アラートシステム

アラートシステム

Pandora FMS ドキュメント一覧に戻る

概要

アラートは、モジュールの値が変化したときに Pandora FMS が行う動作の定義です。このような動作は設定可能で、管理者へメールやSMS を送ったり、SNMP トラップの送信、システムログへのインシデントの記録などができます。アラートは、基本的に、モジュールを実行している Pandora FMS サーバが動作している OS 上で、アクションから起動させるスクリプトです。

Pandora FMS では、アラートは、いくつかの発報条件、そのアラートに対して選択されたいくつかのアクション、そして最後に、アクションの実行を担当する Pandora FMS サーバ上のコマンド定義によって機能します。

アラートにはいくつかのタイプがあります。

- シンプルなアラート
- イベントに関する アラート
- SNMPトラップに関するアラート

アラートの仕組

- コマンド: アラートが発生したときに Pandora FMS サーバが実行するコマンド定義します。コマンドの例としては、ログへの書き込み、email または SMS の送信、スクリプトの実行などです。
- アクション: これは「どのように行われるか」を定義するものであり、コマンドの引数のカスタマイズです。モジュール名やエージェントなどの特定のパラメータをコマンドに渡して、コマンド実行をカスタマイズすることができます。
- テンプレート: これは、「いつ実行されるのか」を指定し、アクションを引き起こす条件を定義します。たとえば、モジュールが障害状態になった場合などです。

アラートシステムの情報の流れ

アクションとテンプレートには、'フィールド1'、'フィールド2'、'フィールド3'、(…) フィールドn といった一般的なフィールドがあります。これらのフィールドは、テンプレート → アクション → コマンド という情報の伝達の優先順位に従って適用され、最後にはコマンドの実行パラメータとして使われます。

次のステップの Fieldn フィールドに情報が定義されていないと、前のステップの情報が引き継がれます。 つまり、フィールドまたはパラメータが上書きされるというのは、アクションのフィールド設定はテンプレートのフィールド設定を上書きするということです。(たとえば、テンプレートに field1 が定義されていて、アクションも定義されている場合、アクションの field1 の設定が利用されます。)

アラートコマンド

概要

管理(Management) メニュー → アラート(Alerts) → コマンド(Commands)

アラート状況が発生した場合に Pandora FMS が実行するアクションは、最終的にサーバ上で コマンド の形式で実行されます。

アラートコマンドを作成するには、Pandora FMS 管理者 で
ログインする必要があります。

アラートのコマンド作成

管理(Management) メニュー → アラート(Alerts) → コマンド(Commands) → 作成(Create)

コマンドの実行が成功するかどうか、また期待した結果が
得られるかどうか (電子メールの送信、ログ ファイルへのエ
ントリの生成など) をコマンドラインから確認することをお
勧めします。

- コマンド(Command): アラート発報時に実行されるコマンドです。アラートの設定でパラメータを置き換える マクロ を利用することができます。
- グループ(Group): これにより、コマンドをどのアラートグループに関連付けることができるかが決まります。 ユーザが明示的にグループ すべて (すべてグループ) に属している場合を除き、アラートコマンドを作成しているユーザが属するグループのみを割り当てることができます。
- フィールドの説明(Field description) および フィールドの値(Vield values):
    - 存在するフィールド値: そのフィールドで使用可能な値のコレクションです。 このフィールドが設定されている (空ではない) 場合、フィールドはテキストボックスではなくコンボ選択になりま

す。 コンボには、可能な値ごとにラベル (表示されるオプション) と値 (送信されたオプション) が必要です。 構文は次のとおりです: value1,label1;value2,label2;value3,label3;valueN,labelN
    - 隠す(Hide): *フィールドにパスワードを含む場合は、このオプションでコンテンツをアスタリスクで隠します。*
- コマンドフィールドに特別なトークン値 `_html_editor_` がある場合、アラートアクションの作成または編集時にコマンドフィールドに HTML エディターを表示できます。

Pandora FMS サーバによって実行されるアラートのコマンドは、Pandora FMS サーバを実行するユーザと同じ権限で実行されることを考慮する必要があります。

定義済のコマンド

- eMail: Pandora FMS サーバからメールを送信します。Perl の sendmail モジュールを利用します。メールはHTML形式で送信されるため、視覚的に魅力的なテンプレートを作成できます。メールの受信者は、画像などテンプレートで使用されるリソースにアクセスできる必要があることに注意してください。
- Internal audit: これは、Pandora FMS の内部監査システムに記録を残す内部アラートです。これは、Pandora FMS のデータベースに保存され、コンソールのイベントビューワから確認することができます。
- Pandora FMS Event: Pandora FMS イベントマネージャにカスタムイベントを生成します。
- Pandora FMS Alertlog: /var/log/pandora/pandora_alert.log に、プレーンテキストのログファイルとしてアラートを出力します。
- SNMP Trap: 引数を使って SNMP トラップを送信します。
- Syslog: アラートを syslog に飛ばします。システムの logger コマンドを利用します。
- Sound Alert: アラートが発生した時に音を鳴らします。
- Jabber Alert: 事前に定義したサーバのチャットルームに Jabber アラートを送信します(先に .sendxmpprc ファイルを編集します)。フィールド3 をテキストメッセージに利用し、フィールド1 が発信者の名前、フィールド2 がチャットルーム名です。
- SMS Text: 指定した携帯に SMS を送信します。ただし、これが実行できるようにアラートを事前に定義しておく必要があります。また、Pandora FMS から SMS を送信できるように設定したゲートウェイが必要です。また、SMS を送信するのみ Gnokii をインストールすることも可能です。この場合、ノキアの携帯を USB ケーブルで接続して直接送信できます。具体的方法は別途説明しています。
- Validate Event: モジュールに関連するすべてのイベントを承諾します。エージェント名とモジュール名を指定します。
- Remote agent control: このコマンドは、UDP サーバが有効になっているエージェントにコマンドを送信するために使用します。UDP サーバは、エージェント(Windows および UNIX)にエージェントの実行を“ リフレッシュ ”するように命令するために使用されます。つまり、エージェントにデータの実行と送信を強制します。
- Generate Notification: このコマンドを使用すると、任意のユーザまたはグループに内部通知を送信できます。
- Send report by e-mail および Send report by e-mail (from template): どちらのオプションでも、さまざまな形式(XML、PDF、JSON、CSV)のレポートをメールで送信できます。2番目のオプションでは、添付レポートにテンプレートを使用できます。

