用して管理されているホストの場合、完全なストレージ情報 ( コントローラー、エンクロージャー、グローバル ホット スペア、専用ホット スペア ) は表示されません。

**i** **メモ:** ホストがシャーシ プロファイルを使用して管理されている場合は、[ ストレージ ] をクリックし、[ 表示 ] ドロップダウンメニューから次を選択します。

- ・ [ エンクロージャ ] - ストレージエンクロージャのコントローラ ID が、正しいコントローラ ID の代わりに **0** と表示されます。
- ・ [ 物理ディスク ] - HDD メディアタイプが、[ ハードディスクドライブ ] の代わりに [ 磁気ドライブ ] と表示されます。

表 15. 単一ホストのストレージ詳細

情報	説明
<b>仮想ディスク</b>	<ul style="list-style-type: none"> <li>・ <b>名前</b> — 仮想ドライブの名前が表示されます</li> <li>・ <b>デバイス FQDD</b> - FQDD が表示されます</li> <li>・ <b>物理ディスク</b> — 仮想ドライブが配置されている物理ディスクが表示されます</li> <li>・ <b>容量</b> — 仮想ドライブの容量が表示されます</li> <li>・ <b>レイアウト</b> — 仮想ストレージのレイアウトタイプ、すなわちこの仮想ドライブに設定された RAID のタイプが表示されます</li> <li>・ <b>メディアタイプ</b> — SSD と HDD のいずれかが表示されます。</li> </ul>

情報	説明
	<p>ストライプ サイズ、バス プロトコル、キャッシュ ポリシーなどの情報を表示するには、仮想ディスクを選択します。</p> <ul style="list-style-type: none"> <li>・ <b>コントローラー ID</b> — コントローラー ID が表示されます。</li> <li>・ <b>デバイス ID</b> — デバイス ID が表示されます。</li> <li>・ <b>ストライプ サイズ</b> — ストライプ サイズが表示されます。ストライプ サイズは、各ストライプが単一ディスク上で消費する容量です</li> <li>・ <b>バスプロトコル</b> — 仮想ドライブ内の物理ディスクが使用するテクノロジーを表示します。可能な値は次のとおりです。 <ul style="list-style-type: none"> <li>・ SCSI</li> <li>・ SAS</li> <li>・ SATA</li> </ul> </li> <li>・ <b>デフォルト読み取りポリシー</b> — コントローラでサポートされているデフォルト読み取りポリシーが表示されます。以下のオプションがあります。 <ul style="list-style-type: none"> <li>・ 先読み</li> <li>・ 先読みなし</li> <li>・ 適応先読み</li> <li>・ 読み取りキャッシュが有効</li> <li>・ 読み取りキャッシュが無効</li> </ul> </li> <li>・ <b>デフォルト書き込みポリシー</b> — コントローラでサポートされているデフォルト書き込みポリシーが表示されます。以下のオプションがあります。 <ul style="list-style-type: none"> <li>・ ライトバック</li> <li>・ ライトバックの強制</li> <li>・ ライトバックが有効</li> <li>・ ライトスルー</li> <li>・ 書き込みキャッシュ有効、保護</li> <li>・ 書き込みキャッシュが無効</li> </ul> </li> <li>・ <b>キャッシュ ポリシー</b> — キャッシュ ポリシーが有効かどうかが表示されます</li> </ul>
<p><b>物理ディスク</b></p> <p>[ 表示 ] ドロップダウン メニューからこのオプションを選択すると、[ フィルター ] ドロップダウン リストが表示されます。</p> <p>フィルターでは次のオプションを使用できません。</p> <ul style="list-style-type: none"> <li>・ <b>すべての物理ディスク</b></li> <li>・ <b>グローバルホットスペア</b></li> <li>・ <b>専用ホットスペア</b></li> <li>・ 最後のオプションでは、仮想ドライブのカスタム名が表示されます</li> </ul>	<ul style="list-style-type: none"> <li>・ <b>名前</b> — 物理ディスクの名前が表示されます</li> <li>・ <b>デバイス FQDD</b> - デバイス FQDD が表示されます</li> <li>・ <b>容量</b> — 物理ディスクの容量が表示されます。</li> <li>・ <b>ディスクのステータス</b> — 物理ディスクのステータスが表示されます。以下のオプションがあります。 <ul style="list-style-type: none"> <li>・ オンライン</li> <li>・ 準備完了</li> <li>・ 劣化</li> <li>・ エラー</li> <li>・ オフライン</li> <li>・ 再構成中</li> <li>・ 互換性なし</li> <li>・ 削除済み</li> <li>・ クリア済み</li> <li>・ SMART アラートが検知されました</li> <li>・ 不明</li> <li>・ 外部</li> <li>・ サポートなし</li> </ul> </li> <li>・ <b>設定済み</b> — ディスクが設定されているかどうかが表示されます</li> <li>・ <b>ホットスペアのタイプ</b> ( PCIe では該当しません ) — ホットスペアのタイプが表示されます。以下のオプションがあります。 <ul style="list-style-type: none"> <li>・ いいえ — ホットスペアなし。</li> <li>・ グローバル — ディスクグループの一部であるが未使用のバックアップディスク</li> </ul> </li> </ul>

情報	説明
	<ul style="list-style-type: none"> <li>・ 専用 — 単一の仮想ドライブに割り当てられた未使用のバックアップディスク。仮想ドライブ内の物理ディスクがクラッシュすると、ホットスワップが有効化されて故障した物理ディスクと交換されるため、システムが中断することや、ユーザー介入が必要になることはありません。</li> <li>・ 仮想ディスク — 仮想ドライブの名前が表示されます</li> <li>・ バスプロトコル — バス プロトコルが表示されます。</li> <li>・ コントローラー ID — コントローラー ID が表示されます。</li> <li>・ メディアタイプ — SSD と HDD のいずれかが表示されます。</li> <li>・ 残留書き込み耐久性 — SSD の残留書き込み耐久性が表示されます。</li> <li>・ コネクタ ID — コネクタ ID が表示されます。</li> <li>・ エンクロージャー ID — エンクロージャーの ID が表示されます。</li> <li>・ デバイス ID — デバイス ID が表示されます。</li> <li>・ モデル — 物理ストレージ ディスクのモデル番号が表示されます</li> <li>・ パーツ番号 — ストレージのパーツ番号が表示されます。</li> <li>・ シリアル番号 — ストレージのシリアル番号が表示されます。</li> <li>・ ベンダー — ストレージのベンダー名が表示されます</li> </ul>
コントローラ	<ul style="list-style-type: none"> <li>・ コントローラー ID — コントローラー ID が表示されます。</li> <li>・ 名前 — コントローラーの名前が表示されます</li> <li>・ デバイス FQDD — デバイスの FQDD が表示されます</li> <li>・ ファームウェア バージョン — ファームウェアのバージョンが表示されます</li> <li>・ 最低限必要なファームウェア — 最低限必要なファームウェアが表示されます。ファームウェアが古くなっていて、新しいバージョンが使用可能な場合に、この列に値が表示されます</li> <li>・ ドライバー バージョン — ドライバーのバージョンが表示されます</li> <li>・ 巡回読み取り状況 — 巡回読み取り状況が表示されます</li> <li>・ キャッシュ サイズ — キャッシュ サイズが表示されます</li> </ul> <p>① <b>メモ:</b> このセクションはチップセット コントローラー情報を表示します。これは iDRAC UI のストレージ コントローラー セクションには表示されませんが、iDRAC のインベントリ ページに関するこの情報を表示することはできません。</p>
エンクロージャ	<ul style="list-style-type: none"> <li>・ コントローラー ID — コントローラー ID が表示されます。</li> <li>・ コネクタ ID — コネクタ ID が表示されます。</li> <li>・ エンクロージャー ID — エンクロージャーの ID が表示されます。</li> <li>・ 名前 — エンクロージャーの名前が表示されます</li> <li>・ デバイス FQDD - デバイス FQDD が表示されます</li> <li>・ サービス タグ — サービス タグが表示されます</li> </ul>

## 単一ホストのファームウェア情報の表示

次のファームウェア関連情報が表示されます。

- ・ 名前 — このホスト上のすべてのファームウェアの名前が表示されます。
- ・ タイプ — ファームウェアの種類が表示されます
- ・ バージョン — このホスト上のすべてのファームウェアのバージョンが表示されます。
- ・ インストール日 — インストール日が表示されます

① **メモ:** シャーシ認証情報プロファイルを使用してホストを管理している場合は、ファームウェア インベントリ データに、Life Cycle Controller やソフトウェア RAID などのいくつかの追加コンポーネントが表示されます。

このページから、ファームウェア アップデートおよびを起動し、システム ロックダウン モード ウィザードを設定することができます。

## 単一ホストの電源監視情報の表示

全般情報、しきい値、予約電力容量、エネルギー統計などの情報を表示できます。

- ・ **一般情報** — 電力バジェットおよび現在のプロファイル名が表示されます
- ・ **しきい値** — 警告および失敗のしきい値がワット単位で表示されます
- ・ **予備電源容量** — インスタントおよびピークの予備電源容量がワット単位で表示されます

#### エネルギー統計

- ・ **タイプ** — エネルギー統計タイプが表示されます
- ・ **測定開始時刻 (ホスト時刻)** — ホストが電力消費を開始した日付と時刻が表示されます
- ・ **測定終了時刻 (ホスト時刻)** — ホストが電力消費を停止した日付と時刻が表示されます
- ・ ⓘ **メモ:** ここで使用するホスト時刻は、ホストが位置する現地時刻を指しています。

読み取り値 - 1分間に測定した平均値が表示されます

- ・ **ピーク時刻 (ホスト時刻)** — ホストのピーク電流の日付と時刻が表示されます
- ・ **ピーク読み取り値** — システム ピーク電力の統計、すなわちシステムが消費するピーク電力がワット単位で表示されます

ⓘ **メモ:** 電源モニタリング情報は、ケーブル接続された PSU またはモジュラー サーバーのホストでは使用できません。

ⓘ **メモ:** シャーシを使用して管理されているホストの場合、完全な電源監視情報は表示されません。

## 単一ホストの保証情報の表示

保証ステータスを表示するには、保証ジョブを実行したことを確認します。「[保証取得ジョブのスケジュール](#)」を参照してください。保証ステータス ページで、保証の期限の日付を監視できます。保証設定は、保証スケジュールを有効化または無効化し、最小日数しきい値アラートを設定することで、Dell オンラインからサーバ保証情報を検索する時期を管理することができます。

- ・ **プロバイダー** — 保証のプロバイダー名が表示されます
- ・ **説明** — 説明が表示されます
- ・ **ステータス** — ホストの保証ステータスが表示されます。ステータスのオプションには、次のものがあります。
  - ・ **アクティブ** — ホストが保証されており、いずれのしきい値も超過していません。
  - ・ **警告** — ホストはアクティブですが、警告しきい値を超過しています。
  - ・ **重要** — 警告と同様ですが、重要なしきい値です
  - ・ **期限切れ** — このホストの保証期限が切れています。
  - ・ **不明** — 保証ジョブが実行されていないか、データ取得中にエラーが発生したか、またはシステムに保証が含まれていないことが原因で、OMIVV が保証ステータスを取得できません。
- ・ **資格タイプ** — 次のステータスが表示されます。
  - ・ 初期
  - ・ 拡張
  - ・ 期限切れ
- ・ **開始日** — 保証の開始日が表示されます
- ・ **終了日** — 保証の終了日が表示されます
- ・ **残日数** — 保証の残り日数が表示されます
- ・ **最終更新日** — 保証が最後に更新された日時

## 単一ホストのシステム イベント ログ情報の表示

システム イベント ログ (SEL) では、OMIVV で検出されたハードウェアのステータス情報が提供され、次の情報が表示されます。

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

重要度は次のように定義されます。

  - ・ 情報
  - ・ 警告
  - ・ エラー
- ・ **時刻 (サーバー時刻)** — イベント発生時の時刻と日付を示します。

システム イベント ログをクリアするには、[ [ログのクリア](#) ] をクリックします。ログをクリアした後は、ログ データを回復できないことを示すメッセージが表示されます。

# クラスターおよびデータセンターでのホスト監視

OMIVV では、データセンターまたはクラスター内のすべてのホストの詳細情報を表示できます。

## OMIVV データセンターおよびクラスター情報の表示

### データセンターおよびクラスターの概要の表示

データセンターまたはクラスター情報、システム ロックダウン モード、ハードウェア リソース、保証情報などの情報を表示できます。このページの情報を表示するには、インベントリが正常に完了していることを確認します。OMIVV データセンターおよびクラスタービューは、iDRAC からデータを直接レポートします。

1. OMIVV ホームページで、[メニュー] を展開し、[ホストとクラスター] を選択します。
2. 左ペインで、データセンターまたはクラスターを選択し、[モニター] > [OMIVV クラスター] または [データセンター情報] をクリックします。
3. 詳細を表示するには、特定のホストを選択します。

iDRAC IP、シャーシ URL、CPU、メモリーなどの情報は、ページの一番下の水平ペインに表示されます。

表 16. データセンターおよびクラスターの概要

情報	説明
データセンター/クラスター情報	次が表示されます： <ul style="list-style-type: none"><li>・ データセンター/クラスター名</li><li>・ 管理下ホスト数</li><li>・ 合計エネルギー消費量</li></ul>
システムロックダウンモード	iDRAC ロックダウンモード機能のステータスを表示します。ホストの総数の iDRAC ロックダウンモードステータスは次のように表示されます。 <ul style="list-style-type: none"><li>・ 電源オン</li><li>・ 電源オフ</li><li>・ 該当しない (iDRAC9 ベースのサーバーのみ)</li></ul> iDRAC9 ベースサーバーのリストについては、「互換性マトリックス」を参照してください。
ハードウェアリソース	次が表示されます： <ul style="list-style-type: none"><li>・ 合計プロセッサ数</li><li>・ 総メモリー量</li><li>・ 仮想ディスク容量</li></ul>
保証サマリ	選択したホストの保証ステータスを表示します。ステータスオプションには次のものがあります。 <ul style="list-style-type: none"><li>・ 期限切れ保証</li><li>・ アクティブな保証</li><li>・ 不明な保証</li></ul>
ホスト	ホスト名を表示します
サービスタグ	ホストのサービスタグを表示します
モデル	PowerEdge のモデルを表示します
資産タグ	設定すると、資産タグが表示されます
シャーシサービスタグ	シャーシのサービスタグを表示します (ある場合)
OS バージョン	ESXi OS のバージョンを表示します
場所	ブレードのみ：スロット位置を表示します。その他の場合は、「該当なし」を表示します

情報	説明
システムロックダウンモード	iDRAC9 ベースのサーバーのみ：ホストの iDRAC ロックダウン モードがオンになっているか、オフになっているか、または不明であるかを表示します。  iDRAC9 ベースより前のすべての PowerEdge サーバーでは、システム ロックダウン モードが [ 該当なし ] として表示されます。iDRAC9 ベース サーバーのリストについては、「互換性マトリックス」を参照してください。
iDRAC IP	iDRAC の IP アドレスを表示します
サービスコンソール IP	サービスコンソールの IP を表示します
CMC または管理モジュール URL	CMC または管理モジュール URL ( ブレード サーバーのシャーシの URL ) を表示します。それ以外の場合は「該当なし」と表示されます
CPU	CPU の数を表示します
メモリ	ホストのメモリを表示します
電源状況	ホストに電源があるかどうかを表示します
最新のインベントリ	最後のインベントリジョブの日付と時刻が表示されます
ホスト認証情報プロファイル	ホスト認証情報プロファイルの名前を表示します
リモートアクセスカードバージョン	リモートアクセスカードのバージョンを表示します
BIOS ファームウェアバージョン	BIOS のファームウェアバージョンを表示します

## データセンターとクラスターのハードウェア情報の表示

表 17. データセンターとクラスターのハードウェア情報

ハードウェア：コンポーネント	情報
ハードウェア：FRU	<ul style="list-style-type: none"> <li>・ ホスト — ホスト名が表示されます。</li> <li>・ サービスタグ — ホストのサービスタグが表示されます</li> <li>・ パーツ名 — FRU のパーツ名が表示されます。</li> <li>・ パーツ番号 — FRU のパーツ番号が表示されます。</li> <li>・ 製造元 — 製造元の名前が表示されます。</li> <li>・ シリアル番号 — 製造元のシリアル番号が表示されます。</li> <li>・ 製造日 — 製造日が表示されます。</li> </ul>
ハードウェア：プロセッサ	<ul style="list-style-type: none"> <li>・ ホスト — ホスト名が表示されます。</li> <li>・ サービスタグ — ホストのサービスタグが表示されます</li> <li>・ ソケット — スロット番号が表示されます。</li> <li>・ 速度 — 現在の速度が表示されます。</li> <li>・ ブランド — プロセッサのブランドが表示されます。</li> <li>・ バージョン — プロセッサのバージョンが表示されます。</li> <li>・ コア — このプロセッサ内のコアの数が表示されます。</li> </ul>
ハードウェア：電源装置	<ul style="list-style-type: none"> <li>・ ホスト — ホスト名が表示されます。</li> <li>・ サービスタグ — ホストのサービスタグが表示されます</li> <li>・ タイプ — 電源装置のタイプが表示されます。電源装置には、次のタイプがあります。 <ul style="list-style-type: none"> <li>・ 不明</li> <li>・ リニア</li> <li>・ スイッチング</li> <li>・ BATTERY</li> <li>・ UPS</li> </ul> </li> </ul>

