Web Client 向け OpenManage Integration for VMware vCenter

ユーザーズガイドバージョン 3.1

メモ、注意、警告

メモ: コンピュータを使いやすくするための重要な情報を説明しています。

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

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

2016 - 02

Rev. A00

目次

1 はじめに 11

OpenManage Integration for VMware vCenter の機能 11

本リリースの新機能 12

2 OpenManage Integration for VMware vCenter の設定または編集方法の理解 13

設定ウィザードようこそページ 13

vCenter の選択 13

初期設定ウィザードを使用した新規接続プロファイルの作成 14

インベントリジョブのスケジュールウィザード 16

保証取得ジョブウィザードの実行 17

イベントおよびアラームの設定ウィザード 17

3 VMware vCenter ウェブクライアントの移動について 19

VMware vCenter 内の OpenManage Integration for VMware vCenter への移動 19

アイコンボタンの理解 19

ソフトウェアバージョンの特定 20

画面コンテンツの更新 20

OpenManage Integration for VMware vCenter ライセンスタブの表示 20

オンラインヘルプを開く 21

ヘルプおよびサポートの検索 21

トラブルシューティングバンドルのダウンロード 22

iDRAC のリセット 22

管理コンソールの起動 23

4 プロファイル 25

接続プロファイルの表示 25

新しい接続プロファイルの作成 26

接続プロファイルの編集 27

接続プロファイルの更新 29

接続プロファイルの削除 29

接続プロファイルのテスト 29

シャーシプロファイルの作成 30

シャーシプロファイルの表示 31

シャーシプロファイルの編集 31

シャーシプロファイルの削除 31

シャーシプロファイルのテスト 32

5 ジョブキュー..... 33
インベントリ履歴..... 33
ホストインベントリの表示 33
インベントリジョブスケジュールの変更..... 34
インベントリジョブを今すぐ実行する..... 35
シャーシのインベントリのジョブを今すぐ実行する..... 35
保証履歴..... 35
保証履歴の表示..... 35
保証ジョブスケジュールの変更..... 36
保証ジョブを今すぐ実行する..... 37
シャーシ保証ジョブを今すぐ実行する..... 37
ログ..... 37
ログの表示..... 38
ログファイルのエクスポート..... 39

6 コンソール管理..... 40
管理コンソールの使用..... 40
必要な権限を持つ Administrator 以外のユーザーによる vCenter サーバの登録..... 40
vCenter サーバーの登録..... 43
OpenManage Integration for VMware vCenter ライセンスを管理コンソールにアップロードする..... 46
仮想アプライアンス管理..... 46
仮想アプライアンスの再スタート..... 46
リポジトリの場所と仮想アプライアンスのアップデート..... 47
仮想アプライアンスソフトウェアのアップデート 47
トラブルシューティングバンドルのダウンロード..... 47
HTTP プロキシの設定..... 47
NTP サーバーの設定..... 48
証明書署名要求の生成..... 48
グローバルアラートの設定..... 49
バックアップおよび復元の管理..... 49
バックアップおよび復元の設定..... 50
自動バックアップのスケジュール..... 50
即時のバックアップの実行..... 51
バックアップからのデータベースの復元..... 51
vSphere Client コンソールについて 51
ネットワークの設定..... 52
仮想アプライアンスパスワードの変更..... 52
ローカルタイムゾーンの設定..... 52
仮想アプライアンスの再起動..... 53
仮想アプライアンスの工場出荷時設定へのリセット..... 53

コンソールビューの更新 54
コンソールからログアウトする 54
読み取り専用ユーザー役割 54
OpenManage Ingetration プラグイン 3.0 バージョンから現在のバージョンへのアップグレード 54
2.x から 3.1 への移行のための移行パス 55

7 設定 56
OMSA リンクの編集 56
11 世代サーバーとの OMSA 使用の理解 56
保証期限通知の設定の表示 58
保証期限通知の設定 58
イベントおよびアラームの設定 58
ファームウェアアップデートについて 60
ファームウェア更新リポジトリの設定 60
単一ホストのためのファームウェアのアップデートウィザードの実行 61
クラスタのためのファームウェアのアップデートウィザードの実行 62
Viewing Firmware Update Status for Clusters and Datacenters 63
インベントリおよび保証のデータ取得スケジュールの表示 64
11 世代サーバーとの OMSA 使用の理解 65
OMSA エージェントの ESXi システムへの展開 65
OMSA トラップ先の設定 65

8 保証期限通知の設定の表示 67
保証期限通知の設定 67

9 ファームウェアアップデートについて 68
ファームウェア更新リポジトリの設定 68
単一ホストのためのファームウェアのアップデートウィザードの実行 69
クラスタのためのファームウェアのアップデートウィザードの実行 70

10 ホストのイベントおよびアラームについて 73
シャーシのイベントおよびアラームについて 74
イベントおよびアラームの設定 74
イベントの表示 75
アラームおよびイベントの設定の表示 76
インベントリおよび保証のデータ取得スケジュールの表示 76

11 シャーシに関連するホストの表示 77

12 シャーシ管理 78
シャーシサマリ詳細の表示 78

ハードウェアインベントリの表示：ファン....79
ハードウェアインベントリの表示：I/O モジュール....79
ハードウェアインベントリの表示：iKVM....80
ハードウェアインベントリの表示：PCIe....81
ハードウェアインベントリの表示：電源装置....82
ハードウェアインベントリの表示：温度センサー....82
保証の詳細の表示....83
ストレージの表示....83
シャーシのファームウェア詳細の表示....84
シャーシの管理コントローラ詳細の表示....84

13 単一ホストの監視....86
ホストサマリ詳細の表示....86
管理コンソールの起動....89
OMSA コンソールの起動....89
Remote Access Console（iDRAC）の起動....89
物理サーバーインジケータライトの点滅の設定....90
物理サーバーインジケータライトの点滅の設定....90

14 ソフトウェアライセンスの購入およびアップロード....91
OpenManage Integration for VMware vCenter ライセンスについて....91

15 ハードウェアの表示: 単一ホストの FRU 詳細....93

16 ハードウェアの表示: 単一ホストのプロセッサ詳細....94

17 ハードウェアの表示: 単一ホストの電源装置詳細....95

18 ハードウェアの表示: 単一ホストのメモリ詳細....96

19 ハードウェアの表示: 単一ホストの NIC 詳細....97

20 ハードウェアの表示: 単一ホストの PCI スロット....98

21 ハードウェアの表示: 単一ホストのリモートアクセスカード詳細....99

22 単一ホストのストレージ詳細の表示....100
ストレージの表示: 単一ホストの仮想ディスク詳細....100
ストレージの表示: 単一ホストの物理ディスク詳細....101
ストレージの表示: 単一ホストのコントローラ詳細....103
ストレージの表示: 単一ホストのエンクロージャ詳細....103

23 単一ホストのファームウェア詳細の表示....104

24 単一ホストの電源監視の表示.....105

25 単一ホストの保証ステータスの表示.....106

26 Dell ホストのみの簡単な表示..... 107

27 クラスタおよびデータセンターでのホスト監視.....108

28 データセンターとクラスタの概要詳細の表示..... 109

29 ハードウェアの表示: データセンターまたはクラスタの **FRU**..... 111

30 ハードウェアの表示: データセンターまたはクラスタのプロセッサ詳細 112

31 ハードウェアの表示: データセンターとクラスタの電源装置詳細..... 113

32 ハードウェアの表示: データセンターとクラスタのメモリ詳細.....115

33 ハードウェアの表示： データセンターとクラスタの **NIC** 詳細.....116

34 ハードウェアの表示： データセンターとクラスタの **PCI** スロット詳細..117

35 ハードウェアの表示：リモートアクセスカード詳細..... 118

36 ストレージの表示: データセンターとクラスタの物理ディスク..... 119

37 ストレージの表示: データセンターとクラスタの仮想ディスク詳細.....121

38 データセンターとクラスタのファームウェア詳細の表示..... 123

39 データセンターとクラスタの保証サマリ詳細の表示.....124

40 データセンターおよびクラスタの電源監視の表示..... 126

41 トラブルシューティング.....128

よくあるお問い合わせ (FAQ).....128

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.....128

重要度カテゴリをフィルタしようとすると、Dell Management Center に、関連するすべてのログが表示されません。すべてのログを表示するにはどうすればいいですか?..... 128

VMware 認証局（VMCA）によるエラーコード 2000000 を解決する方法.....128

ファームウェアアップデートウィザードに、バンドルがファームウェアリポジトリから取得されていないというメッセージが表示されます。どうすればファームウェアアップデートを続行できますか?.....133
クラスタレベルでの 30 台のホストのファームウェアアップデートが失敗する.....133
「Dell Home > 監視 > ジョブキュー > 保証 / インベントリ履歴 > スケジュール」と選択したときに、すべての vCenter に保証とインベントリスケジュールが適用されません.....134
OpenManage Integration for VMware vCenter で DNS の設定を変更した後、vCenter Web Client でウェブ通信エラーが発生します。.....134
「設定」ページから移動した後に「設定」ページに戻ると、ページのロードが失敗します。..134
初期設定ウィザードのインベントリスケジュール / 保証スケジュールページで「過去の時間にタスクをスケジュールすることはできません」と表示されるのはなぜですか?.....134
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 として表示されるのはなぜですか?.....135
連続したグローバル更新によって最近のタスクウィンドウに例外が生成されるのはなぜですか?.....135
IE 10 のデル画面のいくつかで Web Client UI が歪むのはなぜですか?.....135
vCenter へのプラグインの登録に成功したにもかかわらず、Web Client に OpenManage Integration アイコンが表示されないのはなぜですか?.....135
選択した 11G システム用のバンドルがリポジトリにあっても、ファームウェアアップデートがファームウェアアップデート用バンドルがないと表示するのはなぜですか?.....136
保証取得ジョブを実行しているときに、保証ジョブのステータスが保証の ジョブキュー ページに記載されていません.....136
アプライアンスの IP に DHCP を使用し、DNS 設定が上書きされると、なぜ、アプライアンスの再起動後に DNS 構成設定が元の設定に戻るのですか?.....136
OpenManage Integration for VMware vCenter を使用した、ファームウェアバージョン 13.5.2 の Intel ネットワークカードのアップデートはサポートされていません。.....136
Intel ネットワークカードを 14.5 または 15.0 から 16.x にアップデートするために OpenManage Integration for VMware vCenter を使用すると、DUP からのステージング要件のためにアップデートに失敗する。.....137
無効な DUP でファームウェアのアップデートを行おうとすると、ジョブのステータス LC に "FAILED" と表示されるのに何時間も vCenter コンソールが失敗もタイムアウトもしません。なぜこれが起こっていますか ?.....137
管理ポータルに、到達不能なアップデートリポジトリの場所が表示されたままになっています。.....137
1 対多のファームウェアアップデートを実行したときに、システムがメンテナンスモードに入らなかったのはなぜですか?.....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が正常のままになっているのはなぜですか?.....137
システム概要ページのプロセッサビューで、プロセッサバージョンが「該当なし」となっているのはなぜですか?.....138
Web Client を使用して接続プロファイルを編集した後に終了をクリックすると、いつも例外が表示されます。なぜですか?.....138

ウェブ GUI で接続プロファイルを作成 / 編集するときに、ホストが属する接続プロファイルを見ることができません。なぜですか?.....138
接続プロファイルを編集するときに、ウェブ UI の特定のホストウィンドウが空です。なぜですか ?.....138
ファームウェアのリンクをクリックした後、なぜ通信エラーメッセージが表示されるのですか。.....138
OpenManage Integration for VMware vCenter で設定し SNMP トラップをサポートしているのは、どの世代の Dell サーバーですか?.....139
OpenManage Integration for VMware vCenter によって管理されるのはどの vCenter ですか?.....139
OpenManage Integration for VMware vCenter は、リンクモードの vCenter をサポートしていますか?.....139
OpenManage Integration for VMware vCenter にはどのようなポート設定が必要ですか?.....140
仮想アプライアンスの正常なインストールと操作のために最低限必要な要件は何ですか?.....142
新しい iDRAC バージョンの詳細が、vCenter ホストとクラスタ のページに表示されないのはなぜですか?.....142
OMSA を使用してハードウェア温度の異常をシミュレートすることによってイベント設定をテストする方法は?.....142
Dell ホストシステムに OMSA エージェントをインストールしていますが、OMSA がインストールされていないというエラーメッセージが今でも表示されます。どうしたらよいですか?.....143
OpenManage Integration for VMware vCenter はロックダウンモードが有効になっている ESXi をサポートしますか?.....143
ロックダウンモードを使用しようとしたら、失敗しました。.....143
ESXi 4.1 U1 で UserVars.CIMoeMProviderEnable にはどのような設定を使用すべきですか?...143
ハードウェアプロファイルの作成にリファレンスサーバーを使用していますが、失敗しました。どうすればよいですか?.....143
ブレードサーバーに ESXi を展開しようとしていますが、失敗しました。どうすればよいですか?.....144
Dell PowerEdge R210 II マシンでハイパーバイザー展開が失敗するのはなぜですか?.....144
展開ウィザードにモデル情報のない自動検出されたシステムが表示されるのはなぜですか?..144
ESXi ISO で NFS 共有がセットアップされていますが、共有の場所をマウントするときのエラーで失敗します。.....144
仮想アプライアンスを強制削除するにはどのようにしたらよいですか?.....144
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.....145
vSphere Web Client で Dell サーバー管理ポートレットまたは Dell アイコンをクリックすると、404 エラーが返されます。.....145
ファームウェアアップデートが失敗しました。どうしたらよいですか?.....145
vCenter の登録が失敗しました。どうしたらよいですか?.....145
接続プロファイルの資格情報テスト中、パフォーマンスが非常に遅くなったり、応答しなくなります。.....145

OpenManage Integration for VMware vCenter は VMware vCenter Server Appliance をサポートしますか?....146
OpenManage Integration for VMware vCenter は vSphere Web Client をサポートしていますか?....146
次回の再起動時にファームアップデートを適用するオプションでファームウェアのアップデートを行ってシステムを再起動したにも関わらず、ファームウェアのレベルがアップデートされないのはなぜですか?....146
ホストを vCenter ツリーから削除した後でもシャーシにそのホストが引き続き表示されるのはなぜですか?....146
管理コンソールで、アプライアンスを工場出荷時設定にリセットした後、リポジトリパスのアップデート がデフォルトに設定されないのはなぜですか?....146
OpenManage Integration for VMware vCenter のバックアップおよび復元の後、アラーム設定が復元されないのはなぜですか? 147
ベアメタル展開の問題....147
デルへのお問い合わせ....147
OpenManage Integration for VMware vCenter の関連情報....147

42 Dell PowerEdge サーバーの仮想化関連イベント....149
付録 A: セキュリティの役割および許可....161
データ整合性....161
アクセス制御認証、承諾、および役割....161
Dell Operational Role....162
Dell インフラストラクチャ展開の役割....162
権限について....162
付録 B: 自動検出について....165
自動検出の必要条件....165
iDRAC サーバーの管理者アカウントを有効または無効にする....166

1

はじめに

VMware vCenter は、VMware vSphere ESX/ESXi ホストを管理および監視するために IT 管理者が使用するプライマリコンソールです。標準的な仮想化環境では、ハードウェア問題を解決するためのコンソールを別途起動するプロンプトの表示に VMware アラートと監視が使用されます。OpenManage Integration for VMware vCenter は、VMware Web Client 内からの VMware vCenter サーバーの管理を可能にする製品で、Windows システムへの依存から解放してくれます。OpenManage Integration for VMware vCenter を使用することにより、仮想化環境内でデルハードウェアを管理および監視するための次のような機能を実行できます。

- アラートと環境監視 : 主要ハードウェアの障害を検出し、仮想化対応アクション（たとえば、作業負荷の移行、またはホストをメンテナンスモードにするなど）を実行します。
- 単一サーバーの監視と報告 : サーバーの監視および報告機能です。
- ファームウェアアップデート : デルハードウェアを最新バージョンの BIOS とファームウェアにアップデートします。
- 拡張展開オプション : ハードウェアプロファイルとハイパーバイザプロファイルを作成し、vCenter を使用して、リモートかつ PXE 無しでベアメタル Dell PowerEdge サーバーにこの 2 つの任意の組み合わせを展開します。

OpenManage Integration for VMware vCenter の機能

OpenManage Integration for VMware vCenter を使用して、次のタスクを実行することができます。

インベントリ	主要資産のインベントリを実行、設定タスクを実行、Dell プラットフォームのクラスタビューとデータセンタビューを提供。
監視とアラートの実施	主要ハードウェアの障害を検出し、仮想化対応アクション（たとえば、作業負荷の移行、またはホストをメンテナンスモードにするなど）を実行。サーバー問題の診断のための追加インテリジェンス（インベントリ、イベント、アラーム）を提供。データセンターとクラスタビューでの報告、および CSV ファイルへのエクスポート。
ファームウェアアップデート	Dell ハードウェアを最新バージョンの BIOS とファームウェアにアップデート。
展開とプロビジョニング	ハードウェアプロファイル、ハイパーバイザープロファイルを作成し、それらの任意の組み合わせを、 PXE を使用することなく VMware vCenter を使用してベアメタル Dell PowerEdge サーバーにリモート展開。
サーバー情報	Dell からオンラインで保証情報を取得。
セキュリティ役割と許可	標準の vCenter 認証、規則、および許可との統合。

本リリースの新機能

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

- OMSA 8.2 のサポート
- vCenter サーババージョン v5.5 U3 および v6.0 U1 のサポート
- VMware ESXi バージョン v5.5 U3 および v6.0 U1 のサポート
- 必要な権限を持つ Administrator 以外のユーザーによる OMIVV アプライアンスの登録のサポート
- C4130、R230、R330、T330、および T130 プラットフォームのサポート
- 繁体字中国語のサポート
- ファームウェアのアップデート用 64 ビット DUP バンドルのサポート

2

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

OMIVV の基本インストールを完了し、OMIVV アイコンをクリックすると、**初期設定ウィザード** が表示されます。最初の起動時に **初期設定ウィザード** を使って、**設定** を行います。次回のインスタンスには **設定** ページを使用します。**初期設定ウィザード** で、接続プロファイルの作成、保証、インベントリ、イベント、およびアラームの編集ができます。**初期設定ウィザード** の使用は最も一般的な手段ですが、前記の作業は、OMIVV のアプライアンスの **OpenManage Integration → 管理 → 設定** ページからも実行できます。初期設定ウィザードの詳細は、『*OpenManage Integration for VMware vCenter User Guide*』（OpenManage Integration for VMware vCenter ユーザーガイド）（**dell.com/support/manuals**）を参照してください。

設定ウィザード使用の設定タスク

初期設定ウィザードを使用して、1 つの vCenter、または複数の登録済み vCenter に以下を設定することができます。

メモ: DNS 設定を変更した後、OMIVV 関連タスクの実行中に vCenter Web クライアントで Web 通信エラーが表示された場合は、次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。
- Web クライアントからログアウトし、ログインします。

1. vCenter の選択
2. 新しい接続プロファイルの作成
3. インベントリジョブのスケジュール
4. 保証取得ジョブの実行
5. イベントおよびアラームの設定

メモ: 初期設定ウィザードは、**開始** ページの **基本タスク** の下にある **初期設定ウィザードの開始** のリンクからも行うことができます。

設定ウィザードようこそページ

OMIVV をインストールした後は、設定する必要があります。

1. **vSphere ウェブクライアント** で、**ホーム**、**OpenManage Integration** アイコンの順にクリックします。
2. 初めて **OpenManage Integration** アイコンをクリックすると、**設定ウィザード** が表示されます。このウィザードには **OpenManage Integration → はじめに → 初期設定ウィザードの開始** ページからもアクセスできます。

vCenter の選択

vCenter の選択 ページを使用して、次の項目を設定することができます。

- 特定の vCenter
- 使用可能なすべての vCenter

1. **初期設定ウィザード** の **ようこそ** 画面で、**次へ** をクリックします。
2. **vCenters** ドロップダウンリストから 1 つ、またはすべての vCenter を選択します。
   まだ設定されていない、またはお使いの環境に新規 vCenter を追加した場合、個々の vCenter を選択します。vCenter 選択ページでは、1 つまたは複数の vCenter を選択して設定できます。
3. **次へ** をクリックして、**接続プロファイル** の説明ページに進みます。

   メモ: 同じ SSO の一部として複数の vCenter サーバーがある場合、および単一の vCenter サーバーを構成することを選択した場合は、各 vCenter を設定するまで次の手順を繰り返します。

初期設定ウィザードを使用した新規接続プロファイルの作成

接続プロファイルは、仮想アプライアンスが Dell サーバーと通信するのに使用する iDRAC およびホスト資格情報を保存します。各 Dell サーバーは、OMIVV によって管理される接続プロファイルに関連付けらている必要があります。複数のサーバーを 1 つの接続プロファイルに割り当てることができます。接続プロファイルは、設定ウィザードを使って作成することも **OpenManage Integration for VMware vCenter → 設定** から作成することもできます。

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

メモ: 接続プロファイルに Active Directory 資格情報を使用する前に、Active Directory ユーザーのアカウントに存在しており、iDRAC とホストが Active Directory ベースの認証のために設定されている必要があります。

メモ: Active Directory 資格情報は iDRAC とホストの両方に使用することも、アクティブディレクトリ資格情報を別途設定することもできます。ユーザー資格情報は、管理者権限を持っている必要があります。

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

設定ウィザードを使用する新規接続プロファイルの作成には、以下を行います。

1. **接続プロファイルの説明** ページで、**次へ** をクリックします。
2. **名前と資格情報** ページで、**接続プロファイル名** と、オプションの **接続プロファイルの説明** を入力します。
3. **名前と資格情報** ページの **iDRAC 資格情報** で、次のいずれかを実行します。

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

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

     – **Active Directory ユーザー名** に、ユーザー名 を入力します。**ユーザー名** には、**ドメイン/ユーザー名** または **ユーザー名@ドメイン** のいずれかの形式で入力してください。ユーザー名は 256 文字に制限されています。ユーザー名の制限については、Microsoft Active Directory マニュアルを参照してください。

- **Active Directory パスワード** にパスワードを入力します。パスワードは 127 文字に制限されています。
- **パスワードの 確認** にパスワード をもう一度入力します。
- 次のいずれかの手順を実行します。

  * iDRAC 証明書をダウンロードおよび保存して、今後すべての接続でその証明書の検証を行うには、**証明書チェックを有効にする** を選択します。
  * iDRAC 証明書を保存せず、今後すべての接続で iDRAC 証明書チェックを実行しないようにするには、**証明書チェックを有効にする** チェックボックスのチェックを外します。

- Active Directory なしで iDRAC 資格情報を設定するには、次のいずれかを行います。
  - **ユーザー名** にユーザー名を入力します。ユーザー名は 16 文字に制限されています。お使いのバージョンの iDRAC におけるユーザー名の制限についての情報は、iDRAC マニュアルを参照してください。
  - **パスワード** にパスワードを入力します。パスワードは 20 文字に制限されています。
  - **パスワードの 確認** にパスワード をもう一度入力します。
  - 次のいずれかの手順を実行します。

    * iDRAC 証明書をダウンロードおよび保存して、今後すべての接続でその証明書の検証を行うには、**証明書チェックを有効にする** を選択します。
    * iDRAC 証明書を保存せず、今後すべての接続で iDRAC 証明書チェックを実行しないようにするには、**証明書チェックを有効にする** チェックボックスのチェックを外します。

4. **ホストのルート** エリアで、次のいずれかを実行します。
   - 使用する Active Directory 用にホストの設定および有効化が Active Directory ですでに行われている場合は、**Active Directory を使用する** を選択します。それ以外は、**ホスト資格情報** を設定します。
     - **Active Directory ユーザー名** に **ユーザー名** を入力します。ユーザー名は、**ドメイン/ユーザー名**、または **ユーザー名@ドメイン** のいずれかの形式で入力してください。ユーザー名は 256 文字に制限されています。

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

       ホストユーザー名要件：

       a. 1～64 文字長
       b. 印刷可能文字
       c. 無効な文字：" / \ [ ] : ; | = , + * ? < > @

       ホストドメイン要件：

       a. 1～64 文字長
       b. 最初の文字はアルファベットであることが必須
       c. スペースは使用不可
       d. 無効な文字：" / \ : | , * ? < > ~ ! @ # $ % ^ & ' ( ) { } _
     - **Active Directory パスワード** にパスワードを入力します。パスワードは 127 文字に制限されています。

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

• Active Directory なしでホスト資格情報を設定するには、次のいずれかを行います。
- **ユーザー名** にあるユーザー名は root です。これはデフォルトの **ユーザー名** で、変更することはできませんが、Activate Directory が設定されている場合、root に限らず任意の Active Directory ユーザー名を選択することができます。
- **パスワード** にパスワードを入力します。パスワードは 127 文字に制限されています。

  メモ: OMSA 資格情報は、ESXi ホストに使われたものと同じです。
- **パスワードの 確認** にパスワード をもう一度入力します。
- 次のいずれかの手順を実行します。
  - * ホスト証明書をダウンロードおよび保存して、今後すべての接続でその証明書の検証を行うには、**証明書チェックを有効にする** を選択します。
  - * ホスト証明書を保存せず、今後すべての接続で iDRAC 証明書チェックを実行しないようにするには、**証明書チェックを有効にする** チェックボックスのチェックを外します。

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

   メモ: この手順は任意です。これは、ホストおよび iDRAC の資格情報が正しいかどうかを確認するのに使用されます。
8. プロファイルを完成するには、**次へ** をクリックします。

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

インベントリジョブのスケジュールウィザード

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

メモ: OMIVV が常に最新の情報を表示するようにするため、定期的なインベントリジョブをスケジュールすることをお勧めします。インベントリジョブは最小のリソースで実行でき、ホストのパフォーマンスを劣化させることはありません。

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

インベントリジョブのスケジュールには、以下を行います。

1. **設定ウィザード** の **インベントリのスケジュール** ウィンドウで、有効化がまだの場合は 、**インベントリデータの取得を有効にする** を選択します。

デフォルトでは、**インベントリデータの取得を有効にする** が有効になっています。

2. **インベントリデータの取得スケジュール** で、次の手順を行います。
   a. インベントリを実行する各曜日の横にあるチェックボックスを選択します。デフォルトでは **毎日** が選択されています。
   b. テキストボックスに、時刻を HH:MM フォーマットで入力します。

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

保証取得ジョブウィザードの実行

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

保証取得ジョブを実行するには以下を行います。

1. **設定ウィザード** の **保証のスケジュール** ウィンドウで、**保証データの取得を有効にする** を有効化して、保証をスケジュールできるようにします。
2. **保証データの取得スケジュール** の下で、次の操作を実行します。
   a. 保証を実行したい各曜日の横にあるチェックボックスを選択します。
   b. テキストボックスに、時刻を HH:MM フォーマットで入力します。

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

イベントおよびアラームの設定ウィザード

設定ウィザード または **イベントとアラーム** の **設定** オプションからイベントおよびアラームの設定を行うことができます。サーバーからイベントを受信するため、OMIVV がサーバーからのトラップ送信先として設定されています。第 12 世代ホストおよびそれ以降では、SNMP トラップ送信先を iDRAC で設定する必要があります。第 12 世代より前のホストでは、トラップ世代を OMSA に設定する必要があります。

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

イベントおよびアラームを設定するには、以下を行います。

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

メモ: アラームが有効化されている Dell ホストは、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。

3. **Dell アラーム警告の有効化** ダイアログボックスが表示されたら、**続行** をクリックして変更を承諾、または **キャンセル** をクリックします。

   メモ: この手順は、**Dell ホストのアラームを有効にする** が選択されている場合にのみ実行する必要があります。

   メモ: アプライアンスの復元後、**イベントおよびアラーム** の設定は、グラフィックユーザーインタフェースで有効と表示されていても有効化されていません。**設定** ページから **イベントおよびアラーム** 設定を再度有効化する必要があります。

4. **適用** をクリックします。

3

VMware vCenter ウェブクライアントの移動について

VMware vCenter の操作は簡単です。VMware vCenter にログインすると、ホームページとホームタブが開き、**OpenManage Integration** アイコンがメインコンテンツエリアの管理グループ下に表示されます。**OpenManage Integration** アイコンを使用して OpenManage Integration for VMware vCenter タブへ移動します。ナビゲータ エリアに Dell グループが表示されます。

VMware vCenter のレイアウトは、次の 3 つのセクションで構成されています。

ナビゲータ	ナビゲータエリアは、コンソール内の各種ビューにアクセスするための主なメニューです。OpenManage Integration for VMware vCenter には、vCenter メニューの下に、OpenManage Integration for VMware vCenter の主なアクセスポイントである専用グループがあります。
メインコンテンツエリア	ナビゲータ 内で選択してビューを表示します。メインコンテンツエリアは、コンテンツの大部分が表示されるエリアです。
通知	vCenter アラーム、タスク、および進行中の動作が表示されます。OpenManage Integration for VMware vCenter には vCenter のアラーム、イベント、およびタスクシステムが統合され、通知エリアにそれ自体の情報が表示されます。

VMware vCenter 内の OpenManage Integration for VMware vCenter への移動

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

1. VMware vCenter にログインします。
2. VMware vCenter のホームページで、**OpenManage Integration** アイコンをクリックします。
   ここから OpenManage Integration for VMware vCenter の接続プロファイル、製品設定、インベントリおよび保証ジョブの監視、サマリページの表示、その他、メインコンテンツエリアのタブから多くの操作を行うことができます。
3. ホスト、データセンター、クラウドを監視するには、左側のナビゲーターにあるインベントリリストで、調べたいホスト、データセンター、クラウドのいずれかを選択し、オブジェクト タブで希望のオブジェクトをクリックします。

アイコンボタンの理解

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

表 1. アイコンボタンが定義されました。

アイコンボタン	定義
	このプラス記号アイコンを使って、新しい項目を追加したり作成したりします。
	このサーバー追加アイコンを使って、サーバーを接続プロファイル、データセンター、およびクラスタに追加します。
	このアイコンを使ってジョブを停止します。
	このアイコンを使ってリストをたたみます。
	このアイコンを使ってリストを展開します。
	このアイコンを使ってオブジェクトを削除します。
	このアイコンをスケジュールを変更します。
	この鉛筆アイコンを使って編集します。
	このアイコンを使って、ジョブをパージします。
	このアイコンを使ってファイルをエクスポートします。

