モニタリング概要

モニタリング概要

Pandora FMS ドキュメント一覧に戻る

モニタリングの概要

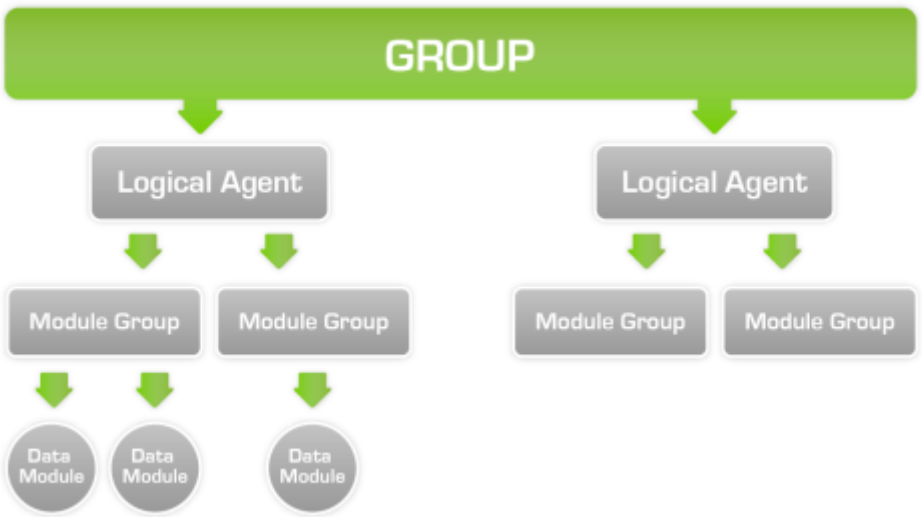
Pandora FMS のすべてのユーザ操作は、ウェブコンソールを通して行います。コンソールへのアクセスは、任意のコンピュータから特別なプログラムを必要とせず HTML5 に対応したブラウザで行うことができます。

監視とは、情報を収集して保存し、そのデータに基づいて決定した処理を実行すために、あらゆるタイプのシステム上のプロセスを実行することです。

Pandora FMS は、収集する情報の範囲や量を拡張できる複数の機能をもったスケール可能な監視システムです。

監視の基本を以下に示します。詳細を知りたい場合
は、Web リンクを参照してください。

Pandora FMS における論理エージェント



Pandora FMS によるすべての監視は、*論理エージェント* で管理され、全ての *論理エージェント* は、*グループ* に属します。これらエージェントは、監視対象のさまざまなコンピュータ、デバイス、Web サイト、またはアプリケーションを表します。

Pandora FMS コンソールで定義された論理エージェントでは、ソフトウェアエージェントを通じて

収集されたローカル情報、ネットワークチェックを通じて収集されたリモート情報、またはその両方を表示できます。 そのためPandora FMS コンソール上で表現されるエージェントと、対象システムにインストールしてローカルでデータを収集するソフトウェアエージェントは異なるということを理解することが重要です。