ウェブコンソールで 公開 URL が設定されている場合、送信されるメールにはそのリンクが設定されます。

アラートのコマンド編集

管理(Management) メニュー → アラート(Alerts) → コマンド(Commands) → 編集するコマンドの名前をクリック。選択したアラートを編集したら、更新(Update) ボタンをクリックします。

eMail, Internal Audit および Pandora FMS Event は変更や削除はできません。

アラートアクション

概要

アクションは、コマンドに、フィールド1フィールド2 ...フィールド10 を関連付けた、アラートのコンポーネントです。

アクションは、どのようにコマンドを起動するかを定義できます。

アクションの作成

管理(Management) メニュー → アラート(Alerts) → アクション(Actions) → 作成(Create)

- グループ(Group): アクショングループです。ユーザが"すべて"グループに属してない場合は、アクションを作成するユーザが属するグループのみを割り当てることができます。コマンドに *全て(All)* 以外のグループが割り当てられている場合、コマンドに関連付けられたグループまたは *全て(All)* グループのみをアクショングループとして設定できます。何らかの理由でこれが実行できない場合は、必要な権限を持つユーザによる修正を求める警告メッセージが表示されます。
- コマンド(Command): アラートが発生したときに実行されるコマンドをこのフィールドで定義しますPandora にあらかじめ定義されているコマンド以外も選択できます。
- しきい値(Threshold): アラートアクションは、アラートが発報された回数に関係なく、この時間間隔内で 1 回だけ実行されます。
- 実行されるコマンドのプレビュ(Command Preview): このフィールドは編集できません。システムで実行されるコマンドが自動的に表示されます。
- フィールド 1-10(Field 1-10): '_field1_' から '_field10_' までのマクロの値をここで定義します。必要に応じて、コマンドとともに使用することを目的としています。 これらのフィールドは、設定されている場合、テキストフィールドまたは選択メニューになります。

障害通知の“ フィールド ”に値を設定すると、デフォルトでは異なる値を割り当てない限り、同じ値が復旧通知用にも使われます。

アクションの編集

管理(Management) メニュー → アラート(Alerts) → アクション(Actions) → 編集するアクションの名前をクリックします。

アクションの削除

管理(Management) メニュー → アラート(Alerts) → アクション(Actions) → 対応するゴミ箱アイコン(削除(Delete)カラムをクリックします。

アラートテンプレート

概要

テンプレートは、アラート発報条件を定義します(いつアクションを実行する必要があるか)。アラートテンプレートはモジュールに関連付けられ、テンプレートの条件にマッチすると関連するアクションが実行されます。

Pandora FMS で多くの場合に利用される個々の汎用テンプレートグループを用意しておくことができます。

テンプレートの作成

管理(Management) メニュー → アラート(Alerts) → テンプレート(Templates) → 作成(Create)

続いて、次の 3つのステップを実施します。

ステップ 1: 概要

- グループ(Group): テンプレートが適用されるグループ。 テンプレートを作成しているユーザがグループ全て (全てグループ) に明示的に属している場合を除き、テンプレートを作成しているユーザが属するグループのみを割り当てることができます。
- 優先度(Priority): アラートに関する情報を提供するフィールドです。 アラートが発報されると、生成されたイベントはこの優先度を継承します。 アラートを検索する際のフィルタリングに役立ちます。

ステップ 2: 状態

- 特別日一覧を利用する(Use special days list): テンプレートで利用する特別日のカレンダーを設定します。
- 再通知間隔(Time Threshold): アラームカウンターをリセットする時間です。これは、アラートが アラートの最大数 を超えて再通知されないようにする時間間隔を定義します。指定された間隔の後、カウンターはリセットされます。アラートが復旧しない状態では、カウンターはリセットされません。継続しないアラートのカウンターリセット(Reset counter for non-sustained alerts) が有効化されていない限り、正常な状態に戻ってアラートが復旧した場合は、すぐにカウンターはリセットされます。
- 最小アラート数(Min. number of Alerts): テンプレートに設定された条件を何回(モジュールの連続抑制回数パラメータで定義された数から数えます)満たした場合にアラートを発報するかの定義です。デフォルトは '0' です。これは、条件を満たす値が最初に受信されたときにアラートを発報することを意味します。これはフィルターとして機能することを目的としており、誤検知を排除するのに役立ちます。
- 最大アラート数(Max number of Alerts): 同じ時間間隔(再通知間隔)内で連続して送信できるアラートの最大数です。これは最大アラートカウンタ値です。 指定した数を超えるアラートは再通知間隔内では発報されません。
- 通常のアクション(Default Action): テンプレートが持つデフォルトのアクションをここで定義します。これは、テンプレートがモジュールに割り当てられたときに自動的に作成されるアクションになります。ここでは、1 つを割り当てるもしくは何も割り当てないことができますが、複数のデフォルトアクションを割り当てることはできません。
- スケジュール(Schedule): アラートが発報される日です。

バージョン NG 760 以降: デフォルトのシンプルモードで表示される組み込みのエディターにより、アラートが毎日有効になるタイミングを表示および設定することができます。さらに、詳細モードにアクセスすると、より正確にスケジュールを設定できます。

- アラートが継続しない場合にカウンターをリセット(Reset counter for non-sustained alerts): これを有効化すると、示された条件が連続して繰り返されない場合にアラートカウンターがリセットされます。これの有効化は、最小アラート数 に示されている数が 0 より大きいことにも依存します。たとえば、フィールド 最小アラート数 の値が 2 の場合、モジュールがアラートを発報するには 条件タイプ で割り当てられた状態を 3 回経る必要があることを意味します。以降、トークンには 2 つのシナリオがあります。
- リセットトークンがチェックされている場合、障害状態の数は連続している必要があります。そうでない場合は、カウンターがリセットされます。

```
normal -> critical -> critical -> critical
```

