セキュリティのベスト プラクティスの概要

ソフトウェア バージョン

この章での推奨事項は、以下のソフトウェア バージョンを対象としています:

Cisco Modeling Labs クライアント

GUI を使用して、ユーザはネットワーク トポロジを設計します。トポロジ設定ファイルは (Cisco Modeling Labs ラボ サーバ ではなく) クライアント コンピュータのローカル ファイルとして保存され、.virl というファイル名拡張子を持ちます。たとえば、**Test_Network** という名前のトポロジは **Test_Network.virl** というファイルに保存されます。ファイルの場所を確認するには、Cisco Modeling Labs クライアントの**プロジェクト** ビューに表示されているファイル名を右クリックし、ファイルのプロパティを表示します。ディレクトリのデフォルトの場所の基準は、次のとおりです:

Windows オペレーティング システムの場合、**Test_Network.virl** ファイルは **c:\Users**<ユーザ *ID*>**\cml\workspace**<プロジェクト フォルダ>\ に保存されます。

Apple OS X の場合、**Test_Network.virl** ファイルは **/Users/**<ユーザ *ID*>**/cml/workspace/**<プロジェクト フォルダ>/ に保存されます。

IP アドレスが公開されないようにするため、このファイルは保護することを推奨します。ファイルの保護のために選択できる方法は、ローカルのセキュリティの実施事項に基づいて決まります。これには、以下のポリシーが含まれます:

- パスワード保護
- データの暗号化
- ディスクの暗号化
- ファイルのバックアップ

Cisco Modeling Labs サーバ

Cisco Modeling Labs サーバは、次のようないくつかのコンポーネントで構成されています。

- オペレーティング システム
- Openstack

Linux ベースのオペレーティング システム

Cisco Modeling Labs サーバは、Linux ベースのオペレーティング システムを使用します。Cisco Modeling Labs をサポートするのに必要でないサービスは、無効にされています。

サーバ管理者は、ソフトウェアのインストールと削除、およびソフトウェアの更新を行えます。

⚠

注意 オペレーティング システムを更新すると、Cisco Modeling Labs 内の機能が失われる場合があります。更新を実行する前に、Cisco Technical Assistance Center (TAC) に問い合わせて、情報と支援を求めてください。

Cisco Modeling Labs を非生産環境に配備した場合、セキュリティ違反の影響は環境に保存されている設定の機密性のために制限されますが、環境を構築して設定するために投資した時間を損失することがあり、外部接続を確立していた場合には、環境がネットワークの他の部分へのジャンプ ホストとして用いられる潜在的な可能性が生じます。

Cisco Modeling Labs サーバ上のセキュリティを設定するときには、次のセキュリティ タスクを実行することお勧めします:

- ファイアウォールをインストールして設定します。
- 共有メモリをセキュアにします。
- ユーザ代理コマンドである **su** コマンドを使用できるユーザを、管理者グループのみに制限します。
- **/etc/sysctl.conf** 設定でネットワーク アクセスを強化します。
- IP スプーフィングを防止します。
- Apache による情報漏えいを制限します。
- Apache Web アプリケーションのファイアウォールをインストールして設定します。
- 疑わしいホストを禁止します。
- 侵入検知をモニタします。

- ルートキット ソフトウェアをスキャンします。
- ログ ファイルの表示と分析を行います。
- システム上で開いているスキャンします。

Cisco Modeling Labs では、Linux ベースのオペレーティング システムでアクティブなポートは、次の表に示されています:

表 *1 : Cisco Modeling Labs* のアクティブ ポート

ポート番号	説明
22	プロジェクト/シミュレーション内の Jumphost への SSH セッションで使用します。
23	外部通信を有効にしていた場合の、仮想ノードへの telnet 接続。
80	Cisco Modeling Labs サーバまたはシミュレーション内の仮想ホストへの HTTP セッションで使用します。
443	Telnet over WebSocket のデフォルト ポート (ws:// と wss://)
3306	MySQL
3333	HTTP
5000	UPnP

OpenStack のセキュリティ概要

Cisco Modeling Labs では、OpenStack の次のコンポーネントを使用します:

