OpenManage Integration for VMware vCenter バージョン 5.4

セキュリティ設定ガイド

2021 年 10 月
Rev. A00

DELL EMC

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

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

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

目次

図

表

1

前書き

製品ラインを改善するための努力の一環として、Dell EMC はソフトウェアおよびハードウェアのリビジョンを定期的にリリースします。このマニュアルで説明されている機能の中には、現在使用中のソフトウェアまたはハードウェアの一部のバージョンではサポートされていないものもあります。製品のリリース ノートには、製品の機能に関する最新情報が記載されています。

製品が正常に機能しない、またはこのマニュアルの説明どおりに動作しない場合には、Dell EMC のテクニカル サポート プロフェッショナルにお問い合わせください。このマニュアルは、発行時点で正確なものとなっています。このマニュアルの最新バージョンを使用していることを確認するには、[https://www.dell.com/support] にアクセスしてください。

目的

このマニュアルには、OpenManage Integration for VMware vCenter（OMIVV）のセキュリティ機能と特徴に関する情報が記載されています。

対象読者

このマニュアルは、OMIVV のセキュリティ管理を担当するユーザーを対象としています。

変更履歴

次の表では、このマニュアルの変更履歴を示します。

表 1. 変更履歴

リビジョン	日付	説明
A00_5.2.0	2020 年 10 月	OpenManage Integration for VMware vCenter 5.2 セキュリティ設定ガイドのイニシャル リリース。
A00_5.3.0	2021 年 3 月	認証とデータ セキュリティのトピックに RESTful API 関連情報が追加されました。
A00_5.4.0	2021 年 10 月	このリリースではなし

関連マニュアル

OMIVV の完全なマニュアル セットは、[https://www.dell.com/support] から入手可能です。[すべての製品の参照] をクリックし、[ソフトウェア] > [仮想化ソリューション] の順にクリックします。[OpenManage Integration for VMware vCenter] をクリックすると、次の文書にアクセスできます。

- *『OpenManage Integration for VMware vCenter バージョン 5.4 ユーザーズ ガイド』*
- *『OpenManage Integration for VMware vCenter バージョン 5.4 リリース ノート』*
- *『OpenManage Integration for VMware vCenter バージョン 5.4 互換性マトリックス』*
- *『OpenManage Integration for VMware vCenter バージョン 5.4 API ガイド』*
- *『OpenManage Integration for VMware vCenter バージョン 5.4 インストール ガイド』*

https://www.dell.com/support では、ホワイトペーパーなどの技術に関する成果物を検索できます。

2

本書で使用される用語

表 2. 本書で使用される用語

用語	説明
OMIVV	OpenManage Integration for VMware vCenter
OVF	オープン仮想化フォーマット
HTTP	ハイパーテキスト転送プロトコル
HTTPS	ハイパーテキスト転送プロトコル セキュア
NFS	ネットワーク ファイル システム
CIFS	共通インターネット ファイル システム
OM MP	OpenManage Management Pack for vRealize Operations
CMC	Chassis Management Controller（M1000e、FX、VRTX）
OME-M	OpenManage Modular Edition（MX7000）
iDRAC	Integrated Dell Remote Access Controller
SNMP	シンプルネットワーク管理プロトコル
VM	仮想マシン
TCP	トランスミッション コントロール プロトコル
UDP	ユーザー データグラム プロトコル
PEM	プライバシーが強化された電子メール
RPM	Red Hat パッケージ マネージャー
OS（オペレーティングシステム）	オペレーティングシステム

3

導入モデル

OpenManage Integration for VMware vCenter（OMIVV）は、VMware vCenter 環境の OVF として導入できます。

トピック：

オープン仮想化フォーマット（OVF）の導入

VMware vSphere 仮想マシン環境がある場合は、OMIVV をオープン仮想化フォーマット（OVF）として導入することをお勧めします。

OVF 導入モデルには、事前構成済みのバンドルが含まれています。これには、OMIVV ソフトウェアと、OMIVV ソフトウェアを実行する Linux オペレーティング システムが含まれています。

OVF 環境には、モニター対象システムとの OMIVV 通信要件に合わせて調整された事前構成済みのファイアウォールも含まれています。

OVF は、OVF テンプレート ファイルとともに導入されます。OVF として OMIVV を導入する方法の詳細については、[https://www.dell.com/support] にある『*OpenManage Integration for VMware vCenter バージョン 5.4 インストール ガイド*』を参照してください。

セキュリティ プロファイル

OMIVV では、セキュアな HTTP アクセス用にデフォルトのセキュリティ プロファイルが用意されています。セキュリティ環境を強化するために、認証局（CA）署名証明書に置き換えることを強く推奨します。

4

製品およびサブシステムのセキュリティ

トピック：

セキュリティ制御マップ

OMIVV は iDRAC を使用して PowerEdge サーバーの導入、インベントリー、およびアップデートを実行し、iDRAC から SNMP トラップを受信します。

