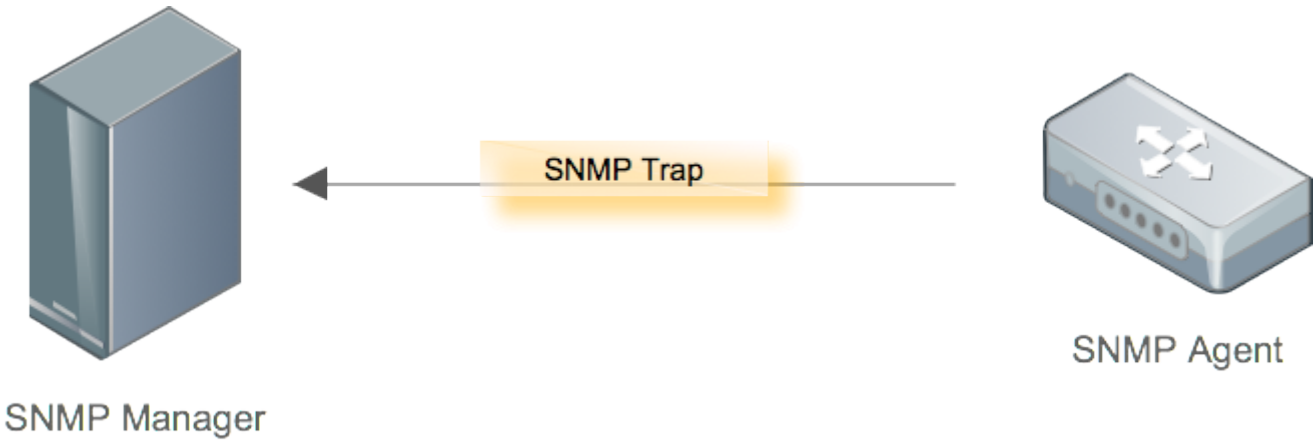
SNMP トラップ監視

SNMP トラップ監視

Pandora FMS ドキュメント一覧に戻る

概要

スイッチ、ルータ、サーバ、プリンタ、AP など、SNMP をサポートするネットワークデバイスは、インターフェイスの障害、CPU またはネットワークの負荷が高すぎたり、UPS の状態が変化したり、ディスクの障害が発生したときなどに、アラーム(SNMP トラップ)を送信することができます。各デバイスには、可能なイベントの独自のコレクションがあり、これは MIB と呼ばれます。この場合、デバイスのポーリングに使用する MIB とは異なります。



トラップは、デバイスにて何かが発生した場合に非同期で送信されます。Pandora FMS には、モニタリング対象から送られてくるトラップを表示するトラップ受信コンソールがあり、また、トラップに対してアラートを設定することができます。SNMP トラップは、Pandora FMS の起動時に起動される、OS の SNMP サーバデーモンで受け取ります。このサーバは通常ログファイルを以下に保存します。

```
/var/log/pandora /pandora_snmptrap.log
```

トラップは、常に生データで受信されます。つまり、数値 OID で受信します。ただし、OS に MIB ファイルがインストールされている場合は、文字に変換することができます。エンタープライズ版の Pandora FMS の SNMP コンソールでは、トラップをより認識しやすいように、OID を数値や文字で表したり、何らかの説明をつけたりする (“ インターフェースダウン ” など) ためのルールを設定できます。このようなルールを自動的に定義するために、Pandora FMS はトラップのベンダ MIB を読み込むことができます。ビデオチュートリアル "Loading MIBs in Pandora FMS" もご覧ください。

最初に、SNMP コンソールを有効化するためには /etc/pandora/pandora_server.conf 内の以下のパラメータを編集する必要があります。

```
snmpconsole 1
```

トラップを文字列変換したい場合(変数のバインディングまたは Enterprise 文字列のいずれか)は、次のオプションも有効化します(Enterpriase 版のみ)。

```
translate_variable_bindings 1
translate_enterprise_strings 1
```

また、/etc/snmp/snmptrapd.conf ファイルを必要なパラメータで設定する必要があります。 例:

```
authCommunity log public
disableAuthorization yes
```

この設定では、コミュニティ “public” 認証無しでトラップを受け付けます。

SNMPv3

SNMPv3 トラップは、送信ユーザが createUser ディレクティブを用いて */etc/snmp/snmptrapd.conf* に追加されていないと受信を拒否します。例を以下に示します。

```
disableAuthorization yes
createUser -e 0x0102030405 snmpv3user SHA mypassword AES
```

engineID は、*-e* オプションと共に指定する必要があります。
そうしないと、SNMPv3 INFORM のみを受信します。

トラップ受信コンソールへのアクセス

操作(Operation) → モニタリング(Monitoring) → SNMP → SNMP コンソール(SNMP Console)。 最初の列の虫眼鏡アイコンを使用すると、すべての SNMP トラップ情報やその他の重要な列を表示できます。

- 状態(Status) :承諾されたトラップは緑の四角で、そうでないものが赤の四角です。
- SNMPエージェント(SNMP Agent): トラップを送信したエージェントです。
- Enterprise 文字列(Enterprise string): 送信されたトラップの OID またはオブジェクト識別子。 トラップは、このフィールドで 1 つのデータのみを送信できます。
- タイムスタンプ(Time Stamp): トラップを受信した時間です。

色

さらに、SNMP トラップには、対応するタイプを示す色 (背景色として表示) があります。

- 青: メンテナンスタイプ
- 紫: 情報タイプ
- 緑: 正常タイプ
- 黄: 警告タイプ
- 赤: 障害タイプ

トラップの承諾

トラップを効果的に管理するために、管理者にすでに確認されたトラップとまだ確認されていないトラップを区別できるようにトラップを承諾することができます。 トラップを承諾するには、左側の円をクリックするか、マークを付けて 承諾(Validate) ボタンを押します。

トラップの削除

トラップは、処理後に個別に、または複数選択して 削除(Delete) アクションによって削除できます。

蓄積を避けるために、経過した SNMP トラップを自動的に
削除する設定オプションがあります。 (デフォルトでは 10
日以上経過したもの)