- リセットトークンがチェックされていない場合、交互または連続した一連の障害状態の後にアラートが発報されます。

```
normal -> critical -> normal -> critical -> normal -> critical
```

不明状態 のモジュールを定期的に確認するには、Pandora FMS サーバ設定 で unknown_updates トークンを有効にします。

ステップ 3: 高度なフィールド

- 復旧アラート (Alert Recovery): 復旧アラートを有効にするかどうかを設定します。復旧アラートが有効になっている場合、モジュールがテンプレートで示された条件を満たさなくなったときに、このカラムに定義されているフィールドで指定された引数で関連付けられたアクションが実行されます。
- フィールド 1 (Field 1) ~ フィールド 10 (Field 10) (アラートテンプレート、コマンド、アクションいずれも) では、マクロ一覧 のマクロを利用できます。

設定が完了したら、終了(Finish) をクリックします。

アラートテンプレートのモジュールへの割当

アラートサブメニューでのアラート管理

アラートサブメニューでのアラート割当

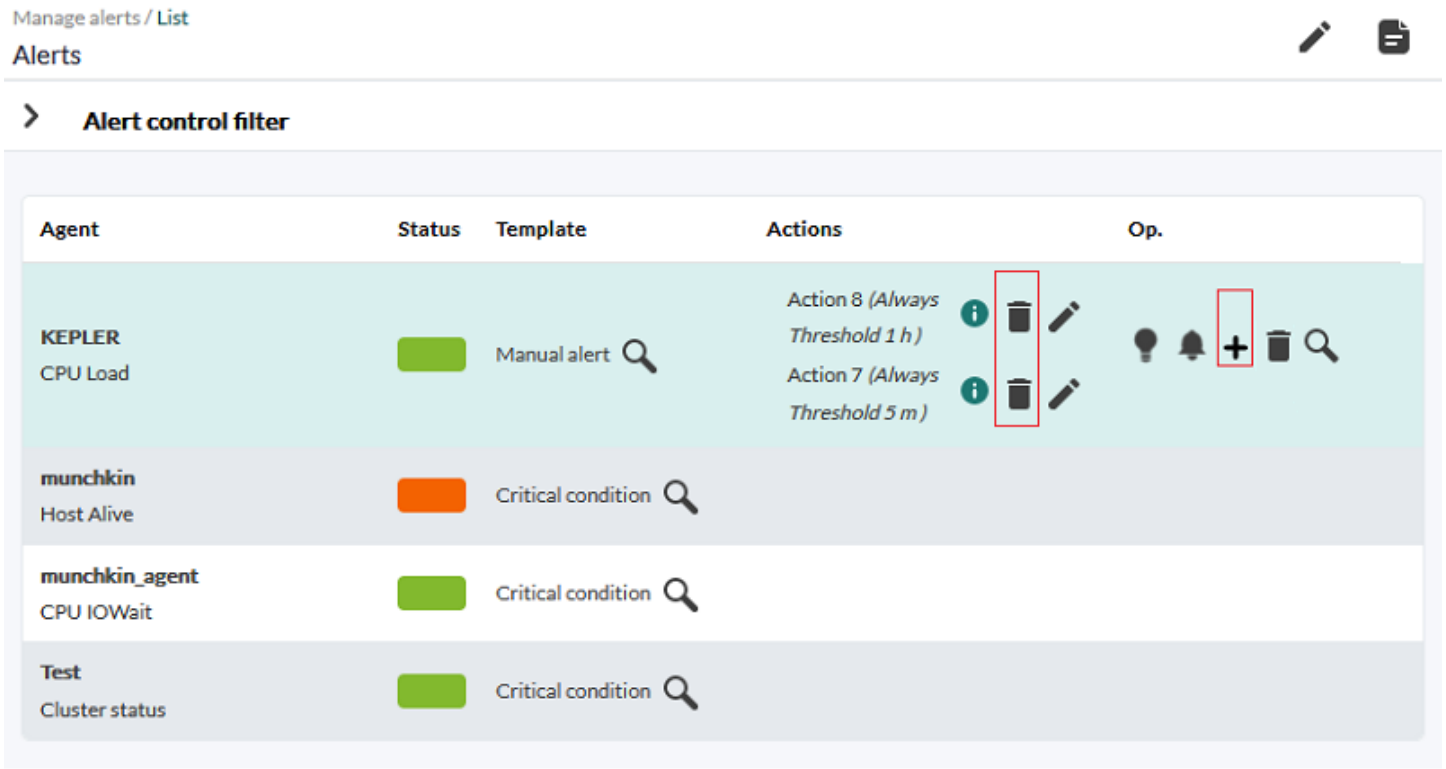
管理(Management) メニュー → アラート(Alerts) → アラート一覧(List of alerts) → 鉛筆アイコン(アラートビルダ(Builder alert))をクリック。

- エージェント(Agent): アラートを割り当てるエージェント名を入力します。
- モジュール(Module): アラートを発生させるモジュールを選択します。
- アクション(Actions):テンプレートで定義済のアクションを選択します。あとから複数のアクションを設定することもできます。
- テンプレート(Template): 割り当てたいアラートテンプレートを選択します。
- 閾値(Threshold): アラート発生回数に関係なく、`action_threshold` で指定した秒数内は、一回のみアラートアクションが実行されます。