ソフトウエアエージェントでのモニタリングと、リモートモニタリング

Pandora FMS には、主にソフトウエアエージェントを使った方法とリモートで行う方法の 2つの監視手法があります。

エージェントベースの監視 は、監視対象にインストールした小さなソフトウエアを用い、ローカルでコマンドやスクリプトを実行して情報を取得します。

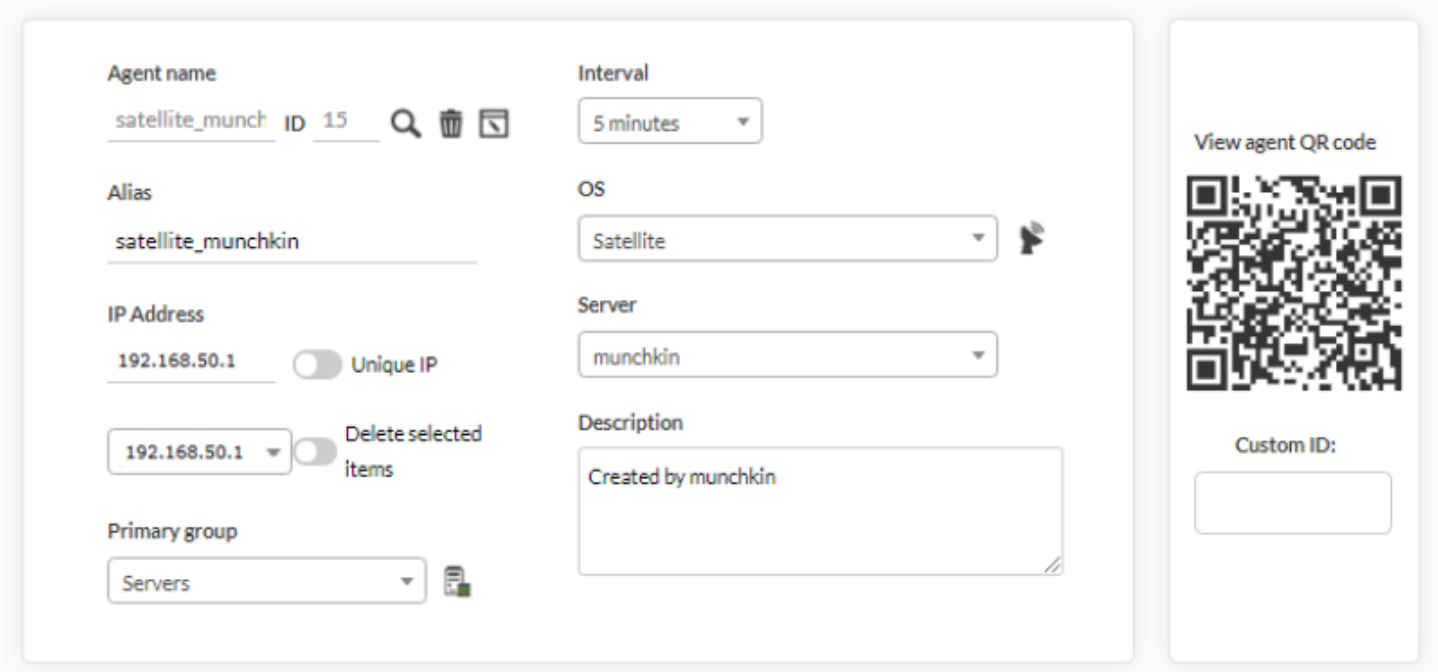
リモート監視 は、監視対象の確認をリモートからネットワークを介して行います。監視対象には、追加のソフトウエアをインストールする必要はありません。

つまり、ソフトウエアエージェントベースの監視は監視対象のローカルでチェックをして情報を取得し、リモート監視は Pandora FMS サーバからリモートでのチェックで情報を取得します。