OMIVV のユーザー インターフェイスは、アプライアンスの管理 Web ページです。OMIVV プラグイン ユーザー インターフェイスは VMware vCenter クライアントから動作し、ホスト ハードウェアのモニタリングおよび管理機能を提供します。

すべてのシステム認証情報は、OMIVV セキュア ストレージ内に保存されます。

次の図は、OMIVV セキュリティ制御マップを示しています。

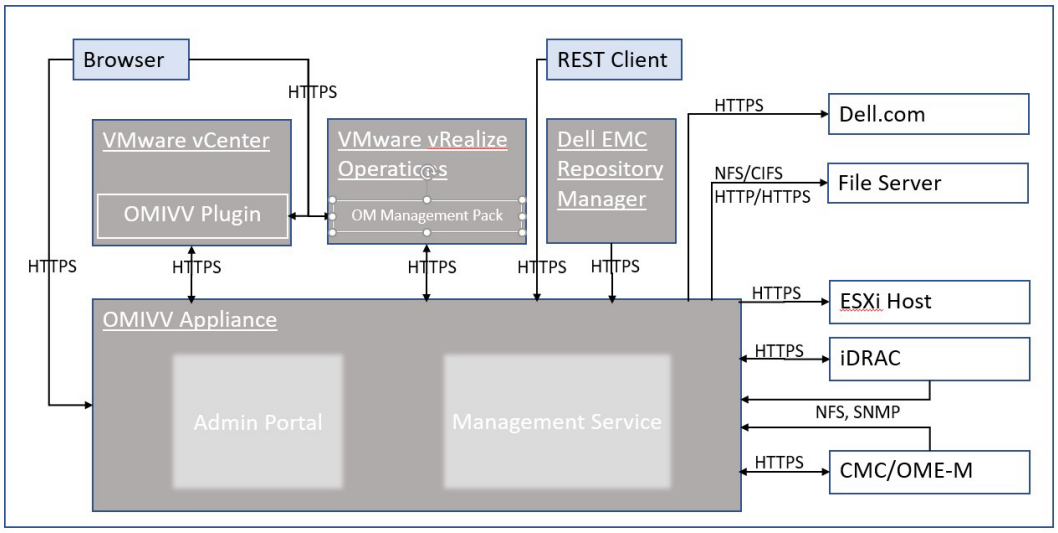

図 1. セキュリティ制御マップ

認証

アクセス制御

アクセス制御の設定によって、不正アクセスからリソースを保護できます。OMIVV プラグイン ページは、VMware vCenter で構成された適切な役割と権限を持つ VMware vCenter ユーザーによりアクセスできます。OMIVV 管理コンソールと RESTful API アクセスは、Administrator 権限を持つユーザー プロファイルにのみ提供されます。

デフォルト ユーザー アカウント

OMIVV には、次のデフォルト ユーザー アカウントが含まれています。

- ローカルユーザーアカウント
- 読み取り専用ユーザー アカウント
- Root アカウント

ローカルユーザーアカウント

OMIVV には、デフォルトで単一のローカル管理者ユーザー アカウントがあります。この内部アカウントのユーザー名は admin です。

ローカル管理者は、Dell EMC OMIVV 管理コンソールでのみ、すべての操作にアクセスできます。

OMIVV を初めて導入する場合は、パスワードの設定を求めるメッセージが表示されます。画面の指示に従って、パスワードを設定します。

読み取り専用ユーザー アカウント

OMIVV には、デフォルトで単一のローカル読み取り専用ユーザー アカウントがあります。読み取り専用アカウントのユーザー名は readonly です。

管理者は、VM のリモート コンソールのみを使用して OMIVV にログインできます。

このアカウントは、トラブルシューティング中に重要なアプライアンスのステータスとログを表示するために使用できます。

OMIVV を初めて導入する場合は、パスワードの設定を求めるメッセージが表示されます。画面の指示に従って、パスワードを設定します。

Root アカウント

OMIVV アプライアンスには、オペレーティング システム(OS)の root アカウントがあります。

このデフォルト アカウントにはアクセスできません。テクニカル サポート チームが、現場の問題をデバッグするために root アカウントを使用します。

外部ユーザー アカウント

vCenter に対して適切な役割と権限を持っている VMware vCenter ユーザーは、vCenter HTML5 クライアントから OMIVV プラグインのユーザー インターフェイスにアクセスできます。役割と権限の詳細については、「Administrator 以外のユーザーに必要な権限 、p. 13」を参照してください。

ログイン セキュリティ設定

ログインが失敗した際の動作

OMIVV には、複数回の認証が失敗した場合のセキュリティ設定が含まれています。

ローカル ユーザー アカウントのロックアウト

ローカル ユーザー アカウントへのログインの試行が 6 回連続で失敗すると、OMIVV は一時的に 1 分間ユーザーをロックアウトします。

自動セッション タイムアウト

アイドル状態のブラウザー セッションのタイムアウト

デフォルトでは、15 分間非アクティブ状態になった後、OMIVV セッションがタイムアウトになり、ユーザーは自動的にログアウトされます。

認証の種類とセットアップに関する考慮事項

vCenter ユーザー認証

OMIVV は、プラグイン ページと RESTful API にアクセスするための vCenter 認証に依存します。vCenter の操作を処理するプラグイン ページと RESTful API には、登録時に vCenter で Dell EMC によって作成された権限が必要です。