ソフトウェアバージョンの特定

ソフトウェアのバージョンは OpenManage Integration for VMware vCenter の開始タブにあります。

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

画面コンテンツの更新

VMware vCenter のリフレッシュアイコンを使用して、画面をいつでも更新できます。

1. 更新したいページを選択します。
2. VMware vCenter タイトルバーで、**更新** ボタンをクリックします。
   更新 アイコンは、検索エリアの左側にある時計回りの形の矢印の左側にあります。

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

OpenManage Integration for VMware vCenter ライセンスをインストールすると、サポートされているホストと vCenter の数がこのタブに表示されます。ページ上部には OpenManage Integration for VMware vCenter のバージョンも表示されます。

ライセンス の下のページには、以下が表示されます。

- ライセンスの購入

ライセンス管理 の下にあるこのページには、以下へのリンクが表示されます。

- Product Licensing Portal（Digital Locker）
- iDRAC Licensing Portal
- 管理コンソール
- ライセンスの購入

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

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

オンラインヘルプを開く

ヘルプおよびサポート タブオンラインヘルプを開くことができます。トピックまたは手順を理解するために、ヘルプのドキュメントを検索できます。

1. OpenManage Integration for VMware vCenter で、次のいずれかを行います。
   - **製品ヘルプ** にある ヘルプおよびサポート で、**OpenManage Integration for VMware vCenter ヘルプ** をクリックします。
2. 左ペインの目次を使用するか検索機能を使用して、トピックを検索します。
3. ヘルプを使い終えたら、右上角でウィンドウまたはタブを閉じます。ブラウザが開いている場合、オンラインヘルプの内容はブラウザウィンドウに表示されます。オンラインヘルプを閉じるには、ブラウザウィンドウの右上角にある **X** をクリックします。

ヘルプおよびサポートの検索

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

製品ヘルプ	次のリンク • **OpenManage Integration for VMware vCenter のヘルプ** 製品内にある製品ヘルプへのリンクを提供します。目次または検索を使って、必要なヘルプを探してください。

	• バージョン情報 バージョン情報のダイアログボックスを表示します。製品情報を確認することができます。
Dell マニュアル	次のリンクを提供します： • サーバー マニュアル • OpenManage Integration for VMware vCenter マニュアル
管理コンソール	管理コンソールへのリンクを提供します。
その他のヘルプおよびサポート	次のリンクを提供します： • Lifecycle Controller 使用 iDRAC のマニュアル • Dell VMware マニュアル • OpenManage Integration for VMware vCenter 製品ページ • Dell ヘルプおよびサポートのホーム • Dell TechCenter
サポート電話のヒント	Dell サポートへの連絡方法と正しい電話の転送についてヒントが記載されています。
トラブルシューティング バンドル	トラブルシューティングバンドルを作成し、ダウンロードするためのリンクを提供します。テクニカルサポートへ連絡するときに、このバンドルを提供するか、参照してください。詳細については、「**トラブルシューティングバンドルのダウンロード**」を参照してください。
Dell 推奨	Dell は Dell Repository Manager を推奨しており、リンクはここに記載されています。Dell Repository Manager を使って、システムに使用できるすべてのファームウェア更新をダウンロードしてください。
iDRAC のリセット	iDRAC が応答しないときに使用する、iDRAC のリンクです。リセットすると通常の iDRAC の再起動が実行されます。

トラブルシューティングバンドルのダウンロード

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

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

iDRAC のリセット

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

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

iDRAC の再起動中、次の状況が生じる場合があります。

- OpenManage Integration for VMware vCenter がその正常性ステータスを取得する間に、遅延または通信エラーが発生する。
- iDRAC とのオープンセッションがすべて閉じられる。
- iDRAC の DHCP アドレスが変わる。
  iDRAC の IP アドレスに DHCP を使用している場合は、IP アドレスが変わる場合があります。この場合、ホストのインベントリジョブを再度実行して、インベントリデータから新規 iDRAC IP アドレスを取得します。

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

管理コンソールの起動

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

1. OpenManage Integration for VMware vCenter にあるヘルプとサポートタブの管理コンソールの下で、コンソールへのリンクをクリックします。
2. 管理コンソールにログインするには、管理者パスワードを使用します。Administration Console では、次の操作を実行できます。
   a. vCenter の登録または登録解除、資格情報の変更、証明書の更新。
   b. ライセンスのアップロード。
   c. 登録済みで使用可能な vCenter の数、使用中 / 使用可能な最大ホストライセンス数についての概要の表示。
   d. 仮想アプライアンスの再起動。
   e. アップデート（最新バージョンへのアップグレード）。
   f. トラブルシューティングバンドルの生成。
   g. ネットワーク設定の表示（読み取り専用モード）。
   h. HTTP プロキシ設定。これは、アプライアンスをアップグレードするための Dell サーバーへの接続、または http://downloads.dell.com/published/Pages/index.html への接続に使用します。
   i. NTP 設定。NTP サーバーを有効化または無効化、および優先またはセカンダリ NTP サーバーの設定が可能です。
   j. 証明書署名要求（CSR）の生成、証明書のアップロード、または HTTPS 証明書のデフォルト証明書を復元します。
   k. すべての vCenter インスタンスに対するアラートの保存方法のグローバル設定。保存するアラートの最大数、アラートの保持日数、および重複アラートのタイムアウトを設定することができます。
   l. バックアップ、または復元の開始。

m. ネットワーク共有へのバックアップ場所の設定、そのバックアップファイル用の暗号化パスワードの設定（ネットワーク接続のテストも行います）。
n. 定期的なバックアップのスケジュール。

4

プロファイル

資格情報プロファイルタブでは、接続プロファイルとシャーシプロファイルの管理と設定を行うことができます。

接続プロファイルは、Dell サーバーへのアクセスに必要な接続プロファイルの管理および設定を可能にします。接続プロファイル では、仮想アプライアンスが Dell サーバーと通信するために使用する認証情報が含まれる接続プロファイルを管理および設定することができます。OpenManage Integration for VMware vCenter による管理には、各 Dell サーバーを 1 つの接続プロファイルのみに関連付けてください。単一の接続プロファイルには複数のサーバーを割り当てることができます。

シャーシプロファイルは、仮想アプライアンスが Dell シャーシと通信するために使用する資格情報が含まれる接続プロファイルの管理および設定を可能にします。OpenManage Integration for VMware vCenter による管理には、検出された各 Dell サーバーを 1 つのシャーシプロファイルに関連付けてください。単一のシャーシロファイルには複数のシャーシを割り当てることができます。

- 接続プロファイルの作成
- 接続プロファイルの表示
- 接続プロファイルの編集
- 接続プロファイルの更新
- 接続プロファイルの削除
- 接続プロファイルのテスト

接続プロファイルの表示

接続プロファイルを表示するには、接続プロファイルが作成されている、および / または存在する必要があります。
1 つ、または複数の接続プロファイルの作成後、これらを接続プロファイルページで表示することができます。OpenManage Integration for VMware vCenter は、Dell ホストとの通信のためにプロファイルで提供される資格情報を使用します。

OpenManage Integration for VMware vCenter の **管理 → プロファイル → 資格情報プロファイル → 接続プロファイル** では、作成した接続プロファイルのすべてを表示することができます。表示できる情報は次のとおりです。

プロファイル名	接続プロファイルの名前を表示します。
説明	説明が表示されます（入力されている場合）。
vCenter	ホスト名もしくは FQDN を表示、またはコンテキストに応じて vCenter の IP アドレスを表示します。

関連ホスト	この接続プロファイルに関連付けられたホストが表示されます。複数ある場合、展開アイコンを使ってすべてを表示します。
iDRAC 証明書チェック	iDRAC 証明書チェックが有効/無効のいずれであるかを表示します。
ホストルート証明書チェック	ホストルート証明書チェックが有効/無効のいずれであるかを表示します。
作成日	作成日を表示します。
変更日	変更日を表示します。
前回変更担当者	ユーザーの詳細を表示します。

新しい接続プロファイルの作成

複数のホストを 1 つの接続プロファイルに関連付けることができます。接続プロファイルを作成するには、次の手順を実行します。

メモ: この手順中に表示される vCenter ホストは、同じシングルサインオン（SSO）で認証されています。vCenter ホストが表示されない場合、別の SSO にあるか、バージョン 5.1 より前の VMware vCenter を使用していることが考えられます。

1. OpenManage Integration for VMware vCenter の左ペインにある**管理** → **プロファイル** → **資格情報プロファイル** → **接続プロファイル** タブで **+** をクリックします。
2. **新規接続プロファイル** ページで以下を入力します。
3. **プロファイル名と説明** エリアで、次の手順を実行します。
   a. プロファイル 下で **プロファイル名**、およびオプションで **説明** を入力します。
   b. 関連ホスト の下で、この接続プロファイルと関連付ける 1 つまたは複数のホストを選択します。このオプションを使用すると、1 台または複数のホストに対して 1 つの接続プロファイルを作成できます。
   c. **次へ** をクリックします。
   d. **iDRAC 資格情報** ページで、次の手順を行います。
      - iDRAC アカウントには、ファームウェアのアップデート、ハードウェアプロファイルの適用、およびハイパーバイザの展開に管理者権限が必要です。
      - **Active Directory ユーザー名** テキストボックスに、ユーザー名を入力します。ユーザー名は、ドメイン\ユーザー名またはユーザー名@ドメインのいずれかの形式で入力してください。ユーザー名は 256 文字に制限されています。ユーザー名の制限については、Microsoft Active Directory マニュアルを参照してください。
      - **Active Directory パスワード** テキストボックスにパスワードを入力します。パスワードは 127 文字に制限されています。
      - **パスワードの確認** テキストボックスにパスワードを再度入力します。
      - 次のアクションを実行します。
        – iDRAC 証明書をダウンロードおよび保存して、今後すべての接続でその証明書の検証を行うには、**証明書チェック** 有効化ドロップダウンを選択します。
        – 証明書をチェックせず、保存しない場合は、**証明書のチェック** を選択しないでください。
   e. **ホストルート** ページで、次の手順を実行します。

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

  Active Directory ユーザー名 テキストボックスに、ユーザー名を入力します。ユーザー名は、ドメイン\ユーザー名またはユーザー名@ドメインのいずれかの形式で入力してください。ユーザー名は 256 文字に制限されています。ユーザー名の制限については、Microsoft Active Directory マニュアルを参照してください。
- **Active Directory パスワード** テキストボックスにパスワードを入力します。パスワードは 127 文字に制限されています。
- **パスワードの確認** テキストボックスにパスワードを再度入力します。
- 次のいずれかの手順を実行します。
  - 今後の接続すべてにおいてホスト証明書をダウンロードおよび保存し、証明書の検証を行うには、 ボックスを選択します。
  - ホストの証明書をチェックせず、保存しない場合は、**証明書チェックを有効にする** ボックスを選択しないでください。
- Active Directory なしでホスト資格情報を設定するには、次のいずれかを行います。
- **ユーザー名** テキストボックスでのユーザー名は root です。このユーザー名はデフォルトで、変更することはできません。
- Active Directory が設定されている場合、root のみではなく、どの Active Directory ユーザーでも選択できます。
- **パスワード** テキストボックスにパスワードを入力します。パスワードは 127 文字に制限されています。

  メモ: OMSA の資格情報は、ESXi ホストに使われる資格情報と同じです。
- **パスワードの確認** テキストボックスにパスワードを再度入力します。
- **証明書チェックを有効にする** チェックボックスで、次のいずれかを選択します。
- ホスト証明書をダウンロードおよび保存して、今後すべての接続でその証明書の検証を行うには、**証明書チェックを有効にする** チェックボックスを選択します。
- ホストの証明書をチェックせず、保存しない場合は、**証明書のチェックを有効にする** チェックボックスを選択しないでください。

4. **次へ** をクリックします。
5. 関連ホスト ページで、接続プロファイル用のホストを 1 つまたは複数選択し、**OK** をクリックします。
6. 接続プロファイルをテストするには、1 つ、または複数のホストを選択し、接続のテストボタンを選択します。この手順はオプションです。これはホストおよび iDRAC の資格情報が正しいかどうかをチェックするために使用します。
7. プロファイルを完了するには、**次へ** をクリックします。iDRAC Express または Enterprise カードがないサーバーでは、iDRAC テスト接続結果は、このシステムには該当なしと表示されます。

接続プロファイルの編集

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

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

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

1. OpenManage Integration for VMware vCenter の **管理 → プロファイル → 資格情報プロファイル → 接続プロファイル** タブで、接続プロファイルを選択します。
2. **編集** アイコンをクリックします。
3. ようこそ タブの接続プロファイルウィンドウで情報を読み、**次へ** をクリックします。
4. 名前と資格情報 タブで、次の手順を行います。
   a. プロファイルの下で **プロファイル名** とオプションで **説明** をタイプします。
   b. vCenter の下で、この接続プロファイルの関連ホストを確認します。ここに表示されるホストが見える理由については、前記の注記を参照してください。
   c. iDRAC 資格情報で、次の手順を行います。
      - ユーザー名はルートで、このエントリは **Active Directory** を選択しない場合は変更できません。iDRAC ユーザーがルート資格情報を使用することは強制ではないため、**Active Directory** が設定されている場合は、Administrator 権限を持つどのユーザーでも使用可能です。
      - Domain\Username：ユーザー名を、ドメイン\ユーザー名、または ドメイン@ユーザー名、のいずれかの形式でタイプします。
        - 次の文字、/（スラッシュ）、&、\（バックスラッシュ）、.（ピリオド）、"（引用符）、@、%（パーセント）を、ユーザー名に使用することができます（最大 127 文字）。
        - ドメインには英数字および -（ダッシュ）、.（ピリオド）のみを使用できます（最大 254 文字）。ドメインの最初と最後の文字は必ず英数字にしてください。
      - パスワード：自分のパスワードをタイプします。

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

        メモ: Active Directory を使用する場合は、**有効にする**を選択する必要があります。
   d. ホストルートで、次の手順を実行します。
      - **Active Directory を使用する** チェックボックスを選択して、アクティブディレクトリに関連付けられたすべてのコンソールにアクセスします。

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

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

チェックを有効にする を選択するか、**証明書のチェックを有効にする** チェックボックスをクリアして証明書のチェックを実行せず証明書を保存しないようにします。

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

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

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

5. **次へ** をクリックします。
6. ホストの選択 ダイアログボックスで、この接続プロファイルのホストを選択します。
7. **OK** をクリックします。
8. 関連ホスト タブで、選択したサーバー上の iDRAC とホストの資格情報をテストできます。次の手順で行います。
   - テストを開始するには、チェックを行うホストを選択し、**テスト接続** アイコンをクリックします。その他のオプションは非アクティブです。
     テストが完了したら、**完了** をクリックします。
   - テストを停止させるには **すべてのテストを中止** をクリックします。テストを中止 ダイアログボックスで **OK** をクリックし、**完了** をクリックします。

接続プロファイルの更新

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

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

接続プロファイルの削除

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

接続プロファイルのテスト

1. OpenManage Integration for VMware vCenter の **管理 → プロファイル → 資格情報プロファイル → 接続プロファイル** タブで、テストする接続プロファイルを選択します。この処置は完了するまで数分かかる場合があります。
2. 接続プロファイルのテスト ダイアログで、テストするホストを選択し、**テスト接続** アイコンをクリックします。
3. 選択したすべてのテストを中止してテストをキャンセルするには、**すべてのテストを中止** をクリックします。テストの中止ダイアログボックスで **OK** をクリックします。
4. 終了するには、**キャンセル**をクリックします。

シャーシプロファイルの作成

OMIVV は OMIVV によって管理されている Dell サーバーに関連付けられたすべての Dell シャーシサーバーを監視できます。シャーシの監視にはシャーシプロファイルが必要です。シャーシ資格情報プロファイルを作成して、単一または複数シャーシと関連付けることができます。シャーシプロファイルは、次の手順を使用して作成されます。

1. **OpenManage Integration for VMware vCenter** で、**管理 → プロファイル → 資格情報プロファイル → シャーシプロファイル** と選択します。
2. **シャーシプロファイル** ページで、**プラス（+）** アイコンをクリックして **新しいシャーシプロファイル** を作成します。
3. **シャーシプロファイルウィザード** ページで、次の手順を実行します。
   a. **プロファイル名** テキストボックスに、プロファイル名を入力します。
   b. **説明** テキストボックスに、オプションで説明を入力します。
4. **資格情報** で、次の手順を行います。
   a. **ユーザー名** テキストボックスに管理者権限のあるユーザー名を入力します。これはシャーシ管理コントローラへのログオンに通常使用されるものです。
   b. **パスワード** テキストボックスに対応するユーザー名のパスワードを入力します。
   c. **パスワードの確認** テキストボックスに、**パスワード** テキストボックスに入力したものと同じパスワードを入力します。パスワードは一致する必要があります。

   メモ: 資格情報は、ローカルまたは Active Directory のものを使用できます。シャーシプロファイルに Active Directory 資格情報を使用する前に、Active Directory に Active Directory ユーザーアカウントが存在している必要があり、シャーシ管理コントローラが Active Directory ベースの認証に対して設定されている必要があります。
5. **次へ** をクリックします。

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

   メモ: シャーシが検出され、任意のモジュラーホストの正常なインベントリ実行がそのシャーシに認められた後に初めてシャーシプロファイルに関連付けることができます。
6. 個々のシャーシまたは複数のシャーシのどちらかを選択するには、**IP/ ホスト名** 列の横にある対応するチェックボックスを選択します。

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

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

   関連付けられたシャーシ ページが表示されます。
8. シャーシを選択し、**接続テスト** アイコンをクリックしてシャーシの接続性をテストします。これによって、資格情報が検証され、その結果が **テスト結果** 列に **合格** または **失敗** として表示されます。
9. **終了** をクリックしてプロファイルを完了します。

   メモ: 関連するシャーシ ページの左上隅に表示されているプラスアイコンをクリックして、シャーシを追加または削除することもできます。

シャーシプロファイルの表示

シャーシプロファイルを表示するには、次の手順を実行します。

1. **OpenManage Integration for VMware vCenter** で、**管理 → プロファイル → 資格情報プロファイル → シャーシプロファイル**ウィンドウと選択します。シャーシプロファイルが表示されます。
2. シャーシプロファイルに複数のシャーシが関連付けられている場合は、矢印アイコンをクリックすると、関連するすべてのシャーシが表示されます。
3. **シャーシビュー** ページでは、プロファイル名、説明、シャーシ IP、サービスタグ、およびシャーシを変更した日付を表示することができます。
4. **シャーシビュー** ページでは、次の処置を実行できます。
   a. 追加
   b. 編集
   c. 削除
   d. 接続性のテスト

シャーシプロファイルの編集

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

1. OpenManage Integration for VMware vCenter の **管理 → プロファイル → 資格情報プロファイル → シャーシプロファイル** タブで、シャーシプロファイルを選択します。
2. 斜めの **Pencil** アイコンとして表示される、メインメニューの **編集** アイコンをクリックします。
3. **シャーシプロファイルの編集** ウィンドウが表示されます。
4. **シャーシプロファイル** エリアでは、**プロファイル名** およびオプションの **説明** を編集することができます。
5. **資格情報** の領域で、**ユーザー名**、 **パスワード**、および **パスワードの確認** 編集することができます。**パスワードの確認** に入力するパスワードは、**パスワード** フィールドに入力したものと同じである必要があります。 入力した資格情報は、シャーシの管理者権限を持っている必要があります。
6. **適用** をクリックします。変更が保存されます。
7. **関連シャーシ** タブでは、選択したシャーシ上でシャーシと資格情報をテストできます。次のいずれかを行います。
   - テストを開始するには、チェックするひとつ、または複数のシャーシを選択して、**テスト接続** をクリックします。**テスト結果** 列に、テスト接続が正常に行われたかどうかが表示されます。
   - **プラス** アイコンをクリックすることによって、ひとつ、または複数のシャーシをシャーシプロファイルに追加または削除することができます。

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

シャーシプロファイルの削除

シャーシプロファイルを削除するには、次の手順を実行します。

1. **OpenManage Integration** で、**管理 → プロファイル → 資格情報プロファイル → シャーシプロファイル** ウィンドウと選択します。
2. 削除するシャーシプロファイルを選択し、**X** アイコンをクリックします。警告メッセージが表示されます。

3. **はい** をクリックして削除を続行するか、**いいえ** をクリックして削除をキャンセルします。

   メモ: シャーシプロファイルに関連付けられているすべてのシャーシの選択が解除されている、または別のプロファイルに移動されている場合は、そのシャーシプロファイルに関連付けられているシャーシがなく、削除されることが記載された削除確認メッセージが表示されます。OK をクリックしてシャーシプロファイルを削除します。

シャーシプロファイルのテスト

1. OpenManage Integration for VMware vCenter の **管理 → プロファイル → 資格情報プロファイル → シャーシプロファイル** タブで、テストする単一または複数のシャーシプロファイルを選択します。この処置は完了するまで数分かかる場合があります。
2. シャーシプロファイルのテストダイアログで,テストするホストを選択してから、**テスト接続** アイコンをクリックします。
3. 選択したすべてのテストを中止してテストをキャンセルするには、**すべてのテストを中止** をクリックします。テストの中止ダイアログボックスで **OK** をクリックします。
4. 終了するには、**キャンセル**をクリックします。

5

ジョブキュー

OpenManage Integration for VMware vCenter の設定後、監視 タブの下に表示されるインベントリ、保証ジョブ、およびファームウェアアップデートを監視することができます。インベントリおよび保証は、設定ウィザードまたは設定タブから設定します。

- インベントリ履歴
- 保証履歴

インベントリ履歴

インベントリジョブのセットアップは、設定タブまたは初期設定ウィザードを使用して行います。インベントリ履歴 タブを使用して、インベントリジョブを表示します。このタブで実行可能なタスクには、次のタスクがあります。

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

ホストインベントリの表示

データを収集するには、インベントリが正常に終了している必要があります。インベントリが完了すると、データセンター全体または個別のホストシステムに関するインベントリ結果を表示することができます。行の表示順は、昇順または降順で並べ替えることができます。

サーバーデータの検索と表示ができない場合、いくつかの原因が考えられます。

- サーバーに接続プロファイルが関連付けられていないため、インベントリジョブを実行できない。
- データを収集するインベントリジョブがサーバーで実行されていないので、表示できるデータがない。
- ホストライセンス数が超過しており、インベントリタスクを完了するには使用可能な追加ライセンスが必要。
- このサーバーには、Dell PowerEdge サーバーの第 12 世代以降に必要な正しい iDRAC ライセンスがないことから、正しい iDRAC ライセンスを購入する必要があります。
- 資格情報が誤っている可能性がある。
- ターゲットが到達不能である可能性がある。

ホストインベントリの詳細を表示するには、次の手順を実行します。

1. OpenManage Integration for VMware vCenter で **監視** タブをクリックします。
2. **ジョブキュー → インベントリ履歴 → ホストインベントリ** とクリックします。

3. 選択した vCenter でサーバー情報を表示するには、表示させる vCenter を選択して関連するすべてのホストの詳細を表示します。
4. ホストインベントリ情報を確認します。

vCenter 詳細	
vCenter	vCenter アドレスを表示します。
ホスト合格	合格したホストを表示します。
次のインベントリ	実行がスケジュールされている次のホストを表示します。
最新のインベントリ	実行された前のインベントリスケジュールを表示します。
ホスト	
ホスト	ホストのアドレスを表示します。
ステータス	状態を表示します。次の状態があります。 • 成功 • 失敗 • 進行中 • スケジュール済み
継続時間（MM:SS）	ジョブの継続時間を分と秒で表示します。
開始日時	インベントリスケジュールが開始した日付と時刻を表示します。
終了日時	インベントリスケジュールが終了した時刻を表示します。

インベントリジョブスケジュールの変更

最新のサーバ情報を確保しておくためには、Dell サーバで定期的にインベントリを実行する必要があります。デルでは、インベントリを週に 1 回実行することをお勧めします。インベントリはホストのパフォーマンスには影響しません。インベントリジョブスケジュールは、**監視 → ジョブキュー → インベントリ履歴 → ホストインベントリ** ページ、または **最初の設定ウィザード** ページから変更することができます。

1. OpenManage Integration for VMware vCenter の **監視 → ジョブキュー** タブで、**インベントリ履歴 → ホストインベントリ** をクリックします。
2. vCenter を選択し、**スケジュールの変更** アイコンをクリックします。
3. インベントリデータの取得 ダイアログボックスで、次の手順を行います。
   a. インベントリデータ の下にある **インベントリデータ取得の有効化** チェックボックスを選択します。
   b. インベントリデータの取得スケジュール の下からジョブを実行する曜日を選択します。
   c. インベントリデータの取得時間 テキストボックスで、このジョブに対するローカル時刻を入力します。

      ジョブ設定時間とジョブ実装時間の時間差を考慮する必要がある場合があります。
4. **適用** をクリックすると設定が保存、**クリア** をクリックすると設定がリセット、**キャンセル** をクリックすると動作が中止されます。

インベントリジョブを今すぐ実行する

これを実行して、選択した VCenter に対するインベントリタスクを直ちにトリガします。

1. OpenManage Integration for VMware vCenter の**監視** → **ジョブキュー** タブで、**インベントリ履歴** → **ホストインベントリ**をクリックします。
2. **今すぐ実行** ボタンをクリックします。
3. 成功 ダイアログボックスで **閉じる** をクリックします。

   メモ: モジュラーホストのインベントリを実行すると、対応するシャーシが自動的に検出されます。

   これでインベントリジョブがキューに入ります。単一ホストに対するインベントリは実行できないことに注意してください。インベントリジョブがすべてのホストに対してジョブを開始します。

シャーシのインベントリのジョブを今すぐ実行する

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

1. OpenManage Integration for VMware vCenter の**監視** → **ジョブキュー**タブで、**インベントリ履歴** → **シャーシインベントリ** をクリックします。
2. 最後のインベントリの実行でインベントリが行われたシャーシとステータスのリストが表示されます。

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

保証履歴

ハードウェア保証情報は Dell Online から取得され、OpenManage Integration for VMware vCenter によって表示されます。サーバーについての保証情報の収集には、サーバーのサービスタグが使用されます。保証データ取得ジョブは、設定ウィザードを使用してセットアップされます。保証ジョブ履歴は、このタブで表示します。このタブでは、次のタスクを行うことができます。

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

保証履歴の表示

保証ジョブは、すべてのシステムに関する保証情報を support.dell.com から取得するスケジュールされたタスクです。列は昇順または降順で並べ替えできます。

1. OpenManage Integration for VMware vCenter で **監視** タブをクリックします。
2. **ジョブキュー** → **保証履歴** をクリックします。
3. 保証履歴を拡張して、**ホストの保証** および **シャーシの保証** を表示します。
4. **ホストの保証** または **シャーシの保証** のいずれかを選択して、対応する保証ジョブ履歴情報を表示します。

vCenter 履歴

vCenters	vCenters のリストを表示します。
ホスト合格	合格した vCenter ホスト数を表示します。
前の保証	実行された前の保証ジョブを表示します。
次の保証	次に実行される保証ジョブを表示します。
スケジュールの変更ボタン	クリックして保証ジョブスケジュールを編集します。
今すぐ実行 ボタン	クリックして保証取得ジョブを実行します。

ホストの履歴

ホスト	ホストのアドレスを表示します。
ステータス	状態を表示します。次の状態があります。 • 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を MM:SS 単位で表示します。
開始日時	保証ジョブが開始した日付と時刻を表示します。
終了日時	保証ジョブが終了した時刻を表示します。

シャーシ履歴

シャーシ IP	シャーシ IP アドレスを表示します。
サービスタグ	シャーシのサービスタグを表示します。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を表示します。
継続時間（MM:SS）	保証ジョブの継続時間を MM:SS 単位で表示します。
開始日時	保証ジョブが開始した日付と時刻を表示します。
終了日時	保証ジョブが終了した時刻を表示します。

保証ジョブスケジュールの変更

保証ジョブは当初初期設定ウィザードで設定されます。その後、**監視タブ → ジョブキュー → 保証履歴 → ホスト保証** ページ、または **管理タブ → 設定** ページから保証ジョブスケジュールを変更することができます。

1. OpenManage Integration for VMware vCenter の **監視 → ジョブキュー** タブで、**保証履歴** をクリックします。
2. **スケジュールの変更** アイコンをクリックします。
3. 保証データの取得 ダイアログボックスで、次の手順を行います。

a. 保証データ の下にある **保証データの取得を有効化** チェックボックスを選択します。
b. 保証データの取得スケジュール の下からジョブを実行する曜日を選択します。
c. 保証データの取得時間 テキストボックスで、このジョブを実行するローカル時刻を入力します。
このジョブを正しい時刻に実行するために、時差を計算する必要がある場合があります。

4. **適用** をクリックします。

保証ジョブを今すぐ実行する

保証ジョブは、最低でも週に 1 回実行してください。

1. OpenManage Integration for VMware vCenter の **監視 → ジョブキュー** タブ。
2. **保証に関する履歴** および **ホストの保証** をクリックして、実行する保証ジョブを選択します。
3. **今すぐ実行** ボタンをクリックします。
4. 成功 ダイアログボックスで **閉じる** をクリックします。

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

これで、保証ジョブがキューに入ります。

シャーシ保証ジョブを今すぐ実行する

保証ジョブは、最低でも週に 1 回実行してください。

1. OpenManage Integration for VMware vCenter の **監視 → ジョブキュー** タブ。
2. **保証に関する履歴** および **シャーシの保証** をクリックして、実行する保証ジョブを選択します。
3. **今すぐ実行** ボタンをクリックします。
4. 成功 ダイアログボックスで **閉じる** をクリックします。
これで、保証ジョブがキューに入ります。

ログ

OpenManage Integration for VMware vCenter の **監視 → ログ** タブで、ユーザーアクションを表示することができます。

このページの内容は、2 つのドロップダウンリストを使用して並べ替えることができます。最初のドロップダウンリストで、次の項目を含むファイルのカテゴリで並べ替えることができます。

