Pandora FMS アーキテクチャ

Pandora FMS アーキテクチャ

Pandora FMS ドキュメント一覧に戻る

Pandora FMS アーキテクチャ

最も重要なコンポーネントは、すべての情報が保存されている MySQL データベース です Pandora FMS の各コンポーネントは複製でき、パッシブ、アクティブ、またはクラスタ環境(アクティブ/アクティブな負荷分散) など、完全な HA環境で動作します。。

Pandora FMS サーバは、自身またはエージェントによって生成された情報のデータをデータベースに入力します。ウェブコンソールは、データベースに存在するデータの表示とエンドユーザとの対話を担当する部分です。**エンドポイント**は、監視対象システムで実行されるアプリケーションであり、情報を収集して Pandora FMS サーバに送信します。

Pandora FMS サーバ

サーバは、Pandora Server という全体を表す名前で単一のアプリケーションに統合されます。これは Pandora FMS のインスタンスまたは機能に特化したサーバをそれぞれ異なるサブプロセス(スレッド)で実行するマルチスレッドアプリケーション(マルチプロセッシング)です。これらは適切な監視の実行を担当する要素です。実行結果を検証し、結果に応じてステータスを変更します。また、データの状態を監視するように設定されたアラートを発報する役割もあります。

同時に複数のサーバが存在する場合があります。そのうちの 1つはメインサーバで、残りのサーバはスレーブです。 マスターサーバとスレーブサーバの関係がありますが、それらは同時に機能します。 2つの違いは、同じタイプのサーバ(ネットワークサーバなど)がダウンしている場合、マスターサーバがダウンしているサーバに関連付けられているすべてのデータの処理を担当することです。

Pandora FMS は、各サーバのステータス、負荷レベル、およびその他のパラメータを自動的に管理します。 ユーザは、ウェブコンソールの**サーバ管理**を介して各サーバの状態を確認できます。

以下も参照:

- **エクスポートサーバ**
- 同期**サーバ**
- SIEM **サーバ**
- NetFlow および sFlow によるネットワーク監視
- NCM **サーバ**
- **ポリシー**管理
- MADE **サーバ**

データ(Data)サーバ

エンドポイント によって XML フォーマットで送信され、特定のディレクトリに置かれた情報パケットを処理します。最初にデータサーバによって処理されてからデータベースに保存されます。

複数のデータサーバを、異なるシステムにインストールすることも、複数の CPU を備えた仮想サーバを使用して同じホストにインストールすることもできます。

データサーバは、そのシンプルさとリソースの使用量の少なさにもかかわらず、すべてのエージェント情報を処理し、それらのデータに従ってアラートとシステムイベントを生成するシステムの重要な要素の 1 つです。

ネットワーク(Network)サーバ

ネットワークサーバは、ICMP テスト(ping, 応答時間)、TCP および SNMP リクエストなど、リモートモニタリングタスクを実行します。ネットワークサーバを実行しているマシンにとって、リモートの監視対象デバイスへのネットワーク接続が確保されていることが非常に重要です。

SNMP トラップサーバ

このサーバは、snmptrapd デーモンが受信したトラップを扱います。このデーモンは SNMP トラップを受信し、Pandora FMS の SNMP サーバはそれをデータベースに保存します。それらを分析して、Pandora FMS の SNMP コンソールにおいて、アラートの定義を行うこともできます。

WMI サーバ

WMI は、MS Windows® ベースのオペレーティングシステムおよび Microsoft Windows® 環境アプリケーションから情報を取得するための Microsoft® 標準です。 Pandora FMS には、WMI プロトコルを通じて Windows® システムをリモート 監視する専用のサーバがあります。

自動検出(Discovery)サーバ

以前は Recon サーバと呼ばれていた 自動検出(Discovery)サーバ は、ネットワークを定期的に探索し、稼働中の新しいシステムを検出するために使用されます。 監視テンプレートを適用して、新し

いシステムの監視を開始します。自動検出は、nmap□xprobe□traceroute などのシステムアプリケーションを使用してオペレーティングシステムを識別し、ネットワークトポロジを検出することもできます。

自動検出サーバは、スケジュールされたタスクを起動し、仮想環境、クラウド、データベース、または監視を開始する前にあらゆる存在するアプリケーションや環境を検出するためにも使用されます。

