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

概要

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:

- サーバアーキテクチャ (バージョン 784)
- 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
- 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。

- WMI は、MS Windows® 環境からオペレーティングシステムの情報とアプリケーションを取得するための Microsoft® 標準規格です。これは、MS Windows® システムを WMI プロトコルを使用 して リモート で監視するための専用サーバーです。
- 最大 30 日間の過去データに基づいて統計データ予測を実行する 人工知能 コンポーネントです。10～15 分間隔でデータ値を予測し、現在のデータが過去のデータと比較して異常かどうかを判断できます。基本的には、週次プロファイルを使用して動的なベースラインを構築します。
- ユーザ識別プロセス、フォームによるパラメータの受け渡し、コンテンツのチェック、メニューナビゲーションなどの 完全な Web チェック を実行します。これは、真の可用性チェックと、完全なブラウジングエクスペリエンスの待ち時間を取得するために使用されます。

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。

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。

イベント(Event)サーバ

この特別なサーバーは、イベントを関連付け、アラートを生成するために使用され、監視タスクは実行しません。このサーバは、他のサーバとは異なり、スレッド設定や高可用性機能を備えていません。

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

有効化すると、すべての監視アラートの実行を担当します。デフォルトでは各サーバが自身のアラートを担当しており、特定のケースでは、アラートがタスクを実行する必要があり、実行予定よりも時間がかかる場合、監視に遅延が発生する可能性があります。

ヘビーサーバ

ヘビーサーバ は、集中管理されたカスタムスクリプトを通じて、複雑なチェックをリモートで実行します。これにより、高度なユーザは 独自の複雑なテスト を定義し、アプリケーションに統合して Pandora FMS から便利かつ集中的に利用できるようになります。

また、次の追加の機能も実行します。

- ネットワーク設定管理 (NCM) に必要なすべての機能をサポートします。
- 監視階層 を扱います。
- インベントリシステム情報 (インストールされているソフトウェア、ハードウェア要素のモデル、ストレージデバイス、実行中のサービスなど) を取得して表示します。これらの情報は、リモートおよび ローカル の両方で取得できます。
- 監視対象デバイスの データを Pandora FMS から別の Pandora FMS にエクスポート し、データを複製することができます。複数の Pandora FMS がインストールされ、集中管理が必要な大規模な展開で特に役立ちます。

ネットワーク高性能サーバ

ネットワーク高性能サーバ(Network HP Server) は ICMP チェック (ping) を実行するために高度な戦略を使用し、事前に検証された OID (オブジェクト識別子) で動作するため、高いパフォーマンスを実現します。