- すべてのカテゴリ
- 情報
- 警告
- エラー

2 つめのドロップダウンリストで、次のような時間のブロックごとに並べ替えます。

- 過去 1 週間
- 過去 1 か月

- 過去 1 年間
- カスタム範囲

  カスタム範囲を選択した場合、開始日および終了日を選択して、適用 をクリックします。

行のヘッダーをクリックして、データグリッドの行を昇順または降順に並べ替えることもできます。

フィルタ テキストボックスを使用して、内容を検索します。

ページのグリッドの下に、次の情報が表示されます。

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

ログの表示

1. OpenManage Integration for VMware vCenter で **監視** タブをクリックします。
2. ログタブで、OpenManage Integration for VMware vCenter のユーザーアクションログを表示します。ログページには、次の内容が表示されます。

すべてのカテゴリ	次のログタイプに基いて、ログをフィルタおよび表示することができます。 • すべてのカテゴリ • 情報 • 警告 • エラー
日付フィルタ	次の条件に基いて、ログをフィルタおよび表示することができます。 • 過去 1 週間 • 過去 1 か月 • 過去 1 年間 • カスタム範囲 特定の日付に基づいて日付をフィルタするには、日付フィルタ ドロップダウンリストから **カスタム範囲** を選択し、フィルタする必要がある対象に基づいて **開始日** と **終了日** を入力してから、**適用** をクリックします。
Search（検索）	ログの説明またはログに含まれる特定のテキストに基づいてフィルタすることができます。

表 2. グリッド表の詳細

カテゴリ	カテゴリのタイプが表示されます。
日付と時刻	ユーザーアクションの日付と時刻が表示されます。
説明	ユーザーアクションの説明が表示されます。

3. グリッド内のデータを並べ替えるには、行のヘッダーをクリックします。
4. カテゴリまたは時間ブロックを使用して並べ替えるには、グリッド上部のドロップダウンリストを使用します。
5. ログアイテムのページ間の移動には、前へおよび次へボタンを使用します。

ログファイルのエクスポート

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

1. OpenManage Integration for VMware vCenter で **監視** タブをクリックします。
2. CSV 形式のログファイルをエクスポートするには、画面右下角で、**すべてをエクスポート** アイコンをクリックします。
3. **ダウンロードする場所の選択** ダイアログボックスを選択し、ログ情報の保存先の場所を参照します。
4. **ファイル名** テキストボックスで、デフォルトのファイル名の ExportList.csv を承諾するか、.CSV 拡張子の独自のファイル名を入力します。
5. **保存** をクリックします。

6

コンソール管理

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

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

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

管理コンソールの使用

管理コンソールの vCenter 登録ウィンドウからは、vCenter サーバーを登録したり、ライセンスをアップロードまたは購入することができます。デモライセンスをお使いの場合は、ソフトウェアの購入リンクが表示され、このリンクから複数ホストを管理するための完全バージョンライセンスを購入することができます。このセクションでは、サーバーの変更、アップデート、および登録解除を行うこともできます。

関連タスク:

- 必要な権限を持つ Administrator 以外のユーザーによる vCenter サーバの登録
- vCenter サーバーの登録
  - vCenter ログインの変更
  - 登録済み vCenter 用の SSL 証明のアップデート
  - vCenter からの OpenManage Integration for VMware vCenter のアンインストール
- OpenManage Integration for VMware vCenter ライセンスのアップロード

必要な権限を持つ Administrator 以外のユーザーによる vCenter サーバの登録

vCenter サーバの vCenter 管理者資格情報または必要な権限を持つ Administrator 以外のユーザーで、OMIVV アプライアンス用の vCenter サーバを登録できます。

必要な権限を持つユーザーを有効にして vCenter サーバーを登録するには、次のステップを実行します。

1. 役割を追加し、その役割に必要な権限を選択するか、既存の役割を変更して、その役割について選択した権限を変更します。vSphere ウェブクライアントで役割を作成または変更し、権限を選択するために必要なステップについては、VMware vSphere のマニュアルを参照してください。役割に対応する必要なすべての権限を選択する場合については、「権限の定義」を参照してください。

   メモ: vCenter の管理者が役割を追加または変更する必要があります。

2. 役割を定義し、その役割の権限を選択したら、ユーザーを、新しく作成した役割に割り当てます。vSphere ウェブクライアントでの権限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。以上で、必要な権限のある Administrator 以外の vCenter サーバユーザーが、vCenter の登録および / または vCenter の登録解除、資格情報の変更、資格情報のアップデートができるようになります。

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

3. 必要な権限のある Administrator 以外のユーザーにより vCenter サーバを登録します。「必要な権限を持つ Administrator 以外のユーザーによる vCenter サーバの登録」を参照してください。
4. ステップ 1 で作成または変更した役割にデルの権限を割り当てます。vSphere Web クライアンでの役割へのデルの権限の割り当て を参照してください。

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

権限の定義

vCenter サーバを登録するために必要な権限を持つ Administrator 以外のユーザーを有効にするには、次の権限を選択します。

- アラーム
  - アラームの作成
  - アラームの変更
  - アラームの削除
- 内線番号
  - 拡張子の登録
  - 拡張子の登録解除
  - 拡張子の更新
- Global（グローバル）
  - タスクのキャンセル
  - ログイベント
  - 設定
- Host（ホスト）
  - CIM
    - CIM インタラクション
  - 構成
    - 詳細設定
    - 接続
    - メンテナンス
    - パッチの問い合わせ
    - セキュリティプロファイルとファイアウォール
  - インベントリ
    - クラスタにホストを追加
    - スタンドアロンホストの追加
- ホストプロファイル

  - 編集
  - 表示
- 許可
  - 権限の変更
  - 役割の変更
- セッション
  - セッションの検証
- タスク
  - タスクの作成
  - タスクの更新

メモ: 必要な権限を持つ Administrator 以外のユーザーにより vCenter サーバを登録するとき、指定された権限が割り当てられていない場合はエラーメッセージが表示されます。

必要な権限を持つ Administrator 以外のユーザーによる vCenter サーバの登録

必要な権限を持つ Administrator 以外のユーザーで OMIVV アプライアンス用に vCenter サーバを登録できます。vCenter サーバ登録の詳細については、「vCenter サーバーの登録」を参照してください。

vSphere Web クライアンでの役割へのデルの権限の割り当て

既存の役割を編集し、デルの権限を割り当てることができます。

メモ: 管理者権限のあるユーザーとしてログインしていることを確認します。

既存の役割にデルの権限を割り当てるには、次の手順を実行します。

1. 管理者権限を持つ vSphere Web Client にログインします。
2. vSphere Web Client で **管理** → **役割マネージャ** の順に移動します。
3. ドロップダウンメニューから、vCenter サーバーシステムを選択します。
4. 役割を選択し、**役割アクションの編集** をクリックします。
5. 次の権限を選択し、**OK** をクリックします。
   - Dell
     - Dell.Configuration
     - Dell.Deploy — プロビジョニング
     - Dell.Inventory
     - Dell.Monitoring
     - Dell.Reporting

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

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

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

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

vCenter サーバーの登録

OpenManage Integration for VMware vCenter のインストール後、OpenManage Integration for VMware vCenter を登録できます。OpenManage Integration for VMware vCenter は、管理者ユーザーアカウントまたは vCenter の操作を実行するために必要な権限のある Administrator 以外のユーザーアカウントを使用します。OpenManage Integration for VMware vCenter は現在、OMIVV アプライアンスあたり 10 台の vCenter をサポートしており、この台数は後で変更できます。

1. サポートされているブラウザから、**管理コンソール** を開きます。
2. 新しい vCenter サーバを登録するには、左ペインで **VCENTER 登録** をクリックし、**新規 vCenter サーバの登録** をクリックします。
3. **新規 vCenter の登録**ダイアログボックスの **vCenter 名**で次を行います。
   a. **vCenter サーバ IP またはホスト名** テキストボックスに vCenter IP アドレスまたはホストの FQDN を入力します。

      メモ: 完全修飾ドメイン名（FQDN）を使用して VMware vCenter で OMIVV を登録することを強くお勧めします。すべての登録で、vCenter のホスト名は、DNS サーバにより適切に解決できる必要があります。次に DNS サーバを使用するための推奨手順を示します。

      - 有効な DNS 登録で OMIVV アプライアンスを展開するときは、静的 IP アドレスとホスト名を割り当てます。静的 IP アドレスにより、システムの再起動中に、OMIVV アプライアンスの IP アドレスが同じまま留まります。
      - OMIVV のホスト名エントリが前方ルックアップと逆引きルックアップの両方にあることを確認します。

   b. **説明** テキストボックスに、オプションで説明を入力します。
4. **vCenter ユーザーアカウント**で、次を行います。
   a. **vCenter ユーザー名** テキストボックスに、Administrator のユーザー名または必要な権限のある Administrator 以外のユーザー名を入力します。
   b. **Password**（パスワード）テキストボックスにパスワードを入力します。
   c. **パスワードの確認** テキストボックスにパスワードを再度入力します。
5. **Register**（登録）をクリックします。

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

例：必要な権限を持つユーザー X が vCenter に OMIVV を登録し、ユーザー Y にはデルの権限のみがあるとします。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ホストを再起動します。

OpenManage Integration for VMware vCenter 要件

OpenManage Integration for VMware vCenter（OMIVV）は古い世代のサーバ上の OpenManage からの情報を必要とし、より新しいプラットフォームは、新しいチップセットを理解する vSphere のバージョンで起動するように制限されています。これにより、OMIVV の所定のバージョンと連動する vSphere のバージョンが制限されます。

表 3. 管理対象ホスト上のサポートされている ESXi バージョン

ESXi バージョンサポート	サーバの世代		
	第 11 世代	12 G	第 13 世代
v5.0	Y	Y	N
v5.0 U1	Y	Y	N
v5.0 U2	Y	Y	N
v5.0 U3	Y	Y	N
v5.1	Y	Y	N
v5.1 U1	Y	Y	N
v5.1 U2	Y	Y	Y
v5.1 U3	N	Y	Y （FC830、M830、および FC430 を除く）
v5.5	Y	Y	N
v5.5 U1	Y	Y	N
v5.5 U2	Y	Y	Y
v5.5 U3	Y	Y	Y
v6.0	Y	Y	Y
v6.0 U1	Y	Y	Y

表 4. リリース 3.1 向けにサポートされている vCenter Server バージョン

vCenter バージョン	Desktop Client サポート	ウェブクライアントサポート
v5.1 U2	Y	N
v5.1 U3	Y	N
v5.5 U1	Y	Y
v5.5 U2	Y	Y
v5.5 U3	Y	Y
v6.0	Y	Y

vCenter バージョン	Desktop Client サポート	ウェブクライアントサポート
v6.0 U1	Y	Y

vCenter ログインの変更

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

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

メモ: 必要な権限が割り当てられていない Administrator 以外のユーザーが vCenter ログイン資格情報を変更しようとすると、エラーメッセージが表示されます。

登録された vCenter サーバーの SSL 証明書のアップデート

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

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

1. ウェブブラウザを起動して https://<ApplianceIPAdrdress> と入力します。
2. 左側のペインで **VCENTER の登録** をクリックします。登録されている vCenter が右側のペインに表示されます。証明書をアップデートするには、**アップデート** をクリックします。

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

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

1. ウェブブラウザを起動し、https://<ApplianceIPAdrdress> を入力します。
2. **vCenter 登録** ページの vCenter サーバー表の下で、**登録解除** をクリックして OpenManage Integration for VMware vCenter の登録を解除します。

   vCenter が複数存在する場合があるので、正しい vCenter を選択するようにしてください。
3. 登録の取り消しを確認する **vCenter の登録解除** ダイアログボックスで **登録解除** をクリックします。

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

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

   メモ: ライセンスファイルが変更されたり、何らかの形で編集された場合、アプライアンスはそれが破損されているとみなし、ファイルは機能しなくなります。

   メモ: ホストをさらに追加する必要がある場合は、ライセンスを追加できます。上記プロセスに従ってライセンスを追加してください。

   メモ: インベントリ実施に成功した 13 世代、第 12 世代、および第 11 世代サーバーの数と、購入したライセンスの数が等しい場合、数が少ない 11 世代、12 世代、および 13 世代サーバーを削除することにより、既存の接続プロファイルを編集します。削除した 11 世代、12 世代、および 13 世代サーバー用に新しい接続プロファイルを作成します。

仮想アプライアンス管理

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

- 仮想アプライアンスの再起動
- 仮想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
- トラブルシューティングバンドルのダウンロード
- NTP サーバーのセットアップ
- HTTPS 証明書のアップロード

仮想アプライアンスの再スタート

仮想アプライアンスを再起動させるとユーザーは管理コンソールからログアウトされ、OpenManage Integration for VMware vCenter は、仮想アプライアンスとそのサービスがアクティブになるまで使用できなくなります。

1. OpenManage Integration for VMware vCenter の管理コンソール下のリンクから管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 左ペインで **アプライアンス管理** をクリックします。
4. OpenManage Integration for VMware vCenter を再起動するには、**仮想アプライアンスの再起動** をクリックします。
5. **仮想アプライアンスの再スタート** ダイアログボックスで、仮想アプライアンスを再スタートするには **適用** をクリックするか、または **キャンセル** をクリックして取り消します。

リポジトリの場所と仮想アプライアンスのアップデート

仮想アプライアンスのアップデート前にバックアップを実行し、すべてのデータを保護します。「バックアップと復元の管理」を参照してください。

1. OpenManage Integration for VMware vCenter の管理コンソール下のリンクから管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 左ペインで **アプライアンス管理** をクリックします。
4. アプライアンスのアップデートの横の **編集** をクリックします。
5. **アプライアンスアップデート** ウィンドウに **リポジトリの場所の URL** を入力し、**適用** をクリックします。

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

仮想アプライアンスソフトウェアのアップデート

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

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

トラブルシューティングバンドルのダウンロード

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

1. ウェブブラウザを起動して https://<ApplianceIPAddress> と入力します。
2. 左ペインで **アプライアンス管理** をクリックします。
3. トラブルシューティングバンドルのダイアログボックスを生成するには、**トラブルシューティングバンドルの作成** をクリックします。
4. **トラブルシューティングバンドルのダウンロード** リンクをクリックします。
5. 終了するには、**閉じる**をクリックします。

HTTP プロキシの設定

管理コンソールを使用して、HTTP プロキシを設定できます。

1. OpenManage Integration for VMware vCenter の管理コンソールの下で、リンクを使って管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 左ペインで **アプライアンス管理** をクリックします。
4. **アプライアンス管理** ページで **HTTP プロキシ設定** にスクロールダウンし、**編集** をクリックします。

5. **編集** ページでは以下を行います。
   a. HTTP プロキシ設定の使用を有効化するには、**HTTP プロキシ設定を使用** の横の **有効** を選択します。
   b. **プロキシサーバーのアドレス** テキストボックスにプロキシサーバーアドレスを入力します。
   c. **プロキシサーバーポート** テキストボックスにプロキシサーバーポートを入力します。
   d. プロキシ資格情報を使用するには、**プロキシ資格情報を使用する** の横で **はい** を選択します。
   e. 資格情報を使用している場合、**ユーザー名** テキストボックスにユーザー名を入力します。
   f. **パスワード** テキストボックスにパスワードを入力します。
6. **適用** をクリックします。

NTP サーバーの設定

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

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

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

証明書署名要求の生成

メモ: OpenManage Integration for VMware vCenter を vCenter に登録する前に、証明書をアップロードする必要があります。

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

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

HTTPS 証明書のアップロード

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

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

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

メモ: 証明書は、PEM フォーマットを使用する必要があります。

デフォルト HTTPS 証明書の復元

メモ: お使いのアプライアンス向けにカスタム証明書をアップロードする場合は、vCenter 登録前に新しい証明書をアップロードする必要があります。vCenter 登録後に新しいカスタム証明書をアップロードすると、Web Client に通信エラーが表示されます。この問題を修正するには、vCenter 登録を解除してから登録する必要があります。

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

グローバルアラートの設定

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

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

バックアップおよび復元の管理

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

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

バックアップおよび復元の設定

バックアップおよび復元機能は、OpenManage Integration for VMware vCenter データベースをリモートロケーションにバックアップし、そのバックアップは後で復元することができます。このバックアップには、プロファイル、テンプレートおよびホスト情報が含まれます。データ喪失に備えるため、自動バックアップをスケジュールすることを推奨します。この手順の後は、バックアップスケジュールを設定する必要があります。

メモ: NTP の設定は保存および復元されません。

1. OpenManage Integration for VMware vCenter の 管理コンソール 下で、リンクを使って管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 左ペインで、**バックアップと復元**をクリックします。
4. 現在のバックアップと復元設定を編集するには、**編集**をクリックします。
5. **設定と詳細**ページで、以下を行います。
   a. **バックアップの場所**テキストボックスにバックアップファイルへのパスをタイプします。
   b. **ユーザー名**テキストボックスにユーザー名をタイプします。
   c. **パスワード**テキストボックスにパスワードをタイプします。
   d. **バックアップを暗号化するために使用するパスワード**の下のテキストボックスに、暗号化パスワードをタイプします。

      暗号化パスワードには、英数字および次の特殊文字を使用できます : !@#$%*。長さの制限はありません。
   e. **パスワードの確認**テキストボックスに暗号化パスワードを再度入力します。
6. これらの設定を保存するには、**適用**をクリックします。
7. バックアップスケジュールを設定します。詳細は、「自動バックアップのスケジュール」を参照してください。

自動バックアップのスケジュール

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

自動バックアップのスケジュールには、以下を行います。

1. OpenManage Integration for VMware vCenter の管理コンソール下のリンクから管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 左ペインで **バックアップと復元** をクリックします。
4. バックアップおよび復元の設定を編集するには、**編集 自動バックアップスケジュール** をクリックします（これによってフィールドがアクティブになります）。
5. バックアップを有効化するには、**有効** をクリックします。
6. バックアップを実行したい曜日のチェックボックスを選択します。
7. **バックアップ時刻（24 時間フォーマット、HH:mm）** テキストボックスに時刻を HH:mm フォーマットで入力します。

次のバックアップ に次にスケジュールされたバックアップの日付と時刻が表示されます。

8. **適用** をクリックします。

即時のバックアップの実行

1. OpenManage Integration for VMware vCenter の管理コンソール下のリンクから管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 左ペインで **バックアップと復元** をクリックします。
4. **今すぐバックアップ** をクリックします。
5. バックアップ設定からロケーションと暗号化パスワードを使用するには、**今すぐバックアップ** ダイアログボックスでそのチェックボックスを選択します。
6. **バックアップの場所**、**ユーザー名**、**パスワード**、および**暗号化パスワード** を入力します。
   暗号化パスワードには、英数字および次の特殊文字を使用できます：!@#$%*。長さの制限はありません。
7. **バックアップ** をクリックします。

バックアップからのデータベースの復元

メモ: 復元の操作では、作業完了後、仮想アプライアンスを再起動させます。

1. OpenManage Integration for VMware vCenter の管理コンソール下のリンクから管理コンソールを開きます。
2. ログイン ダイアログボックスにパスワードを入力します。
3. 左ペインで **バックアップおよび復元** をクリックすると、現在のバックアップおよび復元設定が表示されます。
4. **今すぐ復元** をクリックします。
5. 「今すぐ復元」のダイアログボックスで、**backup.gz** ファイル （CIFS / NFS フォーマット）と共にファイルの場所を入力します。
6. バックアップファイルの **ユーザー名**、**パスワード** および **暗号化パスワード** を入力します。
   暗号化パスワードには、英数字および次の特殊文字を使用できます：!@#$%*。長さの制限はありません。
7. 変更を保存するには、**適用** をクリックします。
   適用をクリックすると、アプライアンスは再起動または再スタートします。

vSphere Client コンソールについて

vSphere Client コンソール は仮想マシン上の vSphere Client 内にあります。この **コンソール** は管理コンソールと連動しています。コンソールには、次の機能があります。

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

- コンソールからログアウトする
- 読み取り専用ユーザー役割
- OMIVV 3.0 バージョンから現在のバージョンにアップグレードする
- 旧バージョンから、OMIVV 3.1 バージョンに移行

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

ネットワークの設定

ネットワーク設定への変更は、vSphere Client Console で行います。

1. vSphere ウェブクライアントのナビゲータで、**vCenter** を選択します。
2. ナビゲータで、管理する仮想マシンを選択します。
3. 次の手順のいずれか 1 つを実行します。
   - オブジェクト タブで、**アクション → コンソールを開く** を選択します。
   - 選択した仮想マシンを右クリックし、**コンソールを開く** を選択します。
4. **コンソール** ウィンドウで **ネットワークの設定** を選択し、**<ENTER>** を押します。
5. **デバイスの編集** または **DNS の編集** 設定下で望ましいネットワーク設定を入力し、**保存して終了** をクリックします。変更を中止するには、**終了** をクリックします。

仮想アプライアンスパスワードの変更

仮想アプライアンスパスワードは、コンソールを使用して vSphere Web Client で変更します。

1. vSphere Web Client のナビゲータで、**vCenter** を選択します。
2. ナビゲータで、管理する仮想マシンを選択します。
3. 次の手順のいずれか 1 つを実行します。
   - オブジェクト タブで、**アクション → コンソールを開く** を選択します。
   - 選択した仮想マシンを右クリックし、**コンソールを開く** を選択します。
4. コンソールで、矢印キーを使用して **管理パスワードの変更** を選択し、 **<ENTER>** を押します。
5. **現在の管理パスワード** を入力し、**<ENTER>** を押します。
   管理パスワードには、1 つの特殊文字、1 つの数字、1 つの大文字、1 つの小文字を含み、少なくとも 8 文字である必要があります。
6. **新規管理パスワードの入力** で新パスワードを入力し、**<ENTER>** を押します。
7. 新しいパスワードを **管理パスワードを確認してください** テキストボックスに再度入力し、**<ENTER>** を押します。

ローカルタイムゾーンの設定

ローカルタイムゾーンをセットアップするには、次の手順を実行してください。

1. メインの VMware vCenter ウィンドウの コンソール タブをクリックして、管理コンソールを起動します。
2. OMIVV の起動が完了するのを待ち、ユーザー名として admin を入力して **Enter** を押します。
3. 新しい管理者パスワードを入力します。パスワードは、表示されているパスワードの複雑性に関するルールに従って設定する必要があります。**Enter** を押します。

パスワードの確認 ダイアログボックスが表示されます。

4. 以前に提供されたパスワードを入力し、**Enter** を押します。
   パスワード設定の確認 メッセージが表示されます。
5. **Enter** を押して、OMIVV アプライアンスでネットワークおよびタイムゾーン情報を設定します。
6. OpenManage Integration for VMware vCenter のタイムゾーン情報を設定するには、日付 / 時刻プロパティ をクリックしてタイムゾーンと日付を設定します。
7. **日付と時刻** タブで、**ネットワーク上で日付と時間の同期化** を選択します。
   NTP サーバー ウィンドウが表示されます。
8. **タイムゾーン** をクリックして、該当するタイムゾーンを選択し、**OK** をクリックします。

仮想アプライアンスの再起動

仮想アプライアンスを再起動するには、以下を行います。

1. vSphere ウェブクライアントのナビゲータで **vCenter** を選択します。
2. ナビゲータで、管理する仮想マシンを選択します。
3. 次の手順のいずれか 1 つを実行します。
   - オブジェクトタブで、**アクション → コンソールを開く** を選択します。
   - 選択した仮想マシンを右クリックし、**コンソールを開く** を選択します。
4. 矢印キーを使用して **この仮想アプライアンスを再起動** を選択し、**<ENTER>** を押します。
5. 次のメッセージが表示されます。

   ```
   If there are any processes running on this appliance they will be
   terminated by this action. Are you sure you wish to do this?
   ```
6. 再起動するには、**y** を、取り消すには、**n** を入力します。これでアプライアンスは再起動されました。

仮想アプライアンスの工場出荷時設定へのリセット

仮想アプライアンスを工場出荷時設定へリセットするには、以下を行います。

1. vSphere Web Client のナビゲータで、**vCenter** を選択します。
2. ナビゲータで、管理する仮想マシンを選択します。
3. 次の手順のいずれか 1 つを実行します。
   - オブジェクト タブで、**アクション → コンソールを開く** を選択します。
   - 選択した仮想マシンを右クリックし、**コンソールを開く** を選択します。
4. 矢印キーを使用して **この仮想アプライアンスを工場出荷時設定にリセット** を選択し、**<ENTER>** を押します。
5. 次の通知が表示されます。

   ```
   This operation is completely Irreversible if you continue you will
   completely reset *this* appliance to its original settings. All changes you
   have made to this appliance will be Lost. Are you sure you wish to Reset
   this Appliance to Factory Settings?
   ```
6. リセットをするには **y**、キャンセルするには **n** を入力します。アプライアンスは工場出荷時の元の設定にリセットされ、その他設定と保存されたデータはすべて失われます。

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

コンソールビューの更新

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

コンソールからログアウトする

コンソールからログアウトするには、アカウントでログオンしている右上隅にある **ログアウト** をクリックします。

読み取り専用ユーザー役割

読み取り専用と呼ばれる、診断目的のシェルアクセス権を持つ、非特権ユーザー役割があります。読み取り専用ユーザーにはマウントを実行するための限定的な特権があります。読み取り専用ユーザーのパスワードは **readonly** に設定されています。セキュリティのために、読み取り専用ユーザーのパスワードは管理者のパスワード（OMIVV v1.0 ～ v2.3.1 まで）から変更になっています。

OpenManage Ingetration プラグイン 3.0 バージョンから現在のバージョンへのアップグレード

OpenManage Ingetration プラグインをバージョン 3.0 から現在のバージョンにアップグレードするには、次のいずれかの手順を実行します。

1. ウェブブラウザを開き、設定する仮想マシンの vSphere vCenter **コンソール** タブに表示されている管理コンソール URL を入力します。また、Dell Management Console の **ヘルプとサポート** ページに表示されているリンクを使用することもできます。URL は https://<アプライアンスの IP アドレス> 形式で表示され、大文字小文字を区別します。
2. **管理コンソール** ウィンドウの左ペインで、**アプライアンス管理** をクリックします。
3. ネットワークの設定により、ネットワークにプロキシが必要な場合は、プロキシを有効にし、プロキシの設定を入力します。
4. OpenManage Integration のプラグインをバージョン 3.0 から現在のバージョンにアップグレードするには、次のいずれかを実行します。
   - **リポジトリパスのアップデート** が http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ パスに設定されていることを確認します。パスが異なっている場合は、**アプライアンスの管理** ウィンドウの **アプライアンスのアップデート** セクションで、**編集** をクリックし、**リポジトリパスのアップデート** テキストボックスでパスを **http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/** に更新します。**適用** をクリックし、更新内容を保存します。
   - インターネット接続がない場合は、**http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/** パスからすべてのファイルとフォルダをダウンロードし、HTTP 共有にコピーします。**アプライアンスの管理** ウィンドウの **アプライアンスのアップデート** セクションで、**編集** をクリックし、**リポジトリパスのアップデート** テキストボックスで、オフライン HTTP 共有へのパスを更新し、**適用** をクリックします。
5. 利用可能な仮想アプライアンスのバージョンと現在の仮想アプライアンスのバージョンを比較し、利用可能な仮想アプライアンスのバージョンが、現在の仮想アプライアンスのバージョンより新しいことを確認します。
6. 仮想アプライアンスにアップデートを適用するには、**アプライアンスの設定**で、**仮想アプライアンスのアップデート** をクリックします。
7. **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** をクリックすると、**管理コンソール** ウィンドウからログオフされます。

メモ: OMIVV を 3.0 から 現在のバージョンにアップグレードする際に、カスタム証明書は移行されないため、証明書に適用した設定を再度適用する必要があります。

2.x から 3.1 への移行のための移行パス

旧バージョンから OMIVV 3.1 バージョンに移行するには、次の手順を実行します。

1. 以前のリリースのデータベースのバックアップを行います。
2. vCenter から旧アプライアンスの電源を切ります。

   メモ: vCenter からプラグインを登録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、そのプラグインによって vCenter で登録されたすべてのアラーム、および vCenter での操作など、アラームで実行されるすべてのカスタマイズ操作が削除されます。
3. 新しい OpenManage Integration バージョン 3.1 OVF を展開します。
4. OpenManage Integration バージョン 3.1 アプライアンスに電源を入れます。
5. アプライアンスでネットワーク、タイムゾーンなどをセットアップします。新規 OpenManage Integration バージョン 3.1 アプライアンスの IP アドレスは旧アプライアンスと同じであることが必須です。

   メモ:

   3.1 アプライアンスの IP アドレスが、旧アプライアンスのものと同じでない場合、プラグインが正常に動作しない可能性があります。この場合、すべての vCenter インスタンスの登録を解除して、再度登録してください。
6. 新しいアプライアンスにデータベースを復元します。
7. アプライアンスを検証します。データベース移行が正常に行われたことを確認するための詳細については、本ガイドの「**インストールの検証**」を参照してください。
8. 登録された vCenter すべてでインベントリを実行します。

   メモ:

   プラグインで管理されているすべてのホスト上で、アップグレード後に再度インベントリを実行することをお勧めします。オンデマンドでインベントリを実行する手順の詳細に関しては、『*OpenManage Integration for VMware vCenter User's Guide*』（OpenManage Integration for VMware vCenter ユーザーズガイド）（**dell.com/support/manuals**）で「**インベントリジョブの実行**」を参照してください。

   新しい OpenManage Integration バージョン 3.1 アプライアンスの IP アドレスを、旧アプライアンスのものから変更した場合、SNMP トラップの送信先を新規アプライアンスに設定する必要があります。第 12 世代以降のサーバーでは、これらのホストでインベントリを実行することで修正されます。以前のバージョンに対応している第 12 世代以前のホストでは、この IP 変更は非対応として表示され、OMSA の設定が必要になります。

7

設定

設定タブは、次の用途で使用します。

- 保証期限通知の設定の表示
- 保証期限通知の設定
- ファームウェアアップデートリポジトリの設定
- アラームおよびイベントの設定の表示
- イベントおよびアラームの設定と管理
- インベントリおよび保証のためのデータ取得スケジュールの表示と設定