ハードウェア：コンポーネント	情報
	<ul style="list-style-type: none"> <li>・ コンバータ</li> <li>・ レギュレータ</li> <li>・ AC</li> <li>・ DC</li> <li>・ VRM</li> <li>・ <b>場所</b> — スロット1など、電源装置の場所が表示されます。</li> <li>・ <b>出力 (ワット)</b> — ワット単位で電力が表示されます。</li> <li>・ <b>ステータス</b> — 電源装置の状態が表示されます。ステータスオプションには次のものがあります。 <ul style="list-style-type: none"> <li>・ その他</li> <li>・ 不明</li> <li>・ OK</li> <li>・ 重要</li> <li>・ 非重要</li> <li>・ 回復可能</li> <li>・ 回復不可能</li> <li>・ 高</li> <li>・ 低</li> </ul> </li> </ul>
ハードウェア：メモリ	<ul style="list-style-type: none"> <li>・ <b>ホスト</b> — ホスト名が表示されます。</li> <li>・ <b>サービスタグ</b> — ホストのサービスタグが表示されます</li> <li>・ <b>スロット</b> — DIMM スロットが表示されます。</li> <li>・ <b>サイズ</b> — メモリーサイズが表示されます。</li> <li>・ <b>タイプ</b> — メモリーのタイプが表示されます。</li> </ul>
ハードウェア：NIC	<ul style="list-style-type: none"> <li>・ <b>ホスト</b> — ホスト名が表示されます。</li> <li>・ <b>サービスタグ</b> — ホストのサービスタグが表示されます</li> <li>・ <b>名前</b> — NIC名が表示されます。</li> <li>・ <b>製造元</b> — 製造元の名前のみが表示されます。</li> <li>・ <b>MAC アドレス</b> — NICのMACアドレスが表示されます。</li> </ul>
ハードウェア：PCI スロット	<ul style="list-style-type: none"> <li>・ <b>ホスト</b> — ホスト名が表示されます。</li> <li>・ <b>サービスタグ</b> — ホストのサービスタグが表示されます</li> <li>・ <b>スロット</b> — スロットを表示します。</li> <li>・ <b>製造元</b> — PCI スロットのメーカー名が表示されます。</li> <li>・ <b>説明</b> — PCI デバイスの説明が表示されます。</li> <li>・ <b>タイプ</b> — PCI スロットタイプが表示されます。</li> <li>・ <b>幅</b> — データ バス幅が表示されます (該当する場合)。</li> </ul>
ハードウェア：リモートアクセスカード	<ul style="list-style-type: none"> <li>・ <b>ホスト</b> — ホスト名が表示されます。</li> <li>・ <b>サービスタグ</b> — ホストのサービスタグが表示されます</li> <li>・ <b>IP アドレス</b> — リモート アクセス カードの IP アドレスが表示されます。</li> <li>・ <b>MAC アドレス</b> — リモート アクセス カードの MAC アドレスが表示されます。</li> <li>・ <b>RAC タイプ</b> — リモート アクセス カードのタイプが表示されます。</li> <li>・ <b>URL</b> — このホストに関連付けられた動作している iDRAC の URL が表示されます。</li> </ul>

## データセンターとクラスターのストレージ情報の表示

表 18. データセンターとクラスターのストレージの詳細

ストレージ：ディスク	説明
物理ディスク	<ul style="list-style-type: none"> <li>・ <b>ホスト</b> — ホスト名が表示されます。</li> <li>・ <b>サービスタグ</b> — ホストのサービスタグが表示されます</li> <li>・ <b>容量</b> — 物理ディスクの容量が表示されます。</li> <li>・ <b>ディスクのステータス</b> — 物理ディスクのステータスが表示されます。以下のオプションがあります。             <ul style="list-style-type: none"> <li>・ オンライン</li> <li>・ 準備完了</li> <li>・ 劣化</li> <li>・ エラー</li> <li>・ オフライン</li> <li>・ 再構成中</li> <li>・ 互換性なし</li> <li>・ 削除済み</li> <li>・ クリア済み</li> <li>・ SMART アラート検知</li> <li>・ 不明</li> <li>・ 外部</li> <li>・ サポートなし</li> </ul> </li> </ul> <p><b>メモ:</b> これらのアラートの意味についての詳細は、<a href="http://dell.com/support">dell.com/support</a> にある『<b>Dell EMC OpenManage Server Administrator Storage Management ユーザーズガイド</b>』を参照してください。</p> <ul style="list-style-type: none"> <li>・ <b>モデル番号</b> — 物理ストレージ ディスクのモデル番号が表示されます。</li> <li>・ <b>最終インベントリ</b> — インベントリが最後に実行された日、月、時刻が表示されます。</li> <li>・ <b>ステータス</b> — ホストのステータスが表示されます。</li> <li>・ <b>コントローラー ID</b> — コントローラー ID が表示されます。</li> <li>・ <b>コネクター ID</b> — コネクター ID が表示されます。</li> <li>・ <b>エンクロージャー ID</b> — エンクロージャーの ID が表示されます。</li> <li>・ <b>デバイス ID</b> — デバイス ID が表示されます。</li> <li>・ <b>バスプロトコル</b> — バス プロトコルが表示されます。</li> <li>・ <b>残留書き込み耐久性</b> — SSD の残留書き込み耐久性が表示されます。</li> <li>・ <b>ホットスペアのタイプ</b> (PCIe では該当しません) — ホットスペアのタイプが示されます。以下のオプションがあります。             <ul style="list-style-type: none"> <li>・ いいえ — ホットスペアなし。</li> <li>・ グローバル — ディスクグループの一部であるが未使用のバックアップディスク</li> <li>・ 専用 — 単一の仮想ドライブに割り当てられた未使用のバックアップ ディスク。仮想ディスク内の物理ディスクに不具合があると、ホットスペアが有効化されて故障した物理ディスクと交換されるため、システムの中断や、ユーザー介入が必要になることもありません。</li> </ul> </li> <li>・ <b>パーツ番号</b> — ストレージのパーツ番号が表示されます。</li> <li>・ <b>シリアル番号</b> — ストレージのシリアル番号が表示されます。</li> <li>・ <b>ベンダー名</b> — ストレージのベンダー名が表示されます。</li> </ul>
仮想ディスク	<ul style="list-style-type: none"> <li>・ <b>ホスト</b> — ホストの名前が表示されます。</li> <li>・ <b>サービスタグ</b> — ホストのサービスタグが表示されます</li> <li>・ <b>名前</b> — 仮想ドライブの名前が表示されます</li> <li>・ <b>物理ディスク</b> — 仮想ドライブが配置されている物理ディスクが表示されます</li> <li>・ <b>容量</b> — 仮想ドライブの容量が表示されます</li> <li>・ <b>レイアウト</b> — 仮想ストレージのレイアウトタイプを表示します。これは、この仮想ドライブに設定された RAID のタイプです。</li> </ul>

ストレージ：ディスク	説明
	<ul style="list-style-type: none"> <li>・ <b>最終インベントリー</b> — インベントリーが最後に実行された曜日、日付および時刻が表示されます。</li> <li>・ <b>コントローラー ID</b> — コントローラー ID が表示されます。</li> <li>・ <b>デバイス ID</b> — デバイス ID が表示されます。</li> <li>・ <b>メディアタイプ</b> — SSD と HDD のいずれかが表示されます。</li> <li>・ <b>バスプロトコル</b> — 仮想ドライブ内の物理ディスクが使用するテクノロジーを表示します。可能な値は次のとおりです。 <ul style="list-style-type: none"> <li>・ SCSI</li> <li>・ SAS</li> <li>・ SATA</li> <li>・ PCIe</li> </ul> </li> <li>・ <b>ストライプ サイズ</b> — ストライプ サイズが表示されます。ストライプ サイズは、各ストライプが単一ディスク上で消費する容量です。</li> <li>・ <b>デフォルト読み取りポリシー</b> — コントローラでサポートされているデフォルト読み取りポリシーが表示されます。以下のオプションがあります。 <ul style="list-style-type: none"> <li>・ 先読み</li> <li>・ 先読みなし</li> <li>・ 適応先読み</li> <li>・ 読み取りキャッシュが有効</li> <li>・ 読み取りキャッシュが無効</li> </ul> </li> <li>・ <b>デフォルト書き込みポリシー</b> — コントローラでサポートされているデフォルト書き込みポリシーが表示されます。以下のオプションがあります。 <ul style="list-style-type: none"> <li>・ ライトバック</li> <li>・ ライトバックの強制</li> <li>・ ライトバックが有効</li> <li>・ ライトスルー</li> <li>・ 書き込みキャッシュ有効、保護</li> <li>・ 書き込みキャッシュが無効</li> </ul> </li> <li>・ <b>ディスク キャッシュ ポリシー</b> — コントローラでサポートされているデフォルトのキャッシュ ポリシーが表示されます。以下のオプションがあります。 <ul style="list-style-type: none"> <li>・ 有効 — キャッシュ I/O</li> <li>・ 無効 — ダイレクト I/O</li> </ul> </li> </ul>

## データセンターとクラスターのファームウェア情報の表示

各ファームウェア コンポーネントについて、次の情報が表示されます。

- ・ **ホスト** — ホストの名前が表示されます。
- ・ **サービスタグ** — ホストのサービスタグが表示されます
- ・ **名前** — このホスト上のすべてのファームウェアの名前が表示されます。
- ・ **バージョン** — このホスト上のすべてのファームウェアのバージョンが表示されます。

## データセンターとクラスターの電源モニタリング情報の表示

- ・ **ホスト** — ホストの名前が表示されます。
- ・ **サービスタグ** — ホストのサービスタグが表示されます
- ・ **現在のプロファイル** — お使いのシステムのパフォーマンスを最大化して電力を節約するための電源プロファイルが表示されます。
- ・ **エネルギー消費量** — ホストのエネルギー消費量が表示されます。
- ・ **ピーク予約容量** — 電力のピーク予約容量が表示されます。
- ・ **電力バジェット** — このホストの電力上限が表示されます。
- ・ **警告しきい値** — お使いのシステムの温度プローブの警告しきい値の設定最大値が表示されます。
- ・ **障害しきい値** — お使いのシステムの温度プローブの障害しきい値の設定最大値が表示されます。
- ・ **インスタント予約容量** — ホストのインスタント ヘッドルーム容量が表示されます。
- ・ **エネルギー消費開始日** — ホストが電力消費を開始した日付と時刻が表示されます
- ・ **エネルギー消費終了日** — ホストが電力消費を停止した日付と時刻が表示されます

- ・ システム ピーク電力 — ホストのピーク電力が表示されます。
- ・ システムピーク電力開始日 — ホストのピーク電力が開始した日付と時間が表示されます
- ・ システムピーク電力終了日 — ホストのピーク電力が終了した日付と時間が表示されます
- ・ システム ピーク電流 — ホストのピーク電流が表示されます。
- ・ システム ピーク電流開始日 — ホストのピーク電流が開始した日付と時間が表示されます。
- ・ システム ピーク電流終了日 — ホストのピーク電流が終了した日付と時間が表示されます。

## データセンターとクラスターの保証情報の表示

保証ステータスを表示するには、保証ジョブを実行します。「保証取得ジョブのスケジュール」を参照してください。保証サマリ ページで、保証の期限の日付を監視できます。保証設定は、保証スケジュールを有効化または無効化し、最小日数しきい値アラートを設定することで、Dell オンラインからサーバ保証情報を検索する時期を管理することができます。

- ・ **保証概要** — ホストの保証概要が表示されます。ここでは、アイコンを使用して、各ステータス カテゴリ内のホスト数が視覚的に示されます。
- ・ **ホスト** — ホスト名が表示されます。
- ・ **サービスタグ** — ホストのサービスタグが表示されます
- ・ **説明** — 説明が表示されます
- ・ **保証ステータス** — ホストの保証ステータスが表示されます。ステータスのオプションには、次のものがあります。
  - ・ **アクティブ** — ホストが保証されており、いずれのしきい値も超過していません。
  - ・ **警告** — ホストはアクティブですが、警告しきい値を超過しています。
  - ・ **重要** — 警告と同様ですが、重要なしきい値です
  - ・ **期限切れ** — このホストの保証期限が切れています。
  - ・ **不明** — 保証ジョブが実行されていない、データ取得中にエラーが発生した、システムに保証がない、のいずれかであるため、OpenManage Integration for VMware vCenter が保証ステータスを取得しません。
- ・ **[ 残日数 ]**: 保証の残り日数が表示されます。

## ファームウェアアップデート

OMIVV では、管理対象ホストで BIOS およびファームウェアのアップデート ジョブを実行できます。複数のクラスタまたは非クラスタホストでファームウェアアップデートジョブを同時に実行することができます。同一クラスタの 2 つのホストで同時にファームウェアをアップデートすることは許可されません。

**① メモ:** マルチアプライアンス環境の場合、クラスターまたはホストでファームウェアをアップデートするには、ターゲット vCenter で登録されたアプライアンスがロードされていることを確認します。

ファームウェア アップデートを実行するには、次の 2 つの方法があります。

- ・ **単一 DUP**: DUP の場所 ( CIFS または NFS のいずれか ) を直接ポイントすることで、iDRAC および BIOS のファームウェア アップデートを実行します。単一 DUP の方法はホスト レベルでのみ使用できます。
- ・ **リポジトリ プロファイル**: ファームウェアおよびドライバーのアップデートを実行します。この方法は、ホスト レベルとクラスターレベルの両方で使用できます。

ファームウェアおよびドライバーのアップデートに使用されるリポジトリ プロファイルは次のとおりです。

- ・ **ファームウェア リポジトリ**: ファームウェア カタログを使用してファームウェア情報を取得するリポジトリ プロファイルです。

次に、ファームウェア リポジトリの 2 つのタイプを示します。

- ・ **ユーザーが作成したファームウェア リポジトリ**
- ・ **工場で作成されるファームウェア リポジトリ**: 工場で作成されるカタログには、次の 2 種類があります。工場で作成されるカタログは、vSAN クラスターのファームウェア アップデートとベースライン化には適用されません。
  - ・ **Dell デフォルトカタログ**: Dell EMC オンライン カタログを使用して最新のファームウェア情報を取得する、工場出荷時作成のファームウェア リポジトリ プロファイルです。アプライアンスがインターネットに接続されていない場合は、ローカル CIFS、NFS、HTTP、または HTTPS ベースの共有を指すようにこのリポジトリを変更します。
  - ・ **[ 検証済み MX スタック カタログ ]**: Dell EMC オンライン カタログを使用して、MX シャーシおよびその対応するスレッドの検証済みのファームウェア情報を取得する、工場で作成されたファームウェア リポジトリ プロファイルです。
- ・ **ドライバー リポジトリ**: リポジトリ プロファイルには、vSAN クラスターのドライバーのアップデートに使用できるオフラインバンドルが含まれています。

ファームウェア アップデート ウィザードは常に、iDRAC と BIOS の最低ファームウェア レベルをチェックし、最低必須のバージョンにアップデートすることを試みます。iDRAC および BIOS の最小ファームウェア レベルの詳細については、『OpenManage

Integration for VMware vCenter 互換性マトリックス』を参照してください。iDRAC および BIOS ファームウェア バージョンが最低要件を満たすと、ファームウェア アップデート プロセスにより、iDRAC、RAID Controller、NIC/LOM、BIOS などを含むすべてのファームウェア バージョンのアップデートが実行されます。

- i** **メモ:** PowerEdge XR2 サーバーをアップデートするには、OMIVV は、Dell オンライン カタログにある R440 ファームウェア コンポーネントを使用します。PowerEdge XR2 をサポートするためにオフライン ファームウェア リポジトリに使用するカスタム カタログ (DRM を使用) を作成する場合は、PowerEdge R440 サーバーに適切なファームウェア コンポーネントを使用します。

## vSAN ホストのファームウェアとドライバーのアップデート

vSAN ホスト (vSAN 対応クラスター内のホスト) でファームウェア アップデートをスケジュールする前に、環境が次の条件を満たしていることを確認してください。

- ホストが対応している (CSIOR が有効で、ホストに対応 ESXi バージョンがある) こと、ホストがホスト認証情報プロファイルに関連付けられていること、およびホストのインベントリが正常に行われていることを確認します。
  - ファームウェア アップデートをスケジュールする前に、次の前提条件がチェックされます。
    - DRS が有効になっている。
    - ホストがメンテナンス モードになっていない。
    - vSAN データオブジェクトが正常である。
- 前提条件をスキップするには、[ **前提条件のチェック** ] チェック ボックス ([ **アップデートのスケジュール** ] ページ) をオフにします。
- ストレージ コントローラー、HDD、SSD コンポーネントの場合、vSAN バージョンに基づく VMware vSAN ガイドラインに従って、選択したリポジトリ内で選択したドライバーとファームウェアのバージョンが対応していることを確認します。
  - ドライバーの場合、OMIVV は、VMware ハードウェア互換性リストにリストされているオフライン バンドルのみをサポートしません。
  - クラスターは、選択されたデータ移行オプションの vSAN 要件を満たしている。選択したデータ移行オプションの要件を vSAN クラスターが満たしていない場合、アップデートはタイムアウトします。
  - ベースライン (クラスター プロファイル) のファームウェアまたはドライバー リポジトリを選択することを強く推奨します。
  - 更新中のクラスターの下ホストに対して、アクティブなファームウェア アップデート ジョブが存在しないことを確認。
  - 「メンテナンス モードの実行」ジョブに必要なタイムアウト値を指定していることを確認。待機時間が指定の時間を過ぎると、アップデートジョブは失敗します。ただし、ホストの再起動時に、コンポーネントが自動的にアップデートされる場合があります。
  - vSAN を有効化した後に、インベントリを再実行している。

ファームウェアのアップデート処理中には、次のものを削除または移動しないことを推奨します。

- ファームウェアのアップデートジョブが進行中の vCenter のホスト
- ファームウェアのアップデート ジョブが進行中のホストの認証情報プロファイル
- CIFS または NFS に配置されているリポジトリ

OMIVV が、ホストの対応性および、同じクラスター内のホストで他のファームウェア アップデート ジョブが進行中かどうかを確認します。検証後、ファームウェアアップデート ウィザードが表示されます。

- ファームウェア アップデート ウィザードを起動するには、OMIVV のホームページで [ **メニュー** ] を展開し、[ **ホストとクラスター** ] を選択して、次のいずれかの操作を実行します。
  - ホストを右クリックして、[ **OMIVV ホスト アクション** ] > [ **ファームウェア アップデート** ] の順に選択します。
  - ホストを選択して、右ペインで [ **監視** ] > [ **OMIVV ホスト情報** ] > [ **ファームウェア** ] > [ **ファームウェアの実行ウィザード** ] の順に選択します。
  - ホストを選択して、右ペインで [ **サマリー** ] を選択し、[ **OMIVV ホスト情報** ] > [ **ホスト アクション** ] > [ **ファームウェアの実行ウィザード** ] の順に選択します。
- [ **ファームウェア アップデート チェック リスト** ] ページで、アップデートをスケジュールする前にすべての前提条件が検証されていることを確認し、[ **開始** ] をクリックします。
- [ **アップデート ソース** ] ページで、次のいずれかのオプションを選択します。
  - リポジトリ プロファイル
  - 単一 DUP**
- ファイルから単一のファームウェアアップデートをロードするには、**単一 DUP** を選択します。
  - 単一 DUP は、OMIVV アプライアンスがアクセスできる CIFS または NFS 共有上に存在することができます。次のいずれかの形式でファイルの位置を入力し、ステップ 9 に進みます。
    - NFS — <ホスト>:/<共有パス/>ファイル名.exe