アラートサブメニューでのアラート編集

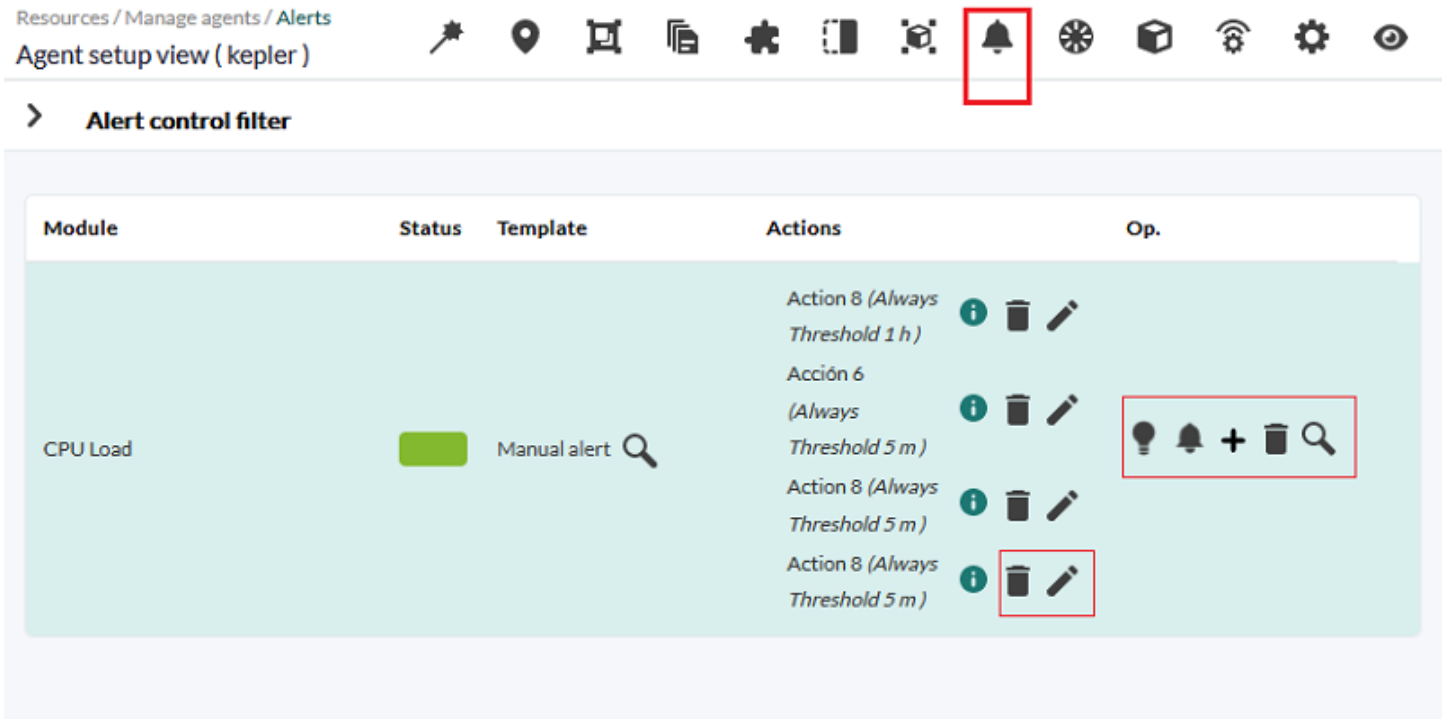
アラートを作成すると、テンプレートが持っているアクションのみ編集することができます。

アクションの右側にあるグレーのごみ箱アイコンをクリックすることにより、選択したアラートを削除することもできます。また、+ ボタンをクリックすることにより新たに追加することもできます。



エージェント管理からのアラート管理

エージェント管理セクションから、対応するタブに移動して、新しいアラートを追加できます。



次の操作ができます。

- エージェントに割り当てられた各アラートの個々またはすべてのアクションを編集または削除(アクション 列)。
- オプション列 (Op.):
  - 無効化または有効化ができます。
  - アラートを *スタンバイ* モードにできます。
  - アクションを追加できます。
  - アラートを完全に クリア できます。
  - アラート詳細を参照できます。

アラートの概要

- モジュールで障害および警告のしきい値を定義します。
- アラートをモジュールに関連付けます。これを行うには、モジュールが存在するエージェント内のアラートタブに移動します。
  - 必要に応じてボタンをクリックすると対応するセクションにリダイレクトされ、新しいアクション または 新しいテンプレート を作成できます。 新しいコンポーネントを作成したら、前のステップに戻る必要があります。
- アラート追加(Add alert) ボタンで、新しいアラートが保存されます。
- *アラートエスカレーション:* アラートエスカレーションは、アラートが一定回数連続して繰り返された場合に実行される追加アクションです。
  - アクションを追加し、アラートが何回連続して繰り返した場合 (一致するアラートの数) にこのアクションを実行するかを決定することが必要です。
  - アラートが復旧すると、現在の 一致するアラートの数 設定に対応するアクションだけでなく、その時点までに実行されたすべてのアクションが再度実行されます。
  - さらに、しきい値 を 2 番目のパラメータとして設定できます。このパラメータに対しては、上記の間隔中に複数回アラートを起動することはできません。
- 最後に、Telegram などのインスタントメッセージングを介してアラートメッセージの送信を設定できます。

スタンバイアラート

アラートは、有効化、無効化、スタンバイにできます。無効化とスタンバイには次の違いがあります。無効化ではアラートは実行されずアラート表示にも表示されません。スタンバイでは動作しアラート表示に表示されますが、表示のみで割り当てられたアクションは実行せずイベントは生成しません。

スタンバイアラートは、何が発生したかを確認するのに便利です。ただし、通知 / アクションの実行が無効化されます。

関連障害検知抑制

関連障害検知抑制は、ある範囲のエージェントへの通信が切れた場合に大量のアラートが発生するのを避けるための Pandora FMS の機能です。

ルータやスイッチ等の中間のデバイスがダウンすると、その先の全てのデバイスに対して Pandora FMS との通信ができなくなるような場合を考えます。おそらく、デバイスは正しく動作していますが Pandora FMS は ping で疎通確認がとれないため、ダウンと認識します。

エージェントが関連障害検知抑制を有効にして動作するには、依存する親エージェント(詳細オプション の 親(Parent) 設定) が正しく設定されている必要があります。

親エージェントに障害状態のモジュールアラートがある場合、関連障害検知抑制が設定された下位エージェントはそのアラートを実行しません。 これは、警告 または 不明 状態のモジュールアラートには適用されません。

関連障害検知抑制は、エージェントの設定で有効にできます。詳細オプション(Advanced options) で 関連障害検知抑制(Cascade protection modules) のチェックボックスをチェックします。