- ダッシュボード（Horizon）
- コンピューティング（Nova）
- ネットワーキング（Neutron）
- イメージ サービス (Glance)
- アイデンティティ サーバ (Keystone)

OpenStack ダッシュ ボードのセキュリティ

OpenStack ダッシュ ボードは、管理者にクラウドベースのリソースのプロビジョニングとアクセスのためのインタフェースを提供します。Cisco Modeling Labs **ユーザ ワークスペース管理**インターフェイスは、OpenStack ダッシュ ボードの修正版です。**「UWM インターフェイスにアクセス - ここでクロスリファレンスを追加 (Access the UWM interface- add in cross-ref here)」**を参照してください。インターフェイスとその使用方法に関する追加情報については、こちらを参照してください。

（注） **ユーザ ワークスペース管理** インターフェイスは、より安全な HTTPS ではなく HTTP を使用します。

ユーザ アカウントを作成するときは、次の推奨事項を検討してください。

- 管理者以外のアカウントに管理者アクセスを割り当てないように、アクセス特権を確認します。
- 各ユーザに割り当てられたリソースを制限して、サービスが制約されずにサーバーの操作が停止しないようにします。
- 有効期限を割り当てます。
- 定期的にユーザ アカウントを確認します。

OpenStack コンピューティングのセキュリティ

OpenStack コンピューティング サービスは、クラウド コンピューティング ファブリックのコントローラで、コンピューティング リソースのプールを管理し、自動化します。Nova は、仮想化テクノロジを使用するようにデザインされていますが、非仮想環境と同じセキュリティ上のリスクに直面します。

Cisco Modeling Labs で展開する場合、OpenStack コンピューティング サービスを強化するための特定の推奨事項はありません。

OpenStack ネットワーキング セキュリティ

以前の Quantum の OpenStack ネットワーキング サービスは、ネットワークと IP アドレスを管理しています。

ネットワーク セキュリティを確保するには:

- 仮想ネットワーク コンピューティング (VNC) および Telnet セッションへの管理者アクセス用のデフォルト パスワードを変更します。
- 実稼動ネットワーク環境と Cisco Modeling Labs ネットワーク間の接続が、ファイアウォールやその他のネットワーク境界セキュリティ ポリシーをバイパスしないようにしてください。

OpenStack イメージ サービスのセキュリティ

OpenStack イメージ サービスは、ディスク イメージとサーバ イメージの検出、登録、および配信サービスを提供します。Cisco Modeling Labs では、Cisco Modeling Labs サーバのイメージ、および Cisco IOSv、Cisco IOS XRv、および Cisco CSR 1000V など、サポートされているイメージ タイプの Cisco ノード イメージをストアで確認できます。

Cisco Modeling Labs を展開する際、OpenStack イメージ サービスを強化するための特定の推奨事項はありません。

OpenStack アイデンティティ サービス セキュリティ

OpenStack アイデンティティ サービスは、ユーザの認証に使用されます。Cisco Modeling Labs 内でのユーザ認証は、LDAP またはその他の外部の方法ではなく、サーバで実行されます。

サーバでユーザ認証がサーバで実行する場合には、Identity Service セキュリティのために、以下のタスクを実行してください:

- ブルートフォース攻撃を示すアクティビティがないか、ログをモニタします。モニタリングは手動で、またはサードパーティの製品を使用しておこなえます。
- 内部のエンドポイントを登録します。内部の URL をエンドポイントとして登録すると、API 通信が制限されますが、それによりセキュリティが向上します。
- 各 OpenStack サービスには **policy.json** というポリシー ファイルがあり、それぞれのリソースを管理するルールを指定しています。

OpenStack データベース セキュリティ

データベースに保持されている .virl ネットワーク トポロジ ファイルのすべての情報は、OpenStack コンピューティング コンポーネント内で管理されています。情報にはノードとその接続、および最初のノードの設定の名前が含まれています。ユーザ名とプロジェクト名も含まれています。パスワードは、[**ユーザ ワークスペース管理**] インターフェイス経由で追加されるプロジェクトと同じではありません。