・ CIFS — \\<ホストがアクセスできる共有パス>\<ファイル名>.exe

**メモ:** シングルコンポーネント DUP のファイル名には、空白スペースが無いことを確認してください。

CIFS 共有の場合、共有ドライブにアクセスできるユーザー名とパスワードの入力を要求するプロンプトが OMIVV から表示されます。

5. [ **リポジトリ プロファイル** ] オプションを選択した場合は、ファームウェアおよびドライバーのリポジトリ プロファイルを選択します。

ホストが存在するクラスターにクラスター プロファイルが関連付けられている場合、デフォルトでは、関連付けられているファームウェアとドライバー リポジトリ プロファイルが選択されます。

ファームウェアまたはドライバー リポジトリ プロファイルを変更すると、選択したリポジトリ プロファイルがベースラインに関連付けられておらず、別のリポジトリを使用するとベースライン比較に影響する可能性があることを示すメッセージが表示されます。

**メモ:** ドライバー リポジトリとファームウェア リポジトリの両方がクラスター プロファイルに関連付けられている場合は、ドライバーとファームウェアの両方を同時にアップデートすることが推奨されます。

ファームウェアまたはドライバーをアップデートしない場合、あるいは、ファームウェアまたはドライバーが最新である場合、ドロップダウン メニューから [ **リポジトリ未選択** ] を選択します。

デフォルトのファームウェア カタログ ( Dell EMC デフォルト カタログおよび検証済み MX スタック カタログ ) は、リポジトリ プロファイル オプションには表示されません。リポジトリ プロファイルを使用するには、OMIVV でカスタム リポジトリを作成します。

カスタム リポジトリ プロファイルを作成するには、以下の手順を実行します。

- a) Dell EMC Repository Manager ( DRM ) に移動して、カタログを作成します。

DRM を使用したカタログ作成に関する詳細については、「[OMIVV を使用して Dell EMC Repository Manager \( DRM \) でカタログを作成する](#)」を参照してください。

- b) カタログと対応するファイルをダウンロードします。

- c) ダウンロードしたカタログを使用して、OMIVV でリポジトリ プロファイルを作成します。

レポジトリ プロファイルの作成に関する詳細については、「[リポジトリ プロファイルの作成](#)」を参照してください。

6. 選択したファームウェア リポジトリ プロファイルに基づいて、適切なバンドルを選択し、[ **次へ** ] をクリックします。64 ビットバンドルのみサポートされます。


7. [ **ドライバー コンポーネントの選択** ] ページで、アップデートの必要があるドライバー コンポーネントを選択して [ **次へ** ] をクリックします。アップデートするドライバコンポーネントを選択すると、パッケージ内のすべてのコンポーネントが選択されます。


フィルター オプションを使用して、特定の列名に基づいてデータをフィルタリングできます。

8. [ **ファームウェア コンポーネントの選択** ] ページで、アップデートの必要があるファームウェア コンポーネントを選択して [ **次へ** ] をクリックします。

緊急、推奨、任意、ダウングレードなどの重要度ステータスに基づくコンポーネントの数が表示されます。

カタログ内の使用可能なバージョンよりも古いバージョンのコンポーネント、または同じレベル ( 最新 ) であるか、アップデートのスケジュールが設定されているコンポーネントは選択できません。使用可能なバージョンよりも古いバージョンのコンポーネントを選択するには、[ **ファームウェアのダウングレードを許可する** ] チェックボックスを選択します。

すべてのページのすべてのファームウェア コンポーネントを選択するには、 をクリックします。

すべてのページのすべてのファームウェア コンポーネントをクリアするには、 をクリックします。

9. [ **アップデートのスケジュール** ] ページで、ファームウェア アップデート ジョブ名と説明を入力します。[ **説明** ] フィールドはオプションです。

ファームウェア アップデート ジョブ名は必須です。ファームウェアアップデートのジョブ名をパージすれば、そのジョブ名を再度使用できます。

10. [ **追加設定** ] セクションで、次の手順を実行します。

- a) メンテナンス モードのタイムアウト値を 60 分 ~ 1440 分の間で入力します。待ち時間が指定の時間を過ぎるとアップデート ジョブは失敗し、メンテナンス開始タスクはキャンセルされるかタイムアウトします。ただし、ホストの再起動時に、コンポーネントが自動的にアップデートされる場合があります。

- b) [ **メンテナンス モード開始オプション** ] ドロップダウン メニューから、適切なデータ移行オプションを選択します。データ移行オプションの詳細については、VMware のマニュアルを参照してください。

**メモ:** クラスター設定で完全なデータ移行がサポートされていない場合、またはストレージ容量が不足している場合は、メンテナンス モード開始タスクが失敗します。

以下のオプションはデフォルトで選択されます。

- ・ **ファームウェア アップデート完了後にメンテナンス モードを終了** - このオプションを無効にすると、ホストはメンテナンス モードのままになります。
  - ・ **電源がオフで一時停止された仮想マシンをクラスター内の他のホストに移動する** - このオプションを無効にすると、ホスト デバイスがオンラインになるまで VM が切断されます。
- c) ファームウェアのアップデート中に問題が生じた場合は、[ **ジョブ キューの削除と iDRAC のリセット** ] をクリックします。これによりアップデートプロセスが正常に完了する場合があります。これにより、ジョブの完了に必要なアップデート時間全体が増加し、iDRAC でスケジュールされている保留中のジョブまたはアクティビティがキャンセルされ、iDRAC がリセットされます。
- シャシ認証情報プロファイルを使用して管理されているホストでは、ジョブ キューの削除はサポートされていません。デフォルトでは、[ **前提条件のチェック** ] オプションが選択されます。

11. [ **アップデート スケジュール** ] セクションで、次のいずれかのオプションを選択します。

- ・ **今すぐアップデート**
- ・ **アップデートのスケジュール**
- ・ **次の再起動でアップデートを適用する**

12. [ **サマリーのレビュー** ] ページで情報を確認し、[ **終了** ] をクリックします。

ファームウェア アップデート ジョブには、選択したコンポーネントとサーバーの数に応じて、最大で数時間かかる場合があります。ジョブのステータスは、[ **ジョブ** ] ページに表示できます。

ファームウェア アップデート タスクが完了すると、選択したホストで自動的にインベントリが実行され、[ **アップデートのスケジュール** ] ページで選択したオプションに基づいて自動的にメンテナンス モードが終了します。

## OMIVV を使用して Dell EMC Repository Manager ( DRM ) でカタログを作成する

本項では、DRM バージョン 3.0 以降でカタログを作成するプロセスについて説明します。

1. **DRM のダウンロード ページ** に移動して、DRM をダウンロードします。
2. DRM ホーム ページで、[ **新規リポジトリの追加** ] をクリックします。  
リポジトリの追加 ウィンドウが表示されます。
3. **リポジトリの追加** ウィンドウで、次の手順を実行します。
  - a. **リポジトリ名** と **説明** に必要な内容を入力します。
  - b. **ベースカタログ** ドロップダウンメニューから、**カタログ** を選択します。
  - c. **統合タイプ** ドロップダウンメニューから、**OpenManage Integration for VMware vCenter** を選択します。
4. **OpenManage Integration for VMware vCenter** ウィンドウで、**仮想アプライアンス IP**、**vCenter サーバ IP**、**ユーザー名**、および **パスワード** を入力し、**接続** をクリックします。  
作成されたカタログが、ホームページに表示されます。
5. カatalogをエクスポートするには、**カタログ** を選択して **エクスポート** をクリックします。

## vSAN クラスターのファームウェアとドライバーのアップデート

ファームウェア アップデートをスケジュールする前に、環境で次の条件が満たされていることを確認してください。

- ・ ホストが対応している ( CSIOR が有効で、ホストに対応 ESXi バージョンがある ) こと、ホストがホスト認証情報プロファイルに関連付けられていること、およびホストのインベントリが正常に行われていることを確認します。ホストがリストされていない場合は、OMIVV からホストの管理対応性ウィザードを実行し、ファームウェア アップデート ウィザードを使用します。
- ・ ファームウェア アップデートをスケジュールする前に、次の前提条件がチェックされます。
  - ・ DRS が有効になっている。
  - ・ ホストがメンテナンス モードになっていない。
  - ・ vSAN データオブジェクトが正常である。
- ・ ストレージ コントローラー、HDD、SSD コンポーネントの場合、vSAN バージョンに基づく VMware vSAN ガイドラインに従って、選択したリポジトリ内で選択したドライバーとファームウェアのバージョンが対応していることを確認します。
- ・ ドライバーの場合、OMIVV は、VMware ハードウェア互換性リストにリストされているオフライン バンドルのみをサポートします。
- ・ クラスターは、選択されたデータ移行オプションの vSAN 要件を満たしている。選択したデータ移行オプションの要件を vSAN クラスターが満たしていない場合、アップデートはタイムアウトします。
- ・ ベースライン ( クラスター プロファイル ) のファームウェアまたはドライバー リポジトリを選択することを強く推奨します。

- ・ 更新中のクラスターの下ノホストに対して、アクティブなファームウェア アップデート ジョブが存在しないことを確認。
- ・ 「メンテナンス モードの実行」ジョブに必要なタイムアウト値を指定していることを確認。待機時間が指定の時間を過ぎると、アップデートジョブは失敗します。ただし、ホストの再起動時に、コンポーネントが自動的にアップデートされる場合があります。
- ・ vSAN を有効にした後で、インベントリーを再実行します。

ファームウェアのアップデート処理中には、次のものを削除または移動しないことを推奨します。

- ・ ファームウェアのアップデート ジョブが進行中の vCenter のクラスターのホスト
- ・ ファームウェアのアップデート ジョブが進行中のホストの認証情報 プロファイル
- ・ CIFS または NFS に配置されているリポジトリー

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

OMIVV が、ホストの対応性および、同じクラスター内のホストで他のファームウェア アップデート ジョブが進行中かどうかを確認します。検証後、ファームウェアアップデート ウィザードが表示されます。

1. ファームウェア アップデート ウィザードを起動するには、OMIVV のホームページで [メニュー] を展開し、[ホストとクラスター] を選択して、次のいずれかの操作を実行します。
  - ・ クラスターを右クリックし、[OMIVV クラスターアクション] > [ファームウェア アップデート] と選択します。
  - ・ クラスターを選択し、右ペインで [監視] > [OMIVV クラスター情報] > [ファームウェア] > [ファームウェアの実行ウィザード] を選択します。
2. [ファームウェア アップデート チェックリスト] ページで、アップデートをスケジュールする前にすべての前提条件が検証されていることを確認し、[開始] をクリックします。
3. [アップデート ソース] ページで、ファームウェアおよびドライバ リポジトリー プロファイルを選択します。

ホストが存在するクラスターにクラスター プロファイルが関連付けられている場合、デフォルトでは、関連付けられているファームウェアとドライバ リポジトリー プロファイルが選択されます。

ファームウェアまたはドライバ リポジトリー プロファイルを変更すると、選択したリポジトリー プロファイルがベースラインに関連付けられておらず、別のリポジトリーを使用するとベースライン比較に影響する可能性があることを示すメッセージが表示されます。

**i** **メモ: ドライバ リポジトリーとファームウェア リポジトリーの両方がクラスター プロファイルに関連付けられている場合は、ドライバとファームウェアの両方を同時にアップデートすることが推奨されます。**

ファームウェアまたはドライバをアップデートしない場合、あるいは、ファームウェアまたはドライバが最新である場合、ドロップダウンメニューから [リポジトリー未選択] を選択します。

デフォルトのファームウェア カタログ (Dell EMC デフォルト カタログおよび検証済み MX スタック カタログ) は、リポジトリー プロファイル オプションには表示されません。リポジトリー プロファイルを使用するには、OMIVV でカスタム リポジトリーを作成します。

カスタム リポジトリー プロファイルを作成するには、以下の手順を実行します。


- a) Dell EMC Repository Manager (DRM) に移動して、カタログを作成します。  
DRM を使用したカタログ作成に関する詳細については、「[OMIVV を使用して Dell EMC Repository Manager \(DRM\) でカタログを作成する](#)」を参照してください。
  - b) カタログと対応するファイルをダウンロードします。
  - c) ダウンロードしたカタログを使用して、OMIVV でリポジトリー プロファイルを作成します。  
レポジトリー プロファイルの作成に関する詳細については、「[リポジトリー プロファイルの作成](#)」を参照してください。
4. 選択したファームウェア リポジトリー プロファイルに基づいて、適切なバンドルを選択し、[次へ] をクリックします。64 ビットバンドルのみサポートされます。


**i** **メモ: OEM (ブランド解除) サーバーが異なるモデルであっても、1つのバンドルのみを選択できます。バンドルが1つまたは複数の OEM サーバーに適用されない場合でも、ファームウェア アップデート ウィザードのコンポーネント ページには、各 OEM サーバーまたはファームウェア コンポーネントのペアがリストされます。特定のファームウェア コンポーネント ペアでファームウェアのアップデートに失敗した場合は、OEM サーバーに表示されている代替バンドルで再試行してください。**

5. [ドライバ コンポーネントの選択] ページで、アップデートの必要があるドライバ コンポーネントを選択して [次へ] をクリックします。アップデートするドライバコンポーネントを選択すると、パッケージ内のすべてのコンポーネントが選択されます。  
フィルター オプションを使用して、特定の列名に基づいてデータをフィルタリングできます。
6. [ファームウェア コンポーネントの選択] ページで、アップデートの必要があるファームウェア コンポーネントを選択して [次へ] をクリックします。  
緊急、推奨、任意、ダウングレードなどの重要度ステータスに基づくコンポーネントの数が表示されます。

フィルター オプションを使用して、特定の列名に基づいてデータをフィルタリングできます。

カタログ内の使用可能なバージョンよりも古いバージョンのコンポーネント、または同じレベル (最新) であるか、アップデートのスケジュールが設定されているコンポーネントは選択できません。使用可能なバージョンよりも古いバージョンのコンポーネントを選択するには、[ **ファームウェアのダウングレードを許可する** ] チェックボックスを選択します。

すべてのページのすべてのファームウェア コンポーネントを選択するには、 をクリックします。


すべてのページのすべてのファームウェア コンポーネントをクリアするには、 をクリックします。

7. [ **アップデートのスケジュール** ] ページで、ファームウェア アップデート ジョブ名と説明を入力します。[ **説明** ] フィールドはオプションです。

ファームウェア アップデート ジョブ名は必須です。ファームウェアアップデートのジョブ名をパージすれば、そのジョブ名を再度使用できます。

8. [ **追加設定** ] セクションで、次の手順を実行します。

- メンテナンス モードのタイムアウト値を 60 分~1440 分の間で入力します。待ち時間が指定の時間を過ぎるとアップデート ジョブは失敗し、メンテナンス開始タスクはキャンセルされるかタイムアウトします。ただし、ホストの再起動時に、コンポーネントが自動的にアップデートされる場合があります。
- [ **メンテナンス モード開始オプション** ] ドロップダウン メニューから、適切なデータ移行オプションを選択します。データ移行オプションの詳細については、VMware のマニュアルを参照してください。

 **メモ:** クラスタ設定で完全なデータ移行がサポートされていない場合、またはストレージ容量が不足している場合は、メンテナンス モード開始タスクが失敗します。

デフォルトでは、[ **電源がオフで一時停止された仮想マシンをクラスター内の他のホストに移動する** ] オプションが選択されます。このオプションを無効にすると、ホスト デバイスがオンラインになるまで VM が切断されます。

- ファームウェアのアップデート中に問題が生じた場合は、[ **ジョブ キューの削除と iDRAC のリセット** ] をクリックします。これによりアップデートプロセスが正常に完了する場合があります。これにより、ジョブの完了に必要なアップデート時間全体が増加し、iDRAC でスケジュールされている保留中のジョブまたはアクティビティがキャンセルされ、iDRAC がリセットされます。

シャシ認証情報プロファイルを使用して管理されているホストでは、ジョブ キューの削除はサポートされていません。

9. [ **アップデート スケジュール** ] セクションで、次のいずれかのオプションを選択します。

- 今すぐアップデート
- アップデートのスケジュール

10. [ **サマリーのレビュー** ] ページで情報を確認し、[ **終了** ] をクリックします。

ファームウェア アップデート ジョブには、選択したコンポーネントとサーバーの数に応じて、最大で数時間かかる場合があります。ジョブのステータスは、[ **ジョブ** ] ページに表示できます。

ファームウェア アップデート タスクが完了すると、選択したホストで自動的にインベントリが実行され、[ **アップデートのスケジュール** ] ページで選択したオプションに基づいて自動的にメンテナンス モードが終了します。


## vSphere ホストのファームウェアのアップデート

vSphere ホスト (ESXi のみ) でファームウェア アップデートをスケジュールする前に、環境が次の条件を満たしていることを確認してください。

- ホストが対応している (CSIOR が有効で、ホストに対応 ESXi バージョンがある) こと、ホストがホスト認証情報プロファイルに関連付けられていること、およびホストのインベントリが正常に行われていることを確認します。
- DRS が有効になっている。

 **メモ:** スタンドアロン ホストの場合、DRS チェックは適用されません。

前提条件のチェックをスキップするには、[ **前提条件のチェック** ] チェックボックス ([ **アップデートのスケジュール** ] ページ) をオフにします。

 **メモ:** ドライバーのアップデートは、vSphere クラスタおよびホストではサポートされていません。

ファームウェアのアップデート処理中には、次のものを削除または移動しないことを推奨します。

- ファームウェアのアップデートジョブが進行中の vCenter のホスト
- ファームウェアのアップデート ジョブが進行中のホストの認証情報プロファイル
- CIFS または NFS に配置されているリポジトリ

OMIVV が、ホストの対応性および、同じクラスター内のホストで他のファームウェア アップデート ジョブが進行中かどうかを確認します。検証後、ファームウェアアップデート ウィザードが表示されます。

1. ファームウェア アップデート ウィザードを起動するには、OMIVV のホームページで [メニュー] を展開し、[ホストとクラスター] を選択して、次のいずれかの操作を実行します。
  - ・ ホストを右クリックして、[OMIVV ホスト アクション] > [ファームウェア アップデート] の順に選択します。
  - ・ ホストを選択して、右ペインで [監視] > [OMIVV ホスト情報] > [ファームウェア] > [ファームウェアの実行ウィザード] の順に選択します。
  - ・ ホストを選択して、右ペインで [サマリー] を選択し、[OMIVV ホスト情報] > [ホスト アクション] > [ファームウェアの実行ウィザード] の順に選択します。
2. [ファームウェア アップデート チェック リスト] ページで、アップデートをスケジュールする前にすべての前提条件が検証されていることを確認し、[開始] をクリックします。
3. [アップデート ソース] ページで、次のいずれかのオプションを選択します。