OMSA リンクの編集

この手順は、すでに OMSA Web Server がインストールされており、以前に初期設定ウィザードを使用してこのリンクを設定したことを前提としています。使用中の OMSA のバージョン、および Web Server のインストールと設定の手順に関しては、『OpenManage Server Administrator インストールガイド』を参照してください。
設定ウィザードの実行中にリンクを入力しなかった場合は、このリンクを OpenManage Integration for VMware vCenter の **管理** → **設定**タブで編集することができます。これは Web Client には適用されません。

メモ: OMSA は Dell PowerEdge 第 11 世代以前のサーバーのみで必要です。Web Client 初期設定ウィザードには、OMSA リンクを提供するためのオプションがありません。OMSA リンクは .Net Client のみに適用されます。

1. OpenManage Integration for VMware vCenter にある **管理** → **設定** タブの vCenter 設定の下、OMSA ウェブサーバー URL の右側で **編集** をクリックします。
2. OMSA ウェブサーバー URL ダイアログボックスに **URL** を入力します。
   HTTPS も含めて完全な URL を入力してください。
3. **これらの設定をすべての vCenter に適用する** チェックボックスを選択して、OMSA URL をすべての vCenter に適用します。このチェックボックスを選択しないと、OMSA URL は 1 つの vCenter にしか適用されません。
4. ホストの サマリ タブに移動して、このリンクが機能することを確認します。Dell ホスト情報内で OMSA コンソールリンクがクリック可能であることを確認します。

11 世代サーバーとの OMSA 使用の理解

Dell PowerEdge 第 12 世代より前のサーバーでは、OpenManage Integration for VMware vCenter での作業用に OMSA をインストールする必要があります。OMSA は、展開中に第 11 世代 Dell PowerEdge ホストに自動でインストールできますが、手動でインストールしたい場合は、それも可能です。

OMSA を Dell PowerEdge 第 11 世代ホストで設定する方法は、次のいずれかを選択します。

- OMSA エージェントの ESXi システムへの展開
- OMSA トラップ先の設定

メモ: 上記オプションの他に、.Net Client を使用してホストコンプライアンス準拠を実行（OMSA エージェントのインストールと設定が可能）することができます。

OMSA エージェントの ESXi システムへの展開

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

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

1. まだインストールされていない場合は、vSphere コマンドラインツール（vSphere CLI）を **http://www.vmware.com** からインストールします。
2. 次のコマンドを入力します。

   ```
   Vihostupdate.pl -server <IP Address of ESXi host> -i -b <OMSA version X.X>
   ```

   メモ: OMSA のインストールには数分かかることがあります。このコマンドの完了後、ホストを再起動する必要があります。

OMSA トラップ先の設定

このタスクは、イベント作成に iDRAC6 の代わりに OMSA を使用するホストシステムのみに適用されます。iDRAC6 には追加設定は必要ありません。

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

1. OpenManage Integration for VMware vCenter **管理 → 設定** タブにある OMSA ユーザーインタフェースへのリンクを使用するか、またはウェブブラウザ（**https://<HostIP>:1311/**）から OMSA エージェントに移動します。
2. インタフェースにログインして、**アラート管理** タブを選択します。
3. **アラート処置** を選択し、監視対象イベントに **ブロードキャストメッセージ** オプションが設定されており、イベントが送出されることを確認します。
4. タブの一番上で **プラットフォームイベント** オプションを選択します。
5. グレーの **宛先の設定** ボタンをクリックし、次に **宛先** リンクをクリックします。
6. **トラップ先を有効にする** チェックボックスを選択します。
7. OpenManage Integration for VMware vCenter アプライアンスの IP アドレスを **送信先の IP アドレス** フィールドに入力します。
8. **変更の適用** をクリックします。
9. さらなるイベントの設定には、手順 1～8 を繰り返します。

保証期限通知の設定の表示

1. OpenManage Integration for VMware vCenter で、**管理 → 設定**タブの アプライアンスの設定 の下にある **保証期限通知** をクリックします。
2. 保証期限通知 で、次の表示を行うことができます。
   - 設定が有効または無効のいずれになっているか
   - 初回の警告までの設定日数。
   - 初回の重大警告までの設定日数。
3. 保証期限通知を設定する方法については、「保証期限通知の設定」を参照してください。

保証期限通知の設定

保証期限しきい値を設定して保証期限を警告することができます。

1. OpenManage Integration for VMware vCenter にある **管理 → 設定**タブの、アプライアンス設定の下、**保証期限通知** の右側で **編集** アイコンをクリックします。
2. 保証期限通知ダイアログボックスで、次の手順を行います。
   a. この設定を有効にするには、**ホストの保証期限通知を有効にする** チェックボックスを選択します。
      チェックボックスを選択すると、保証期限通知が有効化されます。
   b. 最小日数しきい値アラート の下で、次の手順を行います。
      1. 警告 ドロップダウンリストで、保証期限の何日前に警告したいかを日数で選択します。
      2. 重要 ドロップダウンリストで、保証期限の何日前に警告したいかを日数で選択します。
3. **適用** をクリックします。

イベントおよびアラームの設定

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

メモ: OMIVV は、第 12 世代およびそれ以降のホストの SNMP v1 および v2 のアラートをサポートしています。第 12 世代より前のホストでは、OMIVV は vCenter で SNMP v1 のアラートをサポートしています。トラップ先の設定に関する詳細については、「OMSA トラップ先の設定」を参照してください。

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

1. イベントおよびアラーム の右側の **編集** アイコンをクリックします。
2. すべてのハードウェアアラームとイベントを有効化するには、**Dell ホストのアラームを有効にする** チェックボックスを選択します。

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

3. すべての管理されている Dell サーバーで、デフォルトの vCenter アラーム設定を復元するには、**デフォルトのアラームの復元** をクリックします。
   変更が有効になるには、最大 1 分間かかることがあります。

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

4. **イベント掲載レベル** で以下のいずれかを選択します。
   - イベントは掲載しない
     このオプションは、ハードウェアイベントをブロックします。
   - 全イベントを掲載
     このオプションは、すべてのハードウェアイベントを掲載します。
   - 重要および警告イベントのみ掲載
     このオプションは、重要または警告レベルのハードウェアイベントのみを掲載します。
   - 仮想化関連の重要および警告イベントのみを掲載
     このオプションは、仮想化関連の重要および警告イベントのみを掲載します。これは、デフォルトのイベント掲載レベルです。
5. この設定をすべての vCenter に適用したい場合、**これらの設定をすべての vCenter に適用する** チェックボックスを選択します。

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

   すでに、設定ページで 登録済みのすべての vCenter をドロップダウンリストから選択している場合は、このオプションはグレイアウトしています。
6. 保存するには、**適用** をクリックします。

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、どのイベントの掲載レベルが選択されているかを、設定タブで表示することができます。

1. **OpenManage Integration for VMware vCenter** の **管理 → 設定** タブで、vCenter 設定の下にある イベントとアラーム を展開します。
2. イベントとアラーム の下には、次の項目が表示されます。
   - Dell ホスト用の vCenter アラーム。有効、または無効が表示されます。
   - イベント掲載レベル

     表示できるイベント掲載レベルを確認するには、「イベントとアラームの理解」を参照してください。
3. アラームとイベントの設定は、「イベントとアラームの設定」を参照してください。

イベントの表示

イベントを設定すると、イベント タブに設定が表示されます。「イベントおよびアラームの設定」を参照してください。
ホスト、クラスタ、またはデータセンターのイベントを、イベント タブに表示します。

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

3. 監視 タブで、**イベント** をクリックします。
4. さらにイベント詳細を表示したい場合、特定のイベントを選択します。

ファームウェアアップデートについて

サーバーがファームウェアアップデートを受信する場所は、設定タブ上の OpenManage Integration for VMware vCenter で使用できるグローバル設定です。

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

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

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

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

関連情報：

- ファームウェア更新リポジトリの設定

ファームウェア更新リポジトリの設定

OpenManage Integration for VMware vCenter の設定タブで、ファームウェアアップデートのリポジトリを設定することができます。

1. OpenManage Integration for VMware vCenter で、**管理 → 設定** タブの **アプライアンスの設定** の下、ファームウェアアップデートのリポジトリの右側にある、**編集** アイコンをクリックします。
2. ファームウェア更新リポジトリダイアログボックスで、次のいずれかを選択します。
   - Dell Online
     ステージングフォルダがある、デフォルトのファームウェアのリポジトリ（http://downloads.dell.com/published/Pages/index.html）。OpenManage Integration for VMware vCenter が選択したファームウェアアップデートをダンロードし、ステージングフォルダに保存した後、ユーザーがファームウェアウィザードを実行してファームウェアをアップデートします。
   - 共有ネットワークフォルダ
     これらは Dell Repository Manager アプリケーションを使って作成されます。これらのローカルレポジトリは Windows ベースのファイル共有にあります。ライブリンクを使って、Dell Repository Manager に移動します。
3. **共有ネットワークフォルダ** を選択した場合、以下を実行します。
   a. 次のフォーマットを使って、**カタログファイルの場所** を入力します。

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

b. **アップデート元の選択** 画面に、選択したリポジトリのパスでの進行中のファイルのダウンロードが表示される場合、ダウンロードが進行中というエラーメッセージが表示されます。

4. ファイルのダウンロードが完了したら、**適用** をクリックします。

単一ホストのためのファームウェアのアップデートウィザードの実行

この機能は、iDRAC Express または Enterprise カードを備えた第 11 世代、第 12 世代、第 13 世代の Dell サーバーでのみ使用可能です。

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

メモ: ファームウェア ウィザードにアクセスするには、次のいずれかを実行します。

- **ホスト** を右クリックし、**すべての OpenManage Integration アクション**、**ファームウェアアップデート** の順にクリックします。
- **ホスト**、**アクション**、**すべての OpenManage Integration アクション**、**ファームウェアアップデート** の順にクリックします。
- **ホスト**、**概要**、**Dell ホスト情報**、**ファームウェアアップデート** の順にクリックします。

ファームウェアアップデートウィザードを実行するには、次の手順を行います。

1. **vSphere ウェブクライアント** で、**ホスト** をクリックします。利用可能なホストのリストが表示されます。
2. 表示されたリストからホストを選択します。
3. メインメニューで、**監視** をクリックして、**Dell ホスト情報** タブを選択します。Dell ホストのインベントリ情報が表示されます。
4. **ファームウェア** をクリックすると、利用可能なファームウェアとその詳細情報が表示されます。
5. **ファームウェアの実行ウィザード** をクリックします。**ファームウェアアップデート** 画面が表示されます。
6. **次へ** をクリックすると、所定のホスト用のファームウェアアップデートバンドルが記載された **アップデートソースの選択** 画面が表示されます。この画面で、**アップデートバンドルの選択** ドロップダウンリストからファームウェアアップデートバンドルを選択します。

   メモ:
   - 64 ビットバンドルは、iDRAC バージョン 1.51 以前を搭載した第 12 世代ホストではサポートされていません。
   - 64 ビットバンドルは、すべての iDRAC バージョンの第 11 世代ホストでサポートされていません。
7. **次へ** をクリックします。コンポーネントのファームウェア詳細がリストされた **コンポーネントの選択** 画面が表示されます。
8. 使用するファームウェアアップデートを選択し、**次へ** をクリックします。ダウングレード、または現在アップデート用にスケジュール済みのコンポーネントは選択不可になっています。**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する場合は、ダウングレードとしてリストされているオプションを選択します。このオプションの選択は、ファームウェアのダウングレードによる影響を理解している上級ユーザーのみにお勧めします。

9. **次へ** をクリックします。**ファームウェアアップデートのスケジュール** 画面が表示されます。
   - **ファームウェアアップデートジョブ名** フィールドにジョブ名を入力し、**ファームウェアアップデートの説明** フィールドに説明を入力します。このフィールドへの入力はオプションです。
   - **今すぐアップデート** を選択すると、ファームウェアアップデートジョブが直ちに開始されます。
   - **アップデートのスケジュール** ボタン。ファームウェアアップデートジョブを後で実行する場合は、このラジオボタンを選択し、**次へ** をクリックします。ファームウェアアップデートジョブは、現在の時刻より 30 分後以降にスケジュールできます。
   - カレンダーボックスで 月と日 を選択します。
   - 時刻 テキストボックスに、HH:MM 形式で時刻を入力し、次へ をクリックします。時刻は、クライアントが物理的に位置しているローカルタイムゾーンの時刻です。時刻に無効な値を入力すると、アップデートがブロックされます。
   - **次回の再起動でアップデートを適用する。**
     サービスの中断を避けるため、再起動前にホストをメンテナンスモードにすることが推奨されます。
   - **メンテナンスモードにせずにアップデートを適用し、再起動を強制する。**
     アップデートが適用され、ホストがメンテナンスモードでなくても再起動が行われます。この方法は推奨されません。
10. **次へ** をクリックします。ファームウェアアップデート後のすべてのコンポーネントの詳細を示した **サマリ** ページが表示されます。
11. **終了** をクリックします。
12. アップデートが正常に行われたことを確認するには、**監視** タブで **ジョブキュー → ファームウェアアップデート** と選択し、**OpenManage Integration 概要** ページで新規バージョンを確認します。

クラスタのためのファームウェアのアップデートウィザードの実行

この機能が使用できるのは、iDRAC Express または Enterprise カードのいずれかが搭載された第 11、12、および 13 世代の Dell サーバーのみです。お使いのファームウェアが 2010 年 10 月 14 日以降にインストールされた場合は、ファームウェアのアップデートウィザードを使用してファームウェアバージョンを自動的にアップデートすることができます。このウィザードは、接続プロファイルの一部であり、ファームウェア、CSIOR ステータス、ハイパーバイザ、および OMSA ステータス（第 11 世代サーバーのみ）面で適合するホストのみをアップデートします。クラスタ ビューにリストされているクラスタを 1 つ選択し、ファームウェアのアップデートウィザードを使用します。通常、ファームウェアコンポーネントのアップデートには、クラスタごとに 30～60 分かかります。クラスタで DRS を有効化して、ファームウェアアップデートプロセス中にホストがメンテナンスモードに入る / 終了するときに仮想マシンを移行できるようにします。ファームウェアアップデートタスクは、一度に 1 つしかスケジュールまたは実行できません。

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

メモ: VMware では、クラスタを同一のサーバハードウェアで構築することをお勧めしています。ホスト数がクラスタの上限（VMware 推奨）に近い状態のクラスタ、または異なるモデルの Dell で構成されているクラスタでのクラスタレベルのファームウェアアップデートには、vSphere ウェブクライアントの使用が推奨されます。

メモ: デフォルトのタイムアウト設定の変更の詳細については、『User's Guide』（ユーザーズガイド）の「Troubleshooting」（トラブルシューティング）の項を参照して下さい。

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

1. **OpenManage Integration** アイコンをクリックし、左ペインに表示された **クラスタ** をクリックします。クラスタのリストが表示されます。
2. 表示されるリストのクラスタをクリックします。メインメニューと共に各種オプションが表示されます。
3. **監視**、**Dell クラスタ情報**、**ファームウェア** の順にクリックします。**ファームウェアの実行ウィザード** 画面が表示されます。
4. **ファームウェアの実行ウィザード** リンクをクリックします。**ようこそ** ページが表示されます。
5. **次へ** をクリックします。バンドルを選択することができる **アップデートソースの選択** 画面が表示されます。リポジトリの場所も同時に表示されます。
6. **バンドルの選択** エリアに表示されたリストからホストを選択します。ファームウェアのアップデートには少なくとも 1 つのバンドルを選択するようにしてください。各ホストのホスト名の隣にはドロップダウンリストがあり、そこから必要なバンドルを選択できます。

   メモ:
   - 64 ビットバンドルは、iDRAC バージョン 1.51 以前を搭載した第 12 世代ホストではサポートされていません。
   - 64 ビットバンドルは、すべての iDRAC バージョンの第 11 世代ホストでサポートされていません。
7. **次へ** をクリックします。**コンポーネントの選択** 画面が表示されます。この画面には、モデル名、ホスト名、サービスタグ、コンポーネントなどの選択したホストのコンポーネントの詳細が表示されます。
8. リストから少なくとも 1 つのコンポーネントを選択し、**次へ** をクリックして続行します。**フィルタ** フィールドを使用してコンポーネントの内容をフィルタ、またはコンポーネントデータグリッド内の行をドラッグ＆ドロップすることが可能です。**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する場合、既存のファームウェアバージョンを利用可能な以前のバージョンにロールバックします。
9. **次へ** をクリックすると、**ファームウェアアップデートのスケジュール** 画面が表示されます。
   a. ファームウェアアップデートジョブ名を **ファームウェアアップデートジョブ名** フィールドに入力します。この値は必須です。
   b. **ファームウェアアップデートの説明** フィールドにファームウェアアップデートの説明を入力します。この値はオプションです。
10. 次のオプションから選択します。
    a. **今すぐアップデート**。このラジオボタンを選択してファームウェアアップデートジョブを今すぐ実行し、**次へ** をクリックします。
    b. **アップデートのスケジュール** ボタン。ファームウェアアップデートジョブを後で実行する場合は、このラジオボタンを選択し、**次へ** をクリックします。ファームウェアアップデートジョブは、現在の時刻より 30 分後以降にスケジュールできます。
    c. **カレンダー** ボックスで 月と日 を選択します。
    d. **時刻** テキストボックスに、HH:MM 形式で時刻を入力し、**次へ** をクリックします。時刻は、クライアントが物理的に位置しているローカルタイムゾーンの時刻です。時刻に無効な値を入力すると、アップデートがブロックされます。
11. ファームウェアアップデート詳細のすべてが記載された **サマリ** 画面が表示されます。
12. **終了** をクリックすると、正しく行われたファームウェアアップデートに対して **ファームウェアアップデートジョブが作成されました** というメッセージが表示されます。

Viewing Firmware Update Status for Clusters and Datacenters

このページで情報を表示するには、クラスタまたはホストのファームウェアアップデートを実行またはスケジュールします。

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

1. OpenManage Integration で、**監視 → ジョブキュー → ファームウェアアップデート** と選択します。
2. 最近の情報を表示するには、**更新** をクリックします。
3. データグリッドのステータスを確認します。このグリッドは、ファームウェアアップデートジョブに関する次の情報を提供します。
   - 状態
   - スケジュールされた時刻
   - 名前
   - 説明
   - vCenter
   - コレクションサイズ

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

     進捗状況サマリは、このファームウェアアップデートの進捗状況詳細をリストします。
4. 特定のジョブの詳細を見るには、そのジョブのデータグリッドで、マスターデータグリッドのアイテムをクリックします。詳細情報が詳細データグリッドに表示されます。
   ここでは、次の詳細を確認できます。
   - ホスト名
   - 状態
   - 開始時刻
   - 終了時刻
5. 実行されていないスケジュール済みファームウェアアップデートを中止するには、**中止** をクリックします。
6. スケジュール済みジョブを変更する場合は、**変更** をクリックします。
7. スケジュール済みファームウェアアップデートをパージするには、**ジョブキューのパージ** をクリックします。
   正常に完了、失敗、またはキャンセルされたジョブは、パージすることのみが可能です。
8. **日付とジョブステータスより古い** を選択して、**適用** をクリックします。選択したジョブがキューからクリアされます。

インベントリおよび保証のデータ取得スケジュールの表示

1. OpenManage Integration for VMware vCenter の **管理 → 設定** タブで、**vCenter 設定** の下にある **データ取得スケジュール** をクリックします。
   データ取得スケジュール をクリックすると展開して、インベントリおよび保証のスケジュールが表示されます。
2. インベントリまたは保証の取得について、次の設定を表示します。
   - このオプションが有効にされているか、無効にされているかを表示します。
   - 有効にされている曜日を表示します。
   - その日の有効にされている時間を表示します。
3. 再度 **データ取得スケジュール** をクリックすると、情報が 1 行に畳まれて、このオプションが有効になっているか無効になっているかが表示されます。

4. データ取得スケジュールを編集したい場合は、「インベントリジョブスケジュールの変更」または「保証ジョブスケジュールの変更」を参照してください。

11 世代サーバーとの OMSA 使用の理解

Dell PowerEdge 第 12 世代より前のサーバーでは、OpenManage Integration for VMware vCenter での作業用に OMSA をインストールする必要があります。OMSA は、展開中に第 11 世代 Dell PowerEdge ホストに自動でインストールできますが、手動でインストールしたい場合は、それも可能です。

OMSA を Dell PowerEdge 第 11 世代ホストで設定する方法は、次のいずれかを選択します。

- OMSA エージェントの ESXi システムへの展開
- OMSA トラップ先の設定

メモ: 上記オプションの他に、.Net Client を使用してホストコンプライアンス準拠を実行（OMSA エージェントのインストールと設定が可能）することができます。

OMSA エージェントの ESXi システムへの展開

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

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

1. まだインストールされていない場合は、vSphere コマンドラインツール（vSphere CLI）を **http://www.vmware.com** からインストールします。
2. 次のコマンドを入力します。

   ```
   Vihostupdate.pl -server <IP Address of ESXi host> -i -b <OMSA version X.X>
   ```

   メモ: OMSA のインストールには数分かかることがあります。このコマンドの完了後、ホストを再起動する必要があります。

OMSA トラップ先の設定

このタスクは、イベント作成に iDRAC6 の代わりに OMSA を使用するホストシステムのみに適用されます。iDRAC6 には追加設定は必要ありません。

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

1. OpenManage Integration for VMware vCenter **管理 → 設定** タブにある OMSA ユーザーインタフェースへのリンクを使用するか、またはウェブブラウザ（**https://<HostIP>:1311/**）から OMSA エージェントに移動します。
2. インタフェースにログインして、**アラート管理** タブを選択します。
3. **アラート処置** を選択し、監視対象イベントに **ブロードキャストメッセージ** オプションが設定されており、イベントが送出されることを確認します。
4. タブの一番上で **プラットフォームイベント** オプションを選択します。

5. グレーの **宛先の設定** ボタンをクリックし、次に **宛先** リンクをクリックします。
6. **トラップ先を有効にする** チェックボックスを選択します。
7. OpenManage Integration for VMware vCenter アプライアンスの IP アドレスを **送信先の IP アドレス** フィールドに入力します。
8. **変更の適用** をクリックします。
9. さらなるイベントの設定には、手順 1～8 を繰り返します。

8

保証期限通知の設定の表示

1. OpenManage Integration for VMware vCenter で、**管理** → **設定**タブの アプライアンスの設定 の下にある **保証期限通知** をクリックします。
2. 保証期限通知 で、次の表示を行うことができます。
   - 設定が有効または無効のいずれになっているか
   - 初回の警告までの設定日数。
   - 初回の重大警告までの設定日数。
3. 保証期限通知を設定する方法については、「保証期限通知の設定」を参照してください。

保証期限通知の設定

保証期限しきい値を設定して保証期限を警告することができます。

1. OpenManage Integration for VMware vCenter にある **管理** → **設定**タブの、アプライアンス設定の下、**保証期限通知** の右側で **編集** アイコンをクリックします。
2. 保証期限通知ダイアログボックスで、次の手順を行います。
   a. この設定を有効にするには、**ホストの保証期限通知を有効にする** チェックボックスを選択します。
      チェックボックスを選択すると、保証期限通知が有効化されます。
   b. 最小日数しきい値アラート の下で、次の手順を行います。
      1. 警告 ドロップダウンリストで、保証期限の何日前に警告したいかを日数で選択します。
      2. 重要 ドロップダウンリストで、保証期限の何日前に警告したいかを日数で選択します。
3. **適用** をクリックします。

9

ファームウェアアップデートについて

サーバーがファームウェアアップデートを受信する場所は、設定タブ上の OpenManage Integration for VMware vCenter で使用できるグローバル設定です。

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

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

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

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

関連情報：

- ファームウェア更新リポジトリの設定

ファームウェア更新リポジトリの設定

OpenManage Integration for VMware vCenter の設定タブで、ファームウェアアップデートのリポジトリを設定することができます。

1. OpenManage Integration for VMware vCenter で、**管理 → 設定** タブの **アプライアンスの設定** の下、ファームウェアアップデートのリポジトリの右側にある、**編集** アイコンをクリックします。
2. ファームウェア更新リポジトリダイアログボックスで、次のいずれかを選択します。
   - Dell Online
     ステージングフォルダがある、デフォルトのファームウェアのリポジトリ（http://downloads.dell.com/published/Pages/index.html）。OpenManage Integration for VMware vCenter が選択したファームウェアアップデートをダンロードし、ステージングフォルダに保存した後、ユーザーがファームウェアウィザードを実行してファームウェアをアップデートします。
   - 共有ネットワークフォルダ

これらは Dell Repository Manager アプリケーションを使って作成されます。これらのローカルレポジトリは Windows ベースのファイル共有にあります。ライブリンクを使って、Dell Repository Manager に移動します。

3. **共有ネットワークフォルダ** を選択した場合、以下を実行します。
   a. 次のフォーマットを使って、**カタログファイルの場所** を入力します。
      - xml ファイル用の NFS 共有: host:/share/filename.xml
      - gz ファイル用の NFS 共有: host:/share/filename.gz
      - xml ファイル用の CIFS 共有: \\host\share\filename.xml
      - gz ファイル用の CIFS 共有: \\host\share\filename.gz
   b. **アップデート元の選択** 画面に、選択したリポジトリのパスでの進行中のファイルのダウンロードが表示される場合、ダウンロードが進行中というエラーメッセージが表示されます。
4. ファイルのダウンロードが完了したら、**適用** をクリックします。

単一ホストのためのファームウェアのアップデートウィザードの実行

この機能は、iDRAC Express または Enterprise カードを備えた第 11 世代、第 12 世代、第 13 世代の Dell サーバーでのみ使用可能です。

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

メモ: ファームウェア ウィザードにアクセスするには、次のいずれかを実行します。

- **ホスト** を右クリックし、**すべての OpenManage Integration アクション**、**ファームウェアアップデート** の順にクリックします。
- **ホスト**、**アクション**、**すべての OpenManage Integration アクション**、**ファームウェアアップデート** の順にクリックします。
- **ホスト**、**概要**、**Dell ホスト情報**、**ファームウェアアップデート** の順にクリックします。

ファームウェアアップデートウィザードを実行するには、次の手順を行います。

1. **vSphere ウェブクライアント** で、**ホスト** をクリックします。利用可能なホストのリストが表示されます。
2. 表示されたリストからホストを選択します。
3. メインメニューで、**監視** をクリックして、**Dell ホスト情報** タブを選択します。Dell ホストのインベントリ情報が表示されます。
4. **ファームウェア** をクリックすると、利用可能なファームウェアとその詳細情報が表示されます。
5. **ファームウェアの実行ウィザード** をクリックします。**ファームウェアアップデート** 画面が表示されます。
6. **次へ** をクリックすると、所定のホスト用のファームウェアアップデートバンドルが記載された **アップデートソースの選択** 画面が表示されます。この画面で、**アップデートバンドルの選択** ドロップダウンリストからファームウェアアップデートバンドルを選択します。

メモ:

- 64 ビットバンドルは、iDRAC バージョン 1.51 以前を搭載した第 12 世代ホストではサポートされていません。
- 64 ビットバンドルは、すべての iDRAC バージョンの第 11 世代ホストでサポートされていません。

7. **次へ** をクリックします。コンポーネントのファームウェア詳細がリストされた **コンポーネントの選択** 画面が表示されます。
8. 使用するファームウェアアップデートを選択し、**次へ** をクリックします。ダウングレード、または現在アップデート用にスケジュール済みのコンポーネントは選択不可になっています。**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する場合は、ダウングレードとしてリストされているオプションを選択します。このオプションの選択は、ファームウェアのダウングレードによる影響を理解している上級ユーザーのみにお勧めします。
9. **次へ** をクリックします。**ファームウェアアップデートのスケジュール** 画面が表示されます。
   - **ファームウェアアップデートジョブ名** フィールドにジョブ名を入力し、**ファームウェアアップデートの説明** フィールドに説明を入力します。このフィールドへの入力はオプションです。
   - **今すぐアップデート** を選択すると、ファームウェアアップデートジョブが直ちに開始されます。
   - **アップデートのスケジュール** ボタン。ファームウェアアップデートジョブを後で実行する場合は、このラジオボタンを選択し、**次へ** をクリックします。ファームウェアアップデートジョブは、現在の時刻より 30 分後以降にスケジュールできます。
   - カレンダーボックスで 月と日 を選択します。
   - 時刻 テキストボックスに、HH:MM 形式で時刻を入力し、次へ をクリックします。時刻は、クライアントが物理的に位置しているローカルタイムゾーンの時刻です。時刻に無効な値を入力すると、アップデートがブロックされます。
   - **次回の再起動でアップデートを適用する。**
     サービスの中断を避けるため、再起動前にホストをメンテナンスモードにすることが推奨されます。
   - **メンテナンスモードにせずにアップデートを適用し、再起動を強制する。**
     アップデートが適用され、ホストがメンテナンスモードでなくても再起動が行われます。この方法は推奨されません。
10. **次へ** をクリックします。ファームウェアアップデート後のすべてのコンポーネントの詳細を示した **サマリ** ページが表示されます。
11. **終了** をクリックします。
12. アップデートが正常に行われたことを確認するには、**監視** タブで **ジョブキュー → ファームウェアアップデート** と選択し、**OpenManage Integration 概要** ページで新規バージョンを確認します。

クラスタのためのファームウェアのアップデートウィザードの実行

この機能が使用できるのは、iDRAC Express または Enterprise カードのいずれかが搭載された第 11、12、および 13 世代の Dell サーバーのみです。お使いのファームウェアが 2010 年 10 月 14 日以降にインストールされた場合は、ファームウェアのアップデートウィザードを使用してファームウェアバージョンを自動的にアップデートすることができます。このウィザードは、接続プロファイルの一部であり、ファームウェア、CSIOR ステータス、ハイパーバイザ、および OMSA ステータス（第 11 世代サーバーのみ）面で適合するホストのみをアップデートします。クラスタ ビューにリストされているクラスタを 1 つ選択し、ファームウェアのアップデートウィザードを使用します。通常、ファームウェアコンポーネントのアップデートには、クラスタごとに 30～60 分かかります。クラスタで DRS を有効化して、ファームウェアアップデートプロセス中にホストがメンテナンスモードに入る / 終了するときに仮想マシンを移行できるようにします。ファームウェアアップデートタスクは、一度に 1 つしかスケジュールまたは実行できません。