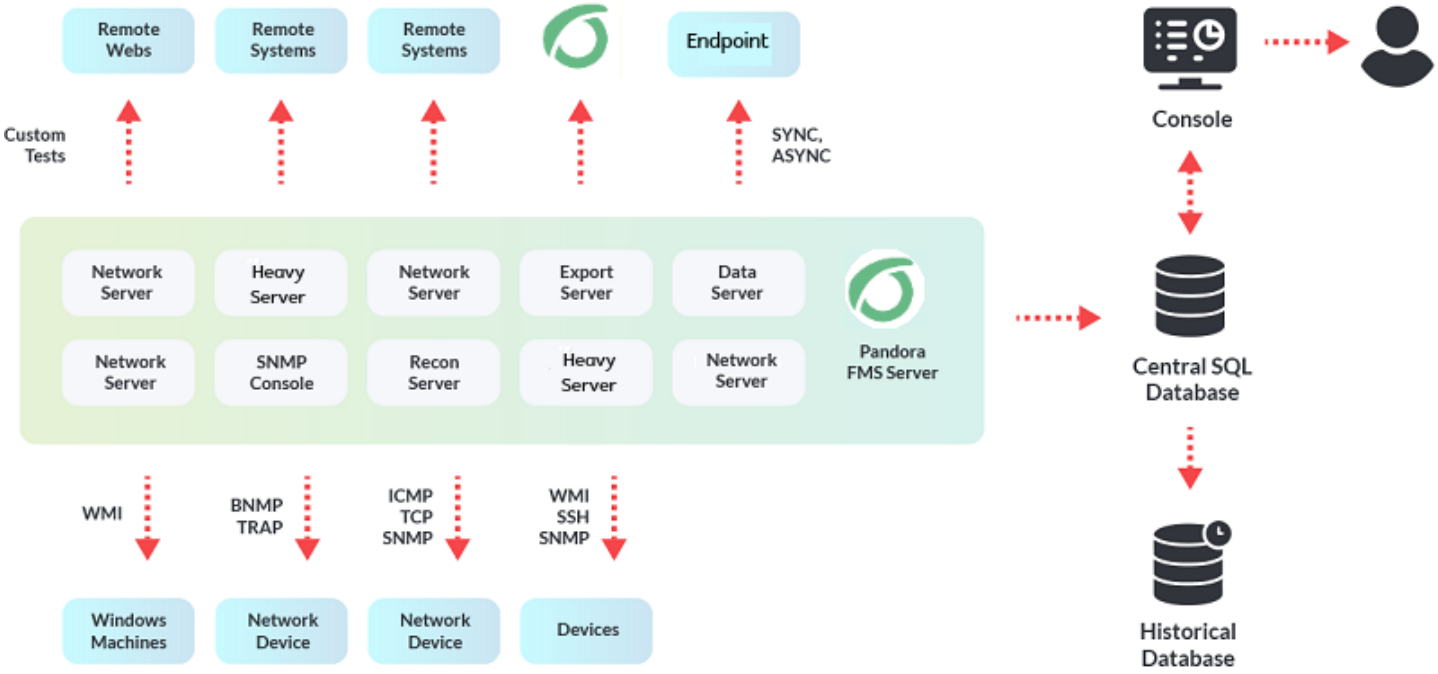
Pandora FMS ウェブコンソール

これはPandora FMSユーザインターフェースです。この管理・操作コンソールでは、異なる権限を持つ複数のユーザが、エージェントの状態管理、統計情報の閲覧、グラフやデータテーブルの作成、そして統合システムによるインシデント管理を行うことができます。また、レポートの生成、新規モジュール、エージェント、アラートの一元的な定義、他のユーザやプロファイルの作成も可能です。

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)

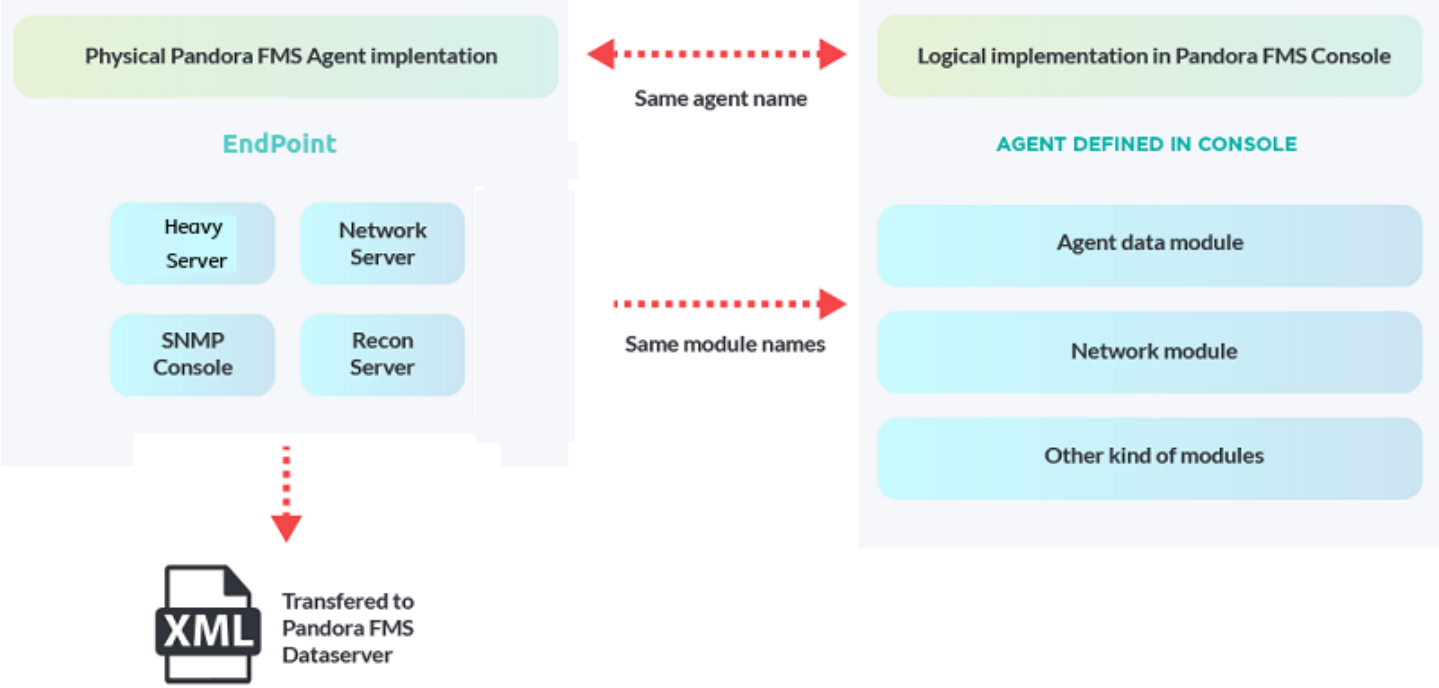
Pandora FMS エージェントは、Pandora FMS ウェブコンソールで作成される組織要素であり、モジュールグループ（または個々の監視要素）に関連付けられます。このエージェントには、オプションで 1 つ以上の IP アドレスを関連付けることができます。