- ・ リポジトリ プロファイル
- ・ 単一 DUP

4. ファイルから単一のファームウェアアップデートをロードするには、**単一 DUP** を選択します。
  - a) 単一 DUP は、OMIVV アプライアンスがアクセスできる CIFS または NFS 共有上に存在することができます。次のいずれかの形式でファイルの位置を入力し、ステップ 8 に進みます。
    - ・ NFS — <ホスト>:/<共有パス/>ファイル名.exe
    - ・ CIFS — \\<ホストがアクセスできる共有パス>\<ファイル名>.exe

**メモ:** シングルコンポーネント DUP のファイル名には、空白スペースが無いことを確認してください。

CIFS 共有の場合、共有ドライブにアクセスできるユーザー名とパスワードの入力を要求するプロンプトが OMIVV から表示されます。

5. [リポジトリ プロファイル] オプションを選択した場合は、ファームウェア リポジトリ プロファイルを選択します。ホストが存在するクラスターにクラスター プロファイルが関連付けられている場合、デフォルトでは、関連付けられているファームウェア リポジトリが選択されます。そうでない場合は、[Dell デフォルト カタログ] が選択されます。ファームウェア リポジトリ プロファイルを変更すると、選択したリポジトリ プロファイルがベースラインに関連付けられておらず、別のリポジトリを使用するとベースライン比較に影響する可能性があることを示すメッセージが表示されます。
6. 選択したファームウェア リポジトリ プロファイルに基づいて、適切なバンドルを選択し、[次へ] をクリックします。64 ビット バンドルのみサポートされます。
7. [ファームウェア コンポーネントの選択] ページで、アップデートの必要があるファームウェア コンポーネントを選択して [次へ] をクリックします。

緊急、推奨、任意、ダウングレードなどの重要度ステータスに基づくコンポーネントの数が表示されます。

フィルター オプションを使用して、特定の列名に基づいてデータをフィルタリングできます。

カタログ内の使用可能なバージョンよりも古いバージョンのコンポーネント、または同じレベル (最新) であるか、アップデートのスケジュールが設定されているコンポーネントは選択できません。使用可能なバージョンよりも古いバージョンのコンポーネントを選択するには、[ファームウェアのダウングレードを許可する] ボックスを選択します。

すべてのページのすべてのファームウェア コンポーネントを選択するには、☑ をクリックします。

すべてのページのすべてのファームウェア コンポーネントをクリアするには、✕ をクリックします。

8. [アップデートのスケジュール] ページで、ファームウェア アップデート ジョブ名と説明を入力します。[説明] フィールドはオプションです。ファームウェア アップデート ジョブ名は必須です。ファームウェアアップデートのジョブ名をパージすれば、そのジョブ名を再度使用できます。

9. [追加設定] セクションで、次の手順を実行します。

- a) メンテナンス モードのタイムアウト値を 60 分~1440 分の間で入力します。待ち時間が指定の時間を過ぎるとアップデート ジョブは失敗し、メンテナンス開始タスクはキャンセルされるかタイムアウトします。ただし、ホストの再起動時に、コンポーネントが自動的にアップデートされる場合があります。

以下のオプションはデフォルトで選択されます。

- ・ **ファームウェア アップデート完了後にメンテナンス モードを終了** - このオプションを無効にすると、ホストはメンテナンス モードのままになります。
- ・ **電源がオフで一時停止された仮想マシンをクラスター内の他のホストに移動する** - このオプションを無効にすると、ホスト デバイスがオンラインになるまで VM が切断されます。

- b) ファームウェアのアップデート中に問題が生じた場合は、[ジョブ キューの削除と iDRAC のリセット] をクリックします。これによりアップデートプロセスが正常に完了する場合があります。これにより、ジョブの完了に必要なアップデート時間全体が増加し、iDRAC でスケジュールされている保留中のジョブまたはアクティビティがキャンセルされ、iDRAC がリセットされます。

シャシ認証情報プロファイルを使用して管理されているホストでは、ジョブキューの削除はサポートされていません。

デフォルトでは、[前提条件のチェック] オプションが選択されます。

10. [アップデートスケジュール] セクションで、次のいずれかのオプションを選択します。

- ・ 今すぐアップデート
- ・ アップデートのスケジュール
- ・ 次回の再起動でアップデートを適用する
- ・ メンテナンスモードにしないでアップデートを適用し、再起動を強制する

11. [サマリーのレビュー] ページで情報を確認し、[終了] をクリックします。

ファームウェアアップデートジョブには、選択したコンポーネントとサーバーの数に応じて、最大で数時間かかる場合があります。ジョブのステータスは、[ジョブ] ページに表示できます。

ファームウェアアップデートタスクが完了すると、選択したホストで自動的にインベントリが実行され、[アップデートのスケジュール] ページで選択したオプションに基づいて自動的にメンテナンスモードが終了します。

## vSphere クラスターのファームウェアのアップデート

ファームウェアアップデートをスケジュールする前に、環境で次の条件が満たされていることを確認してください。

- ・ ホストが対応している (CSIOR が有効で、ホストに対応 ESXi バージョンがある) こと、ホストがホスト認証情報プロファイルに関連付けられていること、およびホストのインベントリが正常に行われていることを確認します。ホストがリストされていない場合は、OMIVV からホストの管理対応性ウィザードを実行し、ファームウェアアップデートウィザードを使用します。
- ・ DRS が有効になっている。
- ・ 更新中のクラスターの下ホストに対して、アクティブなファームウェアアップデートジョブが存在しないことを確認。
- ・ 「メンテナンスモードの実行」ジョブに必要なタイムアウト値を指定していることを確認。待機時間が指定の時間を過ぎると、アップデートジョブは失敗します。ただし、ホストの再起動時に、コンポーネントが自動的にアップデートされる場合があります。

**メモ:** ドライバーのアップデートは、vSphere クラスターおよびホストではサポートされていません。

ファームウェアのアップデート処理中には、次のものを削除または移動しないことを推奨します。

- ・ ファームウェアのアップデートジョブが進行中の vCenter のクラスターのホスト
- ・ ファームウェアのアップデートジョブが進行中のホストの認証情報プロファイル
- ・ CIFS または NFS に配置されているリポジトリ

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

OMIVV が、ホストの対応性および、同じクラスター内のホストで他のファームウェアアップデートジョブが進行中かどうかを確認します。検証後、ファームウェアアップデートウィザードが表示されます。

1. ファームウェアアップデートウィザードを起動するには、OMIVV のホームページで [メニュー] を展開し、[ホストとクラスター] を選択して、次のいずれかの操作を実行します。

- ・ クラスターを右クリックし、[OMIVV クラスターアクション] > [ファームウェアアップデート] と選択します。
- ・ クラスターを選択し、右ペインで [監視] > [OMIVV クラスター情報] > [ファームウェア] > [ファームウェアの実行ウィザード] を選択します。

2. [ファームウェアアップデートチェックリスト] ページで、アップデートをスケジュールする前にすべての前提条件が検証されていることを確認し、[開始] をクリックします。

3. [アップデートソース] ページで、ホストが存在するクラスターにクラスタープロファイルが関連付けられている場合、デフォルトでは、関連付けられているファームウェアとドライバーリポジトリプロファイルが選択されます。そうでない場合は、[Dell デフォルトカタログ] が選択されます。

ファームウェアリポジトリプロファイルを変更すると、選択したリポジトリプロファイルがベースラインに関連付けられておらず、別のリポジトリを使用するとベースライン比較に影響する可能性があることを示すメッセージが表示されます。

4. 選択したファームウェアリポジトリプロファイルに基づいて、適切なバンドルを選択し、[次へ] をクリックします。64 ビットバンドルのみサポートされます。

**メモ:** OEM (ブランド解除) サーバーが異なるモデルであっても、1つのバンドルのみを選択できます。バンドルが1つまたは複数の OEM サーバーに適用されない場合でも、ファームウェアアップデートウィザードのコンポーネントページには、各 OEM サーバーまたはファームウェアコンポーネントのペアがリストされます。特定のファームウェアコンポーネントペアでファームウェアのアップデートに失敗した場合は、OEM サーバーに表示されている代替バンドルで再試行してください。

5. [ **ファームウェア コンポーネントの選択** ] ページで、アップデートの必要があるファームウェア コンポーネントを選択して [ **次へ** ] をクリックします。
- 緊急、推奨、任意、ダウングレードなどの重要度ステータスに基づくコンポーネントの数が表示されます。
- カタログ内の使用可能なバージョンよりも古いバージョンのコンポーネント、または同じレベル (最新) であるか、アップデートのスケジュールが設定されているコンポーネントは選択できません。使用可能なバージョンよりも古いバージョンのコンポーネントを選択するには、[ **ファームウェアのダウングレードを許可する** ] チェックボックスを選択します。
- フィルター オプションを使用して、特定の列名に基づいてデータをフィルタリングできます。
- すべてのページのすべてのファームウェア コンポーネントを選択するには、☑ をクリックします。
- すべてのページのすべてのファームウェア コンポーネントをクリアするには、✕ をクリックします。
6. [ **アップデートのスケジュール** ] ページで、ファームウェア アップデート ジョブ名と説明を入力します。[ **説明** ] フィールドはオプションです。
- ファームウェア アップデート ジョブ名は必須です。ファームウェアアップデートのジョブ名をパージすれば、そのジョブ名を再度使用できます。
7. [ **追加設定** ] セクションで、次の手順を実行します。
- メンテナンス モードのタイムアウト値を 60 分~1440 分の間で入力します。待ち時間が指定の時間を過ぎるとアップデート ジョブは失敗し、メンテナンス開始タスクはキャンセルされるかタイムアウトします。ただし、ホストの再起動時に、コンポーネントが自動的にアップデートされる場合があります。
- デフォルトでは、[ **電源がオフで一時停止された仮想マシンをクラスター内の他のホストに移動する** ] オプションが選択されます。このオプションを無効にすると、ホスト デバイスがオンラインになるまで VM が切断されます。
- ファームウェアのアップデート中に問題が生じた場合は、[ **ジョブ キューの削除と iDRAC のリセット** ] をクリックします。これによりアップデートプロセスが正常に完了する場合があります。これにより、ジョブの完了に必要なアップデート時間全体が増加し、iDRAC でスケジュールされている保留中のジョブまたはアクティビティがキャンセルされ、iDRAC がリセットされます。
- シャシ認証情報プロファイルを使用して管理されているホストでは、ジョブ キューの削除はサポートされていません。
8. [ **アップデート スケジュール** ] セクションで、次のいずれかのオプションを選択します。
- ・ **今すぐアップデート**
  - ・ **アップデートのスケジュール**
9. [ **サマリーのレビュー** ] ページで情報を確認し、[ **終了** ] をクリックします。
- ファームウェア アップデート ジョブには、選択したコンポーネントとサーバーの数に応じて、最大で数時間かかる場合があります。ジョブのステータスは、[ **ジョブ** ] ページに表示できます。
- ファームウェア アップデート タスクが完了すると、選択したホストで自動的にインベントリーが実行され、[ **アップデートのスケジュール** ] ページで選択したオプションに基づいて自動的にメンテナンス モードが終了します。

## 同じファームウェア コンポーネント タイプのアップデート

同じタイプのファームウェア コンポーネントをアップデートする際に覚えておくべき重要なポイントは次のとおりです。

- ・ 同じバージョンの同じタイプの複数のコンポーネントがサーバーに存在する場合、[ **ファームウェア コンポーネントの選択** ] ページにはコンポーネントの1つのバージョンのみが表示されます。アップデートがすべてのコンポーネントに適用され、ドリフトの詳細はコンポーネントの1つのバージョンに対してのみ表示されます。

例：

**表 19. サーバーに同じタイプの複数のコンポーネントが存在する場合の例**

コンポーネント	現在のバージョン	使用可能なバージョン
HDD1	V1	V3
HDD2	V1	V3
HDD3	V1	V3

この場合、[ **ファームウェア コンポーネントの選択** ] ページには次の情報が表示されます。

**表 20. 同じバージョンの複数のコンポーネントがサーバーに存在する場合の例**

コンポーネント	現在のバージョン	使用可能なバージョン
HDD1	V1	V3

- バージョンが異なる同じタイプの複数のコンポーネントがサーバーに存在する場合、バージョンごとに1つのコンポーネントが表示されます。この場合、いずれかのコンポーネントを選択すると、現在のファームウェアバージョンに関係なく、すべてのコンポーネントにアップデートが適用されます。現在のファームウェアバージョンに関係なく、すべてのコンポーネントのドリフトの詳細が表示されます。

例：

**表 21. 異なるバージョンの複数のコンポーネントがサーバーに存在する場合の例**

コンポーネント	現在のバージョン	使用可能なバージョン
HDD1	V1	V3
HDD2	V2	V3
HDD3	V2	V3

この場合、[ファームウェアコンポーネントの選択] ページには次の情報が表示されます。

**表 22. 異なるバージョンの複数のコンポーネントがサーバーに存在する場合の例**

コンポーネント	現在のバージョン	使用可能なバージョン
HDD1	V1	V3
HDD2	V2	V3

- カタログに複数の使用可能なバージョンが含まれている場合は、コンポーネントタイプに使用可能なバージョンを1つだけ選択することをお勧めします。選択したファームウェアは、現在のバージョンに関係なく、すべての該当コンポーネントに適用されます。

例：

**表 23. 複数の使用可能なバージョンがカタログに存在する場合の例**

コンポーネント	現在のバージョン	使用可能なバージョン
HDD1	V1	V3
HDD2	V2	V3
HDD3	V2	V3
HDD1	V1	V4
HDD2	V2	V4
HDD3	V2	V4

この場合、[ファームウェアコンポーネントの選択] ページには次の情報が表示されます。

**表 24. 複数の使用可能なバージョンがカタログに存在する場合の例**

コンポーネント	現在のバージョン	使用可能なバージョン
HDD1	V1	V3
HDD2	V2	V3
HDD1	V1	V4
HDD2	V2	V4

## vSphere Lifecycle Manager の概要

vSphere Lifecycle Manager は vCenter サーバーで実行されるサービスです (vCenter 7.0 以降のバージョンに適用)。

vSphere Lifecycle Manager では、ESXi イメージ、ファームウェア、およびドライバーで構成されるベースラインイメージを作成することができます。vSphere Lifecycle Manager はコンプライアンスチェックを実行して、クラスター内のすべてのホストがベースラインイメージに揃うようにします。非対応のものがあ場合は、クラスターを修復するためのオプションが提供されます。

vSphere Lifecycle Manager では、OMIVV はファームウェアのアドオンプロバイダーとして機能します。vSphere Lifecycle Manager の詳細については、VMware のマニュアルを参照してください。

OMIVV とともに vSphere Lifecycle Manager を使用するには、vCenter の登録が必須です。vCenter および vSphere Lifecycle Manager の登録の詳細については、「[新しい vCenter サーバーの登録](#)」を参照してください。

vCenter 登録時に Dell EMC 管理コンソールで vSphere Lifecycle Manager (vCenter 7.0 以降に適用) を登録することができます。vCenter の登録に成功すると、Dell EMC 管理コンソールの [ **VCENTER の登録** ] ページで vSphere Lifecycle Manager の登録ステータスを変更 (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。

## Dell EMC 管理コンソールでの vSphere Lifecycle Manager ステータスの表示

以下は [ **vSphere Lifecycle Manager** ] 列に表示される可能性のある vSphere Lifecycle Manager のステータスです。

- ・ **登録** (vCenter 7.0 以降にのみ適用): vSphere Lifecycle Manager が登録されていない場合に表示されます。
- ・ **登録解除** (vCenter 7.0 以降にのみ適用): vSphere Lifecycle Manager がすでに登録されている場合に表示されます。
- ・ **NA**: 登録された vCenter がバージョン 7.0 以前の場合にのみ表示されます。vCenter が 7.0 にアップグレードされた場合、ステータスは **NA** のままになります。ステータスを反映するには、OMIVV アプライアンスを再起動します。

## 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メッセージが表示されます。

## 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 の登録解除が正常に完了したことを示すメッセージが表示されます。**DELLEMC OMIVV** は vSphere Lifecycle Manager のハードウェア サービス プロバイダーリストから削除されます。OMIVV の機能には影響がありません。

## vSphere Lifecycle Manager を使用したクラスタの管理

前提条件:

vSphere Lifecycle Manager を使用してクラスタを管理する前に、次のことを確認してください。

- ・ vSphere Lifecycle Manager が、Dell EMC 管理コンソールで有効になっている。詳細については、次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](#)
- ・ クラスタ内のホストが管理に対応している。詳細については、次を参照してください: [管理対応性](#)
- ・ 選択したクラスタのクラスタ プロファイルが作成されていて、クラスタ プロファイルが OMIVV のファームウェア リポジトリに関連付けられている。クラスタ プロファイルの詳細については、「[クラスタ プロファイルの作成](#)」を参照してください。

vSphere Lifecycle Manager のユーザー インターフェイスまたは vSphere オートメーション API を使用して、クラスタを管理することができます。OMIVV は、ユーザー インターフェイスおよび vSphere オートメーション API を使用したクラスタの管理をサポートします。

① **メモ: vSphere Lifecycle Manager 管理対象クラスターでは、システム ロックダウンやファームウェア アップデートなどの OMIVV クラスター アクションを使用できますが、ベースライン レポートに影響を与える可能性があります。**

# vSphere Lifecycle Manager のユーザー インターフェイスでの OMIVV のファームウェア アドオン プロバイダーとしての使用

vSphere Lifecycle Manager で、ファームウェア アドオン プロバイダーとして OMIVV を使用することができます。

OMIVV で作成されたクラスター プロファイルは、vSphere Lifecycle Manager で、**ファームウェアおよびドライバーのアドオン**として選択されています。クラスター プロファイルの詳細については、「[クラスター プロファイル](#)」を参照してください。

選択したクラスターのイメージを設定し、OMIVV を**ファームウェアおよびドライバーのアドオン**として関連付けるには、次のタスクを実行します。

1. vSphere Client で、[ **ホストとクラスター** ] をクリックし、イメージを使用して管理するクラスターを選択します。
2. [ **アップデート** ] ページの左ペインで、[ **ホスト** ] を展開して [ **イメージ** ] をクリックします。
3. **ファームウェアおよびドライバーのアドオン**を選択するには、**選択アイコン**をクリックします。  
[ **ファームウェアおよびドライバーのアドオンの選択** ] ページが表示されます。
4. [ **ハードウェア サポート マネージャーの選択** ] セクションで、[ **DellEMC OMIVV** ] を選択します。  
[ **DellEMC OMIVV** ] を選択すると、すべてのクラスター プロファイル (ファームウェア リポジトリに関連付けられ、選択した vCenter 内のクラスターにリンクされたもの) は [ **ファームウェアおよびドライバーのアドオンの選択** ] セクションにリストされています。