新しい vCenter サーバーの登録

前提条件

vCenter アカウントには、ユーザーを作成するために必要な権限が必要です。必要な権限の詳細については、「Administrator 以外のユーザーに必要な権限 、p. 13」を参照してください。

このタスクについて

OMIVV アプライアンスは、OMIVV のインストール後に登録できます。OMIVV は、管理者ユーザー アカウント、または vCenter を操作するのに必要な権限を持つ管理者以外のユーザー アカウントを使用します。1 つの OMIVV アプライアンス インスタンスでは、15 台の vCenter サーバー (リンク モードを使用する場合としない場合) および最大 2000 の ESXi ホストをサポートできます。

15 を超える vCenter を登録しようとすると、次のエラー メッセージが表示されます。

「お客様のライセンスは<x>台の vCenter にしか対応しておらず、すべて登録済みです」

新規 vCenter サーバーを登録するには、次の手順を実行します。

手順

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

b. [パスワード] ボックスにパスワードを入力します。
c. [パスワードの確認] ボックスにパスワードを再度入力します。
d. [vSphere Lifecycle Manager の登録] チェック ボックスを選択します。

[vSphere Lifecycle Manager の登録] チェック ボックスを選択すると、vCenter 7.0 以降から vSphere Lifecycle Manager の機能を使用できるようになります。

5. [登録] をクリックします。

vCenter の登録に失敗した場合、次のエラー メッセージが表示されます。

「認証情報が間違っているため、所定の vCenter Server <x>に接続できませんでした」ユーザー名とパスワードを確認してください。

タスクの結果

vCenter server を登録した後は、OMIVV が vCenter プラグインとして登録され、「Dell EMC OpenManage Integration」アイコンが vSphere Client に表示されます。このクライアントから OMIVV 機能にアクセスできます。

メモ: OMIVV アプライアンスからのすべての vCenter 操作では、OMIVV は、VMware vCenter または OMIVV アプライアンスのローカル アカウントにログインしているユーザーの特権ではなく、登録ユーザーの特権を使用します。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 Dell の権限のみがあります。ユーザー Y は vCenter にログインでき、OMIVV からファームウェアアップデートタスクをトリガできます。ファームウェアのアップデートタスクの実行中に、OMIVV はユーザー X の権限を使用して、ホストをメンテナンスモードにするか再起動します。

メモ: カスタマイズした認証局 (CA) 署名の証明書を OMIVV にアップロードする必要がある場合、vCenter の登録前に、必ず新しい証明書をアップロードしてください。vCenter 登録後に新しいカスタム証明書をアップロードすると、vSphere Client に通信エラーが表示されます。この問題を解決するには、ログアウトしてから vCenter にログインします。問題が解決しない場合は、vCenter Server で vSphere Client サービスを再起動します。

非管理者アカウントを使用した vCenter Server の登録

前提条件

vCenter の管理者認証情報があるか、または管理者以外でも Dell の権限を持つユーザーであれば、OMIVV アプライアンス用の vCenter Server を登録できます。

このタスクについて

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

手順

1. 役割に必要な権限を持った役割を作成するか既存の役割を変更します。

   役割に必要な権限のリストの詳細については、「Administrator 以外のユーザーに必要な権限」を参照してください。

   役割を作成または変更し、vSphere Client (HTML5) で権限を選択するために必要な手順については、VMware vSphere のマニュアルを参照してください
2. 役割を定義し、その役割の権限を選択したら、新しく作成した役割にユーザーを割り当てます。

   権限への役割の割り当ての詳細については、VMware vSphere のマニュアルを参照してください。

   これで、必要な権限のある管理者以外の vCenter Server ユーザーが、vCenter の登録や登録解除、認証情報の変更、認証情報のアップデートを実行できるようになります。
3. 必要な権限のある管理者以外のユーザーにより vCenter Server を登録します。
4. 登録が完了したら、ステップ 1 で作成または変更した役割に Dell の権限を割り当てます。既存の役割への Dell の権限の割り当て 、p. 15 を参照してください。

タスクの結果

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

Administrator 以外のユーザーに必要な権限

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

管理者以外のユーザーが OMIVV で vCenter サーバーを登録する際に、次の権限が設定されていないとメッセージが表示されます。

- アラーム
  - アラームの作成
  - アラームの変更
  - アラームの削除
- 拡張権限
  - 登録の拡張権限
  - 登録解除の拡張権限
  - 更新の拡張権限
- グローバル
  - タスクのキャンセル
  - ログイベント
  - 設定
- 正常性アップデートプロバイダ
  - 登録
  - 登録解除
  - アップデート
- ホスト
  - CIM
    - CIM インタラクション
- Host.Config
  - 詳細設定
  - 設定の変更
  - 接続
  - メンテナンス
  - ネットワークの設定
  - パッチの問い合わせ
  - セキュリティプロファイルとファイアウォール
- インベントリ
  - クラスタにホストを追加
  - スタンドアロンホストの追加
  - クラスタの変更
- Lifecycle Manager：General Privileges
  - 読み取り