サービスペースの関連障害検知抑制

バージョン NG 727 以上

サービス監視 は、同じインシデントを報告する複数の同一ソースのアラートを回避するために使用できます。

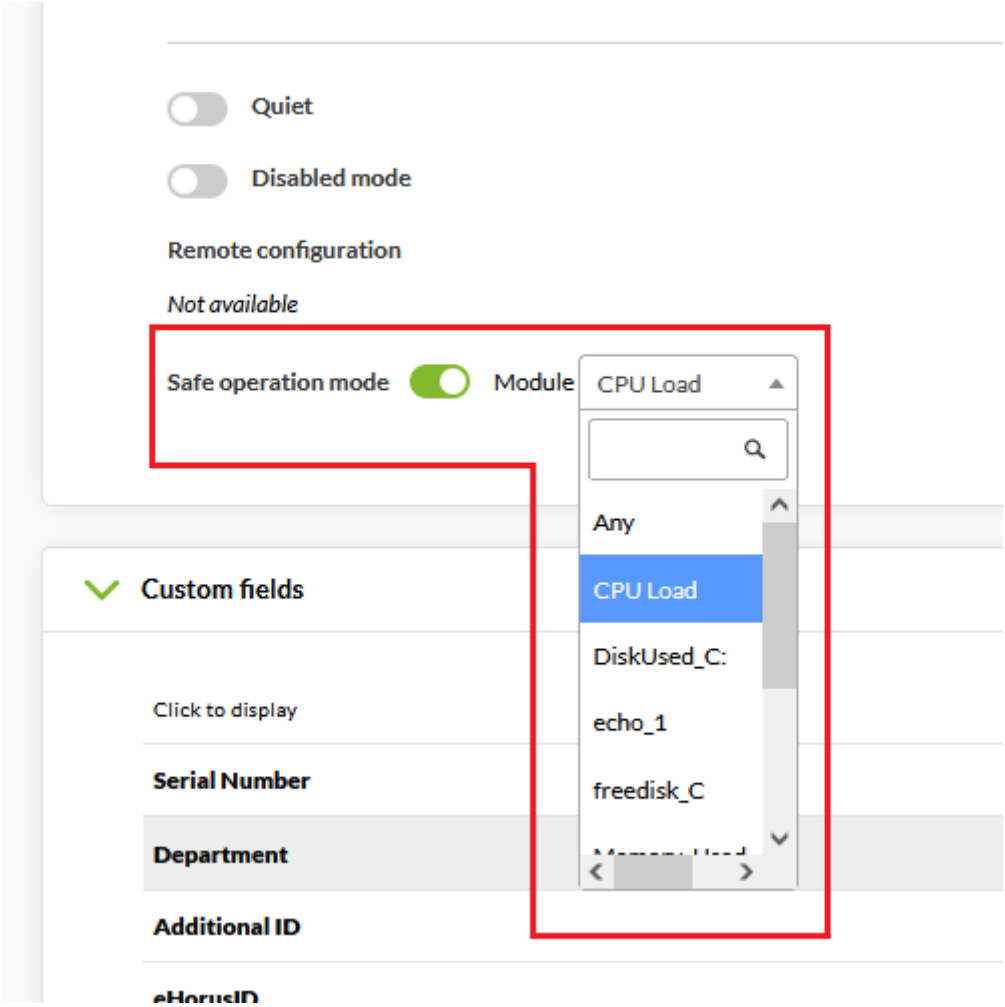
サービスベースの関連検知抑制を有効化すると、サービス要素(エージェント、モジュール、他のサービス)は問題を通知せず、サービス自身が影響を受けている要素の代わりにアラートを発します。

この情報を受け取るためには、根本原因分析マクロである _rca_ を使って新たなアラートテンプレートを作成または編集します。

モジュールベースの関連障害検知抑制

親エージェントのモジュールが障害状態になった場合に、親エージェントのモジュールの状態を使用してエージェントアラートを回避することができます。

セーフオペレーションモード

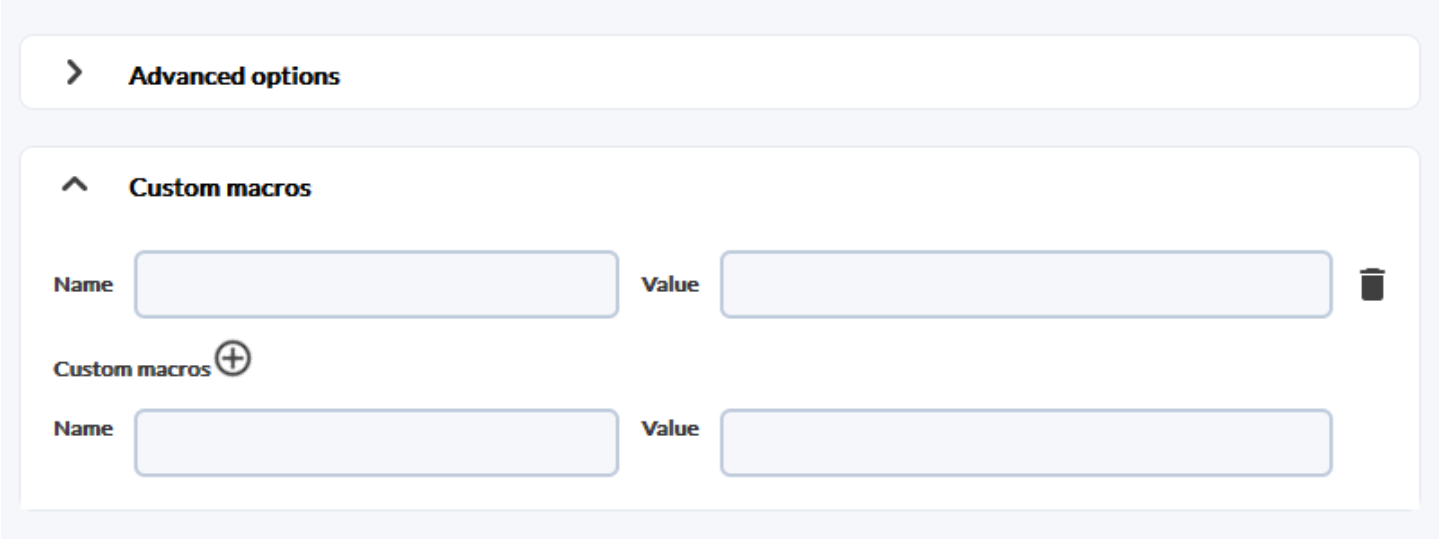


エージェントの拡張オプションでセーフオペレーションモードを有効化することができます。

選択したモジュールの状態が 障害 になった場合、それが 警告 もしくは 正常 状態に戻るまで該当エージェントの残りのモジュールが無効化されます。これにより、例えば、接続障害が発生した場合にリモートモジュールを無効化することができます。