両方のタイプのエージェントは、同じ一般設定とデータ表示を共有しますPandora FMS においては、一つの手法もしくは組み合わせでの監視が可能です。

コンソールでの論理エージェント設定

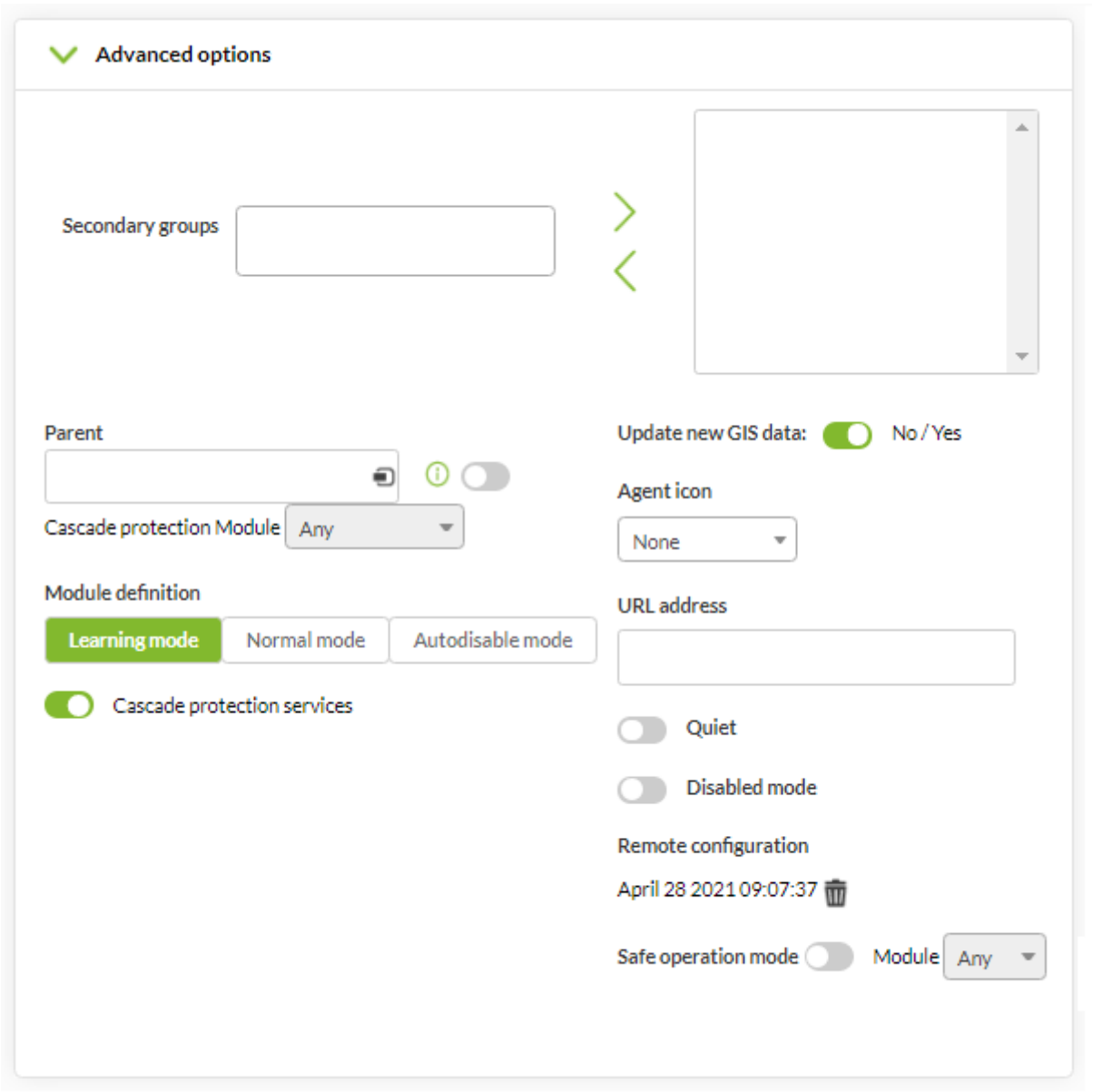
編集画面の例



メインフィールド:

- 別名(Alias): Pandora FMS がエージェント/モジュールを使って実行するすべての機能を正しく処理するために、エージェント名には /, \, |, %, #, & および $ などの文字を使用しないことをお勧めします。これらのエージェントを使うと、システムパスを使用しているときや他のコマンドを実行しているときに誤解を招き、サーバー上でエラーを引き起こす可能性があります。
- サーバ(Server): エージェント監視で設定されたチェックを実行するサーバです。インストールで HA を設定した場合は特別なパラメータです。