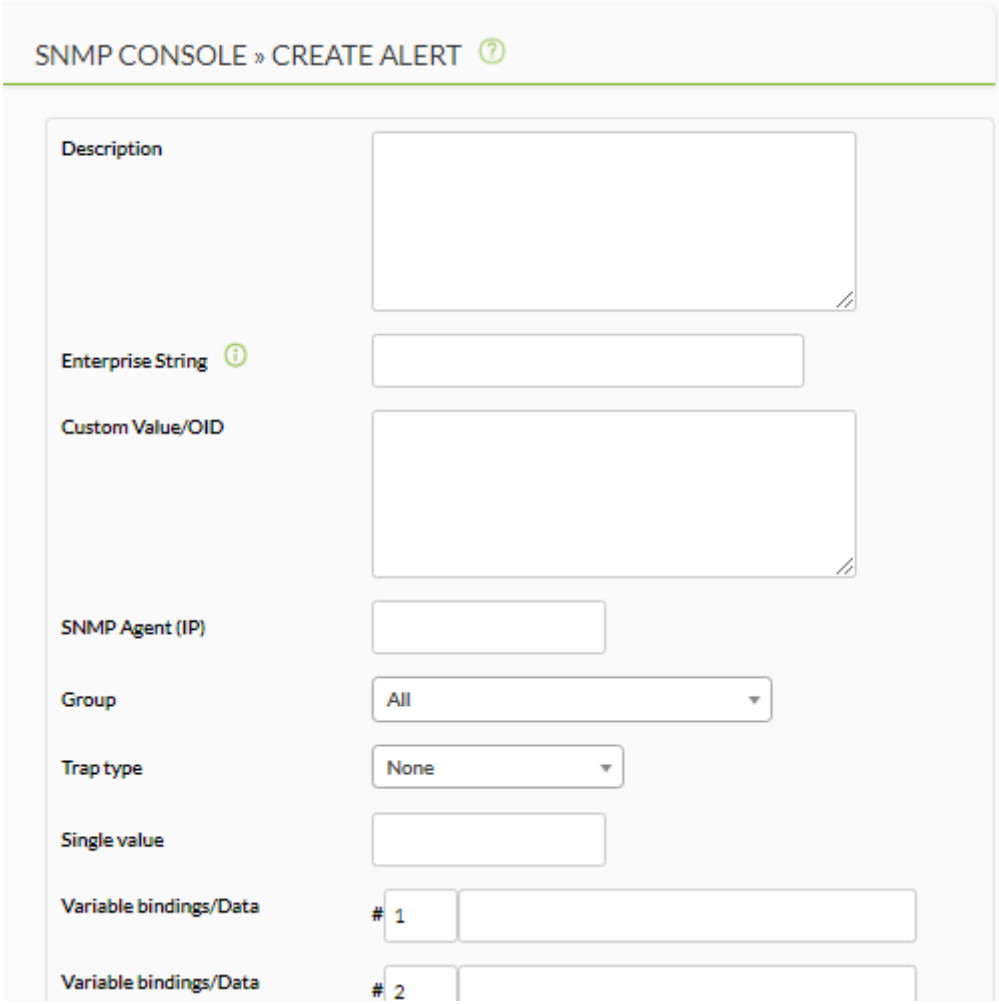
SNMP トラップアラート

概要

Pandora FMS には、受信する SNMP トラップのアラートシステムもあります。 それらは主にフィルタリングルールに基づいており、アラートを発報するように設定したルールに従って、すべてのフィールドで条件に一致するものを検索します。

アラートの追加

SNMP トラップアラートには、コンソールで受信した SNMP トラップがアラート条件にマッチするかを検索するために使用されるいくつかのフィールドがあります。 オプションで、必要に応じて、より一般的なルールやより具体的なルールを作成するフィールドを使用することができます。



説明(Description)

アラートの説明です。

Enterprise 文字列(Enterprise String)

トラップのメイン OID です。 文字列を検索します。 たとえば、OID の一部を検索するなら ば、1.21.34.2.3 という表現が利用でき、それを含むすべての OID をフィルタリングすることができます。同様に、*1.21.34.2.3.* も可能です。ただし、* 文字を使用する必要はありません。

カスタム値/OID(Custom Value/OID)

トラップのその他フィールドである、“Value” フィールドおよび、“Custom OID”、“Custom Value” フィールドを検索します。たとえば、“Testing TRAP 225” という文字列を送信するトラップがある場合、“Testing.*TRAP.*” という正規表現で “Testing TRAP” を検索できます。

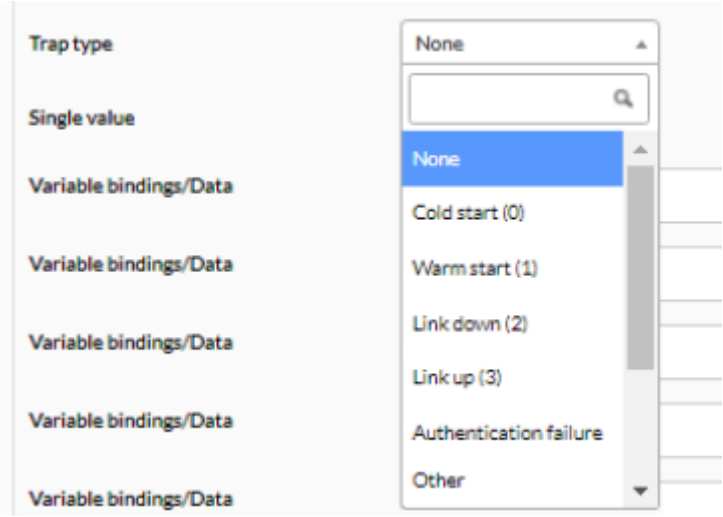
SNMP エージェント(SNMP Agent)

ラップを送信するエージェントの IP です。同様に、正規表現や文字列検索が使えます。

トラップタイプ(Trap type)