カスタムモジュールアラートマクロ

以下の特定のマクロは、任意のモジュールのマクロセクションを展開することで追加できます。



- これらはモジュールで定義されます。
- 情報はデータベースに保存します。
- 任意の名前を持てます。例: _myMacro
- エージェントのローカル設定ファイル(.conf)には影響しません
- アラート専用で使用されます
- ローカルコンポーネントには追加できません
- ポリシー内で定義できます
- 設定値は、アラート定義のフィールドの一部として使用できます。

Pandora FMS でのアラートメール設定

一般的なコンソール設定 で説明しているように Pandora FMS にはメールを送信する機能があります。

ただし、柔軟性があるため、別のメール送信プラットフォームで送信することもできます。

Gmail アカウントを使った Email 設定

Pandora FMS サーバが (Gmail) を介してアラートを送信するには、コンソールの一般設定 または Pandora FMS サーバ 設定を行い、資格情報(ドメイン、ユーザ名、パスワードなど)を入力します。

アクション設定

- たとえば、Mail to Admin という名前のアクションを追加します。
- メールの宛先を設定するには、コマンド eMail を使用して、Destination address Field 1 にカンマで区切った受信者を追加します。

アラート設定

モジュール設定のアラートタブで、作成されたアクションを使用して新しいアラートを作成します。

Office365 でのメール設定

- Office365 アカウントを持っている必要があります。
- コンソールの一般設定 または Pandora FMS サーバ 設定を行い、資格情報(Office365 web ドメイン、ユーザ名、パスワードなど)を入力します。

アラート相関: イベントおよびログアラート

バージョン NG 741 以上

受信したイベントまたはログ収集システムによって収集されたログに基づくアラートを作成できます。論理関係を持つ一連の表現を用いて、単純なものから複雑なものまでのアラートを作成できます。

このタイプのアラートでは、特定のモジュールの状態に応じてアラートが生成されるだけでなく、異なるエージェントの複数の異なるモジュールによって生成されたイベントに基づいてアラートを生成できるため、かなり柔軟な設定ができます。

イベントアラートやログは、次の論理演算子を使用するフィルタルールに基づいています。

- and
- or
- xor
- nand
- nor
- nxor

これらの論理演算子は、設定されたフィルタルールに一致するログ内のイベント/式を検索するために使用され、一致するものが見つかった場合はアラートが発報されます。

イベントに関するアラートを定義する場合、agent□module、
および event パラメータを指定することが重要です。

また、アラートが動作する日などのいくつかのパラメーターを定義したテンプレートを利用します。ただし、この場合、テンプレートはイベントアラートがいつ発報されるかを定義しません。フィルタールールを介して一致するイベントが検索され、対応するアラートが発報されます。

Pandora FMS データベースに保存できるイベントの数が多
い場合、サーバは、pandora_server.conf 設定ファイル
で event_window という名前のパラメータで定義された最

大イベントウィンドウで動作します。指定された時間範囲外に生成されたイベントは、サーバで処理されません。そのため、サーバで設定された時間範囲よりも広い時間範囲をルールで指定することには意味がありません。

相関アラートの作成

イベント相関アラートが機能するためには Pandora FMS サーバ設定ファイルのパラメーター `eventserver 1` でイベント相関サーバを有効化する必要があります。

相関アラート / テンプレート

管理(Management) メニュー → アラート(Alerts) → アラート相関(Alert correlation) へアクセスします。このグローバルビューには、登録済みの相関アラートとそれらに関する情報のリストが表示されるほか、スタンバイモードでアクションを無効化、アクション追、相関アラートの編集または削除などのオプションも表示されます。

作成(Create) ボタンで、新しい相関アラートが追加されます。この処理は アラートテンプレート の作成と似ています。 相関アラートのテンプレートの設定パラメータはモジュールアラートの設定パラメータと似ていますが、イベントアラート固有のパラメータは次の 2 つだけです。

- ルール評価モード(Rule evaluation mode): 通過(Pass) と破棄(Drop) の 2つのオプションがあります。“ 通過 ” とは、イベントがアラートと一致した場合、残りのアラートが引き続き評価されることを意味します。“ 破棄 ” は、イベントがアラートと一致した場合、残ったアラートが評価されなくなることを意味します。
- グループごと(Group by): エージェント、モジュール、アラート、またはグループごとにルールをグループ化できます。例えば。2つの障害イベントを受信したときにルールがオフになるように設定され、エージェントによってグループ化されている場合、2つの障害イベントが同じエージェントから送信される必要があります。 これは無効にできます。

ログルールを含むアラートの場合、エージェントによるグループ化にのみ影響します。 別のグループ化を選択した場合、ログベースのエントリのアラートは決して一致しません

各ルールは、特定のタイプのイベントまたはログの一致により動くように設定されます。 ルールまたはその演算子によって定義された論理評価が満たされると、アラートが発報されます。

相関アラートのルール

アラートルールを定義するには、左側の要素を右側の ドロップエリア にドラッグしてルールを作成する必要があります。

設定可能な項目:

これらの要素は、ユーザがルールの文法を満たすようにするガイドをします。ここで、使用される文法についてさらに説明します。

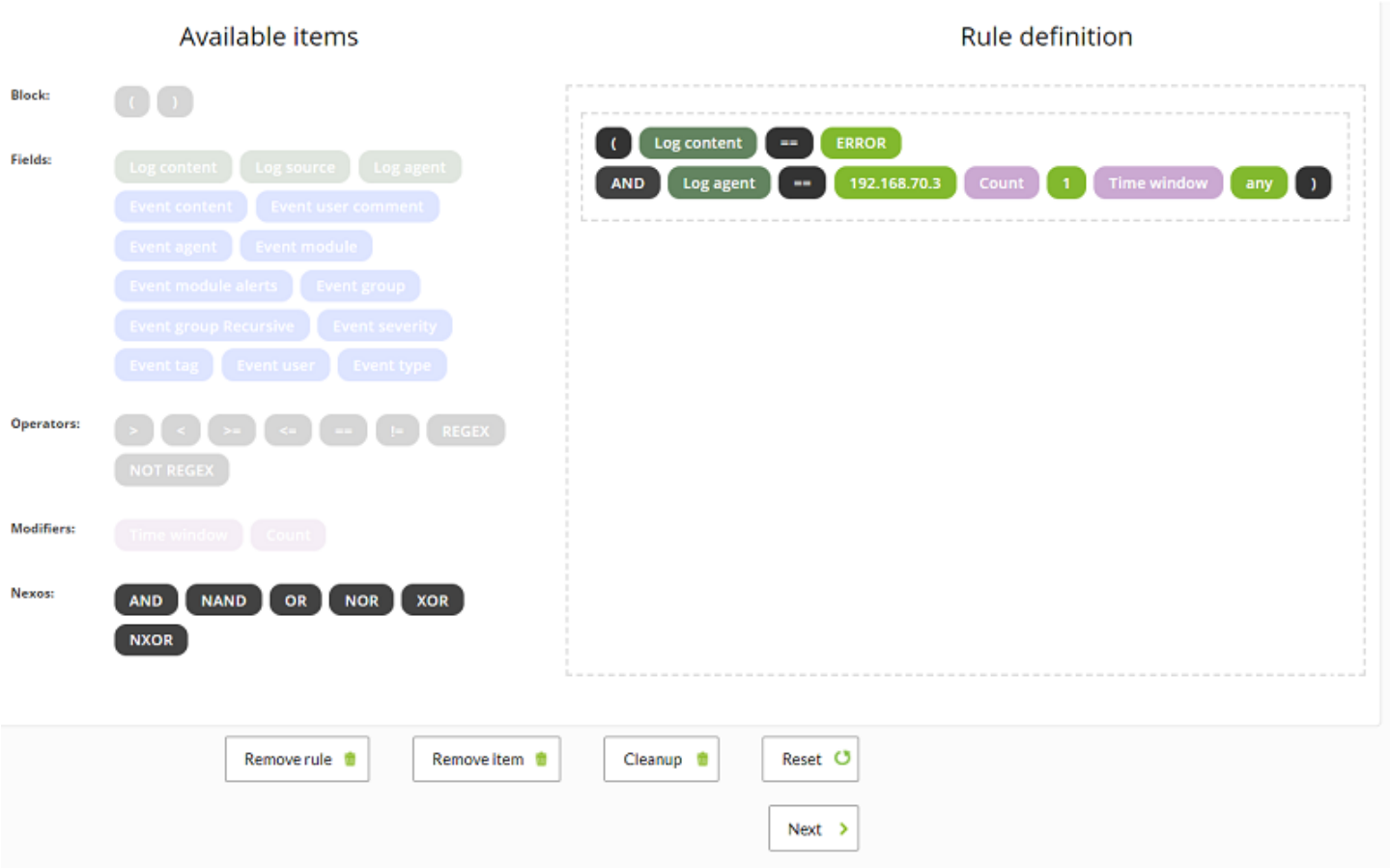
S → R | R + NEXUS +R

R → FIELD + OPERATOR + C | FIELD + OPERATOR + C + MODIFIER

C → VARIABLE

ここで、S は、相関アラートに対して定義されたルールのセットです。

たとえば次のようなイメージになるように、要素をルール定義の領域にドラッグする必要があります。



比較演算子 == および != では、テキスト文字列が文字通り比較されます。 より柔軟な比較には、正規表現を用いる REGEX の利用を検討ください。

すべての変更をクリーンアップして元に戻すには、'クリーンアップ(Cleanup)' および 'リセット(Reset)' ボタンを使用します。

次(Next) ボタンを押さないうちは、変更は保存されません。

条件を満たすブロックが同時にあることに注意してください。次の理論的な例を確認してください。

(A and B)

分析された要素(イベントまたはログ)が A と B を同時に満たすようにします。

A and B

評価ウィンドウで両方のルール（A）と（B）が満たされるようにします。 つまり、最後の数秒間（`log_window` および `event_window` パラメータで定義される)には、両方のルールを満たすエントリが存在する必要があります。

相関アラートのフィールド

バージョン 764 以降:

モジュールとエージェントに関連するマクロは復旧セクションのフィールドでは使用できません。これらのアラートの復旧がしきい値範囲内に戻った際に実行されますが、情報を取得するための復旧イベントがないためです。

アラートのフィールド操作に関する詳細は、"アラートシステム" を参照してください。

相関アラートの発報

ここでは、アラートが発報されたときに実行するアクションを設定と、そのようなアクションを実行する間隔と頻度を設定します。

- アクション(Actions): 実行したいアクションです。
- 一致するアラート数(Number of alerts match): アクションを実行するためにアラートが発生してから何回分の実行間隔を待つかの設定です。常にアクションを実行する場合は、このフィールドを空白のままにする必要があります。
- しきい値(Threshold): アラート発報後、アクションが再度実行される状態になるまでの間隔です。

次に、設定したアクションの一覧を表示します。この一覧の 発報(triggering) フィールドには、 一致するアラート数 で設定したアクションが実行される間隔が表示されます。さらに、オプション 列で、設定したアクションを削除または変更できます。

複数の相関アラート

複数のアラートがある場合、これらには特定の評価順序があります。それらは常にリストの最初から順番に評価されます。

通過(PASS) ルール評価モードが設定されている場合、相関アラートが実行されると、次のアラートも評価されます。 これは *通常* のモードです。

破棄(DROP) ルール評価モードを設定する場合、このモードで設定された相関アラートが実行されると、次のルールの評価は停止します。 この機能により、関連アラート抑制が可能になります。