5. 選択したクラスターに適用可能なクラスター プロファイルを選択し、[ **選択** ] をクリックします。

選択したクラスターに関連付けられているクラスター プロファイルを識別するには、クラスター プロファイルの説明を参照してください。

① **メモ: OMIVV でクラスター プロファイルを作成していない場合は、空のリストが表示されます。クラスター プロファイル作成の詳細については、「[クラスター プロファイルの作成](#)」を参照してください。**

- ・ **アドオン バージョン** — クラスター プロファイルの現在のバージョンを示します。クラスター プロファイルが変更された場合、または OMIVV でバージョンが増加した場合は、vSphere Lifecycle Manager で、**最新バージョンのクラスター プロファイル**を使用していることを確認してください。

① **メモ: vSphere Lifecycle Manager に、非対応のファームウェアが表示されることがあります。ただし、非対応ファームウェアは vSphere Lifecycle Manager にはリストされません。この問題を解決するには、クラスターを修復します。クラスターの修復では vSphere Lifecycle Manager は再起動しません。**

- ・ **サポートされている ESXi バージョン** - OMIVV でサポートされている ESXi バージョン (7.0.0) を示します。

選択したクラスター プロファイルは、[ **アップデート** ] ページにファームウェアのアドオンとして表示されます。

6. [ **保存** ] をクリックします。

vSphere Lifecycle Manager は、クラスターのコンプライアンス チェックを実行します。コンプライアンス チェックの結果は vSphere Lifecycle Manager の [ **イメージのコンプライアンス** ] セクションに表示されます。

全体のコンプライアンスは、ソフトウェア コンプライアンスとファームウェア コンプライアンスで構成されています。OMIVV は、vSphere Lifecycle Manager タスクのファームウェア コンプライアンス部分を管理します。

## クラスター コンプライアンス ステータスの表示

各ホストに対して可能なファームウェア コンプライアンス ステータスは次のとおりです。

- ・ **対応** : ホストにインストールされているすべてのファームウェア コンポーネントのファームウェア バージョンが、OMIVV のクラスター プロファイルにあるファームウェア バージョンと同じ場合に表示されます。
- ・ **非対応** : ホストにインストールされている1つまたは複数のファームウェア バージョンが、OMIVV のクラスター プロファイルにあるファームウェア バージョンと同じでない場合に表示されます。
- ・ **互換性なし** : 次の場合に表示されます。
  - ・ vCenter で選択されたクラスターが、選択された**ファームウェアおよびドライバーのアドオン** (OMIVV 内のクラスター プロファイル) に関連付けられていない場合。
  - ・ 選択したクラスターの vSphere Lifecycle Manager のイメージを保存した後に、クラスター プロファイルのファームウェア リポジトリがアップデートされた場合。

- ・ **不明**: ホストが OMIVV で正常にインベントリーされていない場合に表示されます。詳細については、「[ホスト認証情報プロフィール](#)」を参照してください。

① **メモ: OMIVV と vSphere Lifecycle Manager のドリフト レポートに不整合がある場合があります。**これは、**vSphere Lifecycle Manager** が常に実況のドリフトレポートを表示し、**OMIVV** はスケジュールされた日時に基づいてドリフトレポートを表示するためです。ドリフト レポート間での不整合がある場合は、**OMIVV** の [ドリフト検出ジョブ] ページでドリフト検出ジョブをオンデマンドで実行します。

## クラスターコンプライアンスの問題の修正

1. ホストのステータスが**対応**の場合は、そのホストに対してそれ以上のアクションは必要ありません。
2. ホストのステータスが**非対応**の場合は、修復を続行します。詳細については、次を参照してください: [vSphere Lifecycle Manager でのクラスター修復](#)
3. ホストのステータスが**互換性なし**の場合は、次のようになります。
  - a) vCenter で選択したクラスターが、クラスター プロファイルに関連付けられていることを確認します。vSphere Lifecycle Manager で、**ファームウェアおよびドライバーのアドオン**と同じクラスター プロファイルを選択します。
  - b) vSphere Lifecycle Manager のイメージを編集し、アップデートされたクラスター プロファイル(ファームウェアおよびドライバーのアドオン)を再選択し、イメージを保存します。
4. ホストのステータスが**不明**の場合は、OMIVV のホスト認証情報プロフィールにそのホストが追加され、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。

## ハードウェア互換性チェック

vSphere Lifecycle Manager は、ファームウェアの修復を行う前に vSAN クラスターのハードウェア互換性チェックを実行するオプションを提供します。ハードウェア互換性チェックは、イメージにあるファームウェアとドライバーを、vSAN ハードウェア互換性リスト (HCL) に記載されているハードウェアおよび対応ドライバーと比較します。vSphere Lifecycle Manager は、ストレージコントローラー (PCIe デバイス) に対してのみハードウェア互換性チェックを実行します。サポートされているファームウェア リストを表示するには、vSphere Client で、[ **モニター** ] > [ **vSAN** ] > [ **Skyline Health** ] の順に移動します。

ハードウェアの互換性チェックを実行するには、[ **イメージのコンプライアンス** ] セクションで、[ **コンプライアンスの確認** ] をクリックします。

ハードウェア互換性チェックの実行中、OMIVV はクラスタープロフィールにあるファームウェア バージョンを返します。

ファームウェアのバージョンがハードウェア互換性リスト (HCL) に記載されているファームウェアと互換性がある場合、vSphere Lifecycle Manager はコンプライアンスステータスを**互換性あり**として表示します。コンプライアンスステータスの詳細については、VMware のマニュアルを参照してください。

ハードウェア互換性チェックの結果が、[ **ハードウェア互換性** ] ページに表示されます。

## 修復の事前チェックの実行

事前チェック操作では、クラスター内の各ホストに対してさまざまなチェックを実行し、ファームウェア修復のためのクラスターの準備状況を確認します。

事前チェックは、ホストまたはクラスターレベルで実行できるオプションのタスクです。

事前チェック操作はスキップすることができます。vSphere Lifecycle Manager は、修復時に事前チェックを実行します。

OMIVV は事前チェックの一環として、次の前提条件のチェックを実行します。

- ・ iDRAC 到達可能性
- ・ iDRAC ロック ダウン モード
- ・ 選択したクラスターのホストの、OMIVV からトリガーされたファームウェア アップデート ジョブ (存在する場合) のステータス
- ・ Collect System Inventory On Reboot (CSIOR) の有効化
- ・ ファームウェア リポジトリおよび必要なファームウェア コンポーネントへの接続

ファームウェア修復の前提条件を確認するには、[ **事前チェックの実行** ] をクリックします。

事前チェック タスクのステータスと結果が、[ **イメージのコンプライアンス** ] セクションに表示されます。

ホストの事前チェックが失敗した場合は、問題を修正して事前チェックを再実行するか、修復タスクを続行します。

## vSphere Lifecycle Manager でのクラスター修復

[ [イメージのコンプライアンス](#) ] セクションでは、クラスター内の個々のホストまたはすべてのホストを一度に修復することができます。

- ホストごとに修復タスクを実行するには、[ [イメージのコンプライアンス](#) ] セクションで、ホストの横にある縦の楕円アイコンをクリックして、[ [修復](#) ] を選択します。
- クラスター内のすべてのホストに対する修復タスクを実行するには、[ [イメージのコンプライアンス](#) ] セクションで、[ [すべて修復](#) ] をクリックします。

ファームウェアアップデートを実行する前に、iDRACのリセットを実行することをお勧めします。iDRACのリセットを実行すると、障害の可能性が低下します。

各ホストで vSphere Lifecycle Manager を使用してファームウェアアップデートを実行する前に、iDRAC を自動的にリセットするには、OMIVV の [ [iDRAC ジョブをクリアして iDRAC をリセットする](#) ] チェックボックスを有効にします。詳細については、[次を参照してください：ファームウェアアップデート設定](#)

修復タスクのステータスを確認するには、[ [アップデート](#) ] ページの [ [詳細を表示](#) ] をクリックします。

OMIVV の [ [ログ](#) ] ページに、OMIVV に関連するログを表示することができます。

## vSphere Lifecycle Manager の vSphere オートメーション API での OMIVV をファームウェアのアドオンプロバイダーとしての使用

vSphere オートメーション API を使用してクラスターを管理する前に、vSphere Lifecycle Manager のユーザーインターフェイスを使用して、次のタスクを完了していることを確認します。

- ハードウェア サポート マネージャーを DellEMC OMIVV として選択します。
- 選択したクラスターに適用可能なクラスタープロファイルを選択し、イメージを保存します。

### ファームウェアコンプライアンスのスキャン

コマンド : `POST https://{VC IP/FQDN}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=scan`

```
{
  "spec" : {
    "message": "test commit"
  }
}
```

**説明:** クラスターの希望の状態クラスター内のすべてのホストをスキャンします。この操作の結果を照会するには、`cis/tasks/{task-id}` を呼び出します。ここで、`task-id` はこの操作の応答です。

**HTTP 応答コード:** 200。すべての応答コードのリストについては、[応答コード](#) を参照してください。

**応答例:**

```
{task ID}
```

### コンプライアンスタスクのステータスを取得

コマンド : `GET https://{VC IP/FQDN}/rest/cis/tasks/{task ID}`

**説明:** タスクに関する情報を返します。

**HTTP 応答コード:** 200。すべての応答コードのリストについては、[応答コード](#) を参照してください。

**応答例:** 次の例では、ファームウェア非対応のみが含まれています。

```
"result":
[
{
"value":
```

```

[
{
"value":
{
"hardware_modules":
[
{
"value":
{
"current":
{
"version": "25.5.6.0009"
},
"details":
{
"component_class": "PCI_DEVICE",
"description": "PERC H730 Mini"
}
"notifications":
{
"info":
[
{
"id": "Different versions.",
"time": "2020-02-04T10:47:54.422Z",
"message":
{
"args": [],
"default_message": "Different versions.",
"id": "Different versions."
}
}
]
},
"status": "NON_COMPLIANT",
"target": {
"version": "25.5.5.0005"
}
"key": ""
}
],
"notifications":
{
"info":
[
{
"id": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/
FQDN>] The host is non-compliant",
"time": "2020-02-04T10:47:54.423Z",
"message":
{
"args": [],
"default_message": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/
FQDN>] The host is non-compliant",
"id": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/FQDN>] The host
is non-compliant"
}
}
]
},
"status": "NON_COMPLIANT",
"target": {
"pkg": "<cluster profile name>",
"version": "0.0.0-0"
}
"key": "com.dell.plugin.OpenManager_HWSupportManager"
}
],

```

## 修復の事前チェックの実行

コマンド: POST https://{VC IP/FQDN}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=check

説明: クラスタ内のすべてのホストに希望の状態を適用する前に、クラスタでチェックを実行します。クラスタ内のすべてのホストが、希望の状態へのアップデートが可能で適切な状態にあることを確認します。

HTTP 応答コード: 200。すべての応答コードのリストについては、[応答コード](#)を参照してください。

応答例:

```
{task-id}
```

## 修復の事前チェック タスク ステータスの取得

コマンド: GET https://{VC IP/FQDN}/rest/cis/tasks/{task ID}

説明: タスクに関する情報を返します。

HTTP 応答コード: 200。すべての応答コードのリストについては、[応答コード](#)を参照してください。

応答例:

```
{
  "value":
  {
    "parent": "",
    "cancelable": true,
    "end_time": "2020-02-12T18:03:59.391Z",
    "description":
    {
      "args": [],
      "default_message": "Task created by VMware vSphere Lifecycle Manager",
      "id": "com.vmware.vcIntegrity.lifecycle.Task.Description"
    },
    "target":
    {
      "id": "domain-c8",
      "type": "ClusterComputeResource"
    },
    "result":
    {
      "start_time": "2020-02-12T17:52:09.264Z",
      "commit": "",
      "end_time": "2020-02-12T18:03:59.386Z",
      "entity_results":
      [
        {
          "host": "host-47",
          "type": "HOST",
          "check_statuses": [],
          "status": "OK"
        },
        {
          "host": "host-41",
          "type": "HOST",
          "check_statuses": [],
          "status": "OK"
        },
        {
          "host": "host-22",
          "type": "HOST",
          "check_statuses": [],
          "status": "OK"
        },
        {
          "host": "host-16",
          "type": "HOST",
          "check_statuses": [
            {
              "check":
```

```

{
  "name":
  {
    "args": [],
    "default_message": "Host Hardware support check.",
    "id": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck.Name"
  },
  "description":
  {
    "args": [],
    "default_message": "Checks if the hardware update can be performed.",
    "id": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck.Description"
  },
  "check": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck"
},
"issues": [
{
  "args": [],
  "default_message": "[vCenter: jpvc7dot0d5-2.sped.bdcsv.lab][Cluster: R6415_vSAN_AllFlash_ESXi7.0RC+][Host: 100.100.10.154][Update PreCheck Task] System Lockdown Mode is turned On for iDRAC IP, 172.20.5.5; hence Firmware update cannot continue.",
  "id": "[vCenter: jpvc7dot0d5-2.sped.bdcsv.lab][Cluster: R6415_vSAN_AllFlash_ESXi7.0RC+][Host: 100.100.10.154][Update PreCheck Task] System Lockdown Mode is turned On for iDRAC IP, 172.20.5.5; hence Firmware update cannot continue."
}
],
"status": "ERROR"
},
"status": "ERROR"
},
{
  "host": "host-19",
  "type": "HOST",
  "check_statuses": [],
  "status": "OK"
},
{
  "host": "host-13",
  "type": "HOST",

  "check_statuses": [],
  "status": "OK"
},
}

```

## クラスタの修復

コマンド : POST https://{{VC IP/FQDN}}/api/esx/settings/clusters/{{cluster ID}}/software?vmw-task=true&action=apply

```

{
  "accept_eula" : true
}

```

**説明** : 指定したクラスタに関連付けられている希望の状態を、クラスタ内のホストに適用します。

**HTTP 応答コード** : 200。すべての応答コードのリストについては、[応答コード](#)を参照してください。

**応答例** :

```
{task-id}
```

## 点滅式インジケータライトの設定

大規模なデータセンター環境で物理サーバを見つけやすくするため、設定した期間で前面インジケータライトを点滅させるよう設定できます。

1. [点滅式サーバー LED インジケータ] ウィザードを起動するには、次のいずれかの操作を実行します。

- a) OMIVV のホーム ページで、[メニュー] を展開して [ホストとクラスター] を選択し、ホストまたはクラスターを右クリックして [サマリー] > [OMIVV ホスト情報] > [ホスト アクション] > [点滅式サーバー LED インジケーター] の順に移動します。
  - b) ホストを右クリックして、[OMIVV ホスト アクション] > [点滅式サーバー LED インジケーター] の順に移動します。
2. 右ペインで [サマリー] をクリックして、[OMIVV ホスト情報] > [ホスト アクション] > [点滅式サーバー LED インジケーター] の順に移動します。  
[点滅式サーバー LED インジケーター] ダイアログ ボックスが表示されます。
3. 次のいずれかを選択します。
- a) サーバー LED インジケーターをオンにして期間を設定するには、[オン] をクリックします。
  - b) サーバー LED インジケーターをオフにするには、[オフ] をクリックします。

## システムロックダウンモードの設定

システム ロックダウン モードは、Enterprise ライセンスを持つ iDRAC9 ベース サーバーに対してのみサポートされています。[システム ロックダウン モード] をオンにすると、ファームウェア アップデートを含むシステム設定がロックされます。システム ロックダウン モード設定は、システムが誤って変更されないようにするためのものです。管理対象のホストのシステムロックダウンモードは、OMIVV アプライアンス、または iDRAC コンソールを使用してオンまたはオフにすることができます。OMIVV バージョン 4.1以降から、サーバで iDRAC のロックダウンモードを設定および監視することができます。また、ロックダウンモードを有効にするには、iDRAC にエンタープライズライセンスが必要です。

**❗ メモ:** シャーシ認証情報プロファイルを使用して管理されるホストのシステム ロックダウン モードをユーザーが変更することはできません。

ホストまたはクラスタレベルで、ホストまたはクラスタをロック/ロック解除することでシステムロックダウンモードを設定できます。[システム ロックダウン モード] がオンの場合は、次の機能が制限されます。

- ・ すべての設定タスク (ファームウェア アップデート、OS の展開、システム イベント ログの削除、iDRAC のリセット、iDRAC トラップ送信先の設定など)。
1. システム ロックダウン モードの設定ウィザードを起動するには、次のいずれかのアクションを実行します。
    - a) OMIVV のホームページで、[メニュー] を展開し、[ホストとクラスター] を選択し、ホストまたはクラスターを右クリックして、[サマリー] > [OMIVV ホスト情報] > [ホスト アクション] > [システム ロックダウン モードの設定] と移動します。
    - b) ホストまたはクラスターを右クリックし、[OMIVV ホスト アクション] > [システム ロックダウン モードの設定] と移動します。
    - c) ホストまたはクラスターを選択し、[監視] > [OMIVV ホストまたはクラスター情報] > [ファームウェア] > [システム ロックダウン モードの設定] と移動します。
  2. クラスタレベルの場合、システム ロックダウン モードのジョブ名と説明を入力します。[説明] フィールドはオプションです。
  3. システム ロックダウン モードを有効にするには、[オンにする] をクリックします。このオプションは、システムのシステム構成 (ファームウェアおよび BIOS バージョンを含む) への変更を制限します。
  4. システム ロックダウン モードを無効にするには、[オフにする] をクリックします。このオプションは、システムのシステム構成 (ファームウェアおよび BIOS バージョンを含む) の変更を有効にします。  
第 13 世代以前の PowerEdge サーバーでシステム ロックダウン モードを設定しようとする、システム ロックダウン モードがサポートされていないことを通知するメッセージが表示されます。
  5. [OK] をクリックします。  
システム ロックダウン モードの設定用のジョブが正常に作成されました。ジョブのステータスを確認するには、[ジョブ] > [システム ロックダウン モード] と移動します。システム ロックダウン モード ジョブの管理の詳細については、「[システムロックダウンモードジョブ](#)」を参照してください。

## セキュリティの役割および許可

OpenManage Integration for VMware vCenter は、ユーザー資格情報を暗号化された形式で保存します。不正な要求を避けるため、クライアントアプリケーションにはパスワードを一切提供しません。バックアップデータベースは、カスタムセキュリティフレーズで完全に暗号化されるため、データが誤使用されることはありません。

デフォルトでは、管理者グループのユーザーはすべての権限を持っています。管理者は、VMware vSphere Web Client 内の OpenManage Integration for VMware vCenter のすべての機能を使用できます。製品を管理するのに必要な権限をユーザーに与えるには、次の手順を実行します。

1. 必要な権限を持つ役割を作成します。
2. ユーザーを使用して vCenter サーバを登録します。
3. Dell 役割、Dell Operational Role および Dell インフラストラクチャ導入役割の両方を含めます。