Cold Start, Warm start, Link down, Link up, Authentication failuer, other などのトラップタイプによ

るフィルタです。何も指定しなければ、トラップは通常 “Other” タイプとなり、任意のタイプが検索されます。

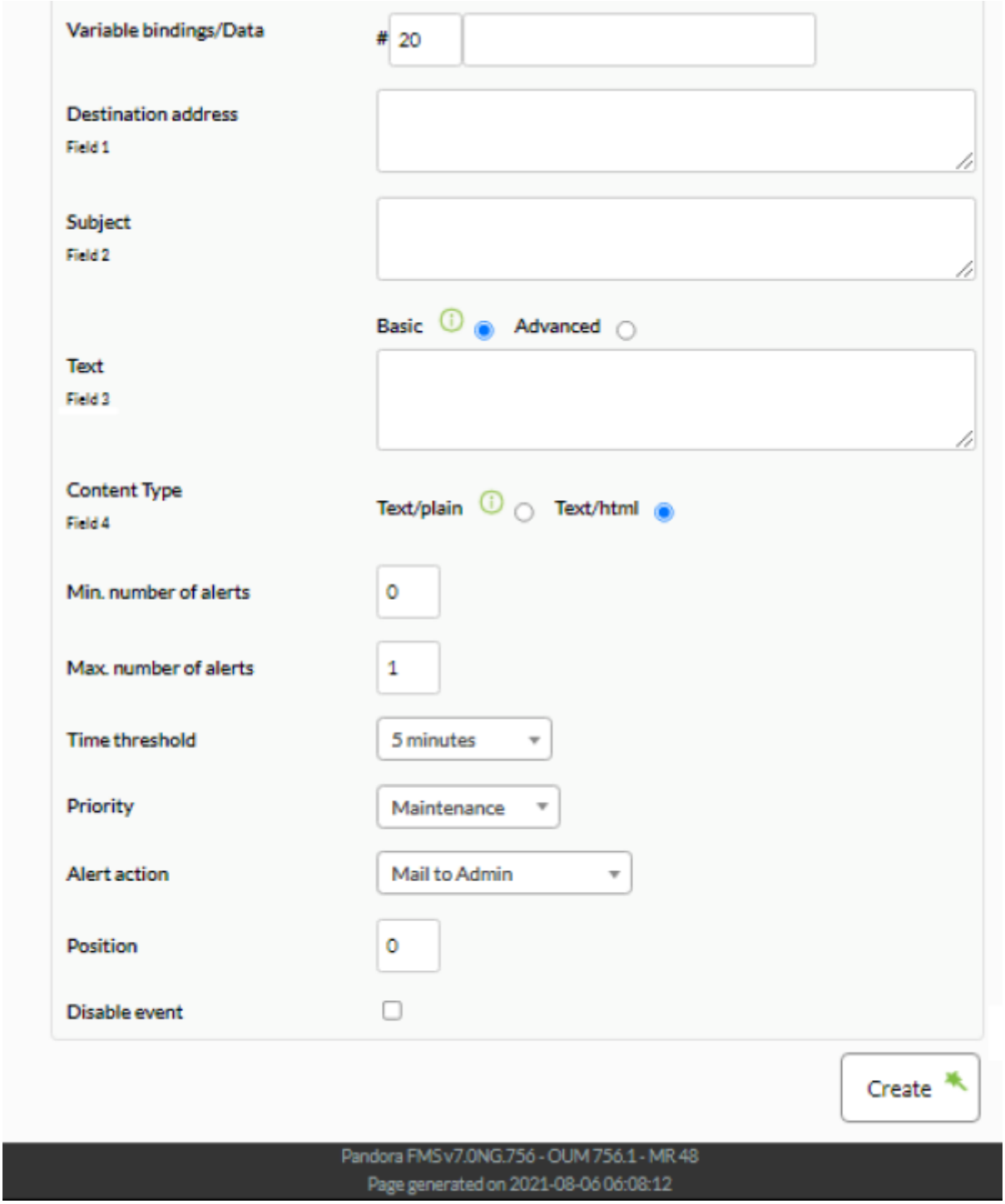


単一値(Single value)

トラップの値によるフィルタです。この例では、.666 で MAIN OID の値のみ参照し、カスタムデータの追加 OID は参照しないことに注意してください。

バインド変数/データ #1-20(Variable bindings/Data #1-20)

マッチする正規表現で、1 から 20 まであります。マッチすると、アラートが発報されます。設定した値は、_snmp_fx_ マクロ(_snmp_f1_, _snmp_f2_,...)で利用できます。マッチング対象として利用できるのは最初の 20変数のみですが、マクロにはいくつでも(_snmp_f11_, _snmp_f12_, ...)指定できます。



フィールド1(Field 1)

アラートのコマンドパラメータに指定するフィールド1です。このフィールドは、イベントの生成を選択した場合に使用されるか、メールアクションを選択した場合の宛先に使われます(アクションのデフォルトのメールの宛先を上書きする場合)。 アクション/アラートテンプレートでのカスタムフィールドの動作を完全に理解するにはPandora FMS のアラートについて説明している章を参照してください。

フィールド2(Field 2)

アラートのコマンドパラメータに指定するフィールド2です。例えば、電子メールを送信する場合は件名になります。 空白のままにするとアクションで定義した内容が使用されます。

フィールド3(Field 3)

アラートのコマンドパラメータに指定するフィールド3です。例えば、電子メールを送信する場合は本文になります。 空白のままにするとアクションで定義した内容が使用されます。

最小アラート数(Min. Number of Alerts)

アラートを発生させるトラップの最小数を指定します。

最大アラート数(Max. Number of Alerts)

