ログの監視と収集

ログの監視と収集

Pandora FMS ドキュメント一覧に戻る

概要

Pandora FMS におけるログ監視には、以下の 2つの異なる手法があります。

1. モジュールベース: 非同期監視としの Pandora でログを表現します。ユーザにより事前設定された条件を満たすデータを検出した場合にアラートを関連付けることができます。 ログのモジュール表現では、以下を行うことができます：
    1. ログの中で正規表現にマッチする数を数えるモジュールの作成
    2. ログメッセージの行および内容を取得
2. 複合表示ベース: キャプチャしたい複数の発生元のログからすべての情報を 1つのコンソールで表示し、ログが処理されたタイムスタンプを使用して情報を順番に整理できます。

バージョン 7.0 NG 774 以降、Pandora FMS にはログ情報を保存するために OpenSearch が組み込まれています。“ OpenSearch のインストールと設定 ”もご確認ください。

動作の仕組み

- ソフトウエアエージェントで分析されたログ (eventlog またはテキストファイル) は、Pandora サーバへ転送されます。エージェントから送信される XML に (RAW) データとして含まれます。
- Pandora FMS データサーバは、エージェントから XML を受け取ります。そこには、監視とログの両方の情報が含まれています。
- データサーバが XML データを処理する時に、ログ情報を識別し、報告されたエージェントに関する情報やログのソースをプライマリデータベースに保存し、ログの保存には情報を自動的に OpenSearch に送信します。
- Pandora FMS はデータを OpenSearch インデックスに保存し、各 Pandora FMS インスタンスの日次インデックスを生成します。
- Pandora FMS サーバには、システム管理者が定義した間隔(デフォルトでは30日)でインデックスを削除するメンテナンスタスクがあります。

ログ収集

バージョン 7.0 NG 774 以降、Pandora FMS にはログ情報を保存するための OpenSearch が組み込まれています。ログの収集を開始する前に、まずこのサーバを用意してください。「OpenSearch のインストールと設定」も参照してください。

コンソールの設定

ログの表示を有効化するには、管理(Management) → セットアップ(Setup) → システム設定 → ログ収集(Log collector) へ行き、設定を有効化する必要があります。ログ収集の有効化(Activate Log Collector) をクリックし、更新(Update) をクリックします。

OpenSearch オプション セクションで次の値を設定する必要があります。

1. OpenSearch IP: Pandora FMS で使用する OpenSearch サーバーの IP アドレス。
2. https の利用(Use https): インストールした OpenSearch 環境において接続に HTTPS が有効になっている場合は有効にする必要があります。
3. OpenSearch ポート(OpenSearch Port): TCP のポート番号。
4. 古い情報を削除する日数(Days to purge old information): 収集したデータを削除するまでの日数。
5. 基本認証(Basic authentication): (オプション) OpenSearch に基本認証が設定されている場合 (推奨)、ユーザ (User) とパスワード (Password) を入力する必要があります。

エージェント設定

ログ収集は、Microsoft Windows® 用エージェントと Unix® エージェント (Linux®、MacOS X®、Solaris®、HPUX®、AIX®、BSD® など) の両方でエージェントを通じて行われます。MS Windows® エージェントの場合、イベントビューワ監視モジュールと同じフィルタを使用して、オペレーティングシステムのイベントビューワから情報を取得することもできます。

MS Windows の例

バージョン 774 以降では、`Logs extraction` の下の行のコメントを外す必要があります。

```
# Log extraction
#module_begin
#module_name X_Server_log
#module_description Logs extraction module
#module_type log
#module_regexp C:\server\logs\xserver.log
#module_pattern .*
#module_end
```

ログタイプモジュールの説明の詳細については、特定のディレクティブ を参照して次のセクションを確認してください。

```
module_type log
```

このタイプのタグ `module_type log` を定義すると、データベースに保存するのではなく、ログコレクターに送信する指定になります。このタイプのデータを持つモジュールは、有効になっている場合はコレクターに送信されます。そうでない場合は、情報は破棄されます。

