Pandora FMS の概要

From:
https://pandorafms.com/manual/!776/
Permanent link:
https://pandorafms.com/manual/!776/ja/documentation/pandorafms/introduction/01_introduction
2024/06/10 14:34

Pandora FMS の概要

Pandora FMS ドキュメント一覧に戻る

概要

Pandora FMS とは?

Pandora FMS は、あらゆる種類の環境を対象としたネットワーク監視ソフトウェアパッケージです。Pandora FMS は、あらゆる役割や組織に適応できるように設計されています。 その主な目的は、他の監視ツールにこれ以上の時間や資金を投資することなく、インフラストラクチャ全体を管理および制御できる十分な柔軟性を備えることです。

FMS は Flexible Monitoring System の頭文字です。

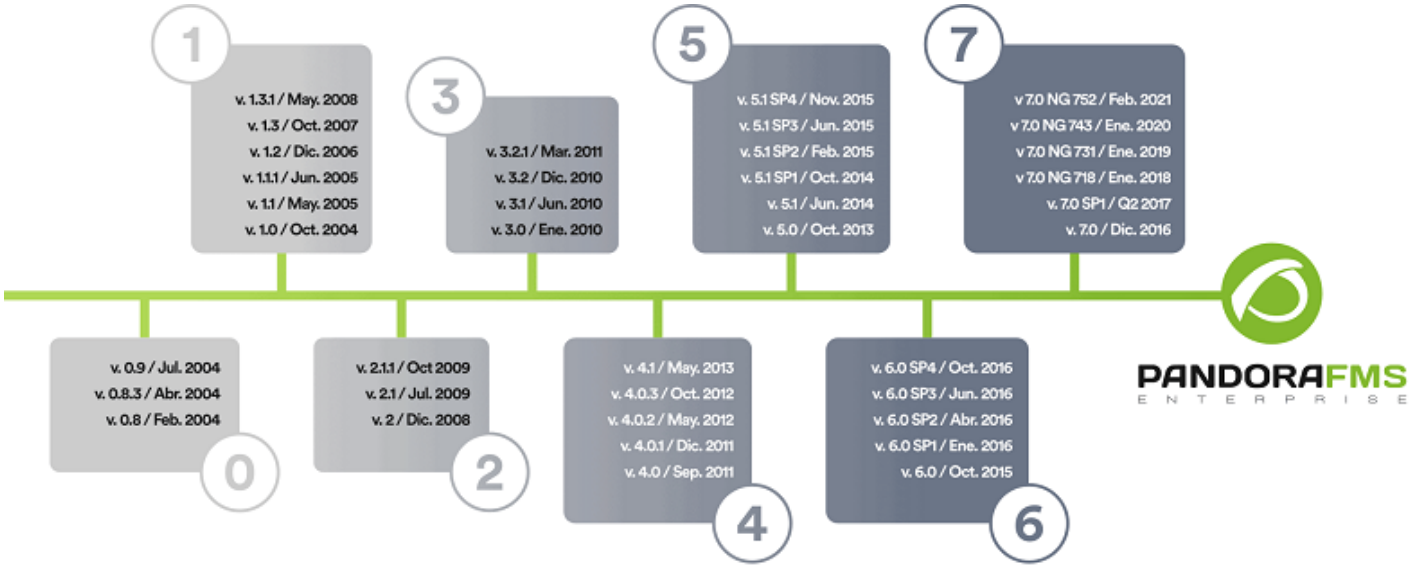
Pandora FMS は現在、市場のすべてのオペレーティングシステムに対して エージェント を利用します。もちろん、システム監視ツールとしてだけでなく、SNMP、TCP プロトコル、または ソフトウエアエージェント などを通して、さまざまなネットワークデバイスの監視ツールとしても使えます。

ドキュメントについて

- 公式ドキュメントに加えて、質問ができる ユーザフォーラム も利用できます。
- Pandora FMS 開発者による 公式トレーニングプログラムもあります。(英語)
- クイックガイド は、Pandora FMS の設定、簡単な監視処理の実装、および GNU/Linux® と MS Windows® の両方のソフトウェアエージェントのインストールに役立ちます。
- より詳細の情報は、http://pandorafms.com を参照してください。