- プライマリグループ(Primary group): グループをエージェントに割り当てることができます。 グループアイコンをクリックすると、割り当てられたグループの情報表示画面にアクセスできます。

高度な編集画面の例



メインフィールド:

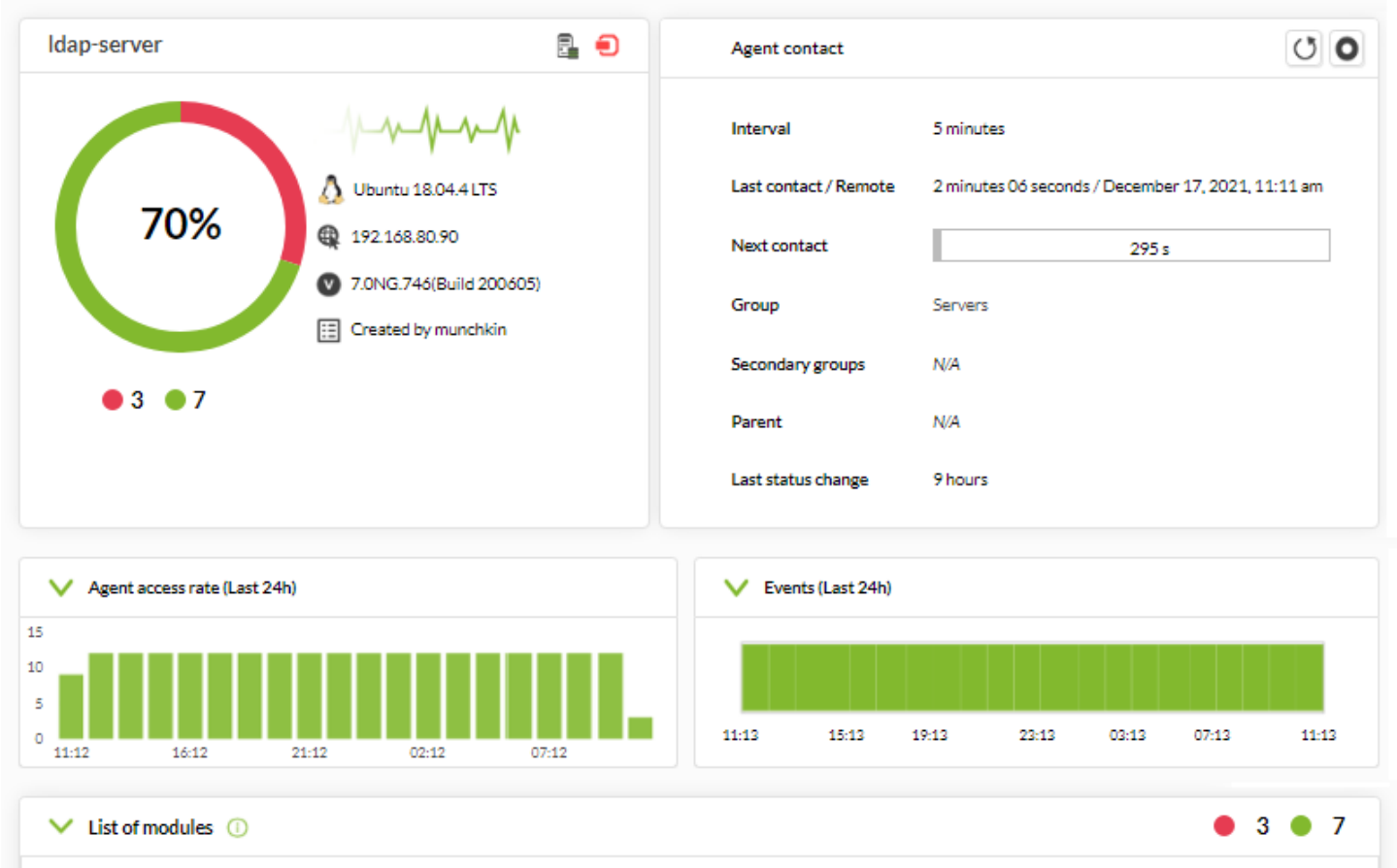
- セカンダリグループ(Secondary groups): エージェントが複数のグループに属するためのオプションパラメータ。
- モジュール定義(Module definition): モジュールを定義する 3つの動作モードを選択できます。
  - 学習モード(Learning mode): 新たなモジュールを含む XML を受け取った場合、モジュールを自動的に作成します。(デフォルト)
  - 通常モード(Normal mode): 新たなモジュールを含む XML を受け取った場合、すでにコンソールに設定が無ければ作成しません。