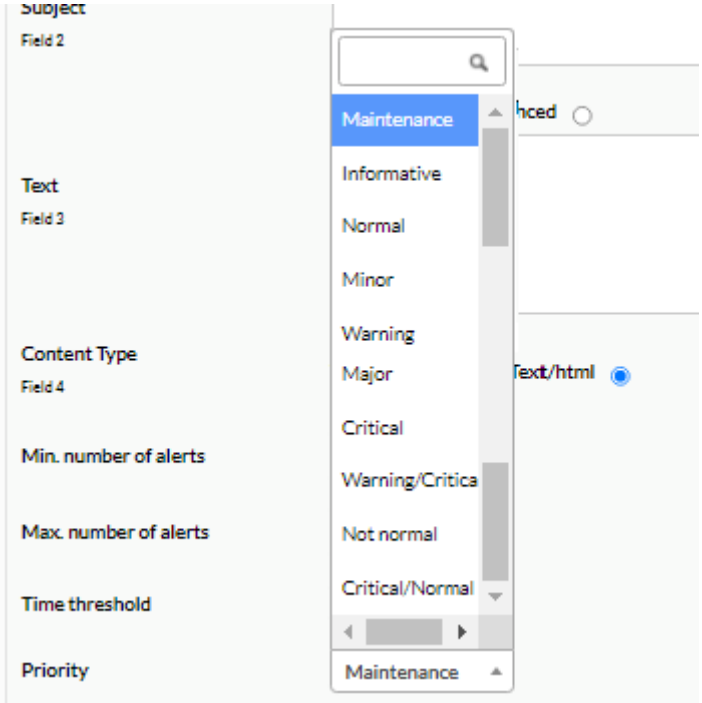
指定された間隔(または時間しきい値)でアクションが実行される最大回数を指定します。

再通知間隔(Time Threshold)

アラートカウンタをリセットする時間を指定します。このカウントは、最小アラート数で利用されます。

優先度(Priority)

アラートの優先度の選択です。



アラートの優先順位は、トラップの優先順位や Pandora FMS イベントとも何の関係もありません。

アラートアクション(Alert Action)

アラート実行時のアクションを選択します。イベントを選択すると、通常のアラート作成イベント

は生成されません。

位置(Position)

低位のアラートが最初に評価されます。複数のアラートが単一のトラップにマッチした場合は、マッチした同じ位置のすべてのアラートが発報されますが、低位のアラートがマッチしても発報されません。

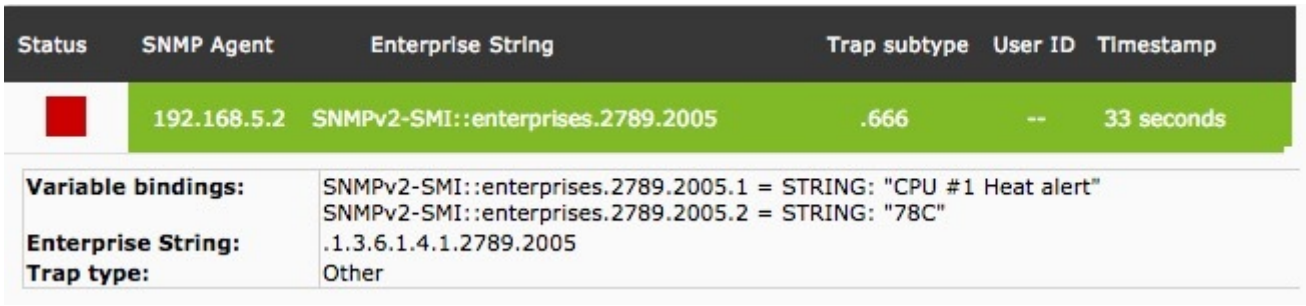
アラートフィールドマクロ

アラート *フィールド* で以下のマクロを利用できます。

- _data_: トラップ全体
- _agent_: エージェント名
- _address_: IP アドレス
- _timestamp_: トラップ日時
- _snmp_oid_: トラップ OID
- _snmp_value_: トラップ OID の値

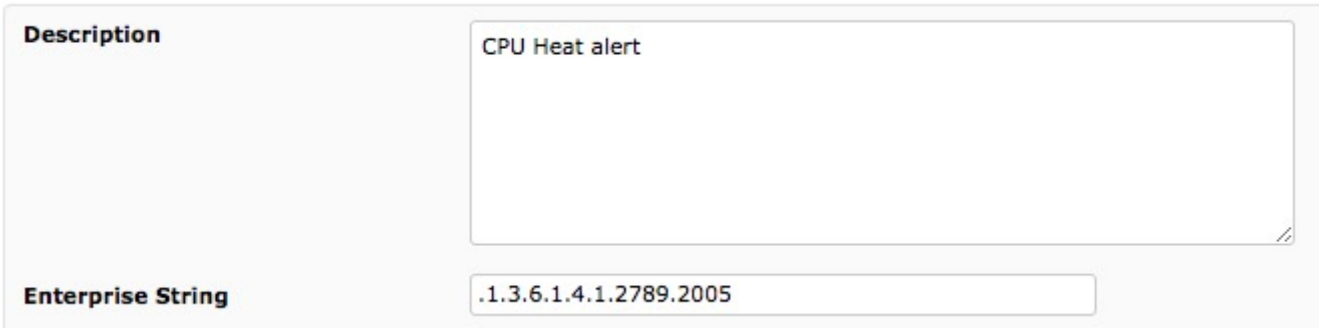
トラップアラートの例

次のようなトラップを受信したと仮定します。

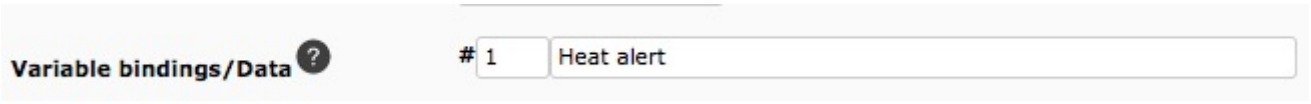


この場合、CPUオーバーヒートメッセージを含む可能性のあるトラップを識別するメインOID (1.3.6.1.4.1.2789.2005)がありますが（それ以外のものはわかりませんが）、1 と 2 の 2つの変数でその時の CPU のヒート状態と温度を表しています。 CPU のオーバーヒートトラップだけを識別したいので、トラップの最初の変数のヒートアラート文字列にマッチさせます(検索には最大20個まで設定できます)。