774 より前のバージョンの場合:

バージョン 750 以降では、詳細オプションを有効にすることで、エージェント プラグイン を使用してこのアクションを実行できます。

以下に示すタイプの処理が実行されます。

logchannel モジュール

```
module_begin
module_name MyEvent
module_type log
module_logchannel
module_source <logChannel>
module_eventtype <event_type/level>
module_eventcode <event_id>
module_pattern <text substring to match>
module_description <description>
module_end
```

logevent モジュール

```
module_begin
module_name Eventlog_System
module_type log
module_logevent
module_source System
module_end
```

regexp モジュール

```
module_begin
module_name PandoraAgent_log
module_type log
module_regexp <%PROGRAMFILES%>\pandora_agent\pandora_agent.log
module_description This module will return all lines from the specified logfile
module_pattern .*
module_end
```

Unix システムの例

バージョン 774 以降では、Logs extraction の下の行を *コメント解除* する必要があります。

```
# Log extraction
```

```
#module_begin
#module_name Syslog
#module_description Logs extraction module
#module_type log
#module_regexp /var/log/logfile.log
#module_pattern .*
#module_end
```

ログタイプモジュールの説明の詳細については、特定のディレクティブ を参照して次のセクションを確認してください。

```
module_type log
```

このタイプのタグ module_type log を定義すると、データベースに保存するのではなく、ログコレクターに送信する指定になります。このタイプのデータを持つモジュールは、有効になっている場合はコレクターに送信されます。そうでない場合は、情報は破棄されます。

744 より前のバージョンの場合:

```
module_plugin grep_log_module /var/log/messages Syslog \.\*
```

ログ解析プラグイン (grep_log) と同様に、grep_log_module プラグインは、処理されたログ情報を、ソースとして “Syslog” という名前のログコレクターに送信します。送信する行と送信しない行を選択するときに、正規表現 \.* (この場合は「すべて」) をパターンとして使用します。

Pandora FMS Syslog サーバ

このコンポーネントにより Pandora FMS は、それが配置されているマシンの syslog を分析し、その内容を対応する OpenSearch サーバに保存できるようになります。

https://www.rsyslog.com/

Syslog サーバの主な利点は、ログの統合を補完することです Syslog サーバの Linux® および Unix® 環境からのエクスポート機能によってサポートされているため Syslog サーバでは、ソースに関係なくログを照会し、単一の共通ポイント (Pandora FMS コンソールログビューア) で検索できます。

Syslog サーバ 8.2102 のインストールは、クライアントとサーバの両方で実行する必要があります。

```
dnf install rsyslog
```

設定ファイル /etc/rsyslog.conf にアクセスして、TCP および UDP 入力を有効にします。

```
  (...)

# Provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# Provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

  (...)
```

rsyslog サービスを再起動します。サービスが利用可能になったら、次のコマンドでポート 514 にアクセスできることを確認します。

```
netstat -ltnp
```

クライアント側 では Syslog サーバにログを送信できるように rsyslog を設定します。/etc/rsyslog.conf にてリモートホストを設定する行を見つけて有効にします (remote-host をサーバの IP アドレスに変更します)。

```
action(type="omfwd Target="remote-host" Port="514" Protocol="tcp")
```

rsyslog が受信するログのサイズは、デフォルトでは 8 キロバイトです。これより大きなログを受信すると、完全なログが受信されるまで、残りのコンテンツを含む新しいエントリが追加されます。これらの新しいエントリには、ログを送信したホストの名前が含まれていないため、この動作により、コンソールに新しい不要なログソースと新しいエージェントの両方が作成されることがあります。これを回避するには、次の行を追加して、受信するログのサイズを増やすことをお勧めします。

```
$MaxMessageSize 512k
```

ファイルを保存してテキストエディタを終了します。

ログを送信すると、クライアントの名前を持つコンテナエージェントが生成されるため、エージェントの重複を避けるために、クライアントのホスト名と一致する「別名」でエージェントを作成することをお勧めします。