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

メモ: VMware では、クラスタを同一のサーバハードウェアで構築することをお勧めしています。ホスト数がクラスタの上限（VMware 推奨）に近い状態のクラスタ、または異なるモデルの Dell で構成されているクラスタでのクラスタレベルのファームウェアアップデートには、vSphere ウェブクライアントの使用が推奨されます。

メモ: デフォルトのタイムアウト設定の変更の詳細については、『User's Guide』（ユーザーズガイド）の「Troubleshooting」（トラブルシューティング）の項を参照して下さい。

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

1. **OpenManage Integration** アイコンをクリックし、左ペインに表示された **クラスタ** をクリックします。クラスタのリストが表示されます。
2. 表示されるリストのクラスタをクリックします。メインメニューと共に各種オプションが表示されます。
3. **監視**、**Dell クラスタ情報**、**ファームウェア** の順にクリックします。**ファームウェアの実行ウィザード** 画面が表示されます。
4. **ファームウェアの実行ウィザード** リンクをクリックします。**ようこそ** ページが表示されます。
5. **次へ** をクリックします。バンドルを選択することができる **アップデートソースの選択** 画面が表示されます。リポジトリの場所も同時に表示されます。
6. **バンドルの選択** エリアに表示されたリストからホストを選択します。ファームウェアのアップデートには少なくとも 1 つのバンドルを選択するようにしてください。各ホストのホスト名の隣にはドロップダウンリストがあり、そこから必要なバンドルを選択できます。

   メモ:
   - 64 ビットバンドルは、iDRAC バージョン 1.51 以前を搭載した第 12 世代ホストではサポートされていません。
   - 64 ビットバンドルは、すべての iDRAC バージョンの第 11 世代ホストでサポートされていません。
7. **次へ** をクリックします。**コンポーネントの選択** 画面が表示されます。この画面には、モデル名、ホスト名、サービスタグ、コンポーネントなどの選択したホストのコンポーネントの詳細が表示されます。
8. リストから少なくとも 1 つのコンポーネントを選択し、**次へ** をクリックして続行します。**フィルタ** フィールドを使用してコンポーネントの内容をフィルタ、またはコンポーネントデータグリッド内の行をドラッグ＆ドロップすることが可能です。**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する場合、既存のファームウェアバージョンを利用可能な以前のバージョンにロールバックします。
9. **次へ** をクリックすると、**ファームウェアアップデートのスケジュール** 画面が表示されます。
   a. ファームウェアアップデートジョブ名を **ファームウェアアップデートジョブ名** フィールドに入力します。この値は必須です。
   b. **ファームウェアアップデートの説明** フィールドにファームウェアアップデートの説明を入力します。この値はオプションです。
10. 次のオプションから選択します。
    a. **今すぐアップデート**。このラジオボタンを選択してファームウェアアップデートジョブを今すぐ実行し、**次へ** をクリックします。
    b. **アップデートのスケジュール** ボタン。ファームウェアアップデートジョブを後で実行する場合は、このラジオボタンを選択し、**次へ** をクリックします。ファームウェアアップデートジョブは、現在の時刻より 30 分後以降にスケジュールできます。
    c. **カレンダー** ボックスで 月と日 を選択します。

d. **時刻** テキストボックスに、HH:MM 形式で時刻を入力し、**次へ** をクリックします。時刻は、クライアントが物理的に位置しているローカルタイムゾーンの時刻です。時刻に無効な値を入力すると、アップデートがブロックされます。

11. ファームウェアアップデート詳細のすべてが記載された **サマリ** 画面が表示されます。
12. **終了** をクリックすると、正しく行われたファームウェアアップデートに対して **ファームウェアアップデートジョブが作成されました** というメッセージが表示されます。

10
ホストのイベントおよびアラームについて

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

4 つのイベント掲載レベルがあります。

表 5. イベント掲載レベルの説明

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

イベントとアラームを設定する際に、それらを有効にすることができます。有効にすると、重要なハードウェアアラームによって OpenManage Integration for VMware vCenter はホストシステムをメンテナンスモードにし、場合によって仮想マシンを別のホストシステムに移行します。OpenManage Integration for VMware vCenter は管理下 Dell ホストから受信したイベントを転送し、それらのイベントに対するアラームを生成します。このアラームを使い、 vCenter に対し、再起動、メンテナンスモードまたは移行などの措置を起動できます。例えば、デュアル電源が故障しアラームが出された場合、その結果の措置としては、そのマシン上の仮想マシンを新しいものに移行することです。

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

クラスタ外のホスト、または VMware Distributed Resource Scheduling (DRS) が起動されていないクラスタにあるホストでは、重要イベントのために仮想マシンはシャットダウンされる可能性があります。DRS は全

リソースプールの使用率を連続的に監視し、使用可能なリソースをビジネスニーズにしたがって各仮想マシンに知的に割り当てます。DRS と Dell Alarms が設定されたクラスタを使って、重要なハードウェアイベントの際に仮想マシンが自動的に移行されるようにしてください。画面上のメッセージの詳細に記載されているのは、この vCenter インスタンスにある、影響を受ける可能性のあるクラスタです。イベントと警報を有効化する前に、クラスタが影響を受けるかどうか確認してください。

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

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

シャーシのイベントおよびアラームについて

シャーシに対応するイベントおよびアラームは、vCenter のレベルでのみ表示されます。各 vCenter で行われたホストのイベントおよびアラームの設定は、シャーシレベルでも適用されます。イベントおよびアラームの設定を編集するには、OpenManage Integration for VMware vCenter の **管理 → 設定** タブから行います。ここから、イベントの投稿レベル、デルのホストおよびシャーシのためのアラームを有効にする、またはデフォルトのアラームに復元できます。すべての登録済み vCenters に対して、イベントおよびアラームの設定は、各 vCenter 毎に、または一度に行うことができます。

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

Viewing Chassis Events

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

シャーシアラームの表示

1. 左ペインで vCenter を選択し、vCenter Server をクリックします。
2. 特定の vCenter をクリックします。
3. アラームが表示されます。表示されるのは最初の 4 つのアラームのみです。すべて表示 をクリックすると、詳細なリストが すべての問題 として 監視 タブに表示されます。
4. **アラームを起動する** でアラームをクリックして、アラームの定義を表示します。

イベントおよびアラームの設定

Dell Management Center のイベントおよびアラーム ページでは、すべてのハードウェアアラームの有効化または無効化を行うことができます。現在のアラートのステータスは、vCenter アラーム タブに表示されます。重要イベントは、データ喪失が実際に起こったか差し迫っていること、またはシステムの不具合を示しています。警告イベントは、必ずしも重要であるとは限りませんが、将来問題になる可能性があるものを示

します。イベントとアラームの有効化は、VMware Alarm Manager を使って行うこともできます。イベントは、ホストとクラスタ ビューの vCenter のタスクおよびイベント タブに表示されます。サーバーからイベントを受信するには、OMIVV を SNMP トラップ先として設定します。第 12 世代およびそれ以降のホストでは、SNMP トラップ先は iDRAC で設定されます。第 12 世代より前のホストでは、トラップ生成は OMSA で設定されます。イベントおよびアラームの設定は、**管理 → 設定** タブから OpenManage Integration for VMware vCenter を使用して行います。Dell ホスト（有効 または 無効）のまたはすべての現在の vCenter アラーム、およびイベント掲載レベルを表示するには、vCenter 設定の下で、イベントおよびアラーム の見出しを展開します。

メモ: OMIVV は、第 12 世代およびそれ以降のホストの SNMP v1 および v2 のアラートをサポートしています。第 12 世代より前のホストでは、OMIVV は vCenter で SNMP v1 のアラートをサポートしています。トラップ先の設定に関する詳細については、「OMSA トラップ先の設定」を参照してください。

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

1. イベントおよびアラーム の右側の **編集** アイコンをクリックします。
2. すべてのハードウェアアラームとイベントを有効化するには、**Dell ホストのアラームを有効にする** チェックボックスを選択します。

   メモ: アラームが有効にされている Dell ホストは重大イベントに反応してメンテナンスモードに入るため、必要に応じてアラームを修正することができます。
3. すべての管理されている Dell サーバーで、デフォルトの vCenter アラーム設定を復元するには、**デフォルトのアラームの復元** をクリックします。

   変更が有効になるには、最大 1 分間かかることがあります。

   メモ: この手順は、Dell ホストのアラームを有効にする が選択されている場合にのみ表示されます。
4. **イベント掲載レベル** で以下のいずれかを選択します。
   - イベントは掲載しない

     このオプションは、ハードウェアイベントをブロックします。
   - 全イベントを掲載

     このオプションは、すべてのハードウェアイベントを掲載します。
   - 重要および警告イベントのみ掲載

     このオプションは、重要または警告レベルのハードウェアイベントのみを掲載します。
   - 仮想化関連の重要および警告イベントのみを掲載

     このオプションは、仮想化関連の重要および警告イベントのみを掲載します。これは、デフォルトのイベント掲載レベルです。
5. この設定をすべての vCenter に適用したい場合、**これらの設定をすべての vCenter に適用する** チェックボックスを選択します。

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

   すでに、設定ページで 登録済みのすべての vCenter をドロップダウンリストから選択している場合は、このオプションはグレイアウトしています。
6. 保存するには、**適用** をクリックします。

イベントの表示

イベントを設定すると、イベント タブに設定が表示されます。「イベントおよびアラームの設定」を参照してください。

ホスト、クラスタ、またはデータセンターのイベントを、イベント タブに表示します。

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

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、どのイベントの掲載レベルが選択されているかを、設定タブで表示することができます。

1. **OpenManage Integration for VMware vCenter** の **管理** → **設定** タブで、vCenter 設定の下にある イベントとアラーム を展開します。
2. イベントとアラーム の下には、次の項目が表示されます。
   - Dell ホスト用の vCenter アラーム。有効、または無効が表示されます。
   - イベント掲載レベル

   表示できるイベント掲載レベルを確認するには、「イベントとアラームの理解」を参照してください。
3. アラームとイベントの設定は、「イベントとアラームの設定」を参照してください。

インベントリおよび保証のデータ取得スケジュールの表示

1. OpenManage Integration for VMware vCenter の **管理** → **設定** タブで、**vCenter 設定** の下にある **データ取得スケジュール** をクリックします。
   データ取得スケジュール をクリックすると展開して、インベントリおよび保証のスケジュールが表示されます。
2. インベントリまたは保証の取得について、次の設定を表示します。
   - このオプションが有効にされているか、無効にされているかを表示します。
   - 有効にされている曜日を表示します。
   - その日の有効にされている時間を表示します。
3. 再度 **データ取得スケジュール** をクリックすると、情報が 1 行に畳まれて、このオプションが有効になっているか無効になっているかが表示されます。
4. データ取得スケジュールを編集したい場合は、「インベントリジョブスケジュールの変更」または「保証ジョブスケジュールの変更」を参照してください。

11

シャーシに関連するホストの表示

選択したシャーシに関連するホストについての情報は、**管理** ページで表示することができます。
関連ホストについての情報を表示するには、次の手順を実行します。

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

12

シャーシ管理

OpenManage Integration for VMware vCenter は、選択したシャーシの追加情報を表示することを可能にします。シャーシ情報タブでは、個々のシャーシのシャーシ概要詳細、ハードウェアインベントリ、ファームウェア、および管理コントローラについての情報を表示することができます。シャーシの異なるモデルに基づいて、各シャーシで以下の 3 つのタブが表示されます。

サマリ タブ

監視 タブ

管理 タブ

シャーシサマリ詳細の表示

シャーシ**サマリ** ページでは、個々のシャーシのシャーシサマリ詳細を表示することができます。
シャーシサマリ詳細を表示するには、次の手順を実行します。

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

     メモ: シャーシをインベントリしない場合は、サービスタグと CMC IP アドレスしか表示されません。
5. 選択したシャーシと関連したデバイスの正常性状態を表示できます。メインのペインには、シャーシの全般的な正常性が表示されます。有効な正常性インジケータは、**正常**、**警告**、**重要**、**なし** です。**シャーシの正常性** のグリッドビューには、各コンポーネントの正常性が表示されます。シャーシの正常性パラメータは、**VRTX バージョン 1.0 以降**、**M1000e バージョン 4.4 以降** のモデルに適用されます。4.3 より以前のバージョンでは、正常性インジケータが 2 つしか表示されず、それらは **正常** および **警告または重要**（逆三角形にオレンジ色の感嘆符）となります。

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

6. CMC **Enterprise** または **Express** のライセンスと終了期限の日付を表示することができます。これは、M 1000 e シャーシには適用されません。
7. **保証** アイコンでは、サーバーの残りの日数および使用済みの日数を表示します。保証が複数ある場合、保証の残りの日数は、最後の保証の最後の日として計算されます。
8. **アクティブエラー** 表は、**シャーシの正常性** ページに表示される、シャーシのエラーをリスト表示します。M 1000 e のバージョン 4.3 以下では、アクティブエラーは表示されません。

ハードウェアインベントリの表示：ファン

選択したシャーシ内にあるファンについての情報を表示することができます。このページでその情報を表示するには、インベントリジョブを実行する必要があります。ファン情報の CSV ファイルをエクスポートすることができます。

ファンについての情報を表示するには、次の手順を実行します。

1. **ホーム** ページで **vCenter** をクリックします。
2. 左ペインの **OpenManage Integration** で、**Dell シャーシ** をクリックします。
3. 左ペインで、対応するシャーシ IP を選択します。
4. **監視** タブをクリックします。
5. ファンについての情報を表示するには、次のいずれかを実行します。

   a. **概要** タブで **ファン** をクリックします。

   b. **監視** タブで左ペインを展開し、**ハードウェアインベントリ** をクリックしてから **ファン** をクリックします。

   次の情報が表示されます。

   - 名前
   - 存在
   - 電源状況
   - 読み取り
   - 警告しきい値
   - 重要しきい値
     - 最小
     - 最大

ハードウェアインベントリの表示：I/O モジュール

選択したシャーシの I/O モジュールについての情報を表示することができます。このページでその情報を表示するには、インベントリジョブを実行する必要があります。I/O モジュール情報の CSV ファイルをエクスポートすることができます。

I/O モジュールについての情報を表示するには、次の手順を実行します。

1. **ホーム** ページで **vCenter** をクリックします。
2. 左ペインの **OpenManage Integration** で、**Dell シャーシ** をクリックします。

3. 左ペインで、対応するシャーシ IP を選択します。
4. **監視** タブをクリックします。
5. **I/O モジュール** についての情報を表示するには、次のいずれかを実行します。

    a. **概要** タブで **I/O モジュール** をクリックします。

    b. **監視** タブで左ペインを展開し、**ハードウェアインベントリ** をクリックしてから **I/O モジュール** をクリックします。

    次の情報が表示されます。

    - スロット / 場所
    - 存在
    - 名前
    - ファブリック
    - Service Tag（サービスタグ）
    - 電源状態

    追加情報を表示するには、対応する I/O モジュールを選択します。次の情報が表示されます。

    - Role（役割）
    - Firmware Version（ファームウェアバージョン）
    - ハードウェアバージョン
    - IP Address（IP アドレス ）
    - Subnet Mask（サブネットマスク ）
    - Gateway（ゲートウェイ）
    - MAC アドレス
    - DHCP が有効

ハードウェアインベントリの表示：iKVM

選択したシャーシの iKVM についての情報を表示することができます。このページでその情報を表示するには、インベントリジョブを実行する必要があります。iKVM 情報の CSV ファイルをエクスポートすることができます。

メモ: iKVM についての情報は、PowerEdge M1000e シャーシに対してのみ表示できます。

iKVM についての情報を表示するには、次の手順を実行します。

1. **ホーム** ページで **vCenter** をクリックします。
2. 左ペインの **OpenManage Integration** で、**Dell シャーシ** をクリックします。
3. 左ペインで、対応するシャーシ IP を選択します。
4. **監視** タブをクリックします。
5. **iKVM** についての情報を表示するには、次のいずれかを実行します。

    a. **概要** タブで **iKVM** をクリックします。

b. **監視** タブで左ペインを展開し、**ハードウェアインベントリ** をクリックしてから **iKVM** をクリックします。

次の情報が表示されます。

- iKVM 名
- 存在
- Firmware Version（ファームウェアバージョン）
- フロントパネル USB/ ビデオが有効
- CMC CLI へのアクセスを許可

メモ: シャーシに iKVM モジュールが含まれている場合にのみ iKVM タブが表示されてます。

ハードウェアインベントリの表示：PCIe

選択したシャーシの PCIe についての情報を表示することができます。このページでその情報を表示するには、インベントリジョブを実行する必要があります。PCIe 情報の CSV ファイルをエクスポートすることができます。

PCIe についての情報を表示するには、次の手順を実行します。

1. **ホーム** ページで **vCenter** をクリックします。
2. 左ペインの **OpenManage Integration** で、**Dell シャーシ** をクリックします。
3. 左ペインで、対応するシャーシ IP を選択します。
4. **監視** タブをクリックします。
5. PCIe についての情報を表示するには、次のいずれかを実行します。

   メモ: PCIe 情報を M 1000 e シャーシには適用されません。

   a. **概要** タブで **PCIe** をクリックします。

   b. **監視** タブで左ペインを展開し、**ハードウェアインベントリ** をクリックしてから **PCIe** をクリックします。

   次の情報が表示されます。

   - PCIe スロット
     - Slot（スロット）
     - 名前
     - 電源状態
     - ファブリック
   - サーバースロット
     - 名前
     - 番号

   追加情報を表示するには、対応する PCIe を選択します。次の情報が表示されます。

   - Slot Type（スロットタイプ）
   - サーバーマッピング

- 割り当てステータス
- スロットに割り当てられた電力
- PCI ID
- ベンダ ID

ハードウェアインベントリの表示：電源装置

選択したシャーシの電源装置ユニットについての情報を表示することができます。このページでその情報を表示するには、インベントリジョブを実行する必要があります。電源装置ユニット情報の CSV ファイルをエクスポートすることができます。

電源装置ユニットについての情報を表示するには、次の手順を実行します。

1. **ホーム** ページで **vCenter** をクリックします。
2. 左ペインの **OpenManage Integration** で、**Dell シャーシ** をクリックします。
3. 左ペインで、対応するシャーシ IP を選択します。
4. **監視** タブをクリックします。
5. 電源装置ユニットについての情報を表示するには、次のいずれかを実行します。

   a. **概要** タブで **電源装置** をクリックします。

   b. **監視** タブで左ペインを展開し、**ハードウェアインベントリ** をクリックしてから **電源装置** をクリックします。

   次の情報が表示されます。

   - 名前
   - 容量
   - 存在
   - 電源状況

ハードウェアインベントリの表示：温度センサー

選択したシャーシの温度センサーについての情報を表示することができます。このページでその情報を表示するには、インベントリジョブを実行する必要があります。温度センサー情報の CSV ファイルをエクスポートすることができます。

温度センサーについての情報を表示するには、次の手順を実行します。

1. **ホーム** ページで **vCenter** をクリックします。
2. 左ペインの **OpenManage Integration** で、**Dell シャーシ** をクリックします。
3. 左ペインで、対応するシャーシ IP を選択します。
4. **監視** タブをクリックします。
5. 温度センサーについての情報を表示するには、次のいずれかを実行します。

   a. **概要** タブで **温度センサー** をクリックします。

   b. **監視** タブで左ペインを展開し、**ハードウェアインベントリ** をクリックしてから **温度センサー** をクリックします。

   次の情報が表示されます。

- Location（場所）
- 読み取り
- 警告しきい値
  - 最小
  - 最大
- 重要しきい値
  - 最小
  - 最大

メモ: PowerEdge M1000e シャーシでは、温度センサーについての情報がシャーシに対してのみ表示されます。他のシャーシでは、温度センサーについての情報がシャーシと関連したモジュラサーバに対して表示されます。

保証の詳細の表示

保証ウィンドウには保証の詳細が保存されます。
保証についての情報を表示するには、次の手順を実行します。

1. **ホーム** ページで **vCenter** をクリックします。
2. 左ペインの **OpenManage Integration** で、**Dell シャーシ** をクリックします。
3. 左ペインで、対応するシャーシ IP を選択します。
4. **監視** タブをクリックします。
5. この **保証** タブには、以下が含まれています。
   a. **プロバイダ**
   b. **説明**
   c. **ステータス**
   d. **開始日**
   e. **終了日**
   f. **残日数**
   g. **最終更新日**

ストレージの表示

ストレージウインドウではシャーシの情報が保存されます。
ストレージについての情報を表示するには、次の手順を実行します。

1. **ホーム** ページで **vCenter** をクリックします。
2. 左ペインの **OpenManage Integration** で、**Dell シャーシ** をクリックします。
3. 左ペインで、対応するシャーシ IP を選択します。
4. **監視** タブをクリックします。
5. **ストレージ** タブには、以下が含まれています。

a. **仮想ディスク**
b. **コントローラ**
c. **エンクロージャ**
d. **物理ディスク**
e. **ホットスペア**

ストレージでハイライト表示された各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。

6. M 1000 e 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。
   a. 名前
   b. Model（モデル）
   c. Service Tag（サービスタグ）
   d. IP アドレス（ストレージへのリンク）
   e. ファブリック
   f. Group Name（グループ名）
   g. グループ IP アドレス（ストレージグループへのリンク

シャーシのファームウェア詳細の表示

選択したシャーシのファームウェア詳細についての情報を表示することができます。ファームウェア情報の CSV ファイルをエクスポートすることが可能です。

ファームウェアについての情報を表示するには、次の手順を実行します。

1. **ホーム** ページで **vCenter** をクリックします。
2. 左ペインの **OpenManage Integration** で、**Dell シャーシ** をクリックします。
3. 左ペインで、対応するシャーシ IP を選択します。
4. **監視** タブをクリックします。
5. 二重矢印マークをクリックして左ペインを展開してから、**ファームウェア** をクリックします。

   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
6. **CMC の起動** をクリックすると、**Chassis Management Controller** ページが表示されます。

シャーシの管理コントローラ詳細の表示

選択したシャーシの管理コントローラ詳細についての情報を表示することができます。

管理コントローラについての情報を表示するには、次の手順を実行します。

1. **ホーム** ページで **vCenter** をクリックします。
2. 左ペインの **OpenManage Integration** で、**Dell シャーシ** をクリックします。
3. 左ペインで、対応するシャーシ IP を選択します。
4. **監視** タブをクリックします。
5. 二重矢印マークをクリックして左ペインを展開してから、**管理コントローラ** をクリックします。

6. **管理コントローラ** ページで追加情報を表示するには、矢印マークをクリックして左の列を展開します。次の情報が表示されます。
   - 一般
     - 名前
     - Firmware Version（ファームウェアバージョン）
     - 最終アップデート時刻
     - CMC の場所
     - ハードウェアバージョン
   - 共通ネットワーク
     - DNS ドメイン名
     - DNS に DHCP を使用
     - MAC アドレス
     - 冗長性モード
   - CMC IPv4 情報
     - IPv4 が有効
     - DHCP が有効
     - IP Address（IP アドレス ）
     - Subnet Mask（サブネットマスク ）
     - Gateway（ゲートウェイ）
     - 優先 DNS サーバー
     - 代替 DNS サーバー

13

単一ホストの監視

OpenManage Integration for VMware vCenter では、単一ホストの詳細情報を表示することができます。VMware vCenter 内のホストには、左側のナビゲーターからアクセスすることができます。ここにはすべてのベンダーのすべてのホストが表示されます。特定の Dell ホストをクリックすると、より詳しい情報が表示されます。Dell ホストのリストを素早く表示するには、OpenManage Integration for VMware vCenter の左側のナビゲーターで、Dell ホスト をクリックします。

- ホストサマリ詳細の表示
- ハードウェアの表示: 単一ホストの FRU 詳細
- ハードウェアの表示: 単一ホストのプロセッサ詳細
- ハードウェアの表示: 単一ホストの電源装置詳細
- ハードウェアの表示: 単一ホストのメモリ詳細
- ハードウェアの表示: 単一ホストの NIC 詳細
- ハードウェアの表示: 単一ホストの PCI スロット詳細
- ハードウェアの表示: 単一ホストのリモートアクセスカード詳細
- 単一ホストのストレージ詳細の表示
  - ストレージの表示: 単一ホストの仮想ディスク詳細
  - ストレージの表示: 単一ホストの物理ディスク詳細
  - ストレージの表示: 単一ホストのコントローラ詳細
  - ストレージの表示: 単一ホストのエンクロージャ詳細
- 単一ホストのファームウェア詳細の表示
- 単一ホストの電源監視の表示
- 単一ホストの保証ステータスの表示
- Dell ホストのみの簡単な表示

ホストサマリ詳細の表示

個々のホストのホストサマリ詳細は、ホストサマリページで表示します。このページには様々なポートレットが表示され、これらのポートレットのうち 2 つが OpenManage Integration for VMware vCenter に適用されます。

ポートレットは次のとおりです。

- Dell ホストの正常性
- Dell ホスト情報

これら 2 つのポートレットは希望する位置にドラッグ & ドロップすることができ、要件に応じてに 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。

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

システムのアラート OpenManage Integration for VMware vCenter にアラートがある場合、ステータスエリアの下、ポートレットの上にある黄色のボックスに表示されます。

タスクトレイ Dell 製品の統合情報がこの右側パネルエリアに表示されます。表示されるのは次の情報です。

- 最近のタスク
- 進行中の作業
- アラーム

  Dell のアラーム情報がこのタスクトレイポートレットに表示されます。

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

サービスタグ お使いの Dell PowerEdge サーバーのサービスタグです。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 サーバーモデル名を表示します。

耐障害性メモリ これは BIOS 属性であり、サーバーの初回セットアップ中に BIOS で有効化され、サーバーのメモリ操作モードを表示します。メモリ操作モード値を変更するときはシステムを再起動する必要があります。これは、ESXi 5.5 バージョン以降搭載の R620、R720、T620、M620 サーバーに当てはまります。これは、耐障害性メモリオプション対応で、ESXi 5.5 以降のバージョンを実行する PowerEdge サーバーの第 12 世代以降に該当します。値は次の 4 つです。

- 有効かつ保護状態：この値は、システムがサポートされており、オペレーティングシステムのバージョンが ESXi 5.5 以降で、BIOS のメモリ操作モードが FRM に設定されていることを示します。
- 有効かつ非保護状態：この値はオペレーティングシステムのバージョンが ESXi 5.5 未満のシステムをサポートすることを示しています。
- 無効：この値はどのオペレーティングシステムのバージョンのシステムでもサポートし、ここでは BIOS のメモリ操作モードは FRM に設定されていないことを示します。
- ブランク：BIOS のメモリ操作モードがサポートされていない場合、FRM 属性が表示されません。

ID

- ホスト名

  Dell ホストの名前。
- 電源状況

  電源がオンかオフかを表示します。
- iDRAC IP

iDRAC の IP アドレスを表示します。

- 管理 IP

  管理 IP アドレスを表示します。
- 接続プロファイル

  このホストの接続プロファイル名を表示します。
- モデル

  Dell サーバーのモデルを表示します。
- サービスタグ

  サーバーのサービスタグを表示します。
- 資産タグ

  資産タグを表示します。
- 保証残日数

  保証の残りの日数を表示します。
- 最新のインベントリスキャン

  最後のインベントリスキャンの日付と時刻が表示されます。

ハイパーバイザー & ファームウェア

- ハイパーバイザ

  ハイパーバイザーのバージョンが表示されます。
- BIOS バージョン

  BIOS のバージョンが表示されます。
- リモートアクセスカードバージョン

  リモートアクセスカードのバージョンを表示します。

管理コンソール 管理コンソールを使って以下のような外部システム管理コンソールを起動します。

- Remote Access Console（iDRAC）
  Integrated Dell Remote Access Controller（iDRAC）のウェブユーザーインタフェースです。

ホストアクション インジケータライトの点滅 で、さまざまな間隔で物理サーバーを点滅させるよう設定することができます。

6. Dell ホストの正常性のポートレットの表示：

Dell ホストの正常性 コンポーネントの正常性は、すべての主要なホストサーバーコンポーネントの状態を、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、イントルージョン、ハードウェアログ、電源管理、電源とメモリがあります。シャーシの正常性パラメータは、**VRTX バージョン 1.0 以降、バージョン 4.4 以降がインストールされている M 1000 e** のモデルに適用されます。バージョン 4.3 より以前では、2 つの正常性インジケータのみが表示され、それらは **正常** および **警告または重要**（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。次のオプションがあります。

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

管理コンソールの起動

Dell Server Management Portlet から起動できる管理コンソールには、次の 2 つがあります。

- Remote Access Console（iDRAC Console）
  Remote Access Console を起動して iDRAC ユーザーインタフェースにアクセスします。
- OMSA コンソール
  OMSA コンソールを起動して OpenManage Server Administrator ユーザーインタフェースにアクセスします。OMSA コンソールを起動する前に、Open Management Integration for VMware vCenter で OMSA URL を設定する必要があります。

OMSA コンソールの起動

OMSA コンソールを起動する前に、OMSA URL をセットアップし、OMSA ウェブサーバーをインストールして設定してください。OMSA URL のセットアップは、設定タブから行います。

メモ: 第 11 世代の Dell PowerEdge サーバーを監視および管理するために、OpenManage Integration for VMware vCenter を使用して、OMSA をインストールする必要があります。

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

Remote Access Console（iDRAC）の起動

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

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

物理サーバーインジケータライトの点滅の設定

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

1. OpenManage Integration for VMware vCenter のナビゲータ エリア にある インベントリリスト で、**ホスト** をクリックします。
2. オブジェクト タブで、希望のホストをダブルクリックします。
3. サマリ タブで、Dell Server Management ポートレットまでスクロールダウンします。
4. **ホスト処理** で、**インジケータライトの点滅** を選択します。
5. 次のいずれかを選択します。
   - 点滅を開始し、期間を設定するには **インジケータライト** ダイアログボックスで **点滅オン** をクリックし、タイムアウトドロップダウンリストでタイムアウト間隔を選択して **OK** をクリックします。
   - 点滅を終了するには、**インジケータライト** ダイアログボックスで **点滅オフ** をクリックし、**OK** をクリックします。