トラップの最初の部分を定義するのは簡単です。最初の最も重要なプレフィルタを作成するために、メイン OID のみを使用します。

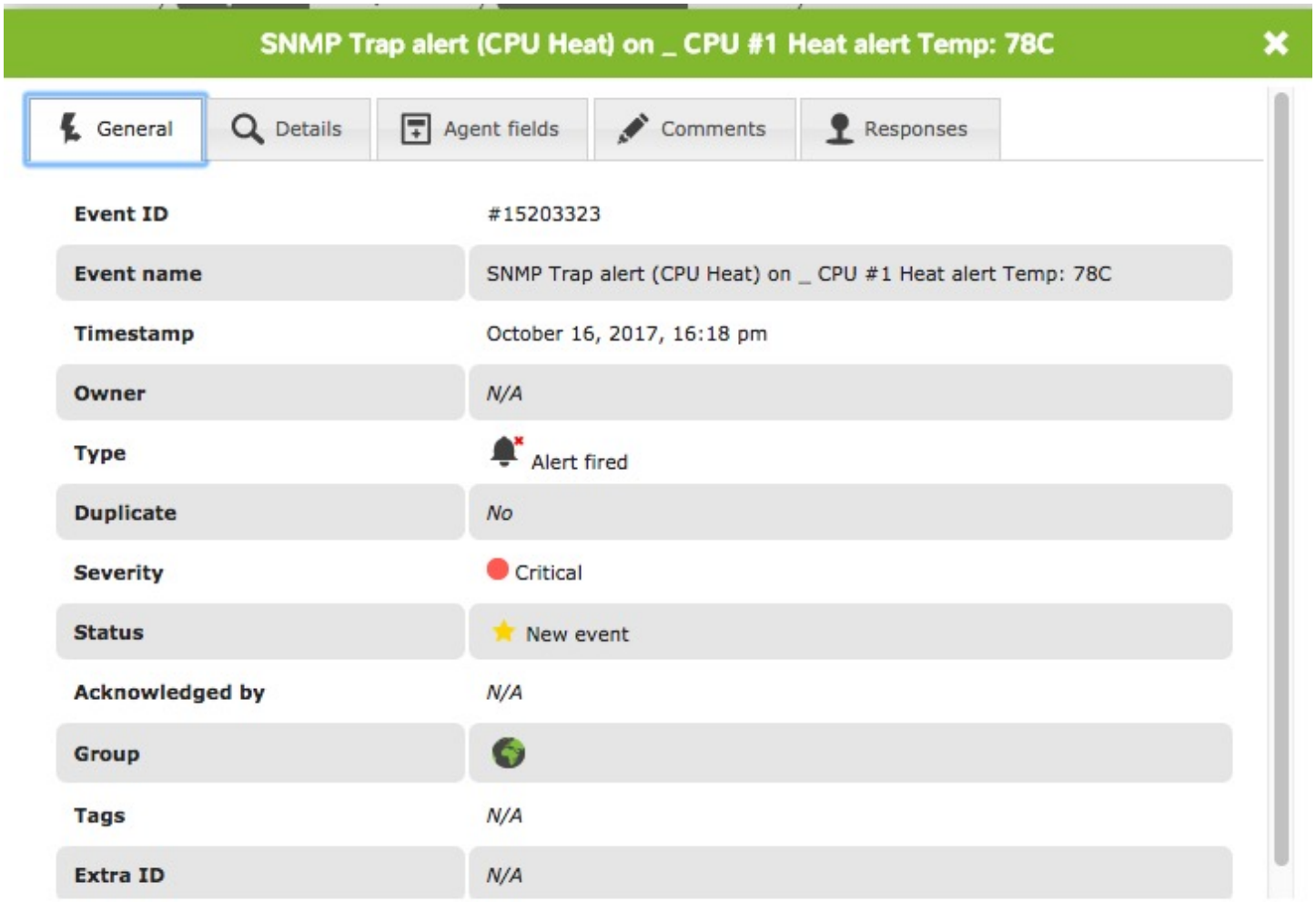


トラップ定義の 2番目は、必須部分を含みます。 トラップの最初の変数で “Heat alert” という文字列を探しますが、トラップをメインの OID で受信すると変数にはテキスト文字列が含まれていないため、アラートは発報されません。



最後に、“Pandora Event” タイプのアラートを選択することで、受け取ったトラップので値を含む変数 1 と 2 を使用してメッセージをマッチさせます。

アラートがオフになると、生成されるイベントは次のようになります。



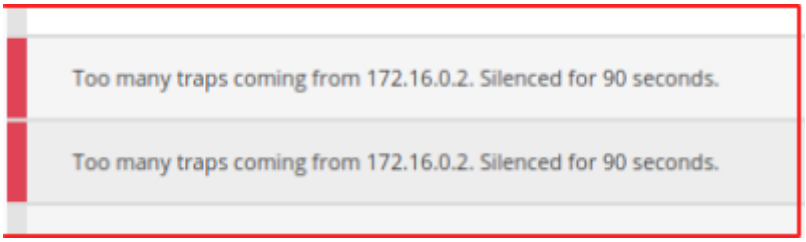
大量のトラップがある環境での動作

トラップストーム保護

同一の発信元から来るトラップストームからシステムを守るために利用する 2つのサーバパラメータがあります。これは、*pandora_server.conf* にて行う次の設定です。

- `snmp_storm_protection`: 同一の発信元 IP から指定した間隔(以下参照)内で処理する SNMP トラップの最大数です。
- `snmp_storm_timeout`: SNMP トラップストームから守る秒単位の間隔です。ここで指定した時間の間は、同一発信元(IP)からは *snmp_storm_protection* で指定した数のトラップのみを処理します。
- `snmp_storm_silence_period`: 特定のソースに対してストーム保護が起動されるたびに 0 より大きい場合は、現在の時間と静観時間が加算されます。 この時間が経過するまで、特定のソースからの新しいトラップは登録されません。