Pandora プロジェクトの進化

Pandora FMS は、2003年に Sancho Lerena によって個人的な開発プロジェクトとして始まりました。当初は 100% オープン ソースでしたが、数年後、大企業向けのバージョンが必要になりました。それは、メタコンソール を通じて大量の情報を処理できる Pandora FMS Enterprise です。

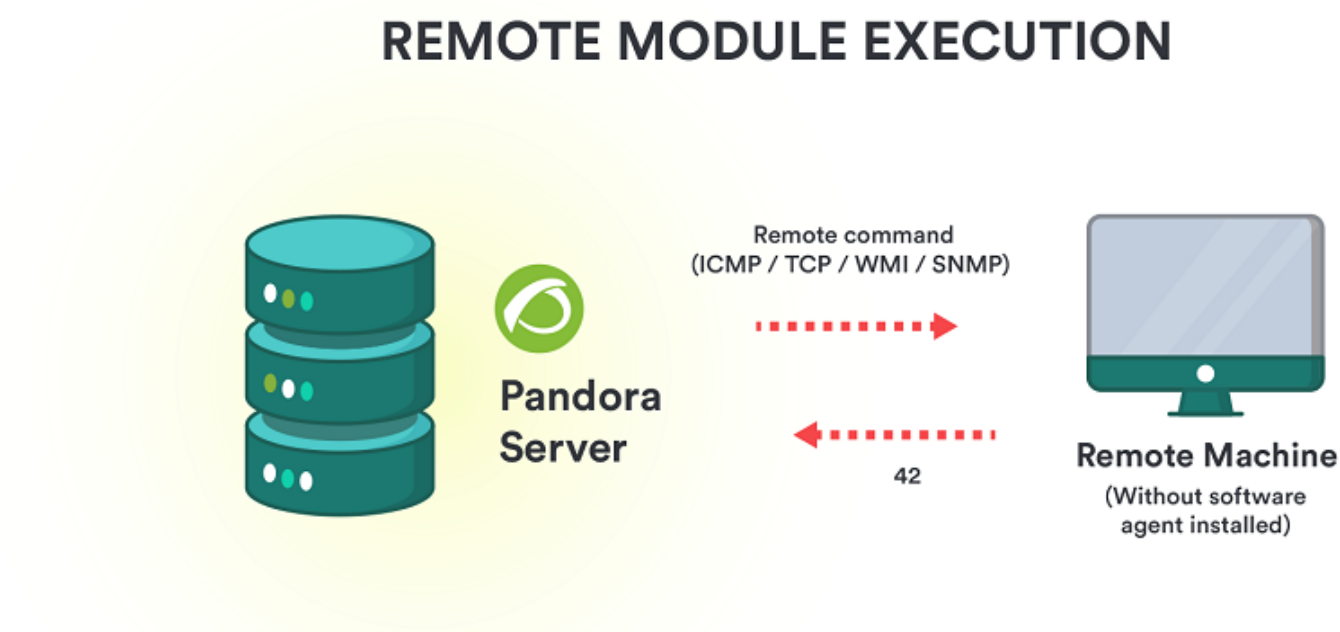


Pandora FMS の機能概要

- 自動検出(ローカル) Pandora エージェントのデフォルトの監視で、ハードディスク、パーティション、データベースサーバにおけるデータベース、その他を検出できます。
- 自動検出(リモート) リモートでネットワークを使って、稼働中のシステムや OS およびモニタリングできる設定などの関連情報を検出することができます。また、ネットワークトポロジーの検出および、ルーティングに基づくネットワーク図を作成することができます。
- モニタリング Pandora FMS のエージェントは最も強力です。基本的なコマンドの実行結果や Windows API から、イベント、ログ、数値データ、プロセスの状態、メモリやCPUの使用率などの情報を取得することができます。Pandora にはデフォルトでモニタリング用のライブラリがあります。しかし、Pandora の最大の利点は、新たなモニタリングを作成し追加できることにあります。
- コントロール エージェントはそれ自身でサービスを有効化したり、テンポラリファイルを削除したり、プロセスを実行したりできます。コンソールからリモートでサービスの停止・起動などのコマンド実行も可能です。さらに、指定した時間にタスクを実行することもできます。*eHorus* を用いて Pandora FMS からリモートのシステムにアクセスすることや、ウェブインタフェースから telnet や ssh のツールを利用することも可能です。
- アラートと警告 通知は障害検出と同様に重要です。Pandora は、ほぼ無限の通知方法とフォーマットを提供します。エスカレーション、アラートの関連、イベントの依存関係による集約なども制限なしで含みます。
- 分析と表示 モニタリングは trap を受信したりダウンしているサービスを表示したりするだけではありません。予測レポートや、長期間収集したデータの関連グラフを出すことができ、ユーザポータルとして第三者に提供したり、独自のグラフや表の定義を作成できます。