物理サーバーインジケータライトの点滅の設定

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

1. OpenManage Integration for VMware vCenter のナビゲータ エリア にある インベントリリスト で、**ホスト** をクリックします。
2. オブジェクト タブで、希望のホストをダブルクリックします。
3. サマリ タブで、Dell Server Management ポートレットまでスクロールダウンします。
4. **ホスト処理** で、**インジケータライトの点滅** を選択します。
5. 次のいずれかを選択します。
   - 点滅を開始し、期間を設定するには **インジケータライト** ダイアログボックスで **点滅オン** をクリックし、タイムアウトドロップダウンリストでタイムアウト間隔を選択して **OK** をクリックします。
   - 点滅を終了するには、**インジケータライト** ダイアログボックスで **点滅オフ** をクリックし、**OK** をクリックします。

14

ソフトウェアライセンスの購入およびアップロード

完全製品版にアップグレードするまでは、試用版ライセンスで実行しています。製品の **ライセンスの購入** リンクを使用して Dell ウェブサイトに移動し、ライセンスを購入してください。購入したら、管理コンソールを使用してアップロードします。この方法は、試用版ライセンスをご使用の場合にのみ使用できます。

1. OpenManage Integration for VMware vCenter で、次のいずれか 1 つを実行します。
   - **ライセンス** タブのソフトウェアライセンスの横にある、**ライセンスの購入** をクリックします。
   - はじめにのタブの基本タスクで、**ライセンスの購入**をクリックします。
2. Dell ウェブページでライセンスを購入して既知の場所にファイルを保存します。
3. ウェブブラウザで、管理コンソールの URL を入力します。
   https://<アプライアンス IP アドレス> の形式を使用してください。
4. 管理コンソールログインウィンドウ で、パスワードを入力し、**ログイン** をクリックします。
5. ライセンスの **アップロード** をクリックします。
6. **ライセンスのアップロード** ウィンドウでライセンスファイルに移動して、**参照** をクリックします。
7. ライセンスファイルを選択して、**アップロード** をクリックします。

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

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

評価用ライセンス	試用版には、OpenManage Integration for VMware vCenter によって管理されている 5 つのホスト（サーバ）の評価用ライセンスが含まれています。これは、第 11 世代以降のバージョンにのみ該当します。これはデフォルトのライセンスであり、90 日間の試用期間限定です。
標準ライセンス	完全製品バージョンには、最高 10 の vCenters 用の標準ライセンスが含まれ、OpenManage Integration for VMware vCenter が管理するホスト接続をいくつでも購入できます。

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

- vCenter 接続ライセンスの最大数 — 最大 10 の登録済みおよび使用中の vCenter 接続が許容されます。
- ホスト接続ライセンスの最大数 — 購入されたホスト接続の数です。
- 使用中 — 使用中の vCenter 接続またはホスト接続ライセンスの数です。ホスト接続では、この数は検出およびインベントリされたホスト（またはサーバ）の数を示します。

- 使用可能 — 将来使用できる vCenter 接続またはホスト接続ライセンスの数です。

メモ: 標準ライセンスの有効期間は 3 年のみで、追加のライセンスは既存のライセンスに付加され、上書きされません。インベントリが正常に行われた第 11、12、または第 13 世代ホストの総数が制限数に到達している場合、第 9 または第 10 世代を新規または既存の接続プロファイルに追加することはできません。

ライセンスの購入時に、XML ファイルは Dell Digital ストアからダウンロードできません。したがって、OMIVV アプライアンスを再インストールする必要がある場合、バックアップとして XML ファイルのコピーを保存しておいてください。XML ファイルを失くし、ファイルが見つからない場合、download_software@dell.com に電子メールを送信して次の詳細を伝えた後で、新しい XML ファイルが送信されます。

- 元のデル注文番号
- 注文中の OpenManage Integration for VMware vCenter SKU
- 各 SKU の数量
- XML ファイルを受信するための電子メールアドレス

スタンダード SLA プロセスには 2 営業日を要します。

15

ハードウェアの表示: 単一ホストの FRU 詳細

Dell ホスト情報タブで、単一ホストのフィールドで交換可能なパーツ（FRU）詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。ハードウェアビューには OMSA および iDRAC からのデータを直接報告します。「インベントリジョブを今すぐ実行する」を参照してください。

1. OpenManage Integration for VMware vCenter の ナビゲータ で、**ホスト** をクリックします。
2. ホスト タブで、ハードウェア： FRU 詳細 を表示したいホストを選択します。
3. 監視 タブで、**Dell ホスト情報** タブを選択し、ハードウェア： FRU サブタブで、次を表示します。

パーツ名	FRU のパーツ名を表示します。
パーツ番号	FRU のバージョン番号を表示します。
製造元	メーカー名を表示します。
シリアル番号	メーカーのシリアル番号を表示します。
Manufacture Date	製造日を表示します。

16

ハードウェアの表示: 単一ホストのプロセッサ詳細

Dell ホスト情報タブで、単一ホストのプロセッサ詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。ハードウェアビューには OMSA および iDRAC からのデータを直接報告します。「インベントリジョブを今すぐ実行する」を参照してください。

1. OpenManage Integration for VMware vCenter のナビゲータで、**ホスト** をクリックします。
2. オブジェクト タブで、プロセッサ詳細を表示したいホストを選択します。
3. 監視 タブで、**Dell ホスト情報** タブを選択し、ハードウェア： プロセッササブタブで、次を表示します。

ソケット	スロット番号を表示します。
速度	現在の速度を表示します。
ブランド	プロセッサのブランドを表示します。
バージョン	プロセッサのバージョンを表示します。
コア	このプロセッサ内のコアの数が表示されます。

17

ハードウェアの表示: 単一ホストの電源装置詳細

Dell ホスト情報タブで、単一ホストの仮想電源装置詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。ハードウェアビューには OMSA および iDRAC からのデータを直接報告します。「インベントリジョブを今すぐ実行する」を参照してください。

1. OpenManage Integration for VMware vCenter のナビゲータで、**ホスト** をクリックします。
2. オブジェクト タブで、ハードウェア： 電源装置詳細を表示したいホストを選択します。
3. 監視 タブで、**Dell ホスト情報** タブを選択し、**ハードウェア： 電源装置** サブタブで、次を表示します。

種類	電源装置のタイプが表示されます。電源装置には、次のタイプがあります。 • 不明 • リニア • スイッチング • バッテリ • UPS • コンバータ • レギュレータ • AC • DC • VRM
場所	電源装置の場所、たとえばスロット 1 などを表示します。
出力（ワット）	出力がワット単位で表示されます。

18

ハードウェアの表示: 単一ホストのメモリ詳細

Dell ホスト情報タブで、単一ホストのメモリ詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。ハードウェアビューには OMSA および iDRAC からのデータを直接報告します。「インベントリジョブを今すぐ実行する」を参照してください。

1. OpenManage Integration for VMware vCenter のナビゲータで、**ホスト** をクリックします。
2. オブジェクト タブで、ハードウェア： メモリ詳細 を表示したいホストを選択します。
3. 監視 タブで、**Dell ホスト情報** タブを選択し、**ハードウェア： メモリ** サブタブで、次を表示します。

メモリスロット	使用済み、合計、および使用可能なメモリ数が表示されます。
メモリ容量	インストール済みメモリ、総メモリ容量、および使用可能メモリが表示されます。
スロット	DIMM スロットを表示します。
サイズ	メモリサイズを表示します。
種類	メモリのタイプを表示します。

19

ハードウェアの表示: 単一ホストの NIC 詳細

Dell ホスト情報タブで、単一ホストのネットワークインタフェースカード（NIC）詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。ハードウェアビューには OMSA および iDRAC からのデータを直接報告します。「インベントリジョブを今すぐ実行する」を参照してください。

1. OpenManage Integration for VMware vCenter のナビゲータで、**ホスト** をクリックします。
2. オブジェクト タブで、ハードウェア： NIC 詳細 を表示したいホストを選択します。
3. 監視 タブで、**Dell ホスト情報** タブを選択し、**ハードウェア： NIC** サブタブで、次を表示します。

合計	使用可能なネットワークインタフェースカードの合計数が表示されます。
名前	NIC 名を表示します。
製造元	メーカー名のみを表示します。
MAC アドレス	NIC の MAC アドレスが表示されます。

20

ハードウェアの表示: 単一ホストの PCI スロット

Dell ホスト情報タブで、単一ホストの PCI スロット詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。ハードウェアビューには OMSA および iDRAC からのデータを直接報告します。「インベントリジョブを今すぐ実行する」を参照してください。

1. OpenManage Integration for VMware vCenter のナビゲータで、**ホスト** をクリックします。
2. オブジェクト タブで、ハードウェア： PCI スロット詳細 を表示したいホストを選択します。
3. 監視 タブで、**Dell ホスト情報** タブを選択し、**ハードウェア： PCI スロット** サブタブで、次を表示します。

PCI スロット	使用済み、合計、および使用可能な PCI スロットが表示されます。
スロット	スロットを表示します。
製造元	PCI スロットのメーカー名を表示します。
説明	PCI デバイスの説明を表示します。
種類	PCI スロットタイプを表示します。
幅	データバス幅を表示します（該当する場合）。

21

ハードウェアの表示: 単一ホストのリモートアクセスカード詳細

Dell ホスト情報タブで、単一ホストのリモートアクセスカード詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。ハードウェアビューには OMSA および iDRAC からのデータを直接報告します。「インベントリジョブを今すぐ実行する」を参照してください。

1. OpenManage Integration for VMware vCenter のナビゲータで、**ホスト** をクリックします。
2. オブジェクト タブで、ハードウェア： リモートアクセスカードの詳細を表示したいホストを選択します。
3. 監視 タブで、**Dell ホスト情報** タブを選択し、**ハードウェア： リモートアクセスカード** サブタブで、次を表示します。

IP アドレス	リモートアクセスカードの IP を表示します。
MAC アドレス	リモートアクセスカードの MAC アドレスを表示します。
RAC タイプ	リモートアクセスカードのタイプを表示します。
URL	このホストに関連付けられた動作している iDRAC の URL を表示します。

22

単一ホストのストレージ詳細の表示

Dell ホスト情報タブで、単一ホストのストレージ詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。「インベントリジョブを今すぐ実行する」を参照してください。このページには、表示ドロップダウンリストで選択した項目により異なるオプションが表示されます。物理ディスクを選択した場合、別のドロップダウン リストが表示されます。この新しいドロップダウンリストはフィルタと呼ばれ、物理ディスクオプションをフィルタすることができます。

メモ: ハードウェアビューには OMSA および iDRAC からのデータを直接報告します。

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

ストレージ	仮想ディスク、コントローラ、エンクロージャ、および関連する物理ディスク（グローバルホットスペアおよび専用ホットスペア数とともに）の数が表示されます。表示ドロップダウンリストから選択するとき、オプションがここでハイライトされます。
表示	このホストで表示するページオプションが表示されます。 • 仮想ディスク • 物理ディスク • コントローラ • エンクロージャ

ストレージの表示: 単一ホストの仮想ディスク詳細

ホストストレージページのストレージオプションは、表示ドロップダウンリストで選択した項目によって異なります。

表示ドロップダウンリストから仮想ディスクを選択した場合、これらのオプションが表示されます：

名前	仮想ディスクの名前を表示します。
デバイス FQDD	FQDD が表示されます。
物理ディスク	仮想ディスクの場所のある物理ディスクを表示します。
容量	仮想ディスクの容量が表示されます。
レイアウト	仮想ストレージのレイアウトタイプ、つまりこの仮想ディスクに設定された RAID のタイプが表示されます。
メディアの種類	SSD または HDD が表示されます。

コントローラ ID コントローラの ID を表示します。

デバイス ID デバイス ID を表示します。

ストライプサイズ ストライプサイズは、単一のディスク上で各ストライプが消費する容量の合計を意味します。

バスプロトコル 仮想ディスクに含まれる物理ディスクが使用する技術を表示します。可能な値は次のとおりです。

- SCSI
- SAS
- SATA

デフォルト読み取りポリシー コントローラでサポートされているデフォルト読み取りポリシーです。次のオプションがあります。

- 先読み
- 先読みなし
- 適応先読み
- 読み取りキャッシュが有効
- 読み取りキャッシュが無効

デフォルト書き込みポリシー コントローラでサポートされているデフォルト書き込みポリシーです。次のオプションがあります。

- ライトバック
- ライトバックの強制
- ライトバックが有効
- ライトスルー
- 書き込みキャッシュ有効、保護
- 書き込みキャッシュが無効

キャッシュポリシー キャッシュポリシーが有効化されているかどうかが表示されます。

ストレージの表示: 単一ホストの物理ディスク詳細

ホストストレージページのストレージオプションは、表示ドロップダウンリストで選択した項目によって異なります。このオプションを選択すると、フィルタドロップダウンリストが表示されます。次のオプションで物理ディスクをフィルタできます：

- すべての物理ディスク
- グローバルホットスペア
- 専用ホットスペア
- 最後のオプションは仮想ディスクという名のカスタムを表示します。

表示ドロップダウンリストから物理ディスクを選択した場合、これらのオプションが表示されます：

名前 物理ディスクの名前を表示します。

デバイス FQDD デバイス FQDD が表はい

容量 物理ディスクの容量を表示します。

ディスクステータス 物理ディスクのステータスを表示します。次のステータスがあります。

- オンライン
- 準備完了
- 劣化
- エラー
- オフライン
- 再構成中
- 互換性なし
- 削除済み
- クリア済み
- SMART アラートが検知されました
- 不明
- 外部
- サポートなし

設定済み ディスクが構成されているかどうかが表示されます。

ホットスペアのタイプ ホットスペアのタイプを表示します。次のタイプがあります。

- いいえ

  いいえ、はホットスペアがないことを意味します。
- Global（グローバル）

  グローバルホットスペアは、ディスクグループの一部である使用されていないバックアップディスクです。
- 専用

  専用ホットスペアは、単一の仮想ディスクに割り当てられた未使用のバックアップディスクです。仮想ディスク内の物理ディスクが故障すると、ホットスペアがアクティブ化されて故障した物理ディスクと交換されるため、システムが中断したり、ユーザー介入が必要になることもありません。

仮想ディスク 仮想ディスクの名前を表示します。

バスプロトコル バスプロトコルを表示します。

コントローラ ID コントローラの ID を表示します。

コネクタ ID コネクタ ID を表示します。

エンクロージャ ID エンクロージャ ID を表示します。

デバイス ID デバイス ID を表示します。

モデル 物理ストレージディスクのモデル番号を表示します。

パーツ番号 ストレージのパーツ番号を表示します。

シリアル番号 ストレージのシリアル番号を表示します。

ベンダー	ストレージのベンダー名を表示します。

ストレージの表示: 単一ホストのコントローラ詳細

ホストストレージページのストレージオプションは、表示ドロップダウンリストで選択した項目によって異なります。

表示ドロップダウンリストからコントローラを選択した場合、これらのオプションが表示されます：

コントローラ ID	コントローラの ID を表示します。
名前	コントローラの名前が表示されます。
デバイス FQDD	デバイスの FQDD を表示します。
ファームウェアバージョン	ファームウェアバージョンを表示します。
ファームウェアの最小要件	ファームウェアの最小要件が表示されます。この列には、ファームウェアが古くなっており、最新バージョンが使用可能になると、データが投入されます。
ドライババージョン	ドライバのバージョンが表示されます。
巡回読み取り状況	巡回読み取り状況が表示されます。
キャッシュサイズ	キャッシュサイズが表示されます。

ストレージの表示: 単一ホストのエンクロージャ詳細

ホストストレージページのストレージオプションは、表示ドロップダウンリストで選択した項目によって異なります。

表示ドロップダウンリストからエンクロージャを選択した場合、これらのオプションが表示されます：

コントローラ ID	コントローラの ID を表示します。
コネクタ ID	コネクタ ID を表示します。
エンクロージャ ID	エンクロージャ ID を表示します。
名前	エンクロージャ名を表示します。
デバイス FQDD	デバイス FQDD が表示されます。
サービスタグ	サービスタグを表示します。

23

単一ホストのファームウェア詳細の表示

Dell ホスト情報タブで、単一ホストの詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行します。ハードウェアビューには OMSA および iDRAC からのデータを直接報告します。「インベントリジョブを今すぐ実行する」を参照してください。このホストページを使用すると、検索フィルタを使って、ファームウェア情報の CSV ファイルをエクスポートできます。

1. OpenManage Integration for VMware vCenter のナビゲータで、**ホスト** をクリックします。
2. オブジェクト タブで、ファームウェア詳細 を表示したいホストを選択します。
3. 監視 タブで、**Dell ホスト情報** タブを選択し、ファームウェア サブタブで、次を表示します。

名前	このホスト上のすべてのファームウェアの名前を表示します。
種類	ファームウェアの種類を表示します。
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を表示します。
インストール日	インストール日を表示します。

24

単一ホストの電源監視の表示

Dell ホスト情報タブで、単一ホストの電源監視詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。ハードウェアビューには OMSA および iDRAC からのデータを直接報告します。「インベントリジョブを今すぐ実行する」を参照してください。

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。

1. OpenManage Integration for VMware vCenter のナビゲータで、**ホスト** をクリックします。
2. オブジェクト タブで、電源監視の詳細を表示したいホストを選択します。
3. 監視タブで、**Dell ホスト情報ホスト** タブを選択し、電源監視サブタブで、次を表示します。

一般情報	電力バジェットおよび現行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をワット単位で表示します。
予約電力容量	インスタントおよびピーク予約電力容量をワット単位で表示します。
	エネルギー統計
タイプ：	エネルギー統計タイプを表示します。
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を表示します。
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を表示します。
読み取り値	この瞬時値は、1 分間の測定値の平均です。
タイプ：	エネルギー統計タイプを表示します。
測定開始時刻（ホスト時刻）	ホストのピーク電力が開始した日付と時刻を表示します。
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を表示します。
ピーク読み取り値	システムピーク電力統計は、システムが消費するピーク電力です（W）。

25

単一ホストの保証ステータスの表示

保証ステータスを表示するには、保証ジョブを実行する必要があります。「保証ジョブを今すぐ実行する」を参照してください。
Dell ホスト情報タブで、単一ホストの保証ステータス詳細を表示します。保証ステータス ページでは、保証失効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/無効化し、最小日数しきい値アラートを設定することにより、Dell オンラインからサーバー保証情報が取得される時点を制御します。「保証履歴」を参照してください。

1. OpenManage Integration for VMware vCenter の ナビゲータで、**ホスト** をクリックします。
2. オブジェクト タブで、保証サマリ詳細を表示したいホストを選択します。
3. 監視タブで **Dell ホスト情報** をクリックして **保証** サブタブをクリックすると、次に関する情報が表示されます。

プロバイダ	保証のプロバイダ 名を表示します。
説明	説明が表示されます。
開始日	保証の開始日を表示します。
終了日	保証の終了日を表示します。
残日数	保証の残りの日数を表示します。
最終更新日	保証が前回更新された日時。

26

Dell ホストのみの簡単な表示

Dell ホストのみを素早く表示したいときは、OpenManage Integration for VMware vCenter でこれを行うことができます。ナビゲータで Dell ホストを選択します。

1. VMware vCenter のホームページで、**OpenManage Integration** アイコンをクリックします。
2. ナビゲータの OpenManage Integration for VMware vCenter の下にある Dell ホストをクリックします。
3. Dell ホストタブに、次の情報が表示されます。

ホスト名	各 Dell ホストの IP アドレスを使用したリンクが表示されます。特定のホストリンクをクリックして Dell ホスト情報を表示します。
vCenter	この Dell ホストの vCenter IP アドレスを表示します。
クラスタ	この Dell ホストがクラスタ内にある場合、そのクラスタ名がここに表示されます。
接続プロファイル	接続プロファイルの名前を表示します。

27

クラスタおよびデータセンターでのホスト監視

OpenManage Integration for VMware vCenter を使用すると、データセンターまたはクラスタに含まれたすべてのホストに関する詳細情報を表示できます。これらのページでは、データグリッドの行のヘッダーをクリックすることによりデータを並べ替えることができます。データセンターおよびクラスタページでは、CSV ファイルに情報をエクスポートし、データグリッドでフィルタ / 検索機能を提供します。詳細は次の通りです。

- ホスト概要詳細の表示
- ハードウェアの表示： FRU
- ハードウェアの表示： プロセッサ詳細
- ハードウェアの表示：電源装置詳細
- ハードウェアの表示： メモリ詳細
- ハードウェアの表示： NIC
- ハードウェアの表示：PCI スロット詳細
- ハードウェアの表示：リモートアクセスカード詳細
- ストレージの表示：物理ディスクの詳細
- ストレージの表示：仮想ディスク詳細
- ファームウェア詳細の表示
- 電源監視の表示
- 保証サマリ詳細の表示

28

データセンターとクラスタの概要詳細の表示

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

メモ: データセンターとクラスタページでは、情報を CSV ファイルにエクスポートすることが可能で、データグリッドでのフィルタ / 検索機能が提供されます。

1. VMware vCenter の ナビゲータ で、**vCenter** をクリックします。
2. **データセンター** または **クラスタ** をクリックします。
3. オブジェクトタブで、ホスト詳細を表示するホスト、データセンター、またはクラスタを選択します。
4. 監視タブで、**Dell データセンター / クラスタ情報** → **概要**タブを選択して、詳細を表示します。

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

データセンター / クラスタ情報

次が表示されます：

- データセンター / クラスタ名
- Dell 管理下ホストの数
- 合計エネルギー消費量

  このリンクをクリックすると、このデータセンターまたはクラスタの電源監視ページが表示されます。

ハードウェアリソース

次が表示されます：

- 合計プロセッサ数

  このリンクをクリックすると、プロセッサ詳細ページが表示されます。
- 総メモリ容量

  このリンクをクリックすると、このデータセンターまたはクラスタのメモリ詳細ページが表示されます。
- 仮想ディスク容量

  このリンクをクリックすると、このデータセンターまたはクラスタの仮想ディスクページが表示されます。

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。次のステータスがあります。

- 期限切れ保証
- アクティブな保証
- 不明な保証

このリンクから保証サマリページに移動できます。

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	Dell PowerEdge のモデルを表示します。
資産タグ	構成すると、アセットタグが表示されます。
シャーシサービスタグ	シャーシのサービスタグを表示します（ある場合）。
OS バージョン	ESXi OS のバージョンが表示されます。
場所	ブレードのみ：ロケーションにはスロットロケーションが表示されます。そうでない場合は、ロケーションには「該当なし」と表示されます。
iDRAC IP	iDRAC の IP アドレスを表示します。
サービスコンソール IP	サービスコンソールの IP を表示します。
CMC URL	ブレードのみ : CMC URL はシャーシ URL です。そうでない場合、「該当なし」と表示されます。
CPU	CPU の数を表示します。
メモリ	ホストのメモリを表示します。
電源状況	ホストに電源があるかを表示します。
最新のインベントリ	最後のインベントリジョブの日付と時刻が表示されます。
接続プロファイル	接続プロファイルの名前を表示します。
リモートアクセスカードバージョン	リモートアクセスカードのバージョンを表示します。
BIOS ファームウェアバージョン	BIOS のファームウェアバージョンを表示します。

29

ハードウェアの表示: データセンターまたはクラスタの FRU

Dell データセンター / クラスタ情報タブでデータセンターまたはクラスタのフィールドで交換可能なパーツ（FRU）詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。データセンターおよびクラスタページでは、情報を CSV ファイルにエクスポートし、データグリッドにフィルタ / 検索機能を提供します。表示するデータは、データにアクセスするビューによって異なります。ハードウェアビューでは、OMSA および iDRAC からデータを直接レポートします。「インベントリジョブを今すぐ実行する」を参照してください。

1. VMware vCenter の ナビゲータ で、**vCenter** をクリックします。
2. **データセンター** または **クラスタ** をクリックします。
3. オブジェクト タブで、ハードウェア： FRU 詳細 を表示したいデータセンター、またはクラスタを選択します。
4. 監視 タブで、**Dell データセンター / クラスタ情報** タブを選択し、**ハードウェア： FRU** サブタブで、次を表示します。

Host（ホスト）	ホスト名を表示します。
サービスタグ	サービスタグを表示します。
パーツ名	FRU のパーツ名を表示します。
パーツ番号	FRU のバージョン番号を表示します。
製造元	メーカー名を表示します。
シリアル番号	メーカーのシリアル番号を表示します。
Manufacture Date	製造日を表示します。

30

ハードウェアの表示: データセンターまたはクラスタのプロセッサ詳細

Dell データセンター / クラスタ情報タブでデータセンター、またはクラスタのプロセッサ詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。データセンターおよびクラスタページでは、情報を CSV ファイルにエクスポートし、データグリッドにフィルタ / 検索機能を提供します。ハードウェアビューでは、OMSA および iDRAC からデータを直接レポートします。インベントリジョブを今すぐ実行するを参照してください。

1. VMware vCenter の ナビゲータ で、**vCenter** をクリックします。
2. **データセンター** または **クラスタ** をクリックします。
3. データセンターまたはクラスタタブで、プロセッサ詳細 を表示したいデータセンター、またはクラスタを選択します。
4. 監視 タブで、**Dell データセンター / クラスタ情報** タブを選択し、ハードウェア： プロセッササブタブで、次を表示します。

ホスト	ホスト名を表示します。
サービスタグ	サービスタグを表示します。
ソケット	スロット番号を表示します。
速度	現在の速度を表示します。
ブランド	プロセッサのブランドを表示します。
バージョン	プロセッサのバージョンを表示します。
コア	このプロセッサ内のコアの数が表示されます。

31

ハードウェアの表示: データセンターとクラスタの電源装置詳細

Dell データセンターまたはクラスタ情報タブで、データセンターまたはクラスタの仮想電源装置の詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。データセンターとクラスタページでは、情報を CSV ファイルにエクスポートすることが可能で、データグリッドでのフィルタ / 検索機能が提供されます。ハードウェアビューは OMSA および iDRAC からのデータを直接報告します。「インベントリジョブを今すぐ実行する」を参照してください

1. VMware vCenter のナビゲータで、**vCenter** をクリックします。
2. **データセンター** または **クラスタ** をクリックします。
3. オブジェクト タブで、ハードウェア： 電源装置詳細を表示したいデータセンター、またはクラスタを選択します。
4. 監視 タブで、**Dell データセンター/クラスタ情報** タブを選択し、**ハードウェア： 電源装置**サブタブで、次を表示します。

ホスト	ホストの名前を表示します。
サービスタグ	サービスタグを表示します。
種類	電源装置のタイプが表示されます。電源装置には、次のタイプがあります。 • 不明 • リニア • スイッチング • バッテリ • UPS • コンバータ • レギュレータ • AC • DC • VRM
場所	電源装置の場所、たとえばスロット 1 などを表示します。
出力（ワット）	出力がワット単位で表示されます。
状態	電源装置の状態が表示されます。次の状態があります。 • その他 • 不明 • OK • 重要 • 非重要 • 回復可能

- 回復不可能
- 高
- 低

32

ハードウェアの表示: データセンターとクラスタのメモリ詳細

Dell データセンター / クラスタ情報タブで、データセンターまたはクラスタのメモリ詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。データセンターとクラスタページでは、情報を CSV ファイルにエクスポートすることが可能で、データグリッドでのフィルタ / 検索機能が提供されます。ハードウェアビューは OMSA および iDRAC からのデータを直接報告します。「インベントリジョブを今すぐ実行する」を参照してください

1. VMware vSphere Web Clinet のナビゲータ エリアで、**vCenter インベントリリスト** を選択します。
2. **データセンター** または **クラスタ** をクリックします。
3. **オブジェクト** タブで、ハードウェア : メモリ詳細 を表示したい特定のデータセンターまたはクラスタを選択します。
4. **監視** タブで **Dell データセンター / クラスタ情報** タブを選択し、**ハードウェア → メモリ** サブタブと移動して、次を表示します。

ホスト	ホスト名を表示します。
サービスタグ	サービスタグを表示します。
スロット	DIMM スロットを表示します。
サイズ	メモリサイズを表示します。
タイプ	メモリのタイプを表示します。

33

ハードウェアの表示： データセンターとクラスタの NIC 詳細

Dell データセンター / クラスタ情報タブで、データセンターまたはクラスタのネットワークインタフェースカード（NIC）の詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。データセンターとクラスタページでは、情報を CSV ファイルにエクスポートすることが可能で、データグリッドでのフィルタ / 検索機能が提供されます。ハードウェアビューは OMSA および iDRAC からのデータを直接報告します。「インベントリジョブを今すぐ実行する」を参照してください

1. VMware vSphere Web Clinet のナビゲータ エリアで、**vCenter インベントリリスト** を選択します。
2. **データセンター** または **クラスタ** をクリックします。
3. **オブジェクト** タブで、ハードウェアに関連する NIC の詳細を表示したい特定のデータセンターまたはクラスタをクリックします。
4. **監視** タブで、**Dell データセンター / クラスタ情報** をクリックし、**ハードウェア → NIC** とクリックして、次を表示します。

ホスト	ホスト名を表示します。
サービスタグ	サービスタグを表示します。
名前	製品名を表示します。
製造元	メーカー名のみを表示します。
MAC アドレス	NIC の MAC アドレスが表示されます。

34

ハードウェアの表示： データセンターとクラスタの PCI スロット詳細

Dell データセンター / クラスタ情報タブで、データセンターまたはクラスタの PCI スロット詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。データセンターとクラスタページでは、情報を CSV ファイルにエクスポートすることが可能で、データグリッドでのフィルタ / 検索機能が提供されます。ハードウェアビューは OMSA および iDRAC からのデータを直接報告します。「インベントリジョブを今すぐ実行する」を参照してください

1. VMware vSphere Web Clinet のナビゲータ エリアで、**vCenter インベントリリスト** を選択します。
2. **データセンター** または **クラスタ** をクリックします。
3. **オブジェクト** タブで、特定のデータセンターまたはクラスタをクリックします。
4. **監視** タブで、**Dell データセンター / クラスタ情報** タブを選択し、**ハードウェア → PCI スロット：** とクリックして、次を表示します。

ホスト	ホスト名を表示します。
サービスタグ	サービスタグを表示します。
スロット	スロットを表示します。
製造元	PCI スロットのメーカー名を表示します。
説明	PCI デバイスの説明を表示します。
タイプ	PCI スロットタイプを表示します。
幅	データバス幅を表示します（該当する場合）。