  メモ: vSphere Lifecycle Manager General Privileges は vCenter 7.0 以降にのみ適用されます。
- ホストプロファイル
  - 編集
  - 表示
- 許可
  - 権限の変更
  - 役割の変更
- セッション
  - セッションの検証
- タスク
  - 作成
  - アップデート

メモ: OMIVV の機能にアクセスするために、管理者以外のユーザーを使用して vCenter サーバーが登録されている場合、管理者以外のユーザーにはデルの権限が必要です。デルの特権を割り当てる方法の詳細については、「既存の役割への Dell の権限の割り当て 、p. 15」を参照してください。

既存の役割への Dell の権限の割り当て

このタスクについて

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

既存の役割を編集し、Dell の権限を割り当てることができます。

手順

1. 管理者権限で vSphere Client（HTML5）にログインします。
2. vSphere Client（HTML5）で、[メニュー] を展開し、[管理] → [役割] の順にクリックします。
3. [役割プロバイダー] ドロップダウン リストから、vCenter Server を選択します。
4. [役割] リストから [Dell 操作] を選択し、[権限] をクリックします。
5. Dell の権限を割り当てるには、編集アイコン（ ）をクリックします。
   [役割の編集] ページが表示されます。
6. 左ペインで [Dell] をクリックし、選択した役割に対して次の Dell の権限を選択して [次へ] をクリックします。
   - Dell.Configuration
   - Dell.Deploy — プロビジョニング
   - Dell.Inventory
   - Dell.Monitoring
   - Dell.Reporting

   vCenter で使用可能な OMIVV の役割の詳細については、『Dell 操作役割 、p. 16
7. 役割名を編集し、必要に応じて、選択した役割の説明を入力します。
8. [終了] をクリックします。
   ログ アウトして vCenter からログ インします。これで、必要な権限を持つユーザーが OMIVV 操作を実行できるようになります。

vCenter ユーザー セキュリティ

セキュリティの役割および許可

OMIVV は、ユーザー資格情報を暗号化された形式で保存します。不正な要求を避けるため、クライアントアプリケーションにはパスワードを一切提供しません。バックアップデータベースは、カスタムセキュリティフレーズで完全に暗号化されるため、データが誤使用されることはありません。

デフォルトでは、管理者グループのユーザーはすべての権限を持っています。管理者は、VMware vSphere Web Client 内の OpenManage Integration for VMware vCenter のすべての機能を使用できます。製品を管理するのに必要な権限をユーザーに与えるには、次の手順を実行します。

1. 必要な権限を持つ役割を作成します。
2. ユーザーを使用して vCenter Server を登録します。
3. Dell 操作および Dell インフラストラクチャ導入の両方の役割が含まれます。

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 を使用しておこないます。OpenManage Integration for VMware vCenter で、vCenter とアプライアンス間の信頼できる通信のために使用される証明書が生成されます。また、vCenter サーバーの証明書を検証および信頼してから通信し、OpenManage Integration for VMware vCenter を登録します。

セキュアな管理コンソール セッションには 15 分間のアイドル タイムアウトがあり、このセッションは現在のブラウザー ウィンドウまたはタブでのみ有効です。新しいウィンドウまたはタブでセッションを開こうとすると、有効なセッションを要求するセキュリティエラーが表示されます。また、このアクションは、管理コンソールセッションを攻撃する可能性がある悪意のある URL をクリックすることも防止できます。

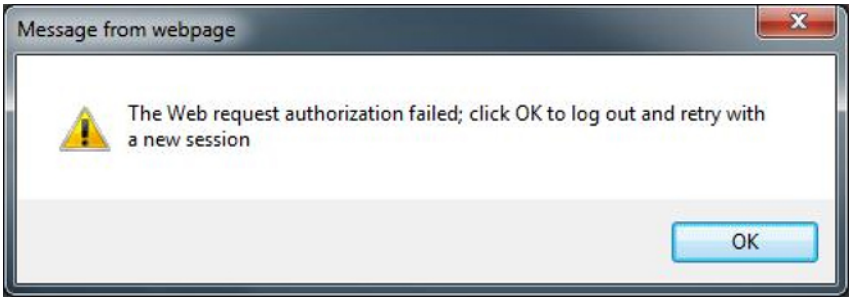

図 2. セキュリティエラーメッセージ

アクセス制御認証、承諾、および役割

OpenManage Integration for VMware vCenter は、vCenter を操作するために、vSphere クライアントの現在のユーザー セッションと、OpenManage Integration の保存された管理認証情報を使用します。OpenManage Integration for VMware vCenter は、vCenter サーバー内で設定された役割と権限モデルに基づいて、OpenManage Integration と vCenter 管理オブジェクト (ホストとクラスター) に対するユーザー アクションを承認します。