プラグイン(Plugin)サーバ

プラグインサーバは、中央管理するカスタムスクリプトを使用して複雑な監視をリモートから実行します。 これにより、上級ユーザは独自の監視の定義をアプリケーションに統合し、Pandora FMS から簡単かつ一元的な方法で使用できるようになります。

予測(Prediction)サーバ

最大 30 日間の範囲の過去データに基づいて統計的なデータ予測を実装する AI コンポーネントです。これにより、10～15 分間隔でデータ項目の値を予測し、特定のデータセットにおいて履歴から異常を示しているかどうかを知ることができます。基本的には週次で動的なベースラインを構築します。

ウェブサーバ

ユーザ認識処理、フォームによるパラメータ転送、またはメニューのナビゲーションへのコンテンツチェックなど、完全な Web テストを実行します。ウェブナビゲーションにおける可用性のチェック (動作するかどうか) と待ち時間 (秒単位) の取得ができます。

エクスポート(Export)サーバ

これは□Pandora FMS の監視対象デバイスのデータを別の Pandora FMS にデータ転送し、あらゆるデータを複製できるようにします。複数の Pandora FMS インストールがあり、データを一元化する必要がある大規模な環境の場合に特に役立ちます。

インベントリ(Inventory)サーバ

インベントリサーバは、インストールされているソフトウエア、ハードウエアモデル、ハードディスク、システムで稼働しているサービスなど、システムのインベントリ情報を収集・可視化することができます。これらの情報は、リモートおよび、エンドポイントを通してローカルで取得できま

す。

イベント(Event)サーバ

この特別なサーバは、イベントを関連付けたり、アラートを生成したりするために使用できますが、監視タスクは実行しません。他のサーバとは異なり、このサーバはスレッドや冗長化設定はありません。

ICMP サーバ

高度な戦略を使用して ICMP チェック (ping) を実行し、事前に検証された OID (Object IDentifier) で動作するため、高いパフォーマンスを発揮します。

サテライトサーバ

このコンポーネントは、Pandora FMS メインサーバとは別にインストールされます。 データファイルを エンドポイント からメインサーバに転送し、分散トポロジでエージェントプロキシとして機能します。tentacle 接続を介して監視データを XML として送信するため、データベース接続は必要ありません。

WUX サーバ

Selenium Grid と組み合わせたサーバで、複雑なウェブアクセスを再現する監視を分散して実行することができます。トランザクションは、実際のブラウザで実行されます。また、ウェブアクセスのステップごとの実行結果、詳細な統計情報が表示され、エラー画面のキャプチャもあります。

Syslog サーバ

このコンポーネントにより、Pandora FMS はサーバ上の Syslog を分析し、その内容を分析して対応する OpenSearch サーバに保存できます。

ログサーバ

これにより、ログを関連付けてアラートを実行 が可能になります。

アラートサーバ

デフォルトでは、各サーバが独自のアラートを担当しますが、必要な場合に、すべての監視アラー

トの実行を担当するサーバです。特殊なケースとして、アラートが何らかのタスクを実行する必要があり、それに予想以上に時間がかかると、監視に遅延が発生する可能性があります。それを避けることができます。