35

ハードウェアの表示：リモートアクセスカード詳細

Dell データセンター / クラスタ情報タブで、データセンターまたはクラスタのリモートアクセスカードの詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。データセンターおよびクラスタページでは、CSV ファイルに情報をエクスポートし、データグリッドでフィルタ / 検索機能を提供します。ハードウェアビューには OMSA および iDRAC からのデータが直接報告されます。「インベントリジョブを今すぐ実行する」を参照してください。

1. VMware vSphere Web Clinet のナビゲータ エリアで、**vCenter インベントリリスト** を選択します。
2. **データセンター** または **クラスタ** をクリックします。
3. **オブジェクト** タブで、特定のデータセンターまたはクラスタをクリックします。
4. **監視** タブで、**Dell データセンター / クラスタ情報** タブをクリックし、**ハードウェア → リモートアクセスカード** に移動して次を表示します。

ホスト	ホスト名を表示します。
サービスタグ	サービスタグを表示します。
IP アドレス	リモートアクセスカードの IP を表示します。
MAC アドレス	リモートアクセスカードの MAC アドレスを表示します。
RAC タイプ	リモートアクセスカードのタイプを表示します。
URL	このホストに関連付けられた動作している iDRAC の URL を表示します。

36

ストレージの表示: データセンターとクラスタの物理ディスク

Dell データセンター / クラスタ情報タブでデータセンターまたはクラスタの物理ストレージ詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。データセンターおよびクラスタページでは、情報を CSV ファイルにエクスポートし、データグリッドにフィルタ / 検索機能を提供します。「インベントリジョブを今すぐ実行する」を参照してください。

メモ: ハードウェアビューには OMSA および iDRAC からのデータを直接報告します。

1. VMware vSphere Web Clinet のナビゲータで、**vCenter インベントリリスト** を選択します。
2. **データセンター** または **クラスタ** をクリックします。
3. **オブジェクト** タブで、特定のデータセンターまたはクラスタを選択します。
4. **監視** タブで、**Dell データセンター / クラスタ情報** タブをクリックし、**ストレージ → 物理ディスク** に移動して次を表示します。

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

ホスト	ホストの名前を表示します。
サービスタグ	サービスタグを表示します。
容量	物理ディスクの容量を表示します。
ディスクステータス	物理ディスクのステータスを表示します。次のステータスがあります。 • オンライン • 準備完了 • 劣化 • エラー • オフライン • 再構成中 • 互換性なし • 削除済み • クリア済み • SMART アラートが検知されました • 不明 • 外部 • サポートなし

メモ: これらのアラートの意味についての詳細は、http://support.dell.com/support/edocs/software/svradmin/5.1/en/omss_ug/html/adprin.html にある、『OpenManage™ Server Administrator Storage Management User's Guide』（OpenManage™ Server Administrator Storage Management ユーザーズガイド）を参照してください。

モデル番号	物理ストレージディスクのモデル番号を表示します。
ホスト	ホスト名を表示します。
最新のインベントリ	インベントリが最後に実行された日、月、時刻が表示されます。
ステータス	ホストのステータスを表示します。
コントローラ ID	コントローラの ID を表示します。
コネクタ ID	コネクタ ID を表示します。
エンクロージャ ID	エンクロージャ ID を表示します。
デバイス ID	デバイス ID を表示します。
バスプロトコル	バスプロトコルを表示します。
ホットスペアのタイプ	ホットスペアのタイプを表示します。次のタイプがあります。 • いいえ いいえ、はホットスペアがないことを意味します。 • グローバル グローバルホットスペアは、ディスクグループの一部である使用されていないバックアップディスクです。 • 専用 専用ホットスペアは、単一の仮想ディスクに割り当てられた未使用のバックアップディスクです。仮想ディスク内の物理ディスクが故障すると、ホットスペアがアクティブ化されて故障した物理ディスクと交換されるため、システムが中断したり、ユーザー介入が必要になることもありません。
パーツ番号	ストレージのパーツ番号を表示します。
シリアル番号	ストレージのシリアル番号を表示します。
ベンダー名	ストレージのベンダー名を表示します。

37

ストレージの表示: データセンターとクラスタの仮想ディスク詳細

データセンターまたはクラスタの仮想ストレージの詳細は、Dell データセンター / クラスタ情報タブで表示します。このページで情報を表示させるには、インベントリジョブを実行します。表示されるデータは、どのビューのデータにアクセスしているかによって異なります。ハードウェアビューは OMSA および iDRAC からのデータを直接報告します。「インベントリジョブを今すぐ実行する」を参照してください。データセンターとクラスタページでは、情報を CSV ファイルにエクスポートすることが可能で、データグリッドでのフィルタ / 検索機能が提供されます。

1. VMware vSphere Web Clinet のナビゲータ エリアで、**vCenter インベントリリスト** を選択します。
2. **データセンター** または **クラスタ** をクリックします。
3. **オブジェクト** タブで、特定のデータセンターまたはクラスタを選択します。
4. **監視** タブで、**Dell データセンター / クラスタ情報** タブをクリックし、**ストレージ → 仮想ディスク** に移動して次を表示します。

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

ホスト	ホストの名前を表示します。
サービスタグ	サービスタグを表示します。
名前	仮想ディスクの名前を表示します。
物理ディスク	仮想ディスクの場所のある物理ディスクを表示します。
容量	仮想ディスクの容量が表示されます。
レイアウト	仮想ストレージのレイアウトタイプ、つまりこの仮想ディスクに設定された RAID のタイプが表示されます。
ホスト	ホスト名を表示します。
名前	仮想ディスク名を表示します。
最新のインベントリ	インベントリが最後に実行された曜日、日付と時刻が表示されます。
コントローラ ID	コントローラの ID を表示します。
デバイス ID	デバイス ID を表示します。
メディアタイプ	SSD または HDD が表示されます。
バスプロトコル	仮想ディスクに含まれる物理ディスクが使用する技術を表示します。可能な値は次のとおりです。 • SCSI • SAS • SATA

ストライプサイズ ストライプサイズは、単一のディスク上で各ストライプが消費する容量の合計を意味します。

デフォルト読み取りポリシー コントローラでサポートされているデフォルト読み取りポリシーです。次のオプションがあります。

- 先読み
- 先読みなし
- 適応先読み
- 読み取りキャッシュが有効
- 読み取りキャッシュが無効

デフォルト書き込みポリシー コントローラでサポートされているデフォルト書き込みポリシーです。次のオプションがあります。

- ライトバック
- ライトバックの強制
- ライトバックが有効
- ライトスルー
- 書き込みキャッシュ有効、保護
- 書き込みキャッシュが無効

ディスクキャッシュポリシー コントローラでサポートされているデフォルトキャッシュポリシーです。次のオプションがあります。

- 有効

  キャッシュ I/O です。
- 無効

  ダイレクト I/O です。

38

データセンターとクラスタのファームウェア詳細の表示

Dell ホストタブでデータセンター、またはクラスタのファームウェア詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。データセンターおよびクラスタページでは、情報を CSV ファイルにエクスポートし、データグリッドにフィルタ / 検索機能を提供します。ハードウェアビューでは、OMSA および iDRAC からデータを直接レポートします。「インベントリジョブを今すぐ実行する」を参照してください。

1. VMware vSphere Web Clinet のナビゲータで、**vCenter** を選択します。
2. **データセンター** または **クラスタ** をクリックします。
3. オブジェクト タブで、ファームウェア詳細 を表示したいデータセンター、またはクラスタを選択します。
4. 監視 タブで、**Dell データセンター / クラスタ情報** タブを選択し、ファームウェアサブタブで、次を表示します。

ホスト	ホストの名前を表示します。
サービスタグ	サービスタグを表示します。
名前	このホスト上のすべてのファームウェアの名前を表示します。
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を表示します。

39

データセンターとクラスタの保証サマリ詳細の表示

保証サマリを表示するには、保証ジョブを実行する必要があります。「保証ジョブを今すぐ実行する」を参照してください。
Dell データセンター / クラスタ情報タブでデータセンター、またはクラスタの保証サマリ詳細を表示します。データセンターとクラスタページでは、情報を CSV ファイルにエクスポートすることが可能で、データグリッドでのフィルタ / 検索機能が提供されます。保証サマリ ページでは、保証期限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 / 無効化し、最小日数しきい値アラートを設定することにより、Dell オンラインからサーバー保証情報が取得される時点を制御します。「保証履歴」を参照してください。

1. VMware vSphere Web Clinet のナビゲータで、**vCenter** を選択します。
2. **データセンター** または **クラスタ** をクリックします。
3. オブジェクト タブで、保証サマリの詳細を表示したいデータセンター、またはクラスタを選択します。
4. 監視 タブで、**Dell データセンター/クラスタ情報** タブを選択し、保証サマリ サブタブで、次を表示します。

保証サマリ	アイコンを使うと、各ステータスカテゴリのホスト数を視覚的に示すホスト保証サマリが表示されます。
ホスト	ホストの名前を表示します。
サービスタグ	ホストのサービスタグを表示します。
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を表示します。次のステータスがあります。 • 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できません。

残日数	保証の残りの日数を表示します。

40

データセンターおよびクラスタの電源監視の表示

Dell データセンター / クラスタ情報タブで、データセンターまたはクラスタの電源監視詳細を表示します。このページで情報を表示させるには、インベントリジョブを実行する必要があります。データセンターおよびクラスタページでは、情報を CSV ファイルにエクスポートし、データグリッドにフィルタ / 検索機能を提供します。ハードウェアビューでは、OMSA および iDRAC からデータを直接レポートします。「インベントリジョブを今すぐ実行する」を参照してください。

1. VMware vSphere Web Clinet のナビゲータで、**vCenter** を選択します。
2. **データセンター** または **クラスタ** をクリックします。
3. オブジェクト タブで、電源監視の詳細を表示したいデータセンター、またはクラスタを選択します。
4. 監視 タブで、**Dell データセンター/クラスタ情報ホスト** タブを選択し、電源監視サブタブで、次を表示します。

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

ホスト	ホストの名前を表示します。
サービスタグ	サービスタグを表示します。
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、電力を節約するための、電源プロファイルを表示します。
エネルギー消費量	ホストのエネルギー消費量を表示します。
ピーク予約容量	電力の PEEK 予約容量を表示します。
電力バジェット	このホストの電力上限を表示します。
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、設定最大値を表示します。
障害しきい値	お使いのシステムの温度プローブのエラー警告しきい値の、設定最大値を表示します。
インスタント予約容量	特定時点でのホストのヘッドルーム容量を表示します。
エネルギー消費量開始日	ホストが電力消費を開始した日付と時刻を表示します。
エネルギー消費量終了日	ホストが電力消費を停止した日付と時刻を表示します。
システムピーク電力	ホストのピーク電力を表示します。
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刻を表示します。

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刻を表示します。

システムピーク電流　ホストのピーク電流を表示します。

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刻を表示します。

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刻を表示します。

41

トラブルシューティング

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

- よくあるお問い合わせ（FAQ）
- ベアメタル展開の問題
- デルへのお問い合わせ
- 関連製品情報

よくあるお問い合わせ (FAQ)

本項には一般的な質問と解決策を記載しています。

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

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

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

影響を受けるバージョン：3.1

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

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

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

影響を受けるバージョン：3.1

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

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

解決策：例外を解決するには、サービスの ssl アンカーを更新する必要があります。ssl アンカーは、PSC で `ls_update_certs.py` スクリプトを実行してアップデートできます。スクリプトは古い証明書サムプリントを入力引数として使用し、新しい証明書がインストールされます。詳細については、http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 と http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689 にアクセスしてください。

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

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

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

次の関連する手順を使用して ssl アンカーをアップデートできます。

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

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

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

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

影響を受けるバージョン：3.0 以降、vCenter 6.0 以降

vCenter の Windows インストールでの証明書の置き換え

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

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

5. 次のコマンドを使用して古い証明書サムプリントを取得します。"%VMWARE_OPENSSL_BIN%" x509 -in C:\certificates\old_machine.crt -noout -sha1 -fingerprint

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

   サムプリントは一連の数字とアルファベットで、次のように表示されます。13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88

6. 次のコマンドを使用して新しい証明書を取得します。"%VMWARE_CIS_HOME%"\vmafdd\vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output c:\certificates\new_machine.crt
7. 次の手順を実行します。
   a. "%VMWARE _PYTHON_BIN%" ls_update_certs.py --url コマンドを使用して、ls_update_certs.py を実行します。
   b. psc.vmware.com を Lookup_Service_FQDN_of_Platform_Services_Controller で置き換え、https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile c:\certificates\new_machine.crt --user Administrator@vsphere.local --password Password コマンドを使用して、13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 サムプリントをステップ 5 で取得したサムプリントと置き換えます。

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

OMIVV が正常に起動します。

vCenter サーバアプライアンスでの証明書の置き換え

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

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

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

   サムプリントは一連の数字とアルファベットで、次のように表示されます。13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88

7. 次のコマンドを使用して新しい証明書を取得します。/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output /certificates/new_machine.crt
8. cd /usr/lib/vmidentity/tools/scripts/ コマンドを実行して、ディレクトリを変更します
9. 次の手順を実行します。

a. `python ls_update_certs.py --url` コマンドを使用して、`ls_update_certs.py` を実行します。
b. psc.vmware.com を Lookup_Service_FQDN_of_Platform_Services_Controller で置き換え、`https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile /certificates/new_machine.crt --user Administrator@vsphere.local --password "Password"` コマンドを使用して、13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 サムプリントをステップ 6 で取得したサムプリントと置き換えます。

メモ: 必ず有効な資格情報を入力してください。

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

OMIVV が正常に起動します。

管理対象オブジェクトブラウザ（MOB）から古い証明書を取得する

管理対象オブジェクトブラウザ（MOB）を使用してプラットフォームサービスコントローラ（PSC）に接続することにより、vCenter サーバシステムの古い証明書を取得することができます。
古い証明書を取得するには、次のステップを実行して、ArrayOfLookupServiceRegistrationInfo 管理対象オブジェクトの sslTrust フィールドを見つけます。

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

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

   メモ: vCenter シングルサインオン（SSO）ドメインにカスタム名を使用している場合は、そのユーザー名とパスワードを使用します。
4. **filterCriteria** で、値フィールドを変更してタグ **<filtercriteria></filtercriteria>** のみを表示し、**メソッドの呼び出し** をクリックします。
5. 置き換える証明書に応じて次のホスト名を検索します。

表 6. 検索条件情報

トラストアンカー	検索条件
vCenter サーバ	Ctrl+F を使用して、ページで vc_hostname_or_IP.example.com を検索
プラットフォームサービスコントローラ	Ctrl+F を使用して、ページで psc_hostname_or_IP.example.com を検索

6. 対応する sslTrust フィールドの値を確認します。sslTrust フィールドの値は古い証明書の Base64 エンコード文字列です。
7. プラットフォームサービスコントローラまたは vCenter サーバのトラストアンカーを更新する際には、次の例を使用します。

   メモ: 実際の文字列が大幅に短縮され、読みやすくなります。

   - vCenter サーバの場合

表 7. vCenter サーバの例

名前	タイプ	値
url	anyURI	https://vcenter.vmware.local:443/sdk

- プラットフォームサービスコントローラの場合

表 8. プラットフォームサービスコントローラの例

名前	タイプ	値
url	anyURI	https://psc.vmware.local/sts/STSService/vsphere.local

8. sslTrust フィールドの内容をテキスト文書にコピーし、その文書を **old_machine.txt** として保存します。
9. テキストエディターで **old_machine.txt** を開きます。
10. 以下を、それぞれ **old_machine.txt** ファイルの最初と最後に追加します。

```
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
```

11. **old_machine.txt** を **old_machine.crt** として保存します。

これでこの証明書からサムプリントを抽出できます。

古い証明書からのサムプリントの抽出

次のオプションを使用して、古い証明書からサムプリントを抽出し、プラットフォームサービス にアップロードできます。

- 証明書ビューアツールを使用して、サムプリントを抽出します。「証明書ビューアツールを使用した証明書サムプリントの抽出」を参照してください。
- アプライアンスでコマンドラインを使用して、サムプリントを抽出します。「コマンドラインを使用してサムプリントを抽出する」を参照してください。

証明書ビューアツールを使用した証明書サムプリントの抽出

次のステップを実行して、証明書サムプリントを抽出します。

1. Windows で、**old_machine.txt** ファイルをダブルクリックして、Windows 証明書ビューアで開きます。
2. Windows 証明書ビューアで、**SHA1 サムプリント** フィールドを選択します。
3. サムプリントの文字列をプレーンテキストエディターにコピーしてスペースをコロンで置き換えるか、文字列からスペースを削除します。

   たとえば、サムプリントの文字列は、次のいずれかのように表示されます。

   - ea87e150bb96fbbe1fa95a3c1d75b48c30db7971
   - ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71

コマンドラインを使用してサムプリントを抽出する

アプライアンスと Windows のインストールでコマンドラインを使用してサムプリントを抽出するには、次の項を参照してください。

vCenter サーバアプライアンスでコマンドラインを使用してサムプリントを抽出する

次の手順を実行します。

1. old_machine.crt 証明書を、古い証明書を取得するためのステップ 1 で作成した **C:\certificates\old_machine.crt** の場所にある PSC に移動またはアップロードします。Windows セキュアコピー（WinSCP）またはその他の SCP クライアントを使用して証明書を移動またはアップロードできます。
2. セキュアシェル（SSH）経由で外付けのプラットフォームサービスコントローラアプライアンスにログインします。
3. 次のコマンドを実行して Bash シェルへのアクセスを有効にします。`shell.set --enabled true`
4. `shell` と入力し、**Enter** を押します。
5. 次のコマンドを実行してサムプリントを抽出します。`openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint`

メモ: サムプリントは、等号に続く一連の数字とアルファベットで、次のように表示されます。`SHA1 Fingerprint= ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71`

Windows のインストールでコマンドラインを使用してサムプリントを抽出する

次の手順を実行します。

1. old_machine.crt 証明書を、古い証明書を取得するためのステップ 1 で作成した **C:\certificates\old_machine.crt** の場所にある PSC に移動またはアップロードします。Windows セキュアコピー（WinSCP）またはその他の SCP クライアントを使用して証明書を移動またはアップロードできます。
2. リモートデスクトップ接続を通じて外付けのプラットフォームサービスコントローラに接続します。
3. 管理モードでコマンドプロンプトを開きます。
4. 次のコマンドを実行してサムプリントを抽出します。`"%VMWARE_OPENSSL_BIN%" x509 -in c:\certificates\old_machine.crt -noout -sha1 -fingerprint`

メモ: サムプリントは、等号に続く一連の数字とアルファベットで、次のように表示されます。`SHA1 Fingerprint=09:0A:B7:53:7C:D9:D2:35:1B:4D:6D:B8:37:77:E8:2E:48:CD:12:1B`

古いサムプリントで ls_update_certs.py を実行します。すべてのサービスが正常にアップデートされた後に、vCenter ウェブクライアントから一度ログアウトしてから再度ログインします。デルプラグインが正常に起動します。

ファームウェアアップデートウィザードに、バンドルがファームウェアリポジトリから取得されていないというメッセージが表示されます。どうすればファームウェアアップデートを続行できますか?

ウェブクライアントでは、単一ホストにファームウェアアップデートウィザードを実行したとき、**コンポーネントの選択** 画面にコンポーネントのファームウェア詳細が表示されます。必要なファームウェアのアップデートを選択して、**戻る** を 2 回クリックし **ようこそ** ページに到着したときに **次へ** をクリックすると、**アップデートソースの選択** 画面に、バンドルがファームウェアリポジトリから取得されていないというメッセージが表示されます。

解決策：目的のファームウェアアップデートを選択し、**次へ** をクリックして、ファームウェアアップデートを続行できます。

影響を受けるバージョン：3.0 以降

クラスタレベルでの 30 台のホストのファームウェアアップデートが失敗する

VMware では、クラスタを同一のサーバーハードウェアで構築することをお勧めしています。ホスト数がクラスタの上限（VMware 推奨）に近い状態のクラスタ、または異なるモデルの Dell で構成されているクラスタでのクラスタレベルのファームウェアアップデートには、vSphere Web Client の使用が推奨されます。

「Dell Home > 監視 > ジョブキュー > 保証 / インベントリ履歴 > スケジュール」と選択したときに、すべての vCenter に保証とインベントリスケジュールが適用されません

ユーザーはジョブキューページに移動し、ひとつの vCenter を選択してスケジュールの変更ボタンを選択します。ダイアログが開くと、この新しい設定をすべての登録済み vCenter に適用するというチェックボックスが表示されます。ユーザーがこれを選択して適用を押すと、すべての vCenter ではなく、当初選択した特定の vCenter のみに設定が適用されます。「すべての登録済み vCenter に適用する」は、ジョブキューページから保証またはインベントリスケジュールが変更されるときには適用されません。

対応処置：ジョブキューページからのインベントリまたは保証スケジュールの変更は、選択した vCenter を変更する場合にのみ、使用してください。

影響を受けるバージョン：2.2 以降

OpenManage Integration for VMware vCenter で DNS の設定を変更した後、vCenter Web Client でウェブ通信エラーが発生します。

DNS 設定の変更後、OMIVV 関連タスクを行っているときに vCenter Web Client で何らかのウェブ通信エラーが発生する場合は、ブラウザキャッシュをクリアする、または Web Client からログアウトしてログインし直してください。

「設定」ページから移動した後に「設定」ページに戻ると、ページのロードが失敗します。

vSphere v5.5 では、Web Client で「設定」ページから移動した後にページに戻ると、ロードが失敗し、スピナーが表示され続けることがあります。これは更新問題で、ページが正しく更新されていません。

対応処置：グローバル更新をクリックすると、画面が正しく更新されます。

影響を受けるバージョン：2.2 および 3.0

初期設定ウィザードのインベントリスケジュール / 保証スケジュールページで「過去の時間にタスクをスケジュールすることはできません」と表示されるのはなぜですか?

Web Client では、ユーザーが初期設定ウィザードで「すべての登録済み vCenter」を選択したときに、ホストのない vCenter がある、またはインベントリ / 保証タスクがすでにスケジュールされている vCenter とされていない vCenter がある場合、ユーザーに「過去の時間にタスクをスケジュールすることはできません」エラーが表示されることがあります。

対応処置：ホストのない vCenter がある、またはインベントリ / 保証タスクがすでにスケジュールされている vCenter とされていない vCenter があるという状態が存在する場合、これらの vCenter の設定ページから、インベントリと保証スケジュールの設定を再度個別に実行します。

影響を受けるバージョン：2.2 以降

ファームウェアページで一部のファームウェアのインストール日が 12/31/1969 として表示されるのはなぜですか?

Web Client では、ホスト向けのファームウェアページで一部のファームウェアアイテムのインストール日が 12/31/1969 として表示されます。ファームウェアのインストール日が使用不可である場合、このように古い日付が表示されます。

対応処置：ファームウェアコンポーネントの一部にこの古い日付が表示される場合は、そのコンポーネントのインストール日が使用不可であると考えてください。

影響を受けるバージョン：2.2 以降

連続したグローバル更新によって最近のタスクウィンドウに例外が生成されるのはなぜですか?

ユーザーが連続して更新ボタンを押すと、VMware UI が例外を生成する場合があります。

対応処置：ユーザーはこのエラーを無視して続行することができます。

影響を受けるバージョン：2.2 以降

IE 10 のデル画面のいくつかで Web Client UI が歪むのはなぜですか?

場合によって、ポップアップダイアログが表示されるときに、バックグラウンドのデータが完全に白くなり、歪むことがあります。

対応処置：ダイアログを閉じると、画面は通常状態に戻ります。

影響を受けるバージョン：2.2 以降

vCenter へのプラグインの登録に成功したにもかかわらず、Web Client に OpenManage Integration アイコンが表示されないのはなぜですか?

OpenManage Integration アイコンは、vCenter Web Client サービスが再起動されるか、Box が再起動されない限り Web Client に表示されません。ユーザーが OpenManage Integration for VMware vCenter アプライアンスを登録すると、アプライアンスは Desktop クライアントと Web Client の両方に登録されます。ユーザーがアプライアンスの登録を解除した後で、そのアプライアンスの同じバージョンの再登録、または新しいバージョンの登録のどちらかを行うと、両方のクライアントに正常に登録されますが、Dell アイコンが Web Client 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、ユーザーが vCenter Server で Web Client サービスを再起動する必要があります。これを行って初めてプラグインが UI に表示されます。

対応処置：vCenter Server で Web Client サービスを再起動します。

影響を受けるバージョン：2.2 以降

選択した 11G システム用のバンドルがリポジトリにあっても、ファームウェアアップデートがファームウェアアップデート用バンドルがないと表示するのはなぜですか?

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

ホストをロックダウンモードにする、またはロックダウンモードから解除する場合、次の操作を実行する前に 30 分待機する必要があり、ファームウェアアップデート用に 11G システムを選択すると、入力したリポジトリにそのシステムのためのバンドルがあったとしても、ファームウェアアップデートウィザードにはバンドルが表示されません。この問題は、11G ホストが OpenManage Integration にトラップを送信するよう OMSA で設定されていない場合に発生します。

対応処置：OpenManage Integration Desktop Client のホストコンプライアンス画面を使用して、ホストが準拠していることを確認します。準拠していない場合は、ホストコンプライアンスの修正を使用して準拠させてください。

対象バージョン： 2.2 以降

保証取得ジョブを実行しているときに、保証ジョブのステータスが保証の ジョブ キュー ページに記載されていません

インターネットに接続するために、ネットワークにプロキシの詳細が必要で、OMIVV アプライアンスにプロキシが設定されていない場合、保証取得ジョブが失敗し、ジョブは保証ジョブキューの下に表示されません。
解決策：プロキシの詳細を設定し、保証ジョブをもう一度トリガします。

対象バージョン：すべて

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

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

対象バージョン：すべて

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

Dell PowerEdge 第 12 世代サーバーとファームウェアバージョン 13.5.2 の一部の Intel ネットワークカードには、既知の問題があります。このバージョンのファームウェアを搭載した Intel ネットワークカードの一部のモデルのアップデートは、このファームウェアのアップデートを Lifecycle Controller を使用して適用すると失敗します。このバージョンのファームウェアを使用しているユーザーは、オペレーティングシステムでネットワークドライバのソフトウェアをアップデートしてください。 Intel ネットワークカードのファーム

ウェアのバージョンが 13.5.2 以外であれば、OpenManage Integration for VMware vCenter を使用してアップデートすることができます。詳細に関しては、http://en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx を参照してください。

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

Intel ネットワークカードを 14.5 または 15.0 から 16.x にアップデートするために OpenManage Integration for VMware vCenter を使用すると、DUP からのステージング要件のためにアップデートに失敗する。

これは NIC 14.5 および 15.0 で既知の問題です。ファームウェアを 16.x にアップデートする前に、まずファームウェアを 15.5.0 にアップデートするためにカスタムカタログを使用する必要があります。

対象バージョン：すべて

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

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

対応処置： このタスクを手動でキャンセルする必要があります。

対象バージョン：すべて

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

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

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

対象バージョン：すべて

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

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

一部の電源装置のステータスが重要に変更されても、シャーシのグローバル正常性が正常のままになっているのはなぜですか?

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、シャーシの電力需要が引き続きオンラインで機能している PSU によって満たされているかどうかに基づいています。従って、一部の PSU が電

力なしとなってもシャーシの全体的な電力要件は満たされており、シャーシのグローバル正常性は正常となります。電源装置および電源管理についての詳細は、ユーザーズガイドで Dell PowerEdge M1000e シャーシ管理コントローラファームウェア文書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、プロセッサバージョンが「該当なし」となっているのはなぜですか?

第 12 世代以降の Dell PowerEdge サーバーの場合、プロセッサバージョンはブランド列に表示されます。それより前の世代では、プロセッサバージョンはバージョン列に表示されます。

Web Client を使用して接続プロファイルを編集した後に終了をクリックすると、いつも例外が表示されます。なぜですか?

この問題は、vCenter Server が FQDN ではなく IP によってアプライアンスに登録されているときに発生します。接続プロファイルは Desktop クライアントを使用して編集することが可能です。この vCenter Server を同じアプライアンスに再登録しても問題は解決されません。FQDN で登録された新しいセットアップが必要です。

ウェブ GUI で接続プロファイルを作成 / 編集するときに、ホストが属する接続プロファイルを見ることができません。なぜですか?

この問題は、vCenter サーバーが FQDN ではなく IP によってアプライアンスに登録されているときに発生します。この vCenter サーバーを同じアプライアンスに再登録しても問題は解決されません。FQDN で登録された新しいセットアップが必要です。

接続プロファイルを編集するときに、ウェブ UI の特定のホストウィンドウが空です。なぜですか ?

この問題は、vCenter サーバーが FQDN ではなく IP によってアプライアンスに登録されているときに発生します。この vCenter サーバーを同じアプライアンスに再登録しても問題は解決されません。FQDN で登録された新しいセットアップが必要です。

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

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

図 1. ファームウェアリンク通信エラー

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

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

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

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

OpenManage Integration for VMware vCenter によって管理されるのはどの vCenter ですか?

OpenManage Integration for VMware vCenter は、リンクモード、非リンクモードのいずれかで登録されている vCenter のみを管理します。

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

はい、OpenManage Integration for VMware vCenter は、リンクモードであるかに関わらず、最大 10 の vCenter をサポートします。リンクモードにおける OpenManage Integration for VMware vCenter の動作については、www.Dell.com に記載されているホワイトペーパー、『OpenManage Integration for VMware vCenter： リンクモードでの作業』を参照してください。

OpenManage Integration for VMware vCenter にはどのようなポート設定が必要ですか?