Pandora FMS サーバでこの機能を有効にするには、pandora_server.conf ファイルで 次の内容を有効にします。

```
# Enable (1) or disable (0) the Pandora FMS Syslog Server
syslogserver 1

# Full path to syslog's output file.
```

```
syslog_file /var/log/messages

# Number of threads for the Syslog Server
syslog_threads 2

# Maximum number of lines queued by the Syslog Server's
syslog_max 65535
```

ログが Pandora FMS サーバに送信されるようにデバイスの
設定を変更する必要があることに注意してください。

PFMS サーバレベルでのフィルタ

Pandora FMS サーバでは、トークン syslog_whitelist を使用して、大文字と小文字を区別する正規表現または regexp に一致するログのみを 許可 し (たとえば、windows は Windows と同じではありません)、それ以外を破棄 することができます。

トークン syslog_blacklist を使用すると、設定された regexp に一致するログを 拒否 することができます (その他はすべて許可)

両方のトークンはデフォルトで無効になっています

- syslog_whitelist: このトークンを有効にすると、regexp に準拠するログのみが受け入れられ、残りは破棄されます。
  - このトークンが有効化され、デフォルトのフィルタ .* が設定されている場合は、すべてが受け入れられます。
  - 重要: 上記のトークンが正規表現なしで有効化されると、何も許可されません
- 許可されたキーワードのフィルタリングが最初に実行されるため、次のステップの作業が削減されます。
- syslog_blacklist: regexp を配置すると、それに準拠するすべてのものが破棄されます (このトークンが有効化されていても、regexp がない状態の場合は、何もブロックされません)。
- syslog_blacklist によるフィルタリングは最後に行われます。

OpenSearch インタフェース

バージョン NG 774 以降

表示と検索

ログ収集ツールでは、主に 2 つの機能が重要です。情報の検索機能 (日付、データソース、キーワードなどでフィルタリング) と、時間単位ごとの発生回数で描画された情報の表示機能 (メニュー 操作(Operation) → モニタリング(Monitoring) → ログビューア(Log viewer)) です。

最も重要かつ便利なフィールドは、検索(Search) テキストボックスに入力する検索文字列と、使用

可能な 3 つの検索タイプ (検索モード(Search mode)) の組み合わせです。

- 完全一致(Exact match): リテラル文字列検索。ログには完全一致が 含まれます
- すべての単語(All words): 同じログ行内の順序に関係なく、指定された単語をすべて含む検索を行います。
- 任意の単語(Any word): 順序に関係なく、指定された単語の いずれか を含むものを検索します。
- フィルタリングされたコンテンツのコンテキストを表示するオプションをオンにすると、検索に関連する他のログ行の情報とともに状況の概要が表示されます。