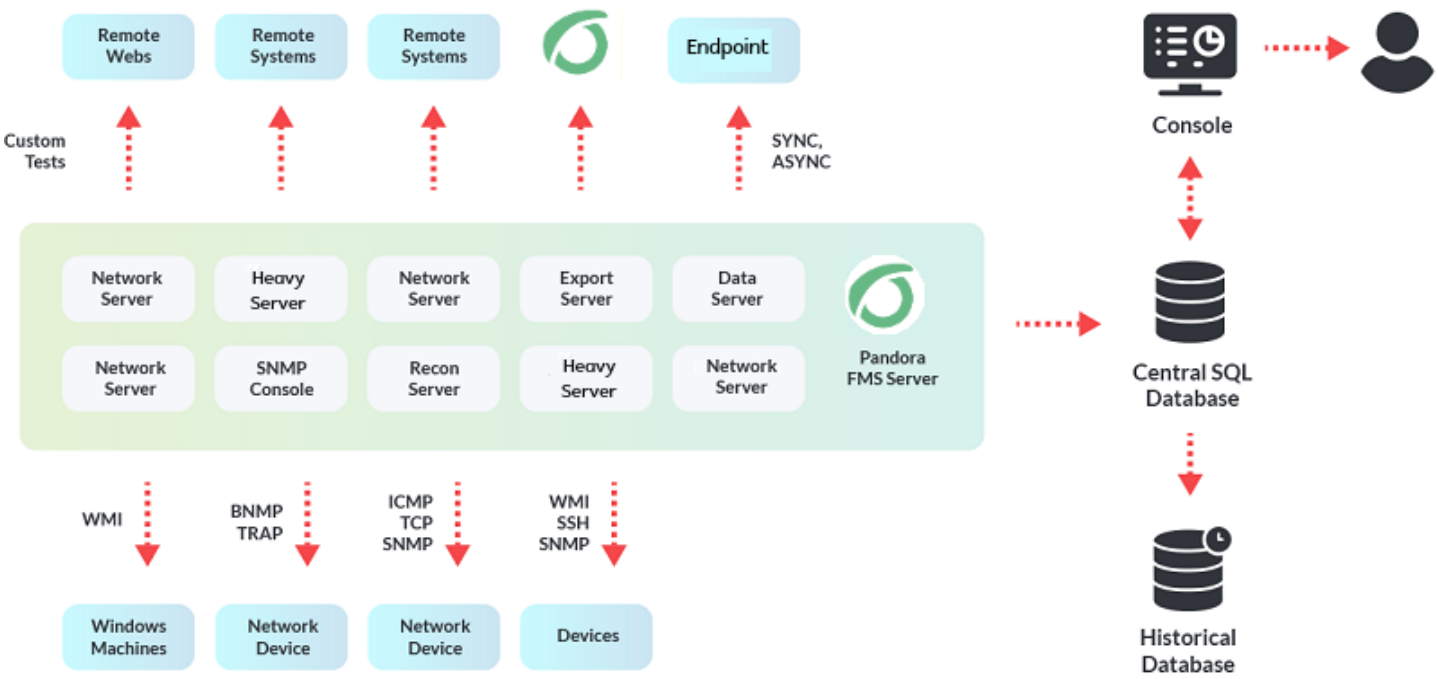
Pandora FMS ウェブコンソール

これはPandora FMS のユーザインタフェースです。この管理およびオペレーションコンソールは、それぞれのユーザに別の権限を設定することが可能で、エージェントの状態の操作、状態の参照、グラフおよびデータの生成、さらにはシステムに組み込まれているインシデント管理までできます。また、レポートの生成や、新たなモジュール、エージェント、アラートおよび、ユーザの作成やポリシー設定を行うことができます。

ウェブコンソールは複数のサーバで動作させることが可能です。ロードバランシングや配置の問題(巨大なネットワーク、多くの異なるユーザグループ、地理的な違い、管理の違いなど)に対してアクセスを簡単にできます。

Pandora FMS データベース

Pandora FMSは、さまざまなソースのすべてのデータを受信し、正規化してリアルタイム MySQL データベースに保存しています。現在は MySQL/MariaDB/Percona のみがサポートされています。



Pandora FMS エンドポイント

コンテナとしての エージェント (コンソールエージェント) と、コンピュータ上で実行される エンドポイント という 2 つの概念を区別することが重要です。

エージェント(コンテナ)