### データ整合性

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

セキュアな管理コンソールセッションには 5 分間のアイドルタイムアウトがあり、セッションは現在のブラウザウィンドウまたはタブでのみ有効です。新しいウィンドウまたはタブでセッションを開こうとすると、有効なセッションを要求するセキュリティエラーが表示されます。また、このアクションは、管理コンソールセッションを攻撃する可能性がある悪意のある URL をクリックすることも防止できます。

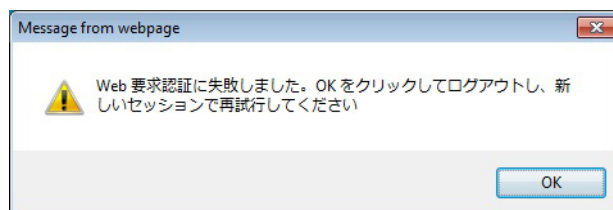


図 1. セキュリティエラーメッセージ

### アクセス制御認証、承諾、および役割

OpenManage Integration for VMware vCenter は、vCenter を操作するために、Web クライアントの現在のユーザーセッションと、OpenManage Integration の保存された管理認証情報を使用します。OpenManage Integration for VMware vCenter は、vCenter サーバ内で設定された役割と権限モデルに基づいて、OpenManage Integration と vCenter 管理オブジェクト (ホストとクラスター) に対するユーザーアクションを承認します。

### Dell 操作役割

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

この役割には次の特権グループが含まれます。

表 25. 権限グループ

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

## Dell インフラストラクチャ導入役割

この役割には、ハイパーバイザー導入機能に関連した権限が含まれます。

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

### 特権グループ — Dell.Deploy-Provisioning

テンプレートの作成、HW 設定プロファイルの設定、ハイパーバイザー導入プロファイルの設定、接続プロファイルの設定、ID の割り当て、導入。

## 特権について

OpenManage Integration for VMware vCenter によって実行されるすべてのアクションは、権限に関連付けられています。次のセクションでは、実行可能なアクションと、それに関連付けられている権限をリストします。

- Dell.Configuration.Perform vCenter-related tasks
  - メンテナンスモードを終了および実行
  - 許可をクエリするために vCenter ユーザーグループを取得
  - 警告を登録および設定。たとえば、イベント設定ページでのアラートの有効化 / 無効化
  - vCenter にイベント / アラートを掲示
  - イベント設定ページでイベント設定を実行
  - イベント設定ページでデフォルトのアラートを復元
  - アラート / イベント設定を実行しながら、クラスタの DRS ステータスをチェック
  - アップデートまたはその他の設定処置を実行した後にホストを再起動
  - vCenter タスクのステータス / 進捗状態を監視
  - vCenter タスクを作成。たとえば、ファームウェアアップデートタスク、ホスト設定タスク、およびインベントリタスク
  - vCenter タスクのステータス / 進捗状態をアップデート
  - ホストプロファイルを取得
  - データセンターにホストを追加
  - クラスタにホストを追加
  - ホストにプロファイルを適用
  - CIM 資格情報を取得
  - コンプライアンスのためにホストを設定
  - コンプライアンスタスクのステータスを取得
- Dell.Inventory.Configure ReadOnly
  - 接続プロファイルの設定中に、すべての vCenter ホストを取得して vCenter ツリーを構築
  - タブが選択されているときにホストが Dell サーバかどうかをチェック
  - vCenter のアドレス / IP を取得
  - ホストの IP / アドレスを取得
  - vSphere クライアントセッション ID に基づいて現在の vCenter セッションユーザーを取得
  - vCenter インベントリツリーを取得して、vCenter インベントリをツリー構造で表示
- Dell.Monitoring.Monitor
  - イベントを掲示するためのホスト名を取得
  - イベントログ操作を実行。たとえば、イベント数の取得、またはイベントログ設定の変更

- ・ イベント/アラートを登録、登録解除、および設定 — SNMP トラップの受信とイベントの受信
- ・ Dell.Configuration.Firmware Update
  - ・ ファームウェアアップデートを実行
  - ・ ファームウェアアップデートウィザードページにファームウェアリポジトリと DUP ファイル情報をロード
  - ・ ファームウェアインベントリをクエリ
  - ・ ファームウェアリポジトリ設定を実行
  - ・ ステージング機能を使用してステージングフォルダを設定およびアップデートを実行
  - ・ ネットワークとリポジトリ接続をテスト
- ・ Dell.Deploy-Provisioning.Create Template
  - ・ HW 設定プロファイルの設定
  - ・ ハイパーバイザ展開プロファイルの設定
  - ・ 接続プロファイルの設定
  - ・ ID の割り当て
  - ・ 導入
- ・ Dell.Configuration.Perform host-related tasks
  - ・ Dell サーバの 管理 タブから LED を点滅、LED をクリア、OMSA URL を設定
  - ・ OMSA コンソールを起動
  - ・ iDRAC コンソールを起動
  - ・ SEL ログを表示およびクリア
- ・ Dell.Inventory.Configure Inventory
  - ・ Dell サーバの 管理 タブでシステムインベントリを表示
  - ・ ストレージ詳細を取得
  - ・ 電源監視詳細を取得
  - ・ 接続プロファイルページで接続プロファイルを作成、表示、編集、削除、およびテスト
  - ・ インベントリスケジュールを計画、アップデート、および削除
  - ・ ホストでインベントリを実行

## よくあるお問い合わせ (FAQ)

本項では、トラブルシューティングの質問に対する回答を記載します。本項には、次の項目が記載されています。

- ・ よくあるお問い合わせ (FAQ)
- ・ ベアメタル展開の問題

### よくあるお問い合わせ (FAQ)

本項には、一般的な質問と解決策が記載されています。

### 非対応 vSphere ホストの場合、iDRAC のライセンスタイプと説明が正しく表示されない

ホストが非対応であり、なおかつ、CSIOR が無効になっている場合、または実行されていない場合、有効な iDRAC ライセンスが使用可能であっても、iDRAC ライセンス情報が正しく表示されません。この場合、vSphere ホストリストにはホストが表示されますが、ホストをクリックして詳細を表示しようとする、[ **iDRAC ライセンスタイプ** ] には何も表示されず、[ **iDRAC ライセンス説明** ] には「ライセンスをアップグレードする必要があります」と表示されます。

解決方法：この問題を解決するには、参照サーバーで CSIOR を有効にします。

影響を受けるバージョン：4.0 以降

### Dell プロバイダーが正常性アップデート プロバイダーとして表示されない

OMIVV で vCenter サーバーを登録し、vCenter サーバーのバージョンをアップグレードした場合 (vCenter 6.0 から vCenter 6.5 へのアップグレードなど)、Dell プロバイダーは **Proactive HA プロバイダー** リストに表示されません。

解決方法：非管理者ユーザーまたは管理者ユーザー向けに登録された vCenter をアップグレードできます。vCenter サーバーの最新バージョンにアップグレードするには、VMware のマニュアルを参照したうえで、次のいずれかの手順を必要に応じて実行します。

- ・ 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。
  2. 登録済み OMIVV アプライアンスを再起動します。
  3. Web クライアントからログアウトし、再度ログインします。
- ・ 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. Web クライアントからログアウトし、再度ログインします。

これで、Dell プロバイダーが **Proactive HA プロバイダー** リストに表示されます。

影響を受けるバージョン：4.0 以降

### 無効または不明な iDRAC IP が原因でホストインベントリまたはテスト接続が失敗します。

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

1. iDRAC 仮想コンソールを開きます。

2. F2 を押して、[トラブルシューティング オプション] に移動します。
3. [トラブルシューティング オプション] で、[管理エージェントの再起動] に移動します。
4. F11 を押して、管理エージェントを再起動します。

これで、有効な iDRAC IP が使用できるようになります。

**①** **メモ:** OMIVV が ESXi 6.5 を実行しているホストで WBEM サービスの有効化に失敗した場合、ホストインベントリも失敗します。WBEM サービスの詳細については、「[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。

## 非準拠 vSphere ホストを修正 ウィザードを実行しているときに、特定のホストのステータスが不明と表示されます

非準拠ホストを修正するために、非準拠 vSphere ホスト修正ウィザードを実行すると、特定のホストのステータスが [不明] と表示されます。不明ステータスは、iDRAC にアクセスできないときに表示されます。

解決方法：ホストの iDRAC 接続を確認し、インベントリが正常に実行されていることを確認します。

対象バージョン：4.0

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

OMIVV アプライアンスで vCenter を登録すると、複数のデル権限が vCenter 権限リストに追加されます。OMIVV アプライアンスから vCenter を登録解除しても、デル権限は削除されません。

**①** **メモ:** デルの権限は削除されませんが、OMIVV の操作への影響はありません。

影響を受けるバージョン：3.1以降

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

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

解決方法：例外を解決するには、各種サービスの ssl アンカーをアップデートする必要があります。ssl アンカーは、PSC で `ls_update_certs.py` スクリプトを実行してアップデートできます。このスクリプトは、古い証明書のサムプリントを入力引数として使用し、新しい証明書をインストールします。古い証明書は、置き換え前の証明書であり、新しい証明書は、置き換え後の証明書となります。詳細については、「[https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT\\_KB\\_1\\_1&externalId=2121701](https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701)」および「[https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT\\_KB\\_1\\_1&externalId=2121689](https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689)」を参照してください。

影響を受けるバージョン：3.0以降、vCenter 6.0以降

## vCenter の Windows インストールでの証明書の置き換え

詳細については、<https://kb.vmware.com/s/article/2121689> を参照してください。

## vCenter サーバアプライアンスでの証明書の置き換え

詳細については、<https://kb.vmware.com/s/article/2121689> を参照してください。

## 管理対象オブジェクトブラウザ (MOB) から古い証明書を取得する

詳細については、<https://kb.vmware.com/s/article/2121701> を参照してください。

## 古い証明書からのサムプリントの抽出

詳細については、<https://kb.vmware.com/s/article/2121701> を参照してください。

## 管理コンソールで、アプライアンスを工場出荷時設定にリセットした後、リポジトリパスのアップデートがデフォルトに設定されない

アプライアンスをリセットした後、管理コンソールに移動し、左側のペインの **アプライアンスの管理** をクリックします。アプライアンスの設定 ページの **リポジトリパスのアップデート** が、デフォルトパスに変更されていません。

解決方法 : [ **管理コンソール** ] で、[ **デフォルトのアップデート リポジトリ** ] フィールドにあるパスを [ **リポジトリパスのアップデート** ] フィールドに手動でコピーします。

## OMIVV で DNS 設定を変更した後、vCenter HTML-5 クライアントで Web 通信エラーが発生したらどうすればよいですか

DNS 設定を変更した後、OMIVV 関連タスクの実行中に vCenter HTML-5 クライアントで何らかの Web 通信エラーが表示された場合は、次のいずれかの手順を実行します。

- ・ ブラウザのキャッシュをクリアします。
- ・ ログアウトして Web クライアントからログインします。

## ファームウェア ページで一部のファームウェアのインストール日が 12-31-1969 と表示される

Web クライアントでは、ホストのファームウェア ページのファームウェア項目に、インストールの日付が 12/31/1969 と表示されることがあります。ファームウェアのインストール日を利用できない場合、古い日付が表示されます。

対応処置 : ファームウェアコンポーネントの一部にこの古い日付が表示される場合は、そのコンポーネントのインストール日が使用不可であると考えてください。

影響を受けるバージョン : 2.2 以降

## vCenter にプラグインを登録できても、HTML-5 クライアントに OpenManage Integration アイコンが表示されない

OpenManage Integration アイコンは、vSphere クライアント サービスが再起動されない限り vSphere クライアントに表示されません。VMware vCenter アプライアンスの OpenManage Integration を登録すると、アプライアンスは vSphere クライアントに登録されます。アプライアンスを登録解除した後、そのアプライアンスの同じバージョンを再登録するか、または新しいバージョンを登録すると、正常に登録されますが、OMIVV アイコンが vSphere クライアントに表示されない場合があります。これは、VMware のキャッシュ問題によるものです。この問題を解決するには、vCenter サーバーで vSphere クライアント サービスを再起動する必要があります。次に、UI にプラグインが表示されます。

解決方法 : vCenter サーバーで vSphere クライアント サービスを再起動します。

影響を受けるバージョン : 2.2 以降

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

静的に割り当てた DNS 設定が DHCP の値に置き換えられるという不具合が確認されています。DNS 値を静的に割り当てた状態で、IP 設定の取得に DHCP を使用すると、この不具合が発生する可能性があります。DHCP のリースが更新されると、またはアプライアンスが再起動されると、静的に割り当てた DNS 設定は削除されます。

解決方法 : DNS サーバー設定が DHCP と異なるときに、IP 設定を静的に割り当てます。

対象バージョン：すべて

## ファームウェア アップデートを実行すると、「ファームウェア リポジトリ ファイルが存在しないか、無効になっています」というエラー メッセージが表示される場合がある

ファームウェア アップデート ウィザードの実行中に、「ファームウェア リポジトリ ファイルが存在しないか、無効になっています」というエラー メッセージがクラスター レベルで表示される場合があります。この場合、日常のバックグラウンド プロセスが、カタログ ファイルをリポジトリ からダウンロードしてキャッシュできなかったことが原因と考えられます。この問題は、バックグラウンド プロセスの実行時にカタログ ファイルにアクセスできない場合に発生します。

解決方法：考えられるカタログ接続の問題をすべて解決した後、ファームウェア リポジトリの場所を変更し、元の場所に戻すことで、バックグラウンド プロセスを再開できます。バックグラウンド プロセスが完了するまでに、約5分かかることがあります。CIFS 用に提供される認証情報に文字@が含まれていないことを確認します。また DUP ファイルが共有の場所に存在することを確認します。

対象バージョン：すべて

## OMIVV を使用しての、ファームウェアバージョン 13.5.2 の Intel ネットワークカードのアップデートはサポートされていない

Dell EMC PowerEdge サーバーとファームウェア バージョン 13.5.2 の一部の Intel ネットワーク カードに既知の問題があります。iDRAC with Lifecycle Controller を使用してファームウェアのアップデートを行うと、ファームウェアのバージョンが 13.5.2 の Intel ネットワーク カードの複数のモデルでアップデートが失敗します。ファームウェアのバージョンが 13.5.2 の場合は、オペレーティング システムを使用してネットワークドライバソフトウェアをアップデートしてください。Intel ネットワークカードのファームウェアのバージョンが 13.5.2 以外の場合は、OMIVV で更新できます。詳細については、<http://en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx> を参照してください。

**①** **メモ:** 1対多のファームウェア アップデートを行う場合は、バージョン 13.5.2 の Intel ネットワーク アダプターを選択しないでください。アップデートが失敗し、アップデート中の残りのサーバーのアップデート タスクが停止します。

## OMIVV を使用して Intel ネットワークカードを 14.5 または 15.0 から 16.x にアップデートすると、DUP からのステージング要件によってアップデートが失敗する

これは、NIC 14.5 と 15.0 の既知の問題です。ファームウェアを 16.x にアップデートする前に、カスタムカタログを使用してファームウェアを 15.5.0 にアップデートしていることを確認してください。

対象バージョン：すべて

## 管理ポータルに、アップデートリポジトリの場所に到達できないと表示される理由

到達不能なアップデート リポジトリ パスを指定すると、アプライアンスのアップデート ビューの上部に「失敗：URL に接続中にエラーが発生しました」というエラー メッセージが表示されます。ただし、アップデートリポジトリパスは、アップデート前の値にクリアされません。

解決方法：別のページに移動して、ページが更新されていることを確認します。

対象バージョン：すべて

# 1対多のファームウェアアップデートを実行したときに、システムがメンテナンスモードに移行しない理由

一部のファームウェアアップデートでは、ホストを再起動する必要がありません。この場合、ホストをメンテナンスモードにせずに、ファームウェアアップデートが実行されます。

## 一部の電源装置のステータスが重要に変更されても、シャーシのグローバル正常性は正常のままになっている

電源装置に関するシャーシのグローバル正常性は、冗長性ポリシーと、オンラインで引き続き動作する PSU によってシャーシの電源要件が満たされるかどうかによって判断されます。PSU の一部の電源が切れている場合でも、シャーシ全体の電源要件は満たされていることとなります。このため、シャーシのグローバル正常性は正常となります。電源装置と電源管理の詳細については、Dell EMC PowerEdge M1000e シャーシ管理コントローラー ファームウェア文書のユーザーズ ガイドを参照してください。

## システム概要ページのプロセッサビューで、プロセッサのバージョンが「該当なし」と表示されます

12G 以降のサーバーでは、プロセッサのバージョンは [ ブランド ] 列に表示されます。それより前の世代では、プロセッサのバージョンは [ バージョン ] 列に表示されます。

## OMIVV は、リンクモードで vCenter をサポートしますか

はい。OMIVV はリンクモードの有効無効にかかわらず、最大 10 台の vCenter サーバをサポートします。

## OMIVV ではどのようなポート設定が必要ですか。

OMIVV では、次のポート設定を使用します。

表 26. 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)	管理対象ノードからの SNMP トラップ受信。
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。

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	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	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	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。
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 27. 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	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。

**① メモ:** iDRAC9 ベースのサーバーでは、iDRAC は NFS を TCP でポート 2049 にマウントします。iDRAC9 ベースサーバーのリストについては、「互換性マトリックス」を参照してください。

## 認証情報が新たに変更されたユーザーを含むシステム プロファイルを iDRAC ユーザー リストに正常に適用した後、ベアメタル検出に使用する同じユーザーのパスワードが変更されない

展開のためにシステム プロファイル (ハードウェアの設定) のみを選択した場合、検出に使用されたユーザーのパスワードは新しい認証情報に変更されません。これは、将来の展開ニーズで、プラグインが iDRAC と通信できるようにするために、意図的に行われています。

## vCenter ホストおよびクラスタページにリストされる新しい iDRAC バージョンの詳細を表示できません

解決方法 : vSphere Web Client でファームウェアアップデートタスクが正常に完了した後、ファームウェアアップデート ページを更新して、ファームウェアのバージョンを確認します。ページに古いバージョンが表示されている場合、OpenManage Integration for VMware vCenter の **ホスト対応性** ページに移動し、そのホストの CSIOR のステータスを確認します。CSIOR が有効になっていない場合、CSIOR を有効にしてホストを再起動します。CSIOR が有効になっている場合、iDRAC コンソールにログインして iDRAC をリセットし、数分待ってから ファームウェアアップデート ページを更新します。