    - 自動無効化モード(Auto-disable mode): 学習モードと同じですが、全モジュールが不明になった場合に情報が再度車でエージェントを無効化します。
- 関連障害検知抑制(Cascade protection services): 関連アラートが大量にあがることを回避することができるパラメータ。 エージェントまたはエージェントのモジュールを選択することができます。 前者の場合、選択されたエージェントが障害状態にあると、エージェントはアラートを生成しません。 後者の場合、指定されたモジュールが障害の場合は、エージェントはアラートを生成しません。

コンソールでのエージェント参照

この画面では、エージェントに関する多くの情報を見ることができます。リモート実行を強制し、データを更新することができます。

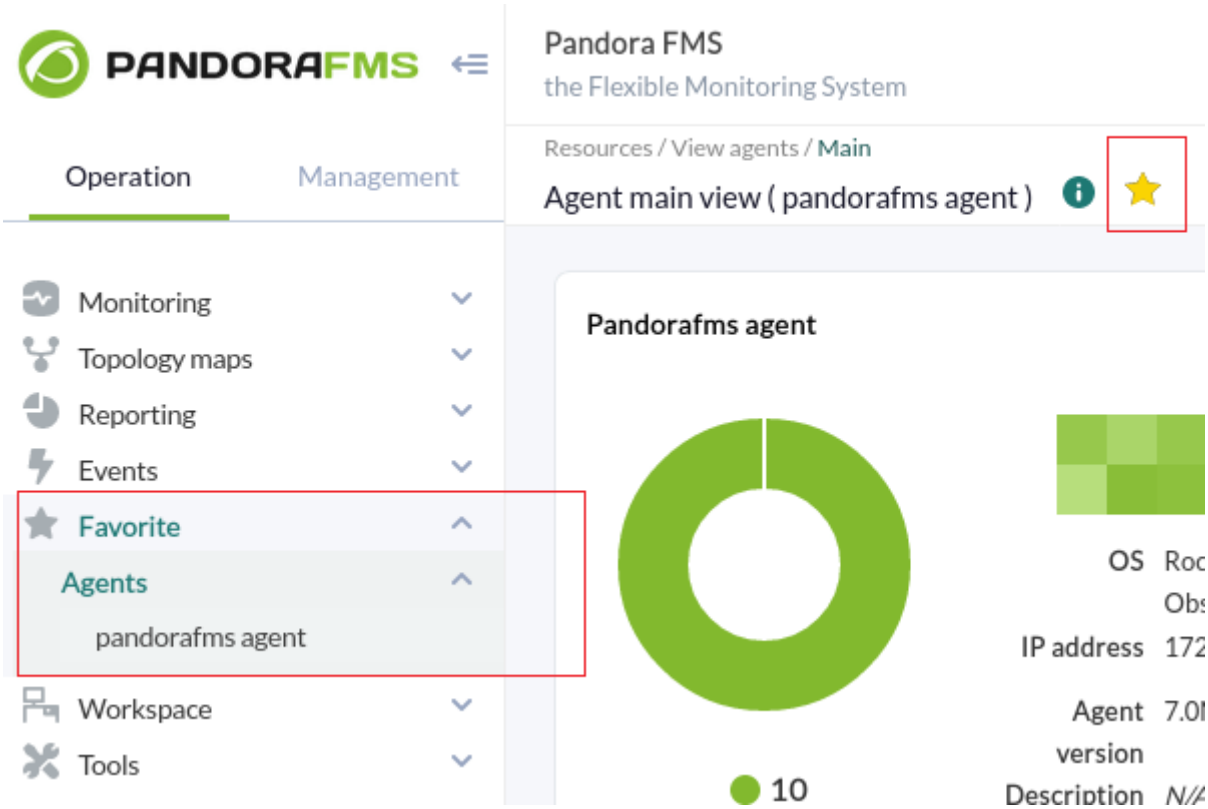
上部には、エージェントデータの概要が表示されます。



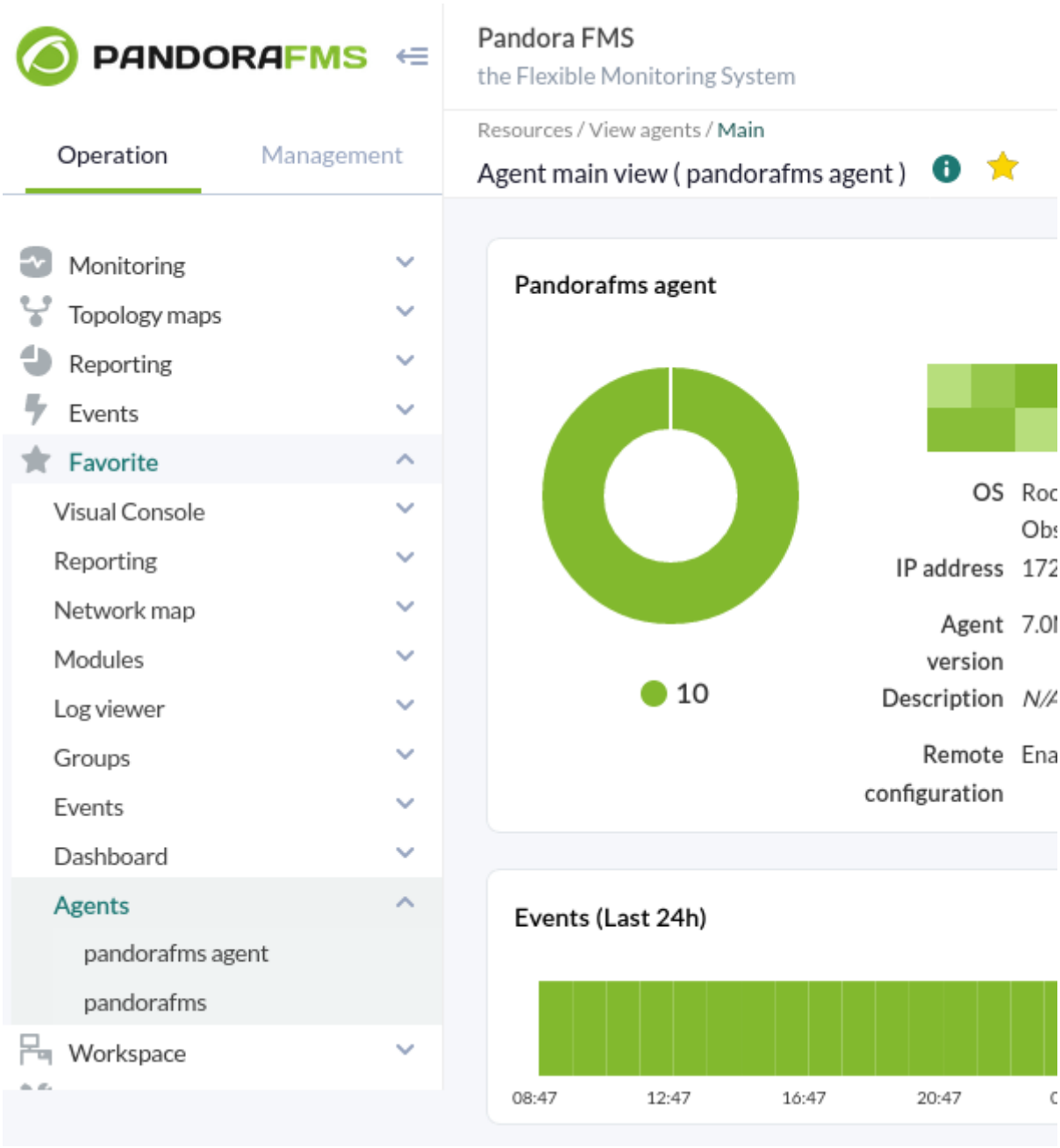
- 全モジュールとその状態
- 直近 24時間のイベント
- エージェント情報
    - 名前
    - バージョン
    - エージェント接続
    - グループ