Dell 操作役割

この役割には、ファームウェアアップデート、ハードウェアインベントリ、ホストの再起動、ホストをメンテナンスモードに設定、vCenter サーバタスクの作成を含む、アプライアンスおよび vCenter サーバのタスクを実行する権限 / グループが含まれます。

この役割には次の特権グループが含まれます。

表 3. 権限グループ

グループ名	説明
権限グループ - Dell.Configuration	ホスト関連タスクの実行、vCenter 関連タスクの実行、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
権限グループ - Dell.Inventory	インベントリの設定、保証取得の設定、読み取り専用の設定
権限グループ - Dell.Monitoring	監視の設定、監視
権限グループ - Dell.Reporting (不使用)	レポートの作成、レポートの実行

Dell インフラストラクチャ導入役割

この役割には、ハイパーバイザー導入機能に関連した権限が含まれます。

この役割によって提供される権限は、ホスト認定資格プロフィールの設定、ID の割り当て、および導入です。

[特権グループ — Dell.Deploy-Provisioning]

ホスト認定資格プロフィールの設定、ID の割り当て、導入をおこないます。

特権について

OpenManage Integration for VMware vCenter によって実行されるすべてのアクションは、権限に関連付けられています。次のセクションでは、実行可能なアクションと、それに関連付けられている権限をリストします。

- Dell.Configuration.Perform vCenter-related tasks
  - メンテナンスモードを終了および実行
  - 許可をクエリするために vCenter ユーザーグループを取得
  - アラームを登録および設定。たとえば、イベント設定ページでのアラームの有効化/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 サーバかどうかをチェック
  - vCenter のアドレス / IP を取得
  - ホストの IP / アドレスを取得
  - vSphere クライアントセッション ID に基づいて現在の vCenter セッションユーザーを取得
  - vCenter インベントリツリーを取得して、vCenter インベントリをツリー構造で表示
- Dell.Monitoring.Monitor
  - イベントを掲示するためのホスト名を取得
  - イベントログ操作を実行。たとえば、イベント数の取得、またはイベントログ設定の変更
  - イベント / アラートを登録、登録解除、および設定 — SNMP トラップの受信とイベントの受信
- Dell.Configuration.Firmware Update
  - ファームウェアアップデートを実行
  - ファームウェアアップデートウィザードページにファームウェアリポジトリと DUP ファイル情報をロード
  - ファームウェアインベントリをクエリ
  - ファームウェアリポジトリ設定を実行
  - ステージング機能を使用してステージングフォルダを設定およびアップデートを実行
  - ネットワークとリポジトリ接続をテスト
- Dell.Deploy-Provisioning.Create Template
  - HW 設定プロファイルの設定
  - ハイパーバイザ展開プロファイルの設定
  - 接続プロファイルの設定
  - ID の割り当て
  - 導入
- Dell.Configuration.Perform host-related tasks
  - LED の点滅、LED のクリア
  - iDRAC コンソールを起動
  - SEL ログを表示およびクリア
- Dell.Inventory.Configure Inventory
  - Dell サーバの 管理 タブでシステムインベントリを表示
  - ストレージ詳細を取得
  - 電源監視詳細を取得
  - 接続プロファイルページで接続プロファイルを作成、表示、編集、削除、およびテスト
  - インベントリスケジュールを計画、アップデート、および削除
  - ホストでインベントリを実行

ユーザーおよび認証情報の管理

プリロード済みアカウント

次の表は、プリロードされた OMIVV アカウントについての説明です。

表 4. プリロード済みアカウント

ユーザーアカウント	説明
OpenManage Integration for VMware vCenter 管理者	OMIVV Web アプリケーション管理用デフォルト ユーザー。
読み取り専用ユーザー	OMIVV には、デフォルトで単一のローカル読み取り専用ユーザー アカウントがあります。 管理者は、VM のリモート コンソールのみを使用して OMIVV にログインできます。 このアカウントは、トラブルシューティング中に重要なアプライアンスのステータスとログを表示するために使用できます。
Linux オペレーティング システム root	root 操作システム アカウントにはアクセスできません。テクニカル サポート チームが、現場の問題をデバッグするために root アカウントを使用します。

デフォルト認証情報

次の表は、プリロードされた OMIVV アカウントのデフォルト認証情報についての説明です。

表 5. デフォルト認証情報

アカウント	ユーザー	パスワード
OpenManage Integration for VMware vCenter 管理者	管理者	導入後の最初の起動時に設定されます。管理者パスワード変更の詳細については、「OMIVV アプライアンスのパスワードの変更 、p. 18」を参照してください。
読み取り専用ユーザー	読み取り専用	導入後の最初の起動時に設定されます。読み取り専用ユーザーのパスワードは、読み取り専用ユーザーとしてログインした後に、標準の Linux パスワード変更コマンドを使用して再設定できます。
Linux オペレーティング システム root	Root	OMIVV が導入されると、root ユーザーのログインは無効になります。