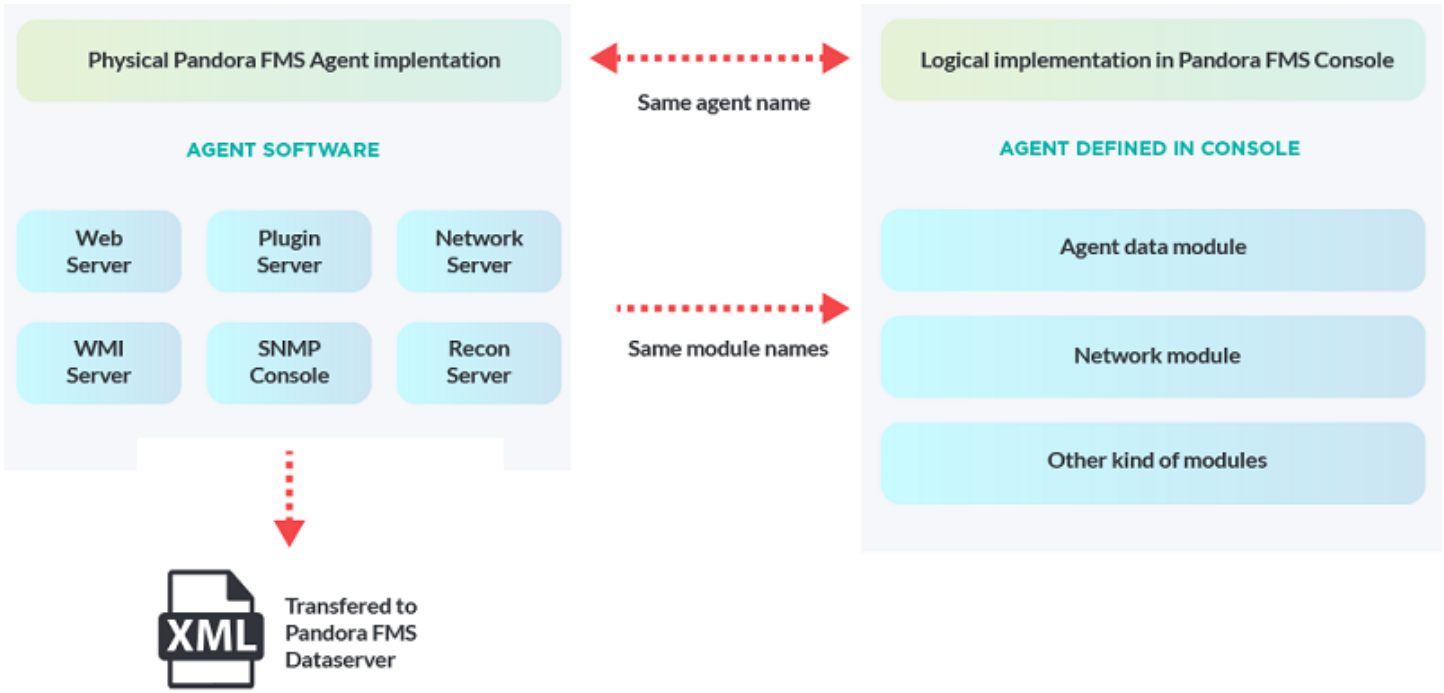
Pandora FMS で単純に「エージェント」と言った場合、それはウェブコンソールで作成したモニタ・管理対象を指します。それは、モジュールのグループ（または個々のモニタリング要素）に関連付けられています。そのため、このエージェントは、(オプションで) 1つ以上の IP アドレスに関連付けることが可能です。

エージェントにはリモートモジュールまたはローカルモジュールを含めることができます。リモートモジュールは情報を取得するサーバから リモート (ネットワークサーバなど) によって実行され、ローカルモジュールはエンドポイントによって実行され、データサーバ によって処理されます。

エンドポイント

エンドポイントは監視対象のコンピュータにインストールされるものであり、それが動作しているマシンの情報をローカルで取得します。主に、サーバリソース(CPU□メモリ、ディスクなど)およびインストールされたアプリケーション(MySQL, Apache, JBoss など)を監視します。一般的にサーバの監視はエンドポイントで実施し、ネットワーク機器は何らかのソフトウエアのインストールは無しでリモートから監視を行います。

実行された監視に関するすべての情報は 1 つの XML 形式のファイルに出力され、このファイルは Tentacle プロトコルを介して 300 秒の所定の間隔で Pandora FMS サーバに送信されます□ SSH または FTP を使用してデータを送信することもできます。