残りの相関ルール(アクションフィールドとアクションアプリケーション)は、他の Pandora FMS アラートと同様に機能するため、追加の説明は行いません。

イベントアラートマクロ

イベントアラートで利用できるマクロはこの章の最後のマクロ一覧を参照ください。

マクロ一覧

コマンドマクロ アクションマクロ および イベントアラートマクロ
は、`_modulelaststatuschange_`, `_rca_` および `_secondarygroups_` を除き共通です。

- `_address_`: アラートを発報したエージェントのアドレス。
- `_addressn_n_`: “n” で示される位置に対応するエージェントのアドレス。 例) `addressn_1_` , `addressn_2_`
- `_agent_`:アラートを発報したエージェントの別名。別名が定義されていない場合は、代わりにエージェント名になります。
- `_agentalias_`: アラートを発報したエージェントと別名。
- `_agentcustomfield_n_`: n 番のエージェントカスタムフィールド。(例: _agentcustomfield_9_).
- `_agentcustomid_`: エージェントのカスタム ID
- `_agentdescription_`: アラートを発報したエージェントの説明。
- `_agentgroup_`: エージェントグループ名。
- `_agentname_`: アラートを発報したエージェント名。
- `_agentos_`: エージェントの OS
- `_agentstatus_`: エージェントの現在の状態。
- `_alert_critical_instructions_`: モジュールの障害状態時の手順。
- `_alert_description_`: アラートの説明。
- `_alert_name_`: アラート名。
- `_alert_priority_`: アラートの数値での重要度。
- `_alert_text_severity_`: テキストでの重要度 (Maintenance, Informational, Normal Minor, Major,

Critical).
- _alert_threshold_: アラートの閾値。
- _alert_times_fired_: アラートが発報された回数。
- _alert_unknown_instructions_: モジュールの不明状態時の手順。
- _alert_warning_instructions_: モジュールの警告状態時の手順。
- _all_address_: アラートを発報したエージェントの全アドレス。
- _critical_threshold_max_: 最大障害閾値
- _critical_threshold_min_: 最小障害閾値
- _data_: アラートを発報する原因となったモジュールデータ。
- _email_tag_: モジュールのタグに関連付けられた Email
- _event_cf_text_ : (イベントアラートのみ) テキストモードで全データを出力(行区切り)。
- _event_cf_json_ : (イベントアラートのみ) JSON フォーマットで全カスタムデータを出力。
- _event_cfX_: (イベントアラートのみ) アラートを発報したイベントカスタムレポートキー。例えば IPAM というキーのカスタムフィールドがある場合、その値は、_event_cfIPAM_ マクロを用いて取得します。
- _event_description_: (イベントアラートのみ) イベントのテキストでの説明。
- _event_extra_id_: (イベントアラートのみ) 拡張 ID
- _event_id_: (イベントアラートのみ) アラートを発報したイベントの ID
- _event_text_severity_: (イベントアラートのみ) イベントのテキストでの重要度 (Maintenance, Informational, Normal Minor, Warning, Major, Critical)
- _eventTimestamp_: イベントが作成されたタイムスタンプ。
- _fieldX_: ユーザ定義フィールド X
- _groupcontact_: グループ連絡情報。グループ作成時に設定されます。
- _groupcustomid_: グループカスタム ID
- _groupother_: グループに関する他の情報。グループ作成時に設定されます。
- _homeurl_: 公開 URL 設定の一般オプションで設定されます。
- _id_agent_: エージェント ID コンソールの該当ページに直接行く URL を生成するのに便利です。
- _id_alert_: エージェントの数値 ID(ユニーク)。他のソフトウエアとの連携に利用します。
- _id_group_: エージェントグループ ID
- _id_module_: モジュール ID
- _interval_: モジュール実行間隔。
- _module_: モジュール名。
- _modulecustomid_: モジュールカスタムID
- _moduledata_X_: このマクロ(“X” はモジュール名)を使用することにより、そのモジュールの最新のデータを取得でき、それが数値の場合、コンソールの設定で指定された 10進形式で、その単位とともに返されます。 たとえば、同じエージェントの他のモジュールに関する情報をアラートメールで送信する場合に役立ちます(これは非常に重要です)。

“X” (モジュール名)にスペースを含む場合は、次のように
HTML エンティティ に置き換える必要があります。

* *

HTML エンティティ一覧は、ウィキペディアで確認してくだ
さい。

- _moduledescription_: アラートを発報したモジュールの説明。
- _modulegraph_nh_: (コマンド eMail を利用するアラートのみ) n 時間の間のモジュールグラフを base64 でエンコードして返します。(例: _modulegraph_24h_) サーバとコンソールのAPI間の接続を正

しく設定する必要があります。 この設定はサーバの設定ファイルで行います。
- _modulegraphth_nh_: (コマンド eMail を利用するアラートのみ) モジュールの障害および警告しきい値が定義されている場合にのみ、前のマクロと同じ操作を行います。
- _modulegroup_: モジュールのグループ名。
- _modulestatus_: モジュールの状態。
- _modulelaststatuschange_: モジュールの最後の状態変更日時。
- _moduletags_: モジュールタグに関連付けられた URL
- _name_tag_: モジュールに関連したタグの名前。
- _phone_tag_: モジュールタグに関連付けられた電話番号。
- _plugin_parameters_: モジュールプラグインパラメータ。
- _policy_: モジュールが所属するポリシー名。(該当する場合)
- _prevdata_: アラートが発報される前のモジュールデータ。
- _rca_: 根本原因分析チェーン。 (サービスのみ)
- _server_ip_: エージェントに割り当てられたサーバ IP
- _server_name_: エージェントに割り当てられたサーバ名。
- _target_ip_: モジュールのターゲット IP アドレス。
- _target_port_: モジュールのターゲットポート番号。
- _time_down_human_: 長いフォーマットでの時刻。例: “1day 10h 35m 40s” (このマクロは復旧アラートでのみ動作します)
- _time_down_seconds_: 秒での時刻 (このマクロは復旧アラートでのみ動作します)
- _timestamp_: アラートが発報された日時(yy-mm-dd hh:mm:ss)
- _timezone_: _timestamp_ のタイムゾーン。
- _warning_threshold_max_: 最大警告閾値
- _warning_threshold_min_: 最小警告閾値

Pandora FMS ドキュメント一覧に戻る