高度な表示と検索

この機能を使用すると、データキャプチャモデルに基づいて情報を分類し、ログエントリをグラフィカルに表示できます。

これらのデータキャプチャモデルは基本的に、データソースを解析してグラフとして表示できる正規表現と識別子です。

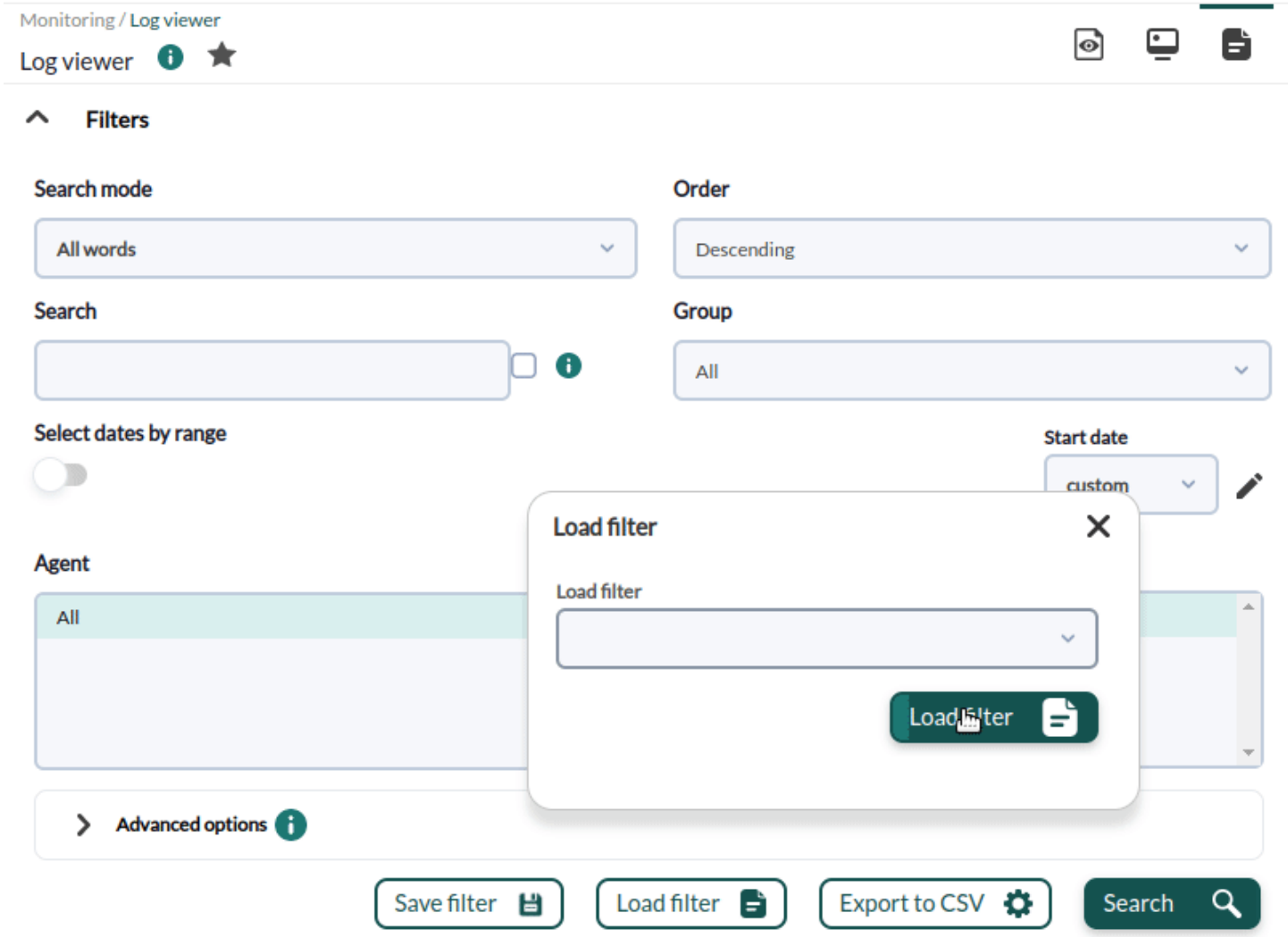
高度なオプションにアクセスするには、高度なオプション(Advanced options) をクリックします。結果の表示タイプを選択できるフォームが表示されます。

- ログエントリを表示します（プレーンテキスト）。
- ロググラフを表示します。
- ロググラフの表示オプション (表示モード) を使用して、キャプチャモデル (キャプチャモデルの使用(Use capture model)) を選択できます。
- デフォルトモデルである Apache ログモデルでは Apache ログを標準形式 (access_log) で処理または解析し、応答時間の比較グラフを取得したり、アクセスしたページと応答コード別にグループ化したりできます。
- 新しいキャプチャ モデルを作成するには、[編集] または [作成] をクリックします。