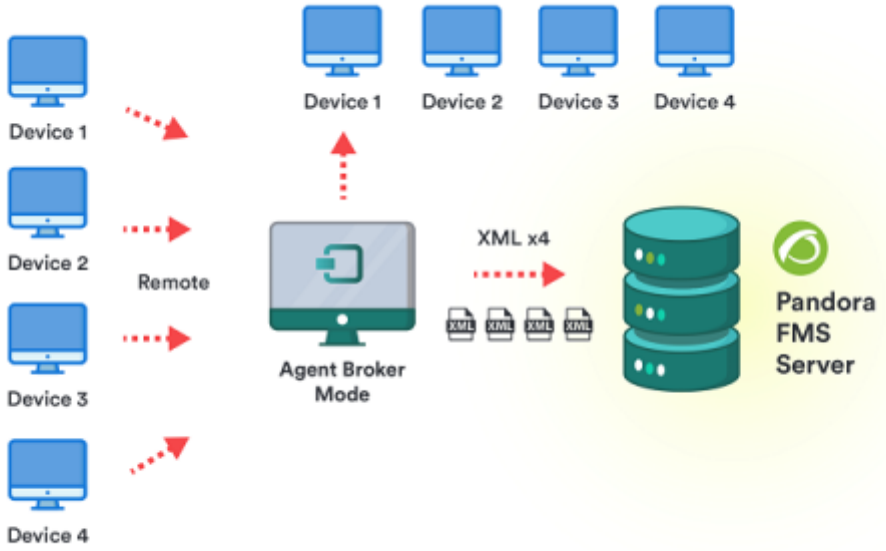
トポロジ、スキーマ、監視モデル

アクセス可能なネットワーク

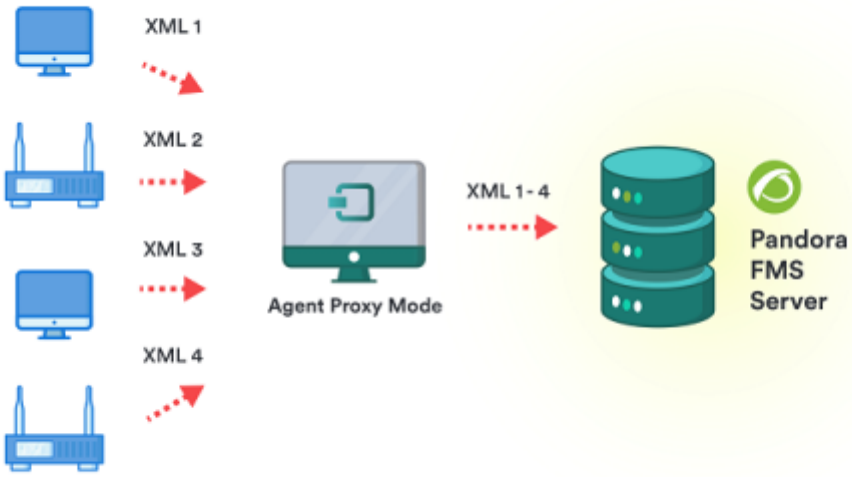
- 集中リモート監視 でのネットワークアクセス。これはPandora FMS からすべてのマシンにリモートでアクセスできることを意味します。
- エージェントベース監視 でのネットワークアクセス。このネットワークでは、監視対象のマシンにインストールされているエンドポイントから Pandora FMS サーバにアクセスできます。

アクセスが制限されたネットワーク

- Pandora FMS のリモートチェックで到達できないネットワーク: ブローカーエージェントモードを利用します。



- Pandora サーバにアクセスできないエンドポイント: この場合、エンドポイントのプロキシ機能もしくは、プロキシとしてサテライトサーバを利用します。



- 異なるネットワークに対するリモートサーバ監視: この場合、*サテライトサーバ*を使うこともできます。または、一つのデータベースに接続する複数の Pandora FMS サーバを利用します。

特別な組織構造

- 複数のレポート: 異なる 2つの Pandora FMS サーバにデータを送るようにエージェントを設定することができます。ただし、管理は一つのサーバからのみ可能です。
- 分散管理: 別の権限の担当者で 監視内容を分散管理する 必要がある場合に便利です。これは、構成というより管理が重要です。管理ポリシーの権限設定によって調整します。

大規模環境

- 大規模ネットワーク: 何千ものネットワーク監視処理がある場合は、異なるリモート監視プローブに分散する必要があります。その数が多い (50,000 以上) の場合、単一のサーバに集約することはできません。そのため、リモートチェックの負荷を分散するブローカーモードでサーバを利用します。
- サーバの冗長化: プライマリサーバのハードウエアが故障した場合にそなえて、冗長化 の設定により監視処理を別のサーバに引き渡すことができます。

Pandora FMS ドキュメント一覧に戻る