- インベントリ生成 一般なソリューションとして構成管理ツールがありますが、Pandora ではこれがオプションとしてついています。インベントリは柔軟で動的です(自動検出可能で、リモート入力等も可能です)。変更(ソフトウエアのアンインストールなど)を通知するために利用したり、単純に一覧を生成するために利用したりできます。

リモート監視

リモート監視とは、Pandora FMS サーバが監視対象のデバイスを 同期 でポーリングすることを意味します。 この処理は、ポーリングまたはリモート監視として知られています。



一般的に言えば、リモートから監視する場合には次の 2つの目的があります。

- 動作しているかかどうかの確認
- 値の取得 (例えば、ネットワークトラフィックやアクティブな接続数)

同期監視は常に同じ方向、つまり監視サーバから監視対象
に対して行われ、SNMP や WMI (MS Microsoft®) などのプロ
トコルを通じて実行できます。

逆の処理は 非同期 監視と呼ばれ、リモート監視の場合は通常 SNMP トラップです。

- ネットワーク環境を監視するには、SNMP デバイスの外部ブラウザを使用した SNMP プロトコル、ネットワークデバイスメーカーの MIB コレクション (OID ライブラリ) へのアクセス、およびトラップリスニングを選択します。 そして、各デバイスのカスタム OID コレクションに追加します。Unix® および GNU/Linux® システムの場合は、SNMP 機能を有効にする必要があります。
- MS Windows® サーバの WMI 監視では、認証を通じて適切に実行され、かつ強力です。

ローカル監視 (ソフトウエアエージェントの利用)

システムおよびアプリケーションに関して情報を収集する最も良い方法は、間違いなくそのシステム自身から取得することです。Pandora FMS ソフトウエアエージェント では、コマンドやスクリプトの実行、またはシステムやアプリケーション上のクエリの実行ができます。

ソフトウェアエージェントには、コマンドによる情報の取得に加えて、インベントリ情報の取得などの高度な機能が含まれています。エージェントは、問題や障害が発生した場合に対応し、システムと自動的に対話したり、一時ファイルを削除したり、指定されたコマンドを実行したりするように設定することもできます。 ソフトウェアエージェントから Pandora FMS サーバに直接接続できない場合は、Pandora FMS サテライトサーバ またはブローカーエージェントを使用できます。

監視の手順

導入や設定を開始する前に、監視対象における技術的なキーポイントを把握しておくことが重要です。それにより、無駄な時間を浪費せずに、システム上の特定のデータに関する情報が何のためにあるのか、最大限に活用するにはどうすべきかが明確になります。