認証情報の管理

初めて Dell EMC 管理コンソールにログインする場合は、管理者としてログインします (デフォルトのユーザー名は admin です)。

メモ: 管理者パスワードを忘れた場合は、OMIVV アプライアンスから回復することはできません。

OMIVV アプライアンスのパスワードの変更

このタスクについて

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

手順

1. OMIVV Web コンソールを開きます。
2. [[OpenManage Integration for VMware vCenter の仮想アプライアンスのセットアップ]] ユーティリティーで、[[管理者パスワードの変更]] をクリックします。
   画面に表示される指示を完了してパスワードを設定します。
3. [[現在のパスワード]] テキスト ボックスに現在の管理パスワードを入力します。
4. [[新規パスワード]] テキスト ボックスに新しいパスワードを入力します。
5. [[新規パスワードの確認]] テキスト ボックスに新しいパスワードを再度入力します。

6. [[管理パスワードの変更]] をクリックします。

許可

OMIVV アプライアンスは、単一の管理者ユーザーをサポートします。

OMIVV にログインした後、管理者は次のような OMIVV アプライアンスの構成機能にのみアクセスできます。

- 新しい vCenter サーバーの登録
- アプライアンスの構成
- RPM を使用した OMIVV アプライアンスのアップグレード、バックアップ、復元
- ネットワーク タイム プロトコル サーバーのセットアップ
- 展開モードの設定
- 証明書署名要求 (CSR) の生成
- HTTPS 証明書のアップロード
- グローバル アラートの設定
- トラブルシューティング バンドルの生成とダウンロード

ネットワークセキュリティ

OMIVV アプライアンスは、事前構成済みファイアウォールを使用して、TCP ポートおよび UDP ポートとのインバウンドおよびアウトバウンド ネットワーク トラフィックを制限することでセキュリティを強化します。次の表は、OMIVV がリモート システムと通信するインバウンドおよびアウトバウンド ポートのリストです。

ネットワークの露出

OpenManage Integration for VMware vCenter は、リモート システムと通信するときに、インバウンド ポートとアウトバウンド ポートを使用します。

アウトバウンド ポート

アウトバウンド ポートは、リモート システムへの接続時に OMIVV によって使用されます。

次の表にリストされているポートは、OMIVV アウトバウンド ポートです。

表 6. アウトバウンド ポート

ポート番号	レイヤー 4 プロトコル	サービス
7	TCP、UDP	ECHO
22	TCP	SSH
25	TCP	SMTP
53	UDP、TCP	DNS
67、68	TCP	DHCP
80	TCP	HTTP
88	TCP、UDP	Kerberos
111	TCP、UDP	ONC RPC
123	TCP、UDP	NTP
161 ~ 163	TCP、UDP	SNMP
389	TCP、UDP	LDAP
443	TCP	HTTPS
448	TCP	Data Protection Search 管理者 REST API

表 6. アウトバウンド ポート（続き）

ポート番号	レイヤー 4 プロトコル	サービス
464	TCP、UDP	Kerberos
514	TCP、UDP	rsh
587	TCP	SMTP
636	TCP、UDP	LDAPS
902	TCP	VMware ESXi
2049	TCP、UDP	NFS
2052	TCP、UDP	mountd、clearvisn
3009	TCP	Data Domain REST API
5672	TCP	RabbitMQ over AMQP
8443	TCP	MCSDK 8443 は 443 の代わりになります
9002	TCP	Data Protection Advisor REST API
9443	TCP	Avamar 管理コンソール Web サービス

インバウンド ポート

OMIVV への接続時にリモート システムが使用できるインバウンド ポート。

次の表にリストされているポートは、OMIVV インバウンド ポートです。

表 7. インバウンド ポート

ポート番号	レイヤー 4 プロトコル	サービス
22	TCP	SSH
80	TCP	HTTP
443	TCP	HTTPS
5671	TCP	RabbitMQ over AMQP