バージョン NG 770 以降

お気に入りシステム を使用すると、エージェントを各ユーザのカスタムリストに追加できます。 メイン画面のエージェント名のすぐ横にある星ボタンをクリックします。

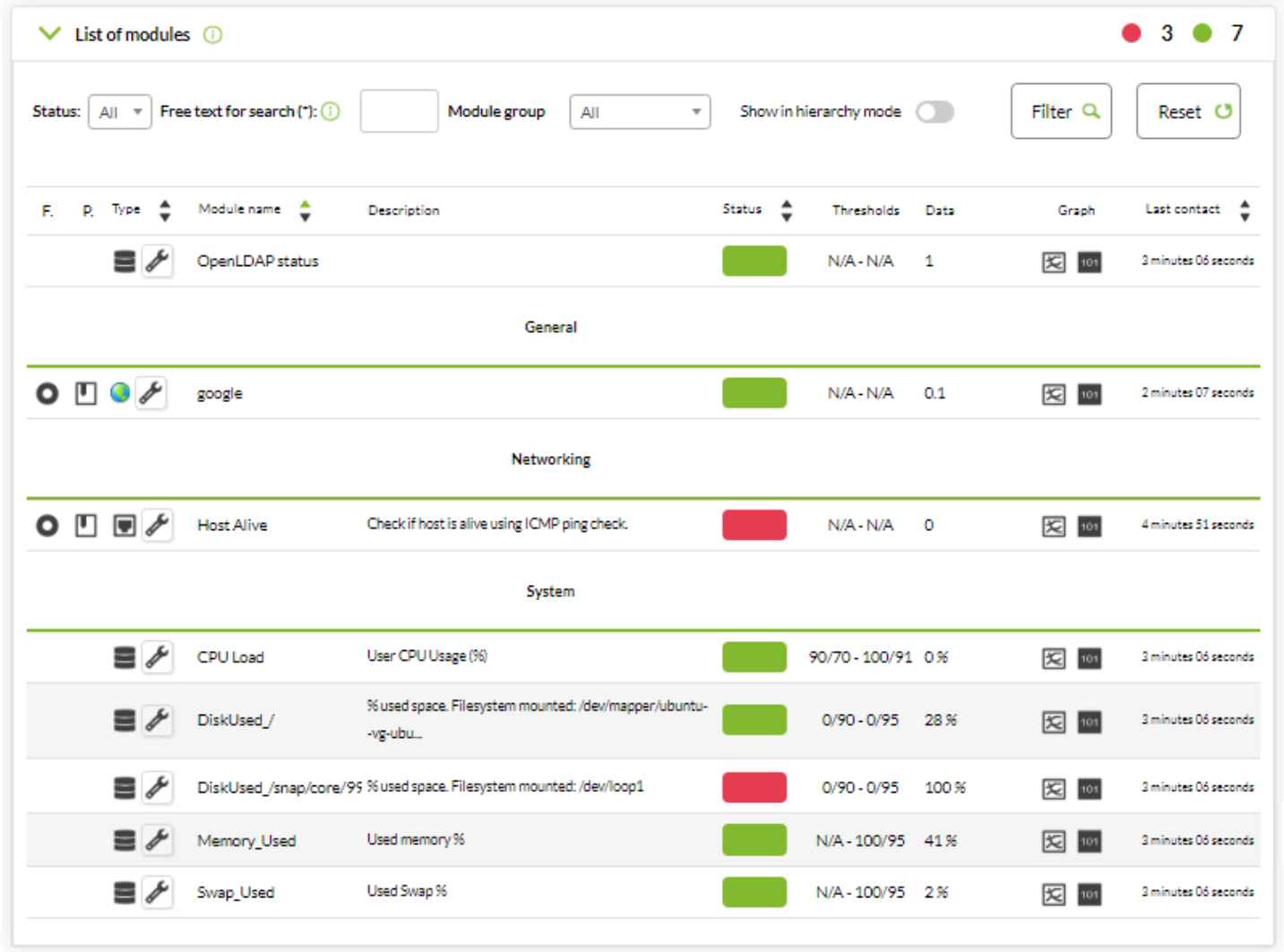


必要な数のエージェントを追加 (または削除) できます。エージェントはすべて、お気に入り(Favorite) メニュー (操作(Operation) セクション) の エージェント(Agents) セクションに常に表示されます。