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。

実行された監視情報はすべて XML 形式の単一データファイルに記録され、Tentacleプロトコルを介して、300秒間隔で 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可能です。



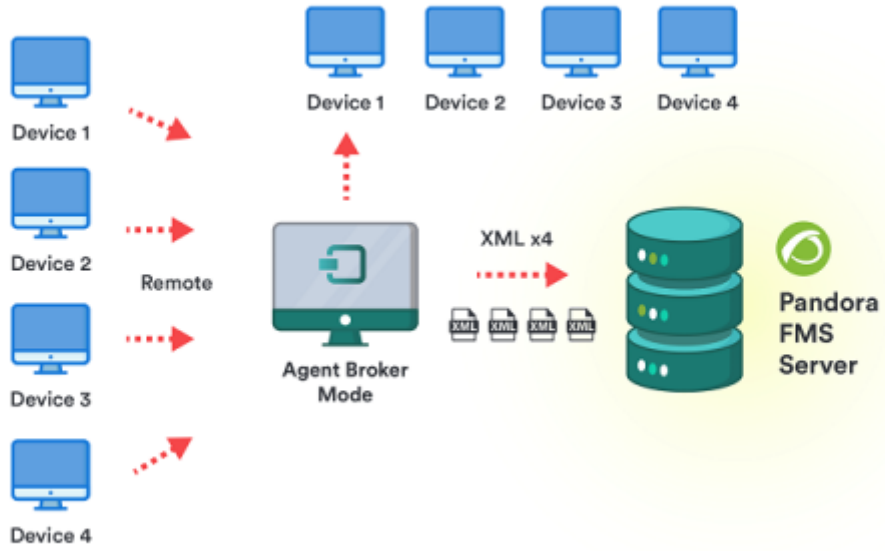
トポロジ、スキーマ、監視モデル

アクセス可能なネットワーク

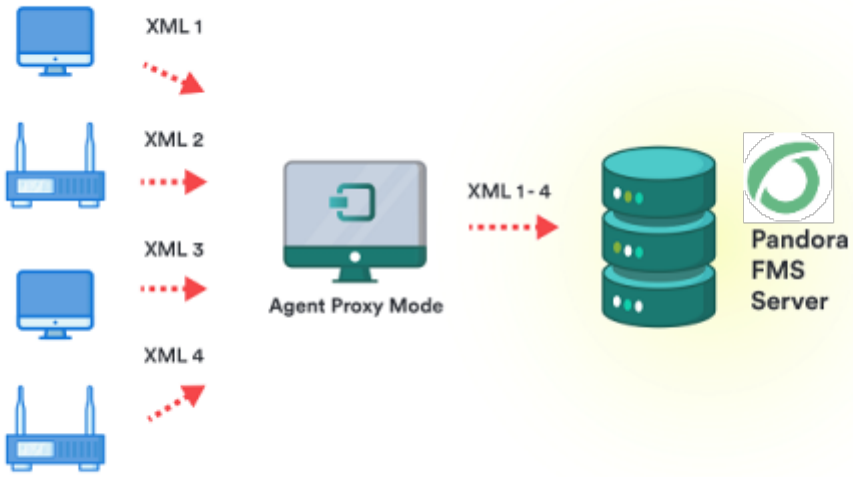
- 集中リモート監視 でのネットワークアクセス。これは、Pandora FMS からすべてのマシンにリモートでアクセスできることを意味します。
- エージェントベース監視 でのネットワークアクセス。このネットワークでは、監視対象のマシンにインストールされているエンドポイントから Pandora FMS サーバにアクセスできます。

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、サテライトサーバまたは同じデータベースに接続された複数の異なる Pandora FMS サーバーを使用することもできます。

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