この保護が行われると、コンソールのイベントに反映されます。



トラップストーム保護は、トラップフィルタリングと合わせて、1日に何百、何千ものトラップを受け取っている場合に、不要なトラップを排除し一部のトラップのみを扱うことができます。

サーバにおけるトラップフィルタリング

一部のシステムでは、大量の SNMP トラップを受信しますが、監視対象となるのはそのうちのほんのわずかです。 モニタリング(Monitoring) → SNMP → SNMP フィルタ(SNMP Filters) で、さまざまなフィルタを定義できます。 作成(Create) ボタンを押し、+ ボタンを使用して説明と必要な数のフィルタを追加します。

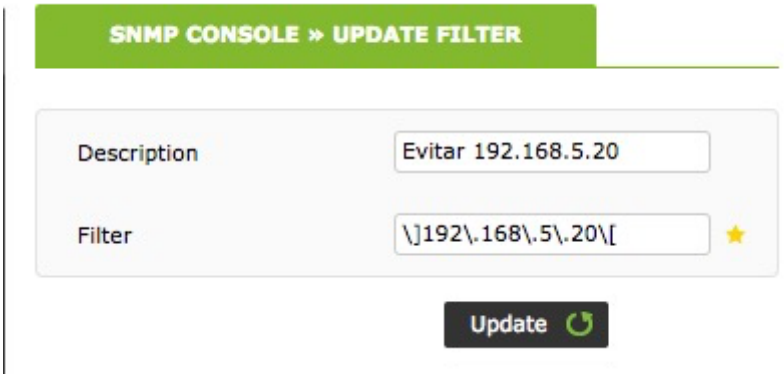
SNMP ログ(デフォルトは `/var/log/pandora/pandora_snmptrap.log`) のトラップエントリーに対して正規表現が適用されています。それは、次のような固定フォーマットです。

```
%4y-%02.2m-%l[**]%02.2h:%02.2j:%02.2k[**]%a[**]%N[**]%w[**]%W[**]%q[**]%v\n
```

それぞれ次の意味です。

- %y: 現在の年。
- %m: 現在の月。(数値)
- %l: 現在の月における日付。
- %h: 現在の時間。
- %j: 現在の分。
- %k: 現在の秒。
- %a: 発信元アドレス。(トラップバージョン 1 のみ)
- %N: OID
- %w: トラップタイプ。(数値)
- %W: トラップの説明。
- %q: トラップのサブタイプ。(数値)
- %v: タブで区切られた値のリスト。(カスタム OID)

例えば、192.168.50.20 からのすべてのトラップをフィルタするには、次のフィルタ設定をします。



複数のフィルタを同時に作成できるため、検索ではすべてのフィルタリング条件を満たすトラップが対象となります。

トラップのカスタマイズ

E この機能は Enterprise 版のみです。

モニタ対象デバイスから送られるトラップをオペレータがわかりやすくするために Pandora FMS にベンダ MIB をロードしたり、トラップを編集することができます。

トラップのリネーム/カスタマイズ

受信済のすべてのトラップは変更されないことに注意してください。これは、新たにシステムに入る新しいトラップから有効になります。

SNMP トラップの編集は、Web コンソールでの SNMP トラップの見え方をカスタマイズするプロセスです。 トラップを編集するには、メニュー 操作(Operation) → モニタリング(Monitoring) → SNMP → SNMP トラップエディタ(SNMP trap editor) を使用します。

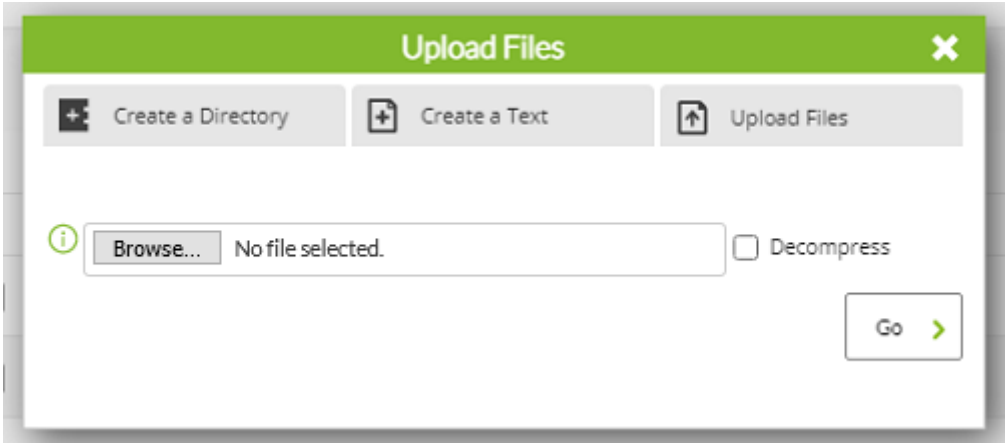
カスタム OID(Custom OID) は、変数バインディングを含む SNMP トラップ文字列の一部と比較される Perl 互換の正規表現です。 通常、トラップを変換する必要はありません。

カスタム OID(Custom OID) は、サポートされる最大長よりも長い可能性があるバインディング変数文字列全体を含めることを目的としたものではなく、1 つ以上の変数に一致する正規表現とすることを目的としています。

ベンダ MIB のロード

このオプションは、MIB をアップロードし、Pandora FMS 内部変換データベースを拡張するために使用されます。これによりSNMP トラップを受信すると、その説明に従って自動的に変換されます。これには、メニュー 操作(Operation) → モニタリング(Monitoring) → SNMP → MIB アップローダ(MIB uploader) からアクセスできます。

ベンダ MIB をアップロードするには、ファイルアップロード(Upload file(s)) をクリックしてファイルを選択し、Go をクリックします。



アップロードが完了すると、システムはそれをトラップライブラリに取り込みます。

複雑な SNMP トラップへのアラート関連付け

これは Enterprise 版の機能であり、管理(Management) → セットアップ(Setup) → セットアップ(Setup) → Enterprise → SNMP トラップをエージェント (存在する場合) に転送(Forward SNMP traps to an agent (if it exists) で設定します。