## ロックダウンモードを有効にした状態で、OMIVV で ESXi をサポートすることができますか

はい。本リリースでは、ESXi 6.0 以降のホストでロックダウン モードがサポートされています。

## ロックダウン モードを使用しようとすると失敗する

ロックダウン モードでホスト認証情報プロファイルにホストを追加したとき、インベントリが開始されましたが、「Remote Access Controller が見つからなかったか、インベントリがこのホスト上でサポートされていません」と表示されて失敗しました。

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

## サーバで ESXi の導入が失敗する

1. ISO の場所 ( NFS パス ) とステージングフォルダパスが正しいことを確認します。
2. サーバー ID の割り当て時に選択された **NIC** に、仮想アプライアンスがアクセスできることを確認します。
3. OMIVV へのネットワーク接続に基づいて、管理 NIC を選択するようにしてください。
4. **静的 IP アドレス** を使用している場合は、設定されているネットワーク情報 ( サブネットマスクとデフォルトゲートウェイを含む ) が正確であることを確認します。また、IP アドレスがまだネットワーク上で割り当てられていないことも確認します。
5. 1 つ以上の仮想ディスク、iSDM、または BOSS がシステムで認識されていることを確認します。

## 自動検出されたシステムで、導入ウィザードでモデル情報が表示されない

これは通常、システムにインストールされているファームウェアのバージョンが推奨最小要件を満たしていないことを意味します。また、ファームウェアアップデートがシステムに登録されていない可能性もあります。

解決方法 : システムをコールドブートするか、ブレードを取り付け直してこの問題を解決します。iDRAC の新しく有効になったアカウントを無効にして、自動検出を再起動し、モデル情報と NIC 情報を OMIVV に提供する必要があります。

## ESXi ISO で NFS 共有がセットアップされているが、共有の場所をマウントするときのエラーで失敗する

解決法を見つけるには、次の手順を行います。

1. iDRAC がアプライアンスに対して ping を実行できることを確認します。
2. ネットワークの稼働速度が遅すぎないことを確認します。
3. ポート 2049、4001~4004 が開いていること、ファイアウォールがそれに応じて設定されていることを確認します。

## vCenter から OMIVV アプライアンスを強制的に削除する方法を教えてください

1. [https://<vcenter\\_serverIPAddress>/mob](https://<vcenter_serverIPAddress>/mob) にアクセスします。
2. VMware vCenter のシステム管理者資格情報を入力します。
3. コンテンツ をクリックします。
4. **ExtensionManager** をクリックします。
5. **UnregisterExtension** をクリックします。
6. 延長キーを入力して `com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient` を登録解除し、**メソッドの呼び出し** をクリックします。
7. vSphere Client に移動し、Proactive HA を有効にしているすべてのクラスターの、Dell プロバイダーのチェック ボックスをクリアします。
8. [ホーム] > [コンテンツ] > [HealthUpdateManager] をクリックします。
9. [QueryProviderList] > [メソッドの呼び出し] をクリックします。
10. プロバイダー ID の文字列値をコピーして、ウィンドウを閉じます。
11. [UnregisterHealthUpdateProvider] をクリックし、コピーしたプロバイダー ID 文字列値を入力します。
12. [メソッドの呼び出し] をクリックします。
13. vSphere クライアントで OMIVV を無効にして削除します。登録解除用のキーは、vSphere クライアント用である必要があります。

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

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

## ファームウェアアップデートに失敗した場合は、どうすればよいでしょうか

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

## vCenter の登録に失敗した場合の対処方法

通信問題によって vCenter の登録に失敗することがあります。この問題が発生した場合は、解決策として、静的 IP アドレスを使用します。静的 IP アドレスを使用するには、OpenManage Integration for VMware vCenter の [コンソール] タブで、[ネットワークの設定] > [デバイスの編集] を順に選択し、正しい [ゲートウェイ] と [FQDN] (完全修飾ドメイン名) を入力します。DNS 設定の編集の下で、DNS サーバ名を入力します。

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

## ホスト認証情報プロファイルの認証情報テスト中、パフォーマンスが遅くなる、または応答しなくなる

サーバ上の iDRAC に存在するユーザーが1人 (たとえば *root*) のみで、そのユーザーが無効になっている場合、またはすべてのユーザーが無効な場合に、無効状態のサーバとの通信で遅延が発生します。この問題を解決するには、サーバの無効状態を解決するか、サーバの iDRAC をリセットして、*root* ユーザーをデフォルト設定で再び有効化します。

無効状態のサーバを修正するには、次の手順を行います。

1. Chassis Management Controller コンソールを開いて、無効状態のサーバを選択します。
2. iDRAC コンソールを自動的に開くには、**iDRAC GUI の起動** をクリックします。
3. iDRAC コンソールでユーザーリストまで移動して、次のいずれかをクリックします。

- ・ iDRAC 7 : **iDRAC 設定** > **ユーザー** タブを選択します。
- ・ iDRAC 8 : **iDRAC 設定** > **ユーザー** タブを選択します。
- ・ iDRAC9 : [ **iDRAC 設定** ] > [ **ユーザー** ] タブを選択します。

iDRAC 7 および 8 の場合 :

- a. 設定を編集するには、ユーザー ID 列で、管理者 (*root*) ユーザーのリンクをクリックします。
- b. **ユーザーの設定** をクリックして、**次へ** をクリックします。
- c. 選択したユーザーの **ユーザー設定** ページで、ユーザーの有効化の横にあるチェックボックスを選択し、**適用** をクリックします。

iDRAC9 の場合 :

- a. **root** ユーザーを選択し、[ **有効化** ] をクリックします。

## OMIVV は VMware vCenter Server アプライアンスをサポートしていますか

はい。OMIVV は、v2.1 以降の VMware vCenter Server アプライアンスをサポートしています。

## サーバーが CSIOR ステータス「不明」で、「非対応」と表示される場合がある

解決方法 : 不明な CSIOR 状態は、ホスト上の iDRAC が応答していないことを示しています。この問題は、ホストで iDRAC を手動でリセットすると解決します。

対象バージョン : すべて

## 次回の再起動時にファームアップデートを適用するオプションでファームウェアアップデートを行ってシステムを再起動したにも関わらず、ファームウェアのレベルがアップデートされません

ファームウェアをアップデートするには、再起動後にホストのインベントリを実行します。再起動イベントがアプライアンスに到達しない場合、インベントリは自動的に実行されません。このような場合、インベントリを手動で再実行して最新のファームウェアのバージョンを取得する必要があります。

## vCenter ツリーからホストを削除した後も、引き続きシャーシにそのホストが表示されます

シャーシの下のホストは、シャーシインベントリの一部として識別されます。シャーシインベントリが正常に終了すると、シャーシの下のホストリストが更新されます。ホストが vCenter ツリーから削除されても、次のシャーシ インベントリが実行されるまで、ホストがシャーシの下に表示されます。

## OMIVV のバックアップと復元の後、アラーム設定が復元されない

OMIVV アプライアンスのバックアップを復元しても、すべてのアラーム設定は復元されません。ただし、OpenManage Integration for VMware GUI のアラームとイベントフィールドに、復元された設定が表示されます。

対応処置：OMIVV GUI の [ 設定 ] タブで、[ イベントおよびアラーム ] 設定を手動で変更します。

## NPAR がターゲット ノード上で有効で、システム プロファイルで無効の場合、OS の導入が失敗する


ターゲット マシンで NIC パーティション (NPAR) が無効にされているシステム プロファイルを適用したとき、OS の導入が失敗します。ここでは、NPAR はターゲットノードで有効にされており、導入ウィザードにより、導入プロセス中、パーティション 1 を除いて、1つのパーティション分割された NIC のみが管理タスク用の NIC のとして選択されています。

解決方法：導入時にシステム プロファイルを使用して NPAR のステータスを変更する場合は、導入ウィザードで管理ネットワークの最初のパーティションのみを選択するようにします。

影響を受けるバージョン：4.1以降

## 使用可能な OMIVV アプライアンスのバージョンが現在のバージョンよりも古い場合、誤った情報が表示される

OMIVV 管理コンソールで、[ アプライアンスの管理 ]、[ 使用可能な仮想アプライアンスのバージョン ] の下に使用可能なモードとして RPM および OVF が表示されます。

 **メモ:** アップデートリポジトリのパスを最新バージョンに設定することをお勧めします。また、仮想アプライアンスのバージョンのダウングレードはサポートされていません。

## 第 12 世代以降のベアメタル サーバーを追加しようとするとき 267027 例外がスローされる

ベアメタル検出中に、不正な資格情報が入力された場合、ユーザーアカウントが自動的に数分間ロックされます。この間、iDRAC が反応しなくなり数分経過すると、正常に復元されます。

解決方法：数分間待ってから、ユーザー資格情報を再入力します。

## 導入時に、システム プロファイルの適用が iDRAC エラーにより失敗する

導入時に、OMIVV は iDRAC 内で設定アップデート ジョブを作成しようとします。ただし、ジョブの作成は失敗することがあり、設定ジョブがすでに作成されているというメッセージが表示されます。

解決方法：古いエントリをクリアして、導入をもう一度試行します。iDRAC にログインしてジョブをクリアします。

## プロキシがドメインユーザー認証で設定されている場合、OMIVV RPM のアップグレードが失敗する

OMIVV アプライアンスでプロキシを設定してインターネットに接続している場合で、NTLM 認証を使用してプロキシを認証している場合は、根本的な yum ツールの問題により、RPM のアップデートが失敗します。

影響を受けるバージョン：OMIVV 4.0 以降

解決方法 / 回避策：OMIVV アプライアンスをアップデートするには、バックアップと復元を実行します。

## FX シャーシに PCIe カードを搭載しているシステムプロファイルが適用できません

FX シャーシを使用する際、ソースサーバに PCIe カード情報があると、ターゲットサーバで OS 導入が失敗します。ソース サーバー上のシステム プロファイルには、ターゲット サーバーとは異なる `fc.chassislot` ID があります。OMIVV はターゲット サーバーに同じ `fc.chassislot` ID を導入しようとして失敗します。プロファイルの適用中に、システムプロファイルが正確なインスタンス (FQDD) を検索します。このプロファイルは、同一のラックサーバでは正常に動作しますが、モジュラーサーバでは若干の制限があります。たとえば、FC640 では、1つのモジュラーサーバから作成されたシステム プロファイルは、NIC レベルの制限によって、同じ FX シャーシ内の他のモジュラー サーバー上に適用できません。

影響を受けるバージョン：4.1 以降

解決方法：FX2s シャーシのスロット 1 の FC640 サーバーから取得されたシステム プロファイルは、他の FX2s シャーシのスロット 1 の別の FC640 サーバーにのみ適用できます。

## ドリフト検出で FX シャーシに PCIe カードを備えるモジュラーサーバが非対応と表示される

ベースラインの比較中に、システムプロファイルが正確なインスタンス (FQDD) を検索します。このプロファイルは、同一のラックサーバでは正常に動作しますが、モジュラーサーバでは若干の制限がある場合があります。たとえば、FC640 では、1つのモジュラーサーバから作成されたシステムプロファイル (ベースライン) は、FQDD 不一致のため、同じ FX シャーシ内の他のモジュラーサーバのドリフトを表示します。

影響を受けるバージョン：4.1 以降

解決方法：システムプロファイルの作成中に、他のサーバと共通しない FQDD をクリアします。

## 選択した NIC の MAC アドレスを iDRAC が入力しない場合に、PowerEdge サーバ上に OS を導入できない

選択した NIC ポートに MAC アドレスを iDRAC が入力しないと、PowerEdge 上に OS を導入することはできません。

解決方法：それぞれの NIC ファームウェアと iDRAC ファームウェアを最新バージョンにアップデートし、MAC アドレスが NIC ポートに入力されていることを確認します。

影響を受けるバージョン：4.3 以降

## ESXi 6.5U1 を持つホストのホスト認証情報プロファイルの作成時に、ホストのサービス タグが選択したホストのページに表示されない

OMIVV が vCenter に ESXi のサービス タグを問い合わせたとき、サービス タグ値が null であると vCenter はサービス タグを返すことができません。

解決方法：ESXi のバージョンを ESXi 6.5U2 もしくは ESXi 6.7 U1 にアップデートします。

影響を受けるバージョン：4.3 以降

## 以前の OMIVV バージョンから最新の OMIVV バージョンにバックアップして復元した後に Dell EMC アイコンが表示されない

以前の OMIVV バージョンから最新の OMIVV バージョンにバックアップして復元した後、次の問題が発生します。

- ・ Dell EMC ロゴが vCenter に表示されません。
- ・ 2000000 エラー
- ・ 3001 エラー

解決策：

- ・ vCenter サーバで vSphere Web Client を再起動します。
- ・ 問題が解決しない場合は、
  - ・ VMware vCenter Server アプライアンスの場合、`/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity` にアクセスします。Windows vCenter の場合、vCenter アプライアンスの `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` フォルダに進み、次のような古いデータが存在するか確認します：`com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX`。
  - ・ 古いバージョンの OMIVV に対応するフォルダを手動で削除します。

## OMIVV を使用して iDRAC ファームウェア バージョンをアップグレードまたはダウングレードすると、ファームウェア アップデートが成功していても、OMIVV ではジョブが失敗したと示される場合がある

ファームウェアのアップデート中に、バージョン 3.20.20.20、3.21.21.21、3.21.21.22 などの iDRAC をダウングレードまたはアップグレードすると、ジョブが正常に実行された場合でもジョブのステータスに失敗と表示されます。

解決方法：ジョブが失敗した後、インベントリを更新して、他のコンポーネントのジョブを再実行します。

対象バージョン：4.3

## クラスタレベルでシステムロックダウンモードを設定すると、「クラスタの下にあるホストに正常なインベントリが含まれていません」というメッセージが時々表示される

クラスタレベルでシステム ロックダウン モードを設定すると、「クラスタの下にあるホストに正常なインベントリが含まれていません」というメッセージが表示されることがあります。OMIVV で管理している iDRAC9 ベース サーバーに関して、クラスタが正常にインベントリを実行した場合でも、このメッセージは表示されます。iDRAC9 ベース サーバーのリストについては、「互換性マトリックス」を参照してください。

解決策：vCenter を再起動します。

vCenter を再起動するには、次の手順を実行します。

1. vCenter のシングルサインオン管理者アカウントを使用して、vSphere Web Client にログインします。
2. 管理 > 導入 > 導入 > システム構成 の順に移動します。
3. [ ノード ] をクリックして、vCenter Server Appliance ノードを選択し、[ 関連オブジェクト ] タブをクリックします。
4. vCenter ノードを再起動します。

## OMIVV アプライアンスの RPM アップグレード後、ログの複数のエントリが vCenter の最新タスクに表示される場合がある

RPM アップグレード後に、vCenter の最新タスクに表示すると、ログに複数のエントリが表示される場合があります。

解決策：vCenter サービスを再起動します。

対象バージョン：4.3

## vCenter の登録後、OMIVV の Dell EMC ロゴが VMware のホームページに表示されない

説明：VMware vCenter は登録完了後すぐにプラグインの検証を行うため、VMware のホームページに OMIVV の Dell EMC ロゴが表示されない場合があります。

対応処置：以下の手順を実行します。

1. ブラウザーの情報を最新にするか、ブラウザー キャッシュをクリアします。または、vSphere クライアントのクライアント サービスを再起動します (HTML-5)。
2. vSphere Web クライアントからログアウトし、再度ログインします。

影響を受けるバージョン：5.0

## バックアップおよび復元後、非対応の第 11 世代 PowerEdge サーバーが OMIVV インベントリーに保持される

OMIVV でバックアップおよび復元操作を実行した後も、非対応でインベントリーされていない第 11 世代ホストはホスト認証情報プロファイルに関連付けられたままになります。ただし、設定コンプライアンスを修正して新しいインベントリーを実行しようとすると、サポートされていない第 11 世代サーバーでジョブが失敗します。

解決方法：OMIVV 5.0 では、第 11 世代サーバーはサポートされません。サポートされていない第 11 世代ホストをホスト認証情報プロファイルから手動で削除します。

影響を受けるバージョン：5.0

## OMIVV アプライアンスをアップグレードした後、Flex クライアントから vCenter を起動できない

対応処置：解決方法については、VMware KB の記事 <https://kb.vmware.com/s/article/54751> を参照してください。

影響を受けるバージョン：5.0

## OMIVV にネットワーク アダプターを追加または削除するときに、既存の NIC が OMIVV コンソールから消える

vSphere Web クライアントを使用して OMIVV アプライアンスにネットワーク アダプターを追加または削除するときに、既存の NIC が OMIVV コンソールから消えることがあります。

回避策：次のいずれかのタスクを実行します。

1.
  - a. ターミナル コンソール ユーティリティーからすべてのネットワーク アダプターを削除します。
  - b. アプライアンスをシャットダウンします。
  - c. アプライアンスからネットワーク アダプターを削除します。
  - d. OMIVV アプライアンスを再起動します。
  - e. アプライアンスをシャットダウンします。

- f. 必要なネットワーク アダプターを追加し、ネットワーク アダプターの設定を完了します。
  - g. アプライアンスを再起動します。
2. a. 管理者ポータルから OMIVV をバックアップします。
  - b. OMIVV アプライアンスを作成します。
  - c. アプライアンスをシャットダウンします。
  - d. 必要なネットワーク アダプターを追加し、ネットワーク アダプターの設定を完了します。
  - e. アプライアンスを再起動します。
  - f. 最新のバックアップ データを復元します。

影響を受けるバージョン : OMIVV 5.0

## 2 番目の NIC を追加または削除した後、[ ネットワーク設定 ] ページに 3 つの NIC が表示される

vSphere Client を使用して OMIVV アプライアンスに NIC を追加または削除した後、OMIVV アプライアンスを起動して OMIVV ターミナル コンソールにログインすると、[ ネットワーク設定 ] ページに実際と一致しない数の NIC が表示されることがあります。

解決方法 : MAC アドレスを使用して正しい NIC を比較および設定し、- ボタンを使用してその他の NIC を削除します。

影響を受けるバージョン : 5.0

## 以前のバージョンでステータスが [ 不明 ] になっていたサーバーが、OMIVV の最新バージョンへのバックアップおよび復元後に [ ベアメタル サーバー ] ページに表示されない

以前のバージョンからバックアップを復元した後、サポートされていないサーバー (11G 以前) はベアメタル インベントリーから削除されます。バックアップ前に以前のバージョンで世代が判別されていなかったサーバーも削除されます。