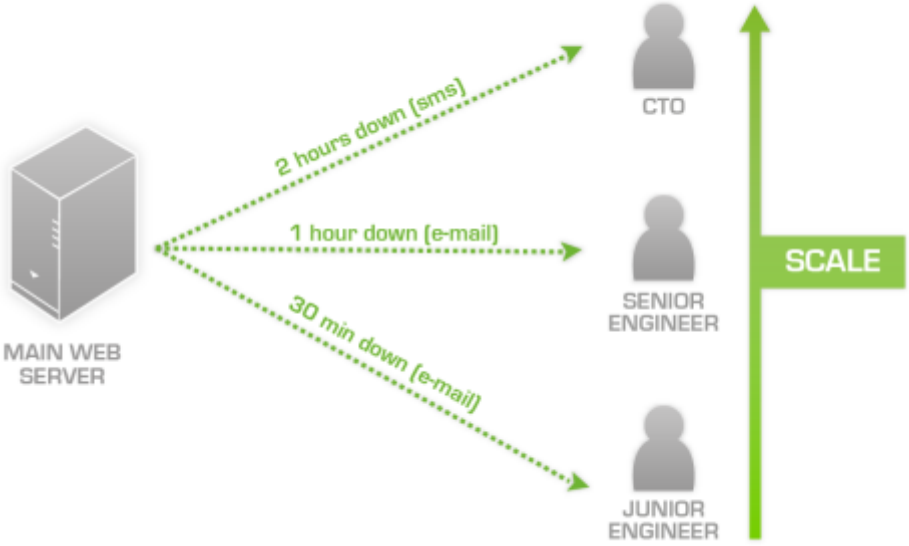
- 可用性: ほとんどの場合、イベントベースの監視と必要に応じてリモート監視で十分な場面が多いでしょう。素早く展開が可能で比較的迅速に結果を得ることができます。 この場合に、SLA レポートが最も役立ちます。
- パフォーマンス: グラフや数値データが重要な要素です。エージェントまたはリモートから情報を取得します。エージェントでシステムのより深い情報をとる必要があるかもしれません。グループレポートおよび組み合わせグラフがポイントです。
- キャパシティプランニング: より独自性が高くなり、2つ目の件とどうようにデータの取得が必要です。ただし、それをもとに、予測監視やより特別な予想レポートを使います。エージェントからの初期のアラートは、警告や障害状態の意味を把握するのに必要です。問題が発生する前に防止するために、発生するイベントの管理(運用)ポリシーを策定します。これは、間違いなく最も複雑で興味深いパターンです。

対応手順の検討

対応の手順を立てるためには、いくつかの要因を考慮する必要があります：

- イベントの緊急性: まれなものや致命的なものと、通常状態の区別
- 通知形態: Email、SMS、Telegram、音声アラートなど。
- スケーリング: 問題が繰り返された後の違う形での報告。一般的なケースでは、問題の解決前に一定時間が経過したらマネージャーに通知するなどです。

設定を実施する前に、これらの概念について明確にし、監視方法、収集されたすべての情報をどのように処理するか、発生した問題をどう報告するかといった、重要な要素の計画を作成することをお勧めします。



まず、最も重要な問題に焦点を当てることで、組織にとって最も重要な問題は何かを定義する論理的な出発点に立つことができます。最も重要な要素が何であるかが分かったら、対象を監視する方法を定義し、そのシステムであがった問題を解決する担当者を考えます。適切な人々に問題の存在を通知する方法について説明します。

管理モデル

- 直接管理モデルは、一人または複数の人が定常的にシステムを見ています。何か障害が発生すればすぐに検出されます。それはちょっとした通知でクリティカルなものではありません。また、より柔軟性があります。すべてのケースを通知 (Pandora でのアラート) する必要はありません。常にシステムで何が起っているかのイベント (状態の変化をみつけます) を参照すれば十分です。多くの画面を定義することができ、集約したアラートを定義することができます。このモデルは、ラートポリシーを定義することが重要ではなく、自動的な管理ができない大規模環境で利用されます。
- 間接管理モデル では、定常的に画面を見る人はいません。イベント、グラフ、マップは誰も見ていないため、自動的にシステムの状態を通知する設定を行う必要があります。このシステムはデバイスが少ない場合や、何が障害状態でどう対処するべきか明確な場合に適しています。

Pandora FMS ドキュメント一覧に戻る