このオプションを変更した場合、有効にするためには
Pandora FMS サーバサービスを再起動する必要があります。

このオプション (サーバに対して一般) は、SNMP トラップの送信元 IP アドレスがエージェントの IP として定義されている場合に限り、SNMP トラップを SNMPTrap という特別なエージェントモジュールにテキスト文字列として転送します。 これが発生するとSNMP トラップはテキスト行としてそのエージェントのモジュール内に到着します。このモジュールは、最初の SNMP トラップが到着したときにのみ定義されるモジュールです。

このモジュールではテキスト アラートを指定できます。これらは他のモジュールと同様に完全に標準的なものです。 これによりSNMP 監視をカスタマイズして、特定のソースからの特定のトラップを別のモジュールとして扱うことができ、アラート相関などを含む他の監視に統合できます。

別の解決策は、エージェントモジュールでの SNMP トラップにアラートを設定することです。 たとえば、ログファイルへの書き込みに関連した SNMP トラップがあり、ファイルを読み取り、1 が書き込まれたときに実行するエージェントがあった場合、目的の SNMP トラップを受信するとモジュールが動作し、受信したトラップに基づいて相関関係を確立できます。

外部SNMPトラップマネージャ

SNMP コンソールは、TRAP を個別のエンティティとしてのみ処理するためSNMP トラップの受信に限定されますがSNMP トラップには多くの情報が含まれる可能性があります。

場合によってはSNMP トラップに基づいた監視しか実行できない場合があります。

そのためSNMP トラップで収集された情報を、プラグインとして機能する外部スクリプトを通じて再度処理することができます。

これを行うには、受信した SNMP トラップを後処理するスクリプトを実行する アラートコマンド を作成する必要があります。

この技術の応用範囲は非常に広く、スクリプトは非常に動的な構造を持つことができるため各スクリプトはカスタマイズする必要があります。 多くのシステムでは、受信する情報はテキストだけでなく数値もあり、数値情報モジュールにフィードしてグラフなどを表すことができますXML で生成されるデータは常に 非同期型であることに留意する必要があります。

SNMP トラップ転送

Pandora FMS ではPandora サーバの設定ファイルでsnmp_forward_trapトークンを有効にすることによりSNMP trap を外部のホストへ転送することができます。

SNMP v1 を使った trap 転送設定例

```
snmp_forward_trap 1
snmp_forward_ip 192.168.1.145
snmp_forward_version 1
snmp_forward_community public
snmp_forward_secName
snmp_forward_engineid
snmp_forward_authProtocol
snmp_forward_authPassword
snmp_forward_privProtocol
```

```
snmp_forward_privPassword
snmp_forward_secLevel
```

SNMP v2c を使った trap 転送設定例

```
snmp_forward_trap 1
snmp_forward_ip 192.168.1.145
snmp_forward_version 2c
snmp_forward_community public
snmp_forward_secName
snmp_forward_engineid
snmp_forward_authProtocol
snmp_forward_authPassword
snmp_forward_privProtocol
snmp_forward_privPassword
snmp_forward_secLevel
```

SNMP v3 を使った trap 転送設定例

この例は、SNMP v3 trap の知識が必要になるため特に難しいです。リモートの SNMP エージェントがsnmp_forward_ipで定義されており、次の設定が /etc/snmp/snmptrapd.conf ファイルに書かれていることを想定します。

```
createUser -e 0x0102030405 myuser MD5 mypassword DES myotherpassword
```

Pandora サーバの設定ファイルは次のようになります。

```
snmp_forward_trap 1
snmp_forward_ip 192.168.1.145
snmp_forward_version 3
snmp_forward_secName myuser
snmp_forward_engineid 0x0102030405
snmp_forward_authProtocol MD5
snmp_forward_authPassword mypassword
snmp_forward_privProtocol DES
snmp_forward_privPassword myotherpassword
snmp_forward_secLevel authNoPriv
```

より詳細は、 NET-SNMP's v3 Trapsを参照してください。

snmptrapd デーモンの個別管理

何らかの理由により snmptrapd デーモンを Pandora FMS から独立して管理したい場合(Pandora FMS デーモンとは独立して停止・起動をしたい場合)は、いくつか考慮すべきことがあります。

1. Pandora FMS サーバにおいて snmpconsole パラメータを有効化する必要があります。

2. Pandora FMS サーバで設定されるログは、snmptrapd を独立して管理する場合でも同じでなければいけません。

3. snmptrapd の呼び出しは特定のフォーマットである必要があり、標準的なシステムからの呼び出しは利用できません。呼び出しは次のようにする必要があります(パラメータ -A はとても重要です)。

```
/usr/sbin/snmptrapd -A -t -On -n -a -Lf /var/log/pandora/pandora_snmptrap.log -p
/var/run/pandora_snmptrapd.pid --format1=SNMPv1[**]%4y-%02.2m-
%l[**]%02.2h:%02.2j:%02.2k[**]%a[**]%N[**]%w[**]%W[**]%q[**]%v\n --
format2=SNMPv2[**]%4y-%02.2m-%l[**]%02.2h:%02.2j:%02.2k[**]%b[**]%v\n
```

4. snmptrapd トークンが、Pandora FMS 設定ファイル内に設定されている必要があります。

```
snmp_trapd manual
```

5. この機能を有効化したら、次の手順を実施する必要があります。

- /etc/pandora/pandora_server.conf の設定を変更
- Pandora FMS サーバを停止
- snmptrapd プロセスが動作していないことを確認 (もし動いていたら、停止するまで待つか kill します)
- snmptrapd を手動で起動 (上記のフォーマットにて)
- Pandora FMS サーバを起動