データ セキュリティ

OMIVV によって保守されるデータは、アプライアンス内の内部データベースに格納されて保護されており、外部からはアクセスできません。

OMIVV を介して転送されているデータは、セキュアな通信チャネルによって保護されています。

メモ: RESTful API ユーザーは、環境制限に従って、取得した認証情報とデータを安全に格納することをお勧めします。

暗号化

OMIVV では、次のコンポーネントのために暗号化を使用します。

- アクセス制御
- 認証
- デジタル署名

OMIVV アプライアンスの HTTPS 証明書のアップデート

OMIVV は、セキュアな HTTP アクセス（HTTPS）に証明書を使用します。

デフォルトでは、OMIVV は、HTTPS のセキュアなトランザクションに自己署名証明書をインストールして使用します。

セキュリティを強化するために、認証局（CA）署名またはカスタム証明書を使用することをお勧めします。

自己署名証明書は、Web ブラウザーとサーバーの間で暗号化されたチャネルを確立するためには十分です。自己署名証明書を認証に使用することはできません。

OMIVV の認証には、次のタイプの証明書を使用できます。

- 自己署名証明書

  OMIVV は、アプライアンスのホスト名が変更された時に自己署名証明書を生成します。

- 信頼できる認証局（CA）ベンダーによって署名された証明書。

メモ: 証明書を作成する場合は、会社のポリシーを検討してください。

証明書署名要求（CSR）の生成

前提条件

デフォルトでは、OMIVV には自己署名証明書があります。OMIVV 用にカスタマイズされた認証局（CA）の署名済み証明書が必要な場合は、vCenter の登録前に新しい証明書をアップロードすることをお勧めします。

このタスクについて

新しい CSR を生成すると、以前生成された CSR で作成された証明書をアプライアンスにアップロードできなくなります。CSR を生成するには、次の手順を実行します。

手順

1. [アプライアンス管理] ページで、[HTTPS 証明書] 領域の [証明書署名要求の生成] をクリックします。
   新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るというメッセージが表示されます。要求を続けるには、[続行] をクリックします。
2. 要求を続行する場合は、[証明書署名要求の生成] ダイアログ ボックスで、共通名、組織名、地域、都道府県、国、メール アドレス、サブジェクト代替名（SAN）に関する情報を入力して、[続行] をクリックします。

   メモ: OMIVV では、SAN に対して複数の値はサポートされていません。

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

HTTPS 証明書のアップロード

前提条件

証明書が PEM フォーマットを使用していることを確認してください。

このタスクについて

HTTPS 証明書は、OMIVV アプライアンスとホスト システムまたは vCenter のセキュアな通信に使用できます。このタイプのセキュアな通信を設定するには、CSR 証明書を署名責任者に送信してから、管理者コンソールを使用してその CSR をアップロードします。また、自己署名によるデフォルト証明書もあり、セキュア通信に使用できます。この証明書は各インストール固有のものです。

手順

1. [アプライアンス管理] ページで、[HTTPS 証明書] 領域の [証明書のアップロード] をクリックします。
2. [証明書のアップロード] ダイアログ ボックスで [OK] をクリックします。
3. 証明書をアップロードするには、[参照] > [アップロード] の順にクリックします。
   ステータスを確認するには、登録済み vCenter の vSphere Client で [イベント コンソール] に移動します。

タスクの結果

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

メモ: 登録済み vCenter の OMIVV アプライアンス証明書参照が自動的にアップデートされます。証明書が OMIVV にアップロードされたら、OMIVV から vCenter にアクセスできることを確認します。

デフォルト HTTPS 証明書の復元

手順

1. [[アプライアンス管理]] ページの [[HTTPS 証明書]] 領域で [[デフォルト証明書の復元]] をクリックします。
2. [デフォルト証明書の復元] ダイアログボックスで [適用] をクリックします。

タスクの結果

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

登録済み vCenter Server の HTTPS 証明書のアップデート

このタスクについて

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

手順

1. https://<アプライアンス IP またはホスト名>に移動します。
2. 左ペインで、[VCENTER の登録] をクリックします。
   登録済み vCenter Server が作業中のペインに表示されます。
3. vCenter Server IP またはホスト名の証明書を更新するには、[アップデート] をクリックします。

監査とログ

管理者ユーザーは、OMIVV 管理コンソールを使用して、関連するすべてのログを含むトラブルシューティング バンドルを生成できます。

詳細については、次を参照してください：トラブルシューティング バンドルの作成およびダウンロード 、p. 22

読み取り専用アカウントでは、実行時にアプライアンスのさまざまなパラメーターの読み取りができるので、アプライアンスのトラブルシューティングに役立ちます。詳細なトラブルシューティングのために、テクニカル サポートが特定パラメーターを確認する手順を指示します。

メモ: アプライアンスで書き込み操作を実行できるのは、OMIVV 管理者ユーザーのみです。ユーザーの監査は、OMIVV ログでは使用できません。vCenter プラグインから実行される vCenter 操作の詳細については、vCenter 監査ログを確認してください。RESTful API の場合、クライアントは監査ログを処理できる必要があります。

トラブルシューティング バンドルの作成およびダウンロード

このタスクについて

トラブルシューティング バンドルには、問題の解決やテクニカル サポートへの送信に役立つ OMIVV アプライアンスのログ情報が含まれています。OMIVV は、ユーザーの機密データをログに記録しません。

手順

1. [サポート] ページで、[トラブルシューティング バンドルの作成およびダウンロード] をクリックします。
   [トラブルシューティング バンドル] ダイアログ ボックスが表示されます。
2. [トラブルシューティング バンドル] ダイアログ ボックスで [作成] をクリックします。

ログのサイズによっては、バンドルの作成に時間がかかる場合があります。

3. ファイルを保存するには、[ダウンロード] をクリックします。
   Dell EMC OMIVV 管理コンソールのログイン ページが表示されます。
4. Dell EMC OMIVV 管理コンソールにログインします。
5. トラブルシューティング バンドルをダウンロードします。