メモ: OpenManage Integration for VMware vCenter のコンプライアンスウィンドウから使用できる *非準拠 vSphere ホストの修正*リンクを使用して OMSA エージェントを展開する場合、OMSA VIB のダウンロードとインストールのため、OpenManage Integration for VMware vCenter は ESXI 5.0 より後のリリースで http クライアントサービスを開始してポート 8080 を有効にします。OMSA のインストールが完了すると、サービスが自動的に停止し、ポートが閉じられます。

これらのポートの設定を OpenManage Integration for VMware vCenter に使用してください。

表 9. 仮想アプライアンスポート

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

表 10. 管理下ノード

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

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

以下の設定は、最低限のアプライアンス要件の概要です。

- Google Chrome バージョン 28 以降

  。
- Microsoft Internet Explorer、バージョン 9 および 10
- Mozilla Firefox バージョン 22 以降
- 予約メモリ： 2 GB

  メモ: 最適なパフォーマンスのため、Dell では 3 GB をお勧めしています。
- ディスク： 43.5 GB。
- CPU： 2 つの仮想 CPU

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

vSphere Desktop Client の 最近のタスク ペインでのファームウェアアップデートタスクが正常に終了したら、ファームウェアアップデート ページを更新してファームウェアバージョンを確認します。そのページに古いバージョンが表示される場合は、OpenManage Integration for VMware vCenter のホストコンプライアンス ページ移動し、そのホストの CSIOR ステータスをチェックします。CSIOR が有効化されていない場合は、CSIOR を有効化してホストを再起動してください。CSIOR がすでに有効化されている場合は、iDRAC コンソールにログインし、iDRAC をリセットしてから数分待って、その後 VMware vSphere Desktop Client でファームウェアアップデートページを更新します。

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

イベントが正しく機能していることを確認するには、次の手順を行います。

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

12. **Apply Changes（変更の適用）**を選択すると、温度警告イベントが生成されます。別のイベントを発生させるには、同じ **Set to Values（値に設定）**オプションを使用して元の設定を復元します。イベントは警告として生成されてから、正常な状態になります。すべてが適切に動作している場合は、**vCenter Tasks & Events（vCenter タスクおよびイベント）**ビューに移動します。温度プローブ警告イベントが表示されています。

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

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

この問題を解決するには、第 11 世代サーバで次の作業を行います。

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

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

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

OpenManage Integration for VMware vCenter はロックダウンモードが有効になっている ESXi をサポートしますか?

はい。本リリースでは、ロックダウンモードは ESXi 5.0 以降のホストにおいてサポートされています。

ロックダウンモードを使用しようとしたら、失敗しました。

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

ホストをロックダウンモードにする、またはロックダウンモードから解除する場合、OpenManage Integration for VMware vCenter で次の操作を実行する前に、30 分待機する必要があります。

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

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

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

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

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

ブレードサーバーに ESXi を展開しようとしていますが、失敗しました。どうすればよいですか?

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

Dell PowerEdge R210 II マシンでハイパーバイザー展開が失敗するのはなぜですか?

連結された ISO からの BIOS 起動の失敗により、Dell PowerEdge R210 II システムにおけるタイムアウト問題がハイパーバイザー展開失敗を生じます。この問題を解決するには、ハイパーバイザーを手動でマシンにインストールしてください。

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

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

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

解決法を見つけるには、次の手順を行います。

1. iDRAC がアプライアンスに対して ping を実行できることを確認します。
2. ネットワークの稼働速度が遅すぎないことを確認します。
3. ポート 2049、4001～4004 が開いていること、ファイアウォールがそれに応じて設定されていることを確認します。

仮想アプライアンスを強制削除するにはどのようにしたらよいですか?

1. **https://<vcenter_serverIPAddress>/mob** にアクセスします。
2. VMware vCenter のシステム管理者資格情報を入力します。
3. **コンテンツ** をクリックします。
4. **ExtensionManager** をクリックします。
5. **UnregisterExtension** をクリックします。
6. 延長キーを入力して com.dell.plugin.openManage_integration_for_VMware_vCenter を登録解除し、**メソッドの呼び出し** をクリックします。

7. 延長キーを入力して com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient を登録解除し、**メソッドの呼び出し** をクリックします。
8. vSphere Web Client で OpenManage Integration for VMware vCenter の電源をオフにして、削除します。登録解除用のキーは Web Client 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する必要があります。

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

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

ファームウェアアップデートが失敗しました。どうしたらよいですか?

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

vCenter の登録が失敗しました。どうしたらよいですか?

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

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

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

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

無効状態のサーバーを修正するには、次の手順を行います。

1. Chassis Management Controller コンソールを開いて、無効になっているサーバーを選択します。
2. iDRAC コンソールを自動的に開くには、**iDRAC GUI の起動** をクリックします。
3. iDRAC コンソールでユーザーリストまで移動して、次のいずれかを選択します。
   - iDRAC 6：**iDRAC 設定 → ネットワーク / セキュリティタブ → ユーザータブ** を選択します。

- 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。

4. 設定を編集するには、User ID（ユーザー ID）列で、管理者（root）ユーザーのリンクをクリックします。
5. **ユーザーの設定** をクリックして、**次へ** をクリックします。
6. 選択され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。

OpenManage Integration for VMware vCenter は VMware vCenter Server Appliance をサポートしますか?

はい。OpenManage Integration for VMware vCenter は、バージョン 2.1 から VMware vCenter Server Appliance をサポートしています。

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

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

次回の再起動時にファームアップデートを適用するオプションでファームウェアのアップデートを行ってシステムを再起動したにも関わらず、ファームウェアのレベルがアップデートされないのはなぜですか?

ファームウェアをアップデートするには、再起動が完了してからホストでインベントリを実行します。時折、再起動イベントがアプライアンスに到達せず、インベントリが自動的にトリガされない場合があります。そのような場合は、インベントリを手動で再実行し、アップデートされたファームウェアバージョンを取得する必要があります。

ホストを vCenter ツリーから削除した後でもシャーシにそのホストが引き続き表示されるのはなぜですか?

シャーシ下のホストはシャーシインベントリの一部として認識されます。シャーシインベントリが正常に行われた後、シャーシ下のホストリストがアップデートされます。したがって、ホストが vCenter ツリーから削除されても、そのホストは次のシャーシのインベントリが実行されるまでシャーシ下に表示されます。

管理コンソールで、アプライアンスを工場出荷時設定にリセットした後、リポジトリパスのアップデート がデフォルトに設定されないのはなぜですか?

アプライアンスをリセットした後、管理コンソールに移動して、左ペインで **アプライアンス管理** をクリックします。**アプライアンス設定** ページでは **リポジトリパスのアップデート** がデフォルトのパスに変更されていません。

対応処置： 管理コンソールで、**デフォルトのアップデートリポジトリ** フィールドにあるパスを、**リポジトリパスのアップデート** フィールドに手動でコピーします。

OpenManage Integration for VMware vCenter のバックアップおよび復元の後、アラーム設定が復元されないのはなぜですか?

OpenManage Integration for VMware vCenter アプライアンスのバックアップを復元しても、一部のアラーム設定は復元されません。ただし、OpenManage Integration for VMware GUI の **アラームとイベント** フィールドには復元された設定が表示されます。

対応処置： OpenManage Integration for VMware GUI の **管理 → 設定** タブで、**イベントおよびアラーム** 設定を手動で変更します。

ベアメタル展開の問題

本項では、展開プロセスで見つかった問題の処理について説明します。

自動検出とハンドシェイクの前提条件

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

ハードウェア設定の失敗

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

デルへのお問い合わせ

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

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

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

OpenManage Integration for VMware vCenter の関連情報

- PowerEdge™ サーバ用 Dell サーバマニュアルの表示またはダウンロード：Dell PoweEdge マニュアル
- Dell OpenManage システム Administrator マニュアル：Dell OMSA 文書

- Dell Lifecycle Controller マニュアル：DLCI マニュアル

42

Dell PowerEdge サーバーの仮想化関連イベント

次の表には、イベント名、説明、重大度レベルを含む、第 11 世代、第 12 世代、および 13 世代 PowerEdge サーバーに対する仮想化関連の重要および警告イベントが記載されています。

表 11. 第 11 世代、第 12 世代、および 13 世代 PowerEdge サーバーの仮想化関連イベント

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

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

イベント名	説明	重大度	推奨処置
	して分類する必要があります。		
Dell - Processor sensor returned to a normal value	センサーが正常値に戻りました	情報	処置は不要
Dell - Processor sensor detected a warning value	指定したシステムのプロセッサセンサーがスロットル状態です。	警告	処置は不要
Dell - Processor sensor detected a failure value	指定したシステムのプロセッサセンサーが無効になっている、設定エラーがある、またはサーマルトリップが発生しました。	エラー	処置は不要
Dell - Processor sensor detected a non-recoverable value	指定したシステムのプロセッサセンサーが故障しました。	エラー	処置は不要
Dell - Device configuration error	指定したシステムのプラグ可能デバイスで設定エラーが検出されました。	エラー	処置は不要
Dell - Battery sensor returned to a normal value	センサーが正常値に戻りました	情報	処置は不要
Dell - Battery sensor detected a warning value	指定したシステムのバッテリセンサーが、バッテリが予測不具合状態にあることを検出しました。	警告	処置は不要
Dell - Battery sensor detected a failure value	指定したシステムのバッテリセンサーが、バッテリの故障を検出しました。	エラー	処置は不要
Dell - Battery sensor detected a nonrecoverable value	指定したシステムのバッテリセンサーが、バッテリの故障を検出しました。	エラー	処置の必要なし
Dell - Thermal shutdown protection has been initiated	このメッセージは、システムがエラーイベントによるサーマルシャットダウンに設定されたときに生成されます。温度センサー読み取り値がシステムで設定されたエラーしきい値を超えると、オペ	エラー	処置は不要

イベント名	説明	重大度	推奨処置
	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。		
Dell - Temperature sensor returned to a normal value	センサーが正常値に戻りました	情報	処置は不要
Dell - Temperature sensor detected a warning value	指定したシステムのバックプレーン基板、システム基板、CPU、またはドライブキャリア上の温度センサーが警告しきい値を超えました。	警告	処置は不要
Dell - Temperature sensor detected a failure value	指定したシステムのバックプレーン基板、システム基板、またはドライブキャリア上の温度センサーが障害しきい値を超えました。	エラー	システムをメンテナンスモードにしてください
Dell - Temperature sensor detected a non-recoverable value	指定したシステムのバックプレーンボード、システム基板、またはドライブキャリアの温度センサーが回復不可能なエラーを検出しました。	エラー	処置は不要
Dell - Fan sensor returned to a normal value	センサーが正常値に戻りました	情報	処置は不要
Dell - Fan sensor detected a warning value	ホスト <x> のファンセンサー読み取り値が警告しきい値を超えました。	警告	処置の必要なし
Dell - Fan sensor detected a failure value	指定したシステムのファンセンサーが 1 つまたは複数のファンの障害を検出しました。	エラー	システムをメンテナンスモードにしてください
Dell - Fan sensor detected a nonrecoverable value	ファンセンサーが回復不可能なエラーを検出しました。	エラー	処置は不要

イベント名	説明	重大度	推奨処置
Dell - Voltage sensor returned to a normal value	センサーが正常値に戻りました	情報	処置は不要
Dell - Voltage sensor detected a warning value	指定したシステムの電圧センサーが警告しきい値を超えました。	警告	処置は不要
Dell - Voltage sensor detected a failure value	指定したシステムの電圧センサーが障害しきい値を超えました。	エラー	システムをメンテナンスモードにしてください
Dell - Voltage sensor detected a nonrecoverable value	指定したシステムの電圧センサーが回復不可能なエラーを検出しました	エラー	処置は不要
Dell - Current sensor returned to a normal value	センサーが正常値に戻りました	情報	処置は不要
Dell - Storage: storage management error	ストレージ管理がデバイス依存のエラー状態を検出しました。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: Controller warning	コントローラの警告です。詳細に関しては、vSphere クライアントのタスクとイベント タブを参照して下さい。	警告	処置は不要
Dell - Storage: Controller failure	コントローラの障害です。詳細に関しては、vSphere の タスクとイベント タブを参照して下さい。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: Channel Failure	チャネル障害です。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: Enclosure hardware information	エンクロージャハードウェア情報です。	情報	処置は不要
Dell - Storage: Enclosure hardware warning	エンクロージャハードウェア警告です。	警告	処置は不要
Dell - Storage: Enclosure hardware failure	エンクロージャハードウェアエラーです。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: Array disk failure	アレイディスク障害です。	エラー	システムをメンテナンスモードにしてください

イベント名	説明	重大度	推奨処置
Dell - Storage: EMM failure	EMM 障害です。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: power supply failure	電源装置障害です。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: temperature probe warning	物理ディスク温度プローブ警告で、低温すぎるか高温すぎます。	警告	処置は不要
Dell - Storage: temperature probe failure	物理ディスク温度プローブエラーで、低温すぎるか高温すぎます。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: Fan failure	ファン障害です。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: Battery warning	バッテリ警告です。	警告	処置は不要
Dell - Storage: Virtual disk degraded warning	仮想ディスクの劣化警告です。	警告	処置は不要
Dell - Storage: Virtual disk degraded failure	仮想ディスク劣化障害です。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: Temperature probe information	温度プローブ情報です。	情報	処置は不要
Dell - Storage: Array disk warning	アレイディスク警告です。	警告	処置は不要
Dell - Storage: Array disk information	アレイディスク情報です。	情報	処置は不要
Dell - Storage: Power supply warning	電源装置警告です。	警告	処置は不要
Dell - Chassis Intrusion - Physical Security Violation	シャーシイントルージョン - 物理的なセキュリティ違反です。	エラー	処置の必要なし
Dell - Chassis Intrusion(Physical Security Violation) Event Cleared	シャーシイントルージョン（物理的セキュリティ違反）イベントがクリアされました	情報	処置の必要なし
Dell - CPU Presence (Processor Presence detected)	CPU 存在（プロセッサの存在が検出されています）	情報	処置の必要なし
Dell - System Event Log (SEL) Full (Logging Disabled)	システムイベントログ（SEL）が満杯です（ログが無効になっています）	エラー	処置の必要なし

イベント名	説明	重大度	推奨処置
Dell - System Event Log (SEL) Cleared	システムイベントログ（SEL）がクリアされました	情報	処置の必要なし
Dell - SD Card redundancy Has Returned to Normal	SD カードの冗長性が正常に戻りました	情報	処置の必要なし
Dell - SD Card Redundancy has been Lost	SD カードの冗長性が失われました	エラー	処置の必要なし
Dell - SD Card Redundancy Degraded	SD カードの冗長性が劣化しています	警告	処置の必要なし
Dell - Module SD Card Present (SD Card Presence Detected)	モジュール SD カードが存在します（SD カードの存在が検出されました）	情報	処置の必要なし
Dell - Module SD Card Failed (Error)	モジュール SD カードの不具合（エラー）です	エラー	処置の必要なし
Dell - Module SD Card Write Protect(Warning)	SD カードモジュールが書き込み保護されています（警告）	警告	処置の必要なし
Dell - Module SD Card not Present	SD カードモジュールが存在しません	情報	処置の必要なし
Dell - Watchdog Timer Expired	ウォッチドッグタイマーが期限切れです	エラー	処置の必要なし
Dell - Watchdog Reset	ウォッチドッグがリセットされました	エラー	処置の必要なし
Dell - Watchdog Power Down	ウォッチドッグの電源が切れています	エラー	処置の必要なし
Dell - Watchdog Power cycle	ウォッチドッグのパワーサイクルです	エラー	処置の必要なし
Dell - System Power Exceeds PSU Wattage	システム消費電力が PSU のワット数を超過しています	エラー	処置の必要なし
Dell - System Power Exceeds Error Cleared	システム消費電力超過のエラーがクリアされました	情報	処置の必要なし
Dell - Power Supply Inserted	電源装置が挿入されました	情報	処置の必要なし
Dell - Internal Dual SD Module is present	内蔵デュアル SD モジュールが存在します	情報	処置の必要なし

イベント名	説明	重大度	推奨処置
Dell - Internal Dual SD Module is online	内蔵デュアル SD モジュールがオンラインです	情報	処置の必要なし
Dell - Internal Dual SD Module is operating normally	内蔵 デュアル SD モージュールが正常に動作しています	情報	処置の必要なし
Dell - Internal Dual SD Module is write protected	内蔵デュアル SD モジュールが書込み防止になっています	警告	処置の必要なし
Dell - Internal Dual SD Module is writable	内蔵ディアル SD モジュールが書き込み可能です	情報	処置の必要なし
Dell - Integrated Dual SD Module is absent	内蔵デュアル SD モジュールが不在です	エラー	処置の必要なし
Dell - Integrated Dual SD Module redundancy is lost	内蔵デュアル SD モジュールの冗長性が失われました	エラー	処置の必要なし
Dell - Internal Dual SD Module is redundant	内蔵デュアル SD モジュールが冗長です	情報	処置の必要なし
Dell - Internal Dual SD Module is not redundant	内蔵デュアル SD モジュールが冗長性を欠いています	情報	処置の必要なし
Dell - Integrated Dual SD Module failure	内蔵デュアル SD モジュールエラーです	エラー	処置の必要なし
Dell - Internal Dual SD Module is redundant	内蔵デュアル SD モジュールがオフラインです	警告	処置の必要なし
Dell - Integrated Dual SD Module redundancy is lost	内蔵デュアル SD モジュールの冗長性が劣化しています	警告	処置の必要なし
Dell - SD card device has detected a warning	SD カードデバイスが警告を検出しました	警告	処置の必要なし
Dell - SD card device has detected a failure	SD カードデバイスがエラーを検出しました	エラー	処置の必要なし
Dell - Integrated Dual SD Module warning	内蔵デュアル SD モジュールの警告です	警告	処置の必要なし
Dell - Integrated Dual SD Module information	内蔵デュアル SD モジュールの情報です	情報	処置の必要なし
Dell - Integrated Dual SD Module redundancy information	内蔵デュアル SD モジュールの冗長性情報です	情報	処置の必要なし

イベント名	説明	重大度	推奨処置
Dell - Network failure or critical event	ネットワークエラーまたは重要なイベントです	エラー	処置の必要なし
Dell - Network warning	ネットワークの警告です	警告	処置の必要なし
Dell - Network information	ネットワーク情報です	情報	処置の必要なし
Dell - Physical disk failure	物理ディスクの障害です	エラー	処置の必要なし
Dell - Physical disk warning	物理ディスクの警告です	警告	処置の必要なし
Dell - Physical disk information	物理ディスクの情報です	情報	処置の必要なし
Dell - An error was detected for a PCI device	PCI デバイスでエラーが検出されました	エラー	処置の必要なし
Dell - A warning event was detected for a PCI device	PCI デバイスで警告イベントが検出されました	警告	処置の必要なし
Dell - An informational event was detected for a PCI device	PCI デバイスで情報イベントが検出されました	情報	処置の必要なし
Dell - Virtual Disk Partition failure.	仮想ディスクのパーティションの障害です。	エラー	処置の必要なし
Dell - Virtual Disk Partition warning.	仮想ディスクのパーティションに関する警告です。	警告	処置の必要なし
Dell - Cable failure or critical event	ケーブルの故障、または重要なイベントです	エラー	処置の必要なし
Dell - Chassis Management Controller detected an error.	Chassis Management Controller がエラーを検出しました。	エラー	処置の必要なし
Dell - IO Virtualization failure or critical event.	I / O 仮想化の失敗、または重要なイベントです。	エラー	処置の必要なし
Dell - Link status failure or critical event.	リンク状態のエラーか、重要なイベントです。	エラー	処置の必要なし
Dell - System: Software configuration failure.	システム： ソフトウェアの設定に障害が発生しています。	エラー	処置の必要なし

イベント名	説明	重大度	推奨処置
Dell - Storage Security failure or critical event.	ストレージセキュリティのエラーか、または重要なイベントです。	エラー	処置の必要なし
Dell - Chassis Management Controller audit failure or critical event.	Chassis Management Controller の監査エラーか、または重要なイベントです。	エラー	処置の必要なし
Dell - Power Supply audit failure or critical event.	電源装置の監査エラーか、または重要なイベントです。	エラー	処置の必要なし
Dell - Power usage audit failure or critical event.	消費電力の監査エラーまたは重要なイベントです。	エラー	処置の必要なし
Dell - Configuration: Software configuration failure.	設定： ソフトウェアの設定エラーです。	エラー	処置の必要なし
Dell - Chassis Management Controller detected a warning.	Chassis Management Controller が警告を検出しました。	警告	処置の必要なし
Dell - Link status warning.	リンク状態に関する警告です。	警告	処置の必要なし
Dell - Security warning.	セキュリティ警告です。	警告	処置の必要なし
Dell - System: Software configuration warning.	システム： ソフトウェア設定の警告です。	警告	処置の必要なし
Dell - Storage Security warning.	ストレージセキュリティの警告です。	警告	処置の必要なし
Dell - Software change update warning	ソフトウェアの変更アップデートに関する警告です	警告	処置の必要なし
Dell - Chassis Management Controller audit warning.	Chassis Management Controller の監査に関する警告です。	警告	処置の必要なし
Dell - PCI device audit warning.	PCI デバイスの監査に関する警告です。	警告	システムをメンテナンスモードにしてください
Dell - Power Supply audit warning.	電源装置の監査の警告です。	警告	処置の必要なし
Dell - Power usage audit warning.	消費電力の監査の警告です。	警告	処置の必要なし
Dell - Security configuration warning.	セキュリティ設定に関する警告です。	警告	処置の必要なし

イベント名	説明	重大度	推奨処置
Dell - Configuration: Software configuration warning.	設定： ソフトウェア設定に関する警告です。	警告	処置の必要なし

A

セキュリティの役割および許可

OpenManage Integration for VMware vCenter は、ユーザー資格情報を暗号化フォーマットで保管します。問題につながる可能性がある不正要求を避けるため、クライアントアプリケーションに対するパスワードは一切提供されません。バックアップデータベースは、カスタムセキュリティフレーズで完全に暗号化されるため、データが誤使用されることはありません。

デフォルトでは、Administrator グループ内のユーザーがすべての権限を有します。Administrator が、VMware vSphere クライアントまたはウェブクライアント内の OpenManage Integration for VMware vCenter のすべての機能を使用できます。必要な権限を持つユーザーに製品の管理を任せる場合、必要な権限がある役割を作成し、ユーザーに役割を割り当て、このユーザーを使用して vCenter サーバを登録し、両方の Dell 役割を含めます。

データ整合性

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

セキュア管理コンソールセッションには 5 分間のアイドルタイムアウトがあり、セッションは現行のブラウザウィンドウおよび / またはタブでのみ有効です。ユーザーが新しいウィンドウまたはタブでセッションを開こうとすると、有効なセッションを求めるセキュリティエラーが作成されます。この処置は、管理コンソールセッションの攻撃を試みる可能性がある悪意ある URL をユーザーがクリックすることも防ぎます。

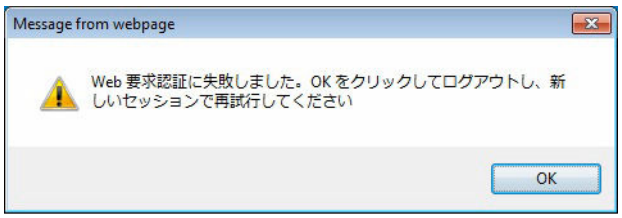

図 2. エラーメッセージ

アクセス制御認証、承諾、および役割

OpenManage Integration for VMware vCenter は、vCenter 操作を実行するために、ウェブクライアントの現在のユーザーセッションと、保存されている OpenManage Integration 用の管理資格情報を使用します。

OpenManage Integration for VMware vCenter は、vCenter サーバーのビルトイン役割と特権モデルを使用して、OpenManage Integration および vCenter 管理対象オブジェクト（ホストおよびクラスタ）とのユーザーアクションを承諾します。VMware vCenter ホームページの「アクセス役割」。

Dell Operational Role

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 12. 権限グループ

Group Name（グループ名）	説明
特権グループ — Dell.Configuration	ホスト関連タスクの実行、vCenter 関連タスクの実行、SelLog の設定、ConnectionProfile の設定、ClearLed の設定、ファームウェアアップデート
特権グループ — Dell.Inventory	インベントリの設定、保証取得の設定、ReadOnly の設定
特権グループ — Dell.Monitoring	監視の設定、監視
特権グループ — Dell.Reporting（使用されていません）	レポートの作成、レポートの実行

Dell インフラストラクチャ展開の役割

この役割には、ハイパーバイザー展開機能に特化した特権が含まれます。

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

権限について

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

- Dell.Configuration.Perform vCenter-Related Tasks
  - メンテナンスモードを終了および実行
  - 許可をクエリするために vCenter ユーザーグループを取得
  - 警告を登録および設定。たとえば、イベント設定ページでのアラートの有効化 / 無効化
  - vCenter にイベント / アラートを掲示

- イベント設定ページでイベント設定を実行
- イベント設定ページでデフォルトのアラートを復元
- アラート / イベント設定を実行しながら、クラスタの DRS ステータスをチェック
- アップデートまたはその他の設定処置を実行した後にホストを再起動
- vCenter タスクのステータス / 進捗状態を監視
- vCenter タスクを作成。たとえば、ファームウェアアップデートタスク、ホスト設定タスク、およびインベントリタスク
- vCenter タスクのステータス / 進捗状態をアップデート
- ホストプロファイルを取得
- データセンターにホストを追加
- クラスタにホストを追加
- ホストにプロファイルを適用
- CIM 資格情報を取得
- コンプライアンスのためにホストを設定
- コンプライアンスタスクのステータスを取得

- Dell.Inventory.Configure ReadOnly
  - 接続プロファイルの設定中に、すべての vCenter ホストを取得して vCenter ツリーを構築
  - タブが選択されてるときにホストが Dell サーバーかどうかをチェック
  - vCenter のアドレス / IP を取得
  - ホストの IP / アドレスを取得
  - vSphere クライアントセッション ID に基づいて現在の vCenter セッションユーザーを取得
  - vCenter インベントリツリーを取得して、vCenter インベントリをツリー構造で表示
- Dell.Monitoring.Monitor
  - イベントを掲示するためのホスト名を取得
  - イベントログ操作を実行。たとえば、イベント数の取得、またはイベントログ設定の変更
  - イベント / アラートを登録、登録解除、および設定 – SNMP トラップの受信とイベントの受信
- Dell.Configuration.Firmware Update
  - ファームウェアアップデートを実行
  - ファームウェアアップデートウィザードページにファームウェアリポジトリと DUP ファイル情報をロード
  - ファームウェアインベントリをクエリ
  - ファームウェアリポジトリ設定を実行
  - ステージングフォルダを設定、およびステージング機能を使用したアップデートを実行
  - ネットワークとリポジトリ接続をテスト
- Dell.Deploy-Provisioning.Create Template
  - HW 設定プロファイルの設定
  - ハイパーバイザ展開プロファイルの設定
  - 接続プロファイルの設定
  - ID の割り当て

  - 導入
- Dell.Configuration.Perform Host-Related Tasks
  - Dell Server Management（Dell サーバー管理）タブから LED を点滅、LED をクリア、OMSA URL を設定
  - OMSA コンソールを起動
  - iDRAC コンソールを起動
  - SEL ログを表示およびクリア
- Dell.Inventory.Configure Inventory
  - Dell Server Management（Dell サーバー管理）タブでシステムインベントリを表示
  - ストレージ詳細を取得
  - 電源監視詳細を取得
  - 接続プロファイルページで接続プロファイルを作成、表示、編集、削除、およびテスト
  - インベントリスケジュールを計画、アップデート、および削除
  - ホストでインベントリを実行

B

自動検出について

自動検出とは、OpenManage Integration for VMware vCenter による使用のため、使用可能なサーバーのプールに第 11 世代、第 12 世代、および第 13 世代の Dell PowerEdge ベアメタルサーバーを追加するプロセスです。サーバーが検出されたら、これをハイパーバイザーおよびハードウェアの導入に使用します。本付録は、システム設定に役立てるために十分な自動検出についての情報を提供します。自動検出は、コンソールを使用して新規サーバーをセットアップおよび登録するための Lifecycle Controller 機能です。この機能を使用する利点には、面倒な新規サーバーの手動でのローカル設定を排除し、ネットワークおよび電源に接続済みの新しいサーバーをコンソールが自動的に検出するための手段を実現することです。

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

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

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

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

自動検出が正しく行われると、検出時に **設定 → 展開** ページで入力された展開資格情報がターゲット iDRAC 上で作成され、その後自動検出機能がオフになります。これで、OpenManage Integration for VMware vCenter の展開下にある使用可能なベアメタルサーバーのプール内にサーバーが表示されるようになります。

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

自動検出の必要条件

Dell PowerEdge ベアメタルサーバーの第 11 世代、第 12 世代、またはそれ以降の世代の検出を行う前に、OpenManage Integration for VMware vCenter をインストールしてください。OpenManage Integration for VMware vCenter のベアメタルサーバーのプールで検出することができるのは、iDRAC Express または iDRAC Enterprise を搭載した 第 11 世代以降の Dell PowerEdge サーバーのみです。デルのベアメタルサー

バーの iDRAC から OpenManage Integration for VMware vCenter 仮想マシンへのネットワーク接続が必要です。

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

自動検出させるには、次の条件を満たしている必要があります。

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

iDRAC サーバーの管理者アカウントを有効または無効にする

自動検出をセットアップする前に、root 以外のすべての管理者アカウントを無効にします。root アカウントは、自動検出処理中に無効化されます。自動検出のセットアップを正しく行ったら、Integrated Dell Remote Access Controller 6 GUI に戻り、オフにしていたアカウントを再度有効にします。この手順は、第 11 世代、第 12 世代、および第 13 世代の Dell PowerEdge サーバー向けです。

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

1. ブラウザで、**iDRAC IP アドレス**をタイプします。
2. **Integrated Dell Remote Access Controller GUI** にログインします。
3. 次の手順のいずれか 1 つを実行します。
   - iDRAC6：左ペインで、**iDRAC 設定 → ネットワーク / セキュリティ → ユーザー** タブを順に選択します。
   - iDRAC7：左ペインで、**iDRAC 設定 → ユーザー認証 → ユーザー** タブを順に選択します。
   - iDRAC8：左ペインで、**iDRAC 設定 → ユーザー認証 → ユーザー** タブを順に選択します。
4. ユーザー タブで、ルート以外の管理者アカウントを探します。
5. アカウントを無効にするには、ユーザー ID の下で **ID** を選択します。
6. **次へ** をクリックします。
7. ユーザー設定 ページの 一般 の下で、**ユーザーを有効にする** チェックボックスのチェックを外します。
8. **適用** をクリックします。

9. 自動検出を正しくセットアップしたら、各アカウントを再度有効にするため、ステップ 1 ～ 8 を繰り返しますが、今回は **ユーザーを有効にする** チェックボックスを選択して **適用** をクリックします。