対応処置 : サーバーを再検出します。見つからないサーバーがサポートされている場合、ベアメタル インベントリーに表示されません。

影響を受けるバージョン : 5.0

## OS の導入後、OMIVV が vCenter への ESXi ホストの追加に失敗したか、ホスト プロファイルの追加に失敗したか、ホストのメンテナンス モードの開始に失敗した

OS の導入後、OMIVV は vCenter にクエリーを行うことによってホスト アクション (ホストの追加、ホスト プロファイルの追加、またはメンテナンス モードの開始) を実行します。クエリーが 2 分以内に応答を受信しないと vCenter でそのアクションがタイムアウトし、通信障害を示すメッセージがタスク履歴に表示されます。ただし、vCenter クエリー操作は成功している場合があります。

対応処置 : タスク履歴からホスト IP を取得し、手動で追加します。

## iDRAC IP に到達できないときに、iDRAC ライセンスのステータスが [ 対応性の管理 ] ページに [ 対応 ] と表示される

定期的なインベントリーの実行後、iDRAC に到達できない場合、iDRAC ライセンスのステータスが [ 対応性の管理 ] ページに [ 対応 ] と表示されます。

対応処置 : iDRAC が到達可能であることを確認し、インベントリーを再実行して、正しい iDRAC ライセンスの詳細を取得します。

## OMIVV で OS を正常に導入した後、ESXi ホストが切断されるか、応答しない状態になる

vCenter の FQDN をルックアップするように DNS が正しく設定されていないため、ESXi ホストがハートビート パケットの vCenter への送信に失敗します。

対応処置：以下のタスクを実行します。

1. ESXi ホストを vCenter インベントリーから削除します。
2. [ホストの追加] ウィザードを使用して vCenter にホストを追加します。
3. ホスト認証情報プロファイルを作成し、インベントリーを実行します。

## OMIVV のネットワーク インターフェイス カード (NIC) が ESXi ホスト ネットワークに接続されていない場合、導入ジョブがタイムアウトする

OS の導入は、NIC の選択に影響を受けます。正しい NIC を選択しないと、OSD ジョブがタイムアウトします。

解決方法：導入ウィザードの [ホスト設定] ページで、[ホストに接続されているアプライアンス NIC] から適切な NIC を選択します。この選択は、OMIVV が OS のインストール プロセス中に ESXi ネットワークにアクセスするために必要です。

## 特定のホストで保証ジョブが実行されない

複数の vCenter を持つ PSC 環境で、ある vCenter に FQDN を使用してホストを追加し、別の vCenter には IP を使用してホストを追加すると、保証ジョブは1つのホスト インスタンスに対してのみ実行されます。

対応処置：接続されていないホスト インスタンスをホスト認証情報プロファイルから削除し、インベントリーおよび保証ジョブを実行します。

影響を受けるバージョン：5.0

## バックアップおよび復元の実行後に Proactive HA の初期化が実行されない

vSphere クライアントに登録されている以前のバージョンから OMIVV を復元すると、Proactive HA 対応クラスターの場合、Dell プロバイダーが切断されます。

解決方法：クラスターの Proactive HA を無効にしてから有効にします。

影響を受けるバージョン：5.0

## Firefox ブラウザーの環境で、OMIVV ページに無効なセッション、タイムアウト例外、または 200 万件のエラーが表示される

OMIVV ページで操作がない状態が続くと (5~10 分)、無効なセッション、タイムアウト例外、または 200 万件のエラーが表示されます。

解決方法：ブラウザーを最新の状態に更新します。問題が解決しない場合は、vCenter からログアウトしてもう一度ログインします。

OMIVV で正しいデータを表示するには、「解決策」のタスクを完了したことを確認します。

影響を受けるバージョン：5.0

## vCenter の最近のタスク ペインでは、一部の OMIVV タスク通知の詳細列が表示されない

解決方法：タスク通知を表示するには、vCenter で vCenter の [ タスク コンソール ] に移動します。

影響を受けるバージョン：5.0

## vCenter 6.5 U2 を使用している場合、OMIVV のすべてのページに 2000002 エラーが表示されることがある

解決処置：VMware から 6.5 U2 用の最新パッチを使用するか、6.5 U3 以降のバージョンに移行します。

影響を受けるバージョン：5.1

## RPM アップグレードの実行後、または以前の OMIVV バージョンからそれ以降の OMIVV バージョンへのバックアップおよび復元を実行した後、OMIVV のすべてのページに 2000002 エラーが表示される

現在のバージョンを登録する前に、vCenter サーバーに以前のバージョンの OMIVV がある場合、SSL ハンドシェイクの例外により、vCenter が新しいプラグイン データを更新するまで、新しいバージョンの OMIVV に到達できません。これは vCenter には、SSL トラフィックを異なる方法で処理する以前の OMIVV バージョンのデータが含まれているためです。

解決策：

- ・ vCenter サーバーで vSphere Web Client を再起動します。
- ・ 問題が解決しない場合は、
  - ・ VMware vCenter Server アプライアンスの場合、`/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity` にアクセスします。Windows vCenter の場合、vCenter アプライアンスの `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` フォルダに進み、`com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX` のような古いデータが存在するか確認します。
  - ・ 古いバージョンの OMIVV に対応するフォルダを手動で削除します。
  - ・ vSphere Client services for vSphere Client ( HTML5 ) を再起動します。

影響を受けるバージョン：5.0 以降

## OMIVV が vCenter の登録解除を完了するまでに長時間かかる場合がある

ホスト数が多い ( 300 以上 ) vCenter の登録を解除すると、OMIVV は長時間読み込み状態のままになります。

解決方法：ブラウザを最新の状態に更新します。

vCenter の登録解除が正常に行われなかった場合は、vCenter の登録を再度解除します。

影響を受けるバージョン：5.1

## ベアメタル展開の問題

本項では、展開プロセスで見つかった問題の処理について説明します。

### 自動検出とハンドシェイクの前提条件

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

## ハードウェア設定の失敗

- ・ 展開タスクを開始する前に、システムが CSIOR を完了していて、再起動中ではないことを確認してください。
- ・ リファレンス サーバーがまったく同じシステムになるように、BIOS 設定をクローン モードで実行する必要があります。
- ・ コントローラによっては、1台のドライブでは RAID 0 アレイを作成できません。この機能はハイエンドのコントローラでのみサポートされており、そのようなハードウェアプロファイルの適用は失敗の原因となることがあります。

## 新しく購入したシステムでの自動検出の有効化

ホストシステムの自動検出機能はデフォルトで有効になっていません。購入時に有効化を請求する必要があります。購入時に自動検出の有効化を請求した場合、iDRAC で DHCP が有効化され、管理アカウントが無効化されます。iDRAC 用に静的 IP アドレスを設定する必要はありません。ネットワーク上の DHCP サーバから取得されます。自動検出機能を使用するには、検出プロセスをサポートするように、DHCP サーバまたは DNS サーバ (または両方) を設定する必要があります。出荷処理中に、CSIOR が既に実行されている必要があります。

購入時に自動検出を請求しなかった場合は、次の手順で有効化できます。

1. 起動ルーチン中に **Ctrl + E** を押します。
2. iDRAC セットアップウィンドウで、NIC を有効にします (ブレードサーバーのみ)。
3. 自動検出を有効にします。
4. DHCP を有効にします。
5. 管理者アカウントを無効にします。
6. **DHCP から DNS サーバアドレスを取得** を有効にします。
7. **DHCP から DNS ドメイン名を取得** を有効にします。
8. プロビジョニングサーバフィールドに次を入力します。

```
<OpenManage Integration virtual appliance IPaddress>:4433
```

# システム固有属性

## iDRAC

表 28. システム固有属性 iDRAC

属性名	表示属性名	グループ表示名
DNS RAC 名	DNS RAC 名	NIC 情報
DataCenterName	データセンター名	サーバトポロジ
通路名	通路名	サーバトポロジ
ラック名	ラック名	サーバトポロジ
ラックスロット	ラックスロット	サーバトポロジ
RacName	Active Directory RAC 名	Active Directory
Address	IPv4 アドレス	IPv4 静的情報
ネットマスク	ネットマスク	IPv4 静的情報
ゲートウェイ	ゲートウェイ	IPv4 静的情報
DNS2	DNS サーバ 2	IPv4 静的情報
Address 1	IPv6 アドレス 1	IPv6 静的情報
ゲートウェイ	IPv6 ゲートウェイ	IPv6 静的情報
プレフィックス長	IPv6 リンクのローカルプレフィックスの長さ	IPv6 静的情報
DNS1	IPv6 DNS サーバ 1	IPv6 静的情報
DNS2	IPv6 DNS サーバ 2	IPv6 静的情報
DNSFromDHCP6	DHCP6 からの DNS サーバ	IPv6 静的情報
HostName	サーバホスト名	サーバオペレーティングシステム
RoomName	RoomName	サーバトポロジ
NodeID	システムノード ID	サーバー情報

## BIOS

表 29. BIOS のシステム固有属性

属性名	表示属性名	グループ表示名
AssetTag	資産タグ	その他の設定
IscsiDev1Con1Gateway	イニシエータゲートウェイ	接続 1 設定
IscsiDev1Con1Ip	イニシエータ IP アドレス	接続 1 設定
IscsiDev1Con1Mask	イニシエータサブネットマスク	接続 1 設定
IscsiDev1Con1TargetIp	ターゲット IP アドレス	接続 1 設定
IscsiDev1Con1TargetName	ターゲット名	接続 1 設定
IscsiDev1Con2Gateway	イニシエータゲートウェイ	接続 1 設定

属性名	表示属性名	グループ表示名
IscsiDev1Con2Ip	イニシエーター IP アドレス	接続 1 設定
IscsiDev1Con2Mask	イニシエーターサブネットマスク	接続 1 設定
IscsiDev1Con2TargetIp	ターゲット IP アドレス	接続 1 設定
IscsiDev1Con2TargetName	ターゲット名	接続 1 設定
IscsilInitiatorName	iSCSI イニシエーター名	ネットワーク設定
Ndc1PcieLink1	内蔵ネットワークカード 1 PCIe Link1	内蔵デバイス
Ndc1PcieLink2	内蔵ネットワークカード 1 PCIe Link2	内蔵デバイス
Ndc1PcieLink3	内蔵ネットワークカード 1 PCIe Link3	内蔵デバイス
UefiBootSeq	UEFI 起動シーケンス	UEFI 起動設定

## RAID

表 30. RAID のシステム固有属性

属性名	表示属性名	グループ表示名
エンクロージャの要求された設定モード	該当なし	該当なし
エンクロージャの現在の設定モード	該当なし	該当なし

## CNA

表 31. CNA のシステム固有属性

属性名	表示属性名	グループ表示名
ChapMutualAuth	CHAP 相互認証	iSCSI の一般的なパラメータ
ConnectFirstTgt	接続	iSCSI の最初のターゲットパラメータ
ConnectSecondTgt	接続	iSCSI の 2 番目のターゲットのパラメータ
FirstFCoEBootTargetLUN	ブート LUN	FCoE 設定
FirstFCoEWWPNTarget	ワールドワイドポート名ターゲット	FCoE 設定
FirstTgtBootLun	ブート LUN	iSCSI の最初のターゲットパラメータ
FirstTgtChapId	CHAP ID	iSCSI の最初のターゲットパラメータ
FirstTgtChapPwd	CHAP シークレット	iSCSI の最初のターゲットパラメータ
FirstTgtIpAddress	IP アドレス	iSCSI の最初のターゲットパラメータ
FirstTgtIscsiName	iSCSI 名	iSCSI の最初のターゲットパラメータ
FirstTgtTcpPort	TCP ポート	iSCSI の最初のターゲットパラメータ
IP 自動設定	IpAutoConfig	iSCSI の一般的なパラメータ
IscsilInitiatorChapId	CHAP ID	iSCSI イニシエーターのパラメータ
IscsilInitiatorChapPwd	CHAP シークレット	iSCSI イニシエーターのパラメータ
IscsilInitiatorGateway	デフォルトゲートウェイ	iSCSI イニシエーターのパラメータ
IscsilInitiatorIpAddr	IP アドレス	iSCSI イニシエーターのパラメータ
IscsilInitiatorIpv4Addr	IPv4 アドレス	iSCSI イニシエーターのパラメータ
IscsilInitiatorIpv4Gateway	IPv4 デフォルトゲートウェイ	iSCSI イニシエーターのパラメータ
IscsilInitiatorIpv4PrimDns	IPv4 プライマリ DNS	iSCSI イニシエーターのパラメータ
IscsilInitiatorIpv4SecDns	IPv4 セカンダリ DNS	iSCSI イニシエーターのパラメータ

属性名	表示属性名	グループ表示名
IscsilInitiatorIpv6Addr	IPv6 アドレス	iSCSI イニシエータのパラメータ
IscsilInitiatorIpv6Gateway	IPv6 デフォルトゲートウェイ	iSCSI イニシエータのパラメータ
IscsilInitiatorIpv6PrimDns	IPv6 プライマリ DNS	iSCSI イニシエータのパラメータ
IscsilInitiatorIpv6SecDns	IPv6 セカンダリ DNS	iSCSI イニシエータのパラメータ
IscsilInitiatorName	iSCSI 名	iSCSI イニシエータのパラメータ
IscsilInitiatorPrimDns	プライマリ DNS	iSCSI イニシエータのパラメータ
IscsilInitiatorSecDns	セカンダリ DNS	iSCSI イニシエータのパラメータ
IscsilInitiatorSubnet	サブネットマスク	iSCSI イニシエータのパラメータ
IscsilInitiatorSubnetPrefix	サブネットマスクプレフィックス	iSCSI イニシエータのパラメータ
SecondaryDeviceMacAddr	セカンダリデバイス MAC アドレス	iSCSI セカンダリデバイスのパラメータ
SecondTgtBootLun	ブート LUN	iSCSI の 2 番目のターゲットのパラメータ
SecondTgtChapPwd	CHAP シークレット	iSCSI の 2 番目のターゲットのパラメータ
SecondTgtIpAddress	IP アドレス	iSCSI の 2 番目のターゲットのパラメータ
SecondTgtIscsiName	iSCSI 名	iSCSI の 2 番目のターゲットのパラメータ
SecondTgtTcpPort	TCP ポート	iSCSI の 2 番目のターゲットのパラメータ
UseIndTgtName	独立したターゲット名の使用	iSCSI セカンダリデバイスのパラメータ
UseIndTgtPortal	独立したターゲットポータルの使用	iSCSI セカンダリデバイスのパラメータ
VirtFIPMacAddr	仮想 FIP MAC アドレス	メイン設定ページ
VirtIscsiMacAddr	仮想 iSCSI オフロード MAC アドレス	メイン設定ページ
VirtMacAddr	仮想 MAC アドレス	メイン設定ページ
VirtMacAddr[Partition:n]	仮想 MAC アドレス	パーティション n 構成
VirtWWN	仮想ワールドワイドノード名	メイン設定ページ
VirtWWN[Partition:n]	仮想ワールドワイドノード名	パーティション n 構成
VirtWWPN	仮想ワールドワイドポート名	メイン設定ページ
VirtWWPN[Partition:n]	仮想ワールドワイドポート名	パーティション n 構成
ワールドワイドノード名	WWN	メイン設定ページ
ワールドワイドノード名	WWN[Partition:n]	パーティション n 構成

## FC

表 32. FC のシステム固有属性

属性名	表示属性名	グループ表示名
VirtualWWN	仮想ワールドワイドノード名	ポート設定ページ
VirtualWWPN	仮想ワールドワイドポート名	ポート設定ページ

## 追加情報

**delltechcenter.com** で取得できる次の Dell テクニカルホワイトペーパーは、システムプロファイル設定テンプレート、属性、およびワークフローについての詳細情報を提供します。

- ・ [サーバー設定プロファイルでのサーバークローン](#)
- ・ [サーバー設定XML ファイル](#)
- ・ [設定XML ワークフロー](#)
- ・ [設定XML ワークフロースクリプト 133](#)
- ・ [XML 設定ファイル例](#)

## カスタマイズ属性

表 33. カスタマイズ属性

FQDD	属性	OMIVV のカスタマイズ
BIOS	仮想化テクノロジー	常に有効
iDRAC	再起動時のシステムインベントリの収集	常に有効
RAID	IncludedPhysicalDiskID	IncludedPhysicalDiskID 値が自動選択の場合、その値を削除します
RAID	RAIDPDState	削除
iDRAC	ユーザー管理パスワード パスワード	iDRAC 対応ユーザーのみにパスワードを入力するためのパスワードリンクが表示されます。
PCIeSSD	PCIeSSDSecureErase	常に無効

# コンポーネントとベースラインのバージョン比較表

表 34. コンポーネントとベースラインのバージョン比較表

ドリフトのタイプ				
ハードウェア	関連するベースライン	ターゲットコンポーネント	シナリオ	対応状態
	使用可能	使用可能	ハードウェアコンポーネントが関連するベースラインと一致します。	対応
	使用可能	使用可能	コンポーネントのハードウェア属性が関連するベースラインと一致しません。	非対応
	該当なし	使用可能	比較のステータスが計算されておらず、無視されます。	対応
	使用可能	該当なし	ハードウェアコンポーネントは関連するベースラインで使用可能ですが、コンポーネントまたは属性がホストで使用できません。	非対応
	該当なし	該当なし	比較のステータスが計算されておらず、無視されます。	対応
ファームウェア	関連するベースライン	ターゲットコンポーネント	シナリオ	対応状態
	使用可能	使用可能	ファームウェア コンポーネント バージョンが関連するベースラインと一致します。	対応
	使用可能	使用可能	ファームウェア コンポーネント バージョンが関連するベースラインと一致しません。	非対応
	使用不可	使用可能	ファームウェア コンポーネント バージョンは関連するベースラインで使用できませんが、コンポーネントがホストで使用可能です。 比較のステータスが計算されておらず、無視されます。	対応
	使用可能	該当なし	比較のステータスが計算されておらず、無視されます。	対応
	該当なし	該当なし	比較のステータスが計算されておらず、無視されます。	対応
ドライバ	関連するベースライン	ターゲットコンポーネント	シナリオ	対応状態
	使用可能	使用可能	ドライバ コンポーネント バージョンが関連するベースラインと一致します。	対応

ドリフトのタイプ				
	使用可能	使用可能	ドライバー コンポーネント バージョンが関連するベースラインと一致しません。	非対応
	該当なし	使用可能	比較のステータスが計算されておらず、無視されます。	対応
	使用可能	該当なし	ドライバー コンポーネント バージョンは関連するベースラインで使用可能ですが、コンポーネントがホストで使用できません。	非対応
	該当なし	該当なし	比較のステータスが計算されておらず、無視されます。	対応

# 応答コード

表 35. 応答コード

応答コード	説明
200	タスク情報またはタスク リストが正常に生成されたまたは返されました。
202	任意のタスクが正常に開始されました。
400	不正なリクエスト
401	許可されていないリクエスト
404	見つかりません
409	競合しています
500	内部サーバー エラー
503	サービス利用不可