共通フィルタ

バージョン 771 以上

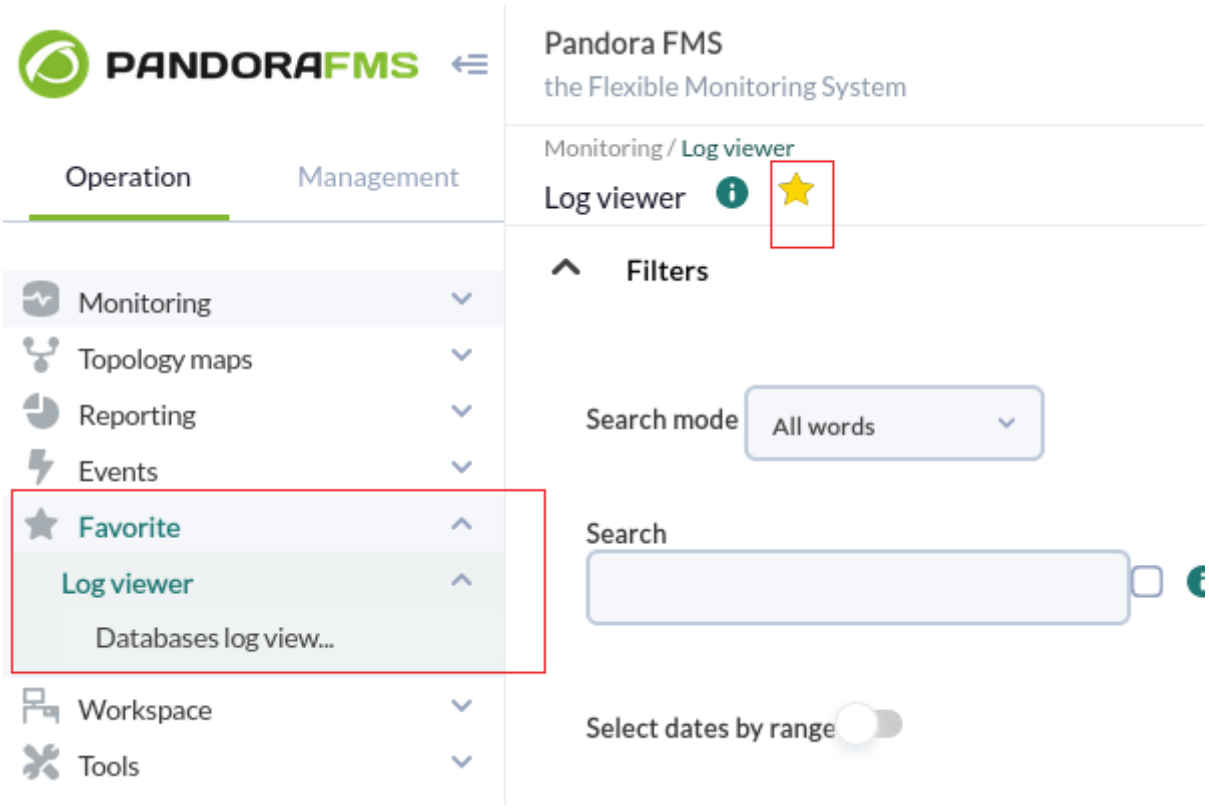
このオプションを使用すると、頻繁に使用するフィルタリング設定を保存して、頻繁に使用するフィルタのリストを作成できます。すべてのフィルタ値を設定したら、フィルタを保存(Save filter) をクリックし、名前を割り当てて 保存(Save) をクリックします。他のときはいつでも、フィルタ読み込み(Load filter) ボタンを使用してこれらの設定を読み込み、保存したフィルタのリストをダウンロードして、そのうちの 1 つを選択して フィルタ読み込み(Load filter) をクリックできます。



お気に入りアイテムとして保存されたフィルタ

バージョン 770 以上

PFMS のお気に入りシステムを使用すると、セクションタイトルの星アイコンをクリックして、フィルタリング設定を含む ログビューワ のショートカットを保存できます。



エージェント表示でのログソース

Pandora FMS バージョン 749 以降、**ログソース状態** と呼ばれるボックスがエージェント表示に追加され、そのエージェントによる最後のログ更新の日付が表示されます。虫眼鏡のアイコンをクリックすると、そのログにフィルタした**ログビューワ**表示にリダイレクトされます。

バージョン 774 以降: デフォルトでは、両方のビューに表示されるデータは過去 24 時間に制限されていますが、必要に応じて変更できます。

Pandora FMS ドキュメント一覧に戻る