トラップログファイルの管理

pandora_snmptrap.log.index および pandora_snmptrap.log が変更されていなければ、snmptrapd プロセスは、pandora サーバプロセスの停止および起動に依存せず、停止および起動することができます。これらのファイルに変更が加わっている場合は、pandora サーバの再起動が必要です。トラップのログファイルを外部でローテートする必要がある場合は、前述の 2つのファイルを削除したあとに pandora サーバを再起動する必要があります。

SNMP トラップバッファリング

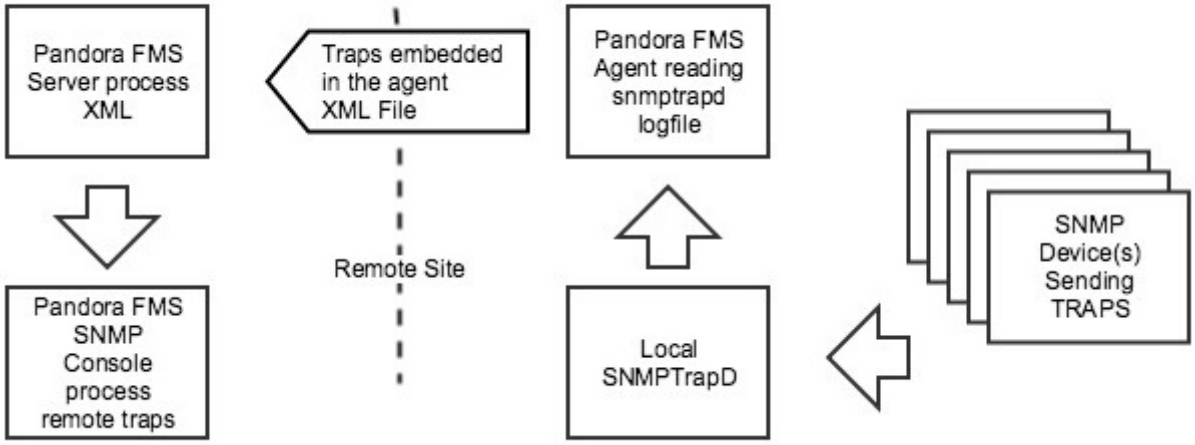
SNMP コンソールが snmptrapd ログファイルからトラップを直接処理する方が効率的です。 この設定は、信頼性または直接接続に何らかの懸念がある場合にのみ推奨されます。

SNMP トラップが信頼性の低い接続を介して外部マネージャに送信されると、一部の情報が失われます。 Pandora FMS では、ローカル snmptrapd からトラップを信頼できる方法で Pandora FMS サーバに転送できます。

前提条件:

- ローカルの snmptrapd がトラップを受信すること。
- ローカルの Pandora FMS エージェントがあること。
- Pandora FMS がインストールされていること。

アーキテクチャ



- SNMP エージェントは、ローカルの *snmptrapd* にトラップを送信します。
- ローカルの Pandora FMS エージェントが *snmptrapd* のログファイルからトラップを読み取り、XML データファイルを用いて指定の Pandora FMS サーバへ送信します。それは XML バッファに保存され必要に応じてリトライされます。
- データサーバは、XML データファイルからトラップを読み込み、プレーンテキストファイルに展開します。
- SNMP コンソールは、プレーンテキストファイルからトラップを処理します。

設定

snmptrapd

/etc/snmp/snmptrapd.conf を編集し、Pandora FMS と互換性があるフォーマットでログをファイルに記録する設定になっているか確認します。(必要に応じてログファイル名を変更することができます)

```
[snmp] logOption f /var/log/snmptrapd.log
format1 SNMPv1[**]%4y-%02.2m-
%l[**]%02.2h:%02.2j:%02.2k[**]%a[**]%N[**]%w[**]%W[**]%q[**]%v\n
format2 SNMPv2[**]%4y-%02.2m-%l[**]%02.2h:%02.2j:%02.2k[**]%b[**]%v\n
```

Pandora FMS エージェント

snmptrapd のログファイルからデータを読む Pandora FMS エージェントに付属の *grep_snmptrapd*

プラグインを利用します。

ローカルのエージェント設定ファイル */etc/pandora/pandora_agent.conf* を編集し、必要に応じて *snmptrapd* のログファイルのパスを指定する次の行を追加します。

```
module_plugin grep_snmptrapd /var/log/snmptrapd.log
```

Pandora FMS サーバ

SNMP コンソールが、データサーバにて書かれた外部ログファイルからトラップを処理するよに設定する必要があります。

サーバ設定ファイル */etc/pandora/pandora_server.conf* 編集し、次の設定をします。

- SNMP コンソールが有効であるか確認します。

```
snmpconsole 1
```

- データサーバが有効であるか確認します。

```
dataserver 1
```

- 外部 SNMP ログファイルを設定します。存在しない場合は、SNMP コンソールが作成します。

```
snmp_extlog /var/log/pandora/pandora_snmptrap.ext.log
```

snmp_extlog には Pandora FMS サーバが書き込むことができる任意のファイルを指定できますが、snmp_logfile (`/etc/pandora/pandora_agent.conf` でも定義されています) とは異なるものである必要があります。

トラップジェネレータ

このツールを使用すると、後で SNMP コンソールで表示できるカスタム SNMP トラップを生成できます。 これには、メニュー 操作(Operation) → SNMP → SNMP トラップジェネレータ(SNMP trap generator) からアクセスできます。

SNMP タイプ(SNMP Type) で、次のオプションから SNMP タイプを選択します。

- Cold Start: エージェントが開始または再開されたことを意味します。
- Warm Start: エージェント設定が変更されたことを意味します。
- Link down: 通信インタフェースが利用できない状態になった(無効化)ことを意味します。
- Linu up: 通信インタフェースが利用できる状態になったことを意味します。
- Authentication failure: エージェントが(コミュニティによって)認証できない NMS を受信したことを意味します。
- EGP neighbor loss: ルータが EGP プロトコルを使用しているシステムで、近くのホストが利用できない

状態になったことを示します。
- Enterprise: ベンダトラップを含む、すべての新規トラップです。

Pandora FMS ドキュメント一覧に戻る