トラブルシューティング バンドルの生成とダウンロード

前提条件

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

このタスクについて

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

手順

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

サービス化

サポート Web サイト ([https://www.dell.com/support]) は、ライセンス情報、製品マニュアル、アドバイザリー、ダウンロード、トラブルシューティング情報へのアクセスを提供します。この情報は、サポート チームに問い合わせる前に、製品の問題を解決するために役立ちます。

サービス担当者が OMIVV を使用するには、特別なログインは必要ありません。トラブルシューティング バンドルが十分ではない場合は、担当者は root ユーザーが詳細情報を収集できるようにすることができます。

OMIVV vCenter オペレーティング システムのアップデートなどのセキュリティ パッチおよびその他のアップデートが使用可能な場合は、必ずそれらをインストールしてください。

セキュリティ パッチ

定期的な OMIVV アップデートにはセキュリティ アップデートが含まれ、必要に応じてセキュリティのみのアップデートがリリースされています。

アップデートは累加的でサポートに公開され、同時に OMIVV のユーザーは vCenter で通知を受け取ります。

OMIVV OS アップデート

OMIVV OS のセキュリティ パッチおよび修正は、定期的にリリースされています。

これらの修正は、RPM アップデート パッケージを使用して OMIVV の既存の OVF 導入環境にインストールされている必要があります。可能な場合は、RPM アップデートを使用して、これらのセキュリティ パッチおよび修正を OMIVV サーバーにインストールすることを強くお勧めします。

製品コードの整合性

OMIVV ソフトウェア インストーラーは Dell によって署名されています。OMIVV インストーラーの署名の信頼性を確認することをお勧めします。

5

その他の構成と管理

トピック：

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

OMIVV には、次の 2 種類のライセンスがあります。

- 評価ライセンス — OMIVV アプライアンスの初回電源投入時に、自動的にインストールされます。評価バージョンには、OMIVV で 5 つのホスト（サーバー）を管理することを可能にする評価ライセンスが含まれています。この 90 日間評価バージョンは、出荷時に提供されるデフォルトのライセンスです。
- 標準ライセンス：OMIVV が管理するホストライセンスは、任意の数で購入できます。このライセンスには、製品サポートと OMIVV アプライアンスのアップデートも含まれています。標準ライセンスは 3 年または 5 年間利用できます。追加のライセンスを購入すると、既存のライセンス期間が延長されます。標準ライセンスは、評価版ライセンスを上書きします。

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

OMIVV は最大 15 の vCenter インスタンスをサポートします。評価ライセンスから完全標準ライセンスにアップグレードすると、注文の確認に関する電子メールが届きます。その後、Dell Digital Locker からライセンスファイルをダウンロードできます。ライセンス .XML ファイルをローカルシステムに保存し、[管理コンソール] を使用して新しいライセンスファイルをアップロードします。

ライセンスを購入すると.XML ファイル（ライセンス キー）を https://www.dell.com/support の Dell Digital Locker からダウンロードできるようになります。ライセンス キーをダウンロードできない場合は、[https://www.dell.com/support] の「オーダーサポートに問い合わせる」ページに掲載されている、地域および製品ごとの Dell サポートの電話番号までお問い合わせください。

ライセンスによって、OMIVV 管理コンソールでは次の情報が提供されます。

- vCenter 接続ライセンスの最大数：最大 15 の登録済みおよび使用中の vCenter 接続が可能です。
- ホスト接続ライセンスの最大数：購入したホスト接続数です（1 つの OMIVV インスタンスで最大 2000 ホストをサポート）。
- 使用中 - 使用中の vCenter 接続ライセンスまたはホスト接続ライセンスの数です。ホスト接続では、この数はインベントリーされたホスト（またはサーバー）の数を示します。
- 使用可能 — 将来使用できる vCenter 接続またはホスト接続ライセンスの数です。

認定資格プロフィールにホストを追加しようとする際に、ライセンスを保有するホスト数がライセンス数を超える場合、さらにホストを追加することはできません。OMIVV は、使用可能なホスト ライセンス数より多いホスト数の管理をサポートしていません。

OMIVV RESTful API を使用して、ライセンスに関する詳細情報を取得します。詳細については、https://www.dell.com/support にある『*OpenManage Integration for VMware API ガイド*』を参照してください。

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

信頼性と整合性の保護

製品の整合性を確保するため、OMIVV のインストールおよびアップデート コンポーネントは署名されています。

通信の整合性を確保するために、CA 署名証明書を使用することをお勧めします。

OMIVV でのバックアップおよび復元の管理

災害シナリオから OMIVV を保護するために、OMIVV のバックアップを実行することをお勧めします。必要に応じて、これらのバックアップから OMIVV を復元することができます。バックアップと復元の詳細については、[https://www.dell.com/support] にある『OMIVV ユーザーズ ガイド』を参照してください。