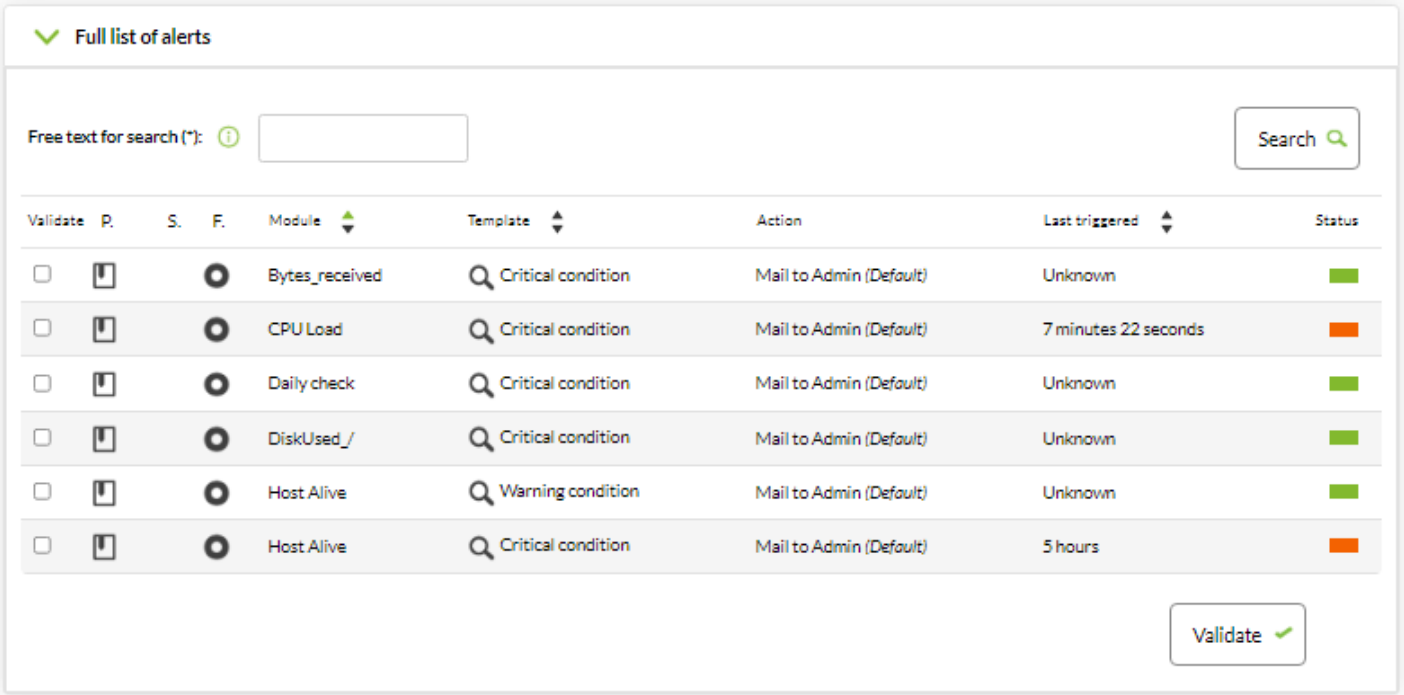


エージェントに属するモジュールの一覧 (モジュール一覧(List of modules)) とそれに対応する状態。

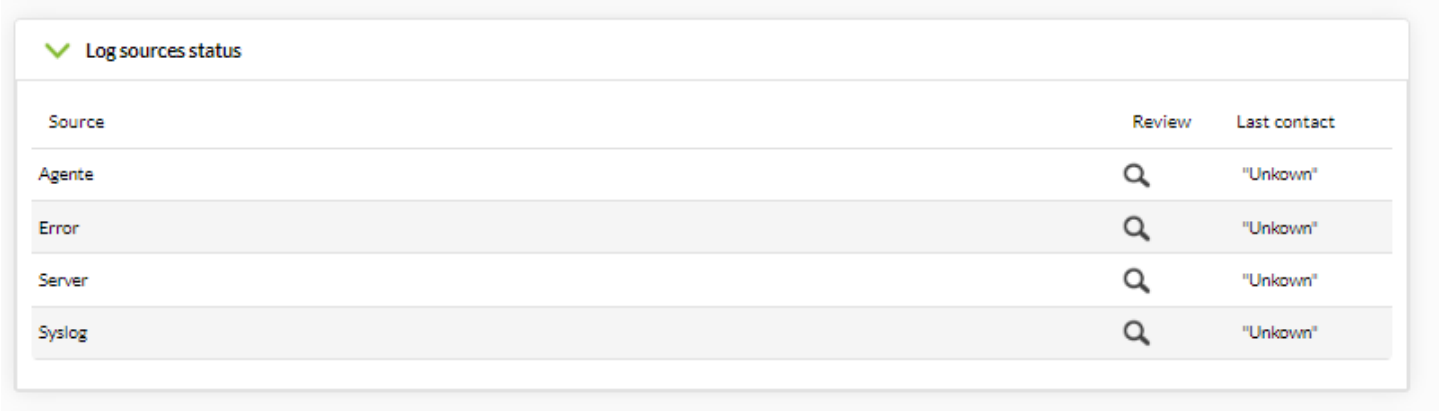
初期化**されたモジュールのみが表示されます。**



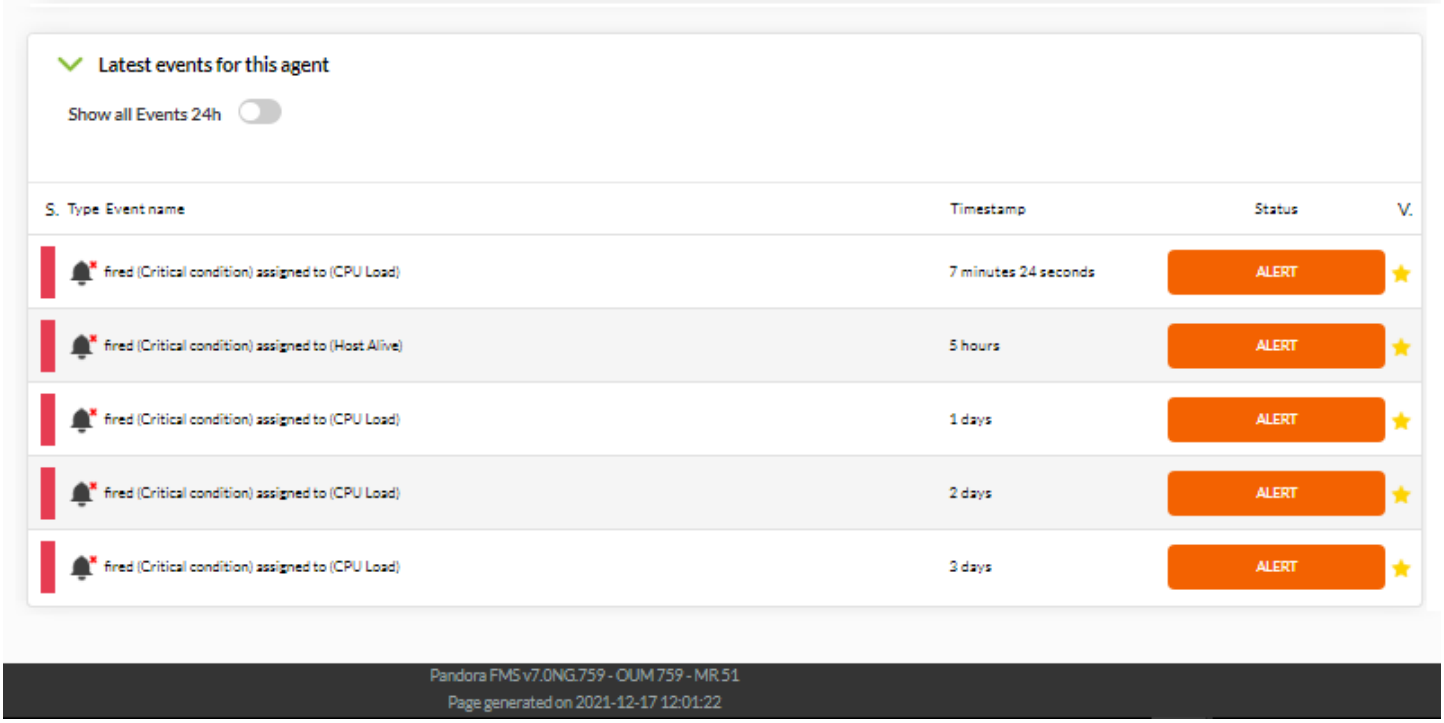
エージェントのアラートの完全な一覧です。1つまたは複数のアラートを選択し、承諾(Validate) ボタンで承諾するオプションがあります:



ログ収集 で設定された ログソースの状態 です。



このエージェントの最新の イベント を一覧表示します(このエージェントの最新のイベント(Latest events for this agent))。過去 24 時間のイベントのみを表示するオプションがあります (24 時間以内の全イベント表示(Show all Events 24h)):



モジュール

モジュールは、エージェント内に格納されている情報の単位です。 これらは、エージェントが指しているデバイスまたはサーバの状態を見る監視項目です。

各モジュールに格納できるメトリックは 1つだけです。 同じエージェント内に同じ名前の 2つのモジュールを設定することはできません。

すべてのモジュールは以下の状態を持ちます。

- 未初期化(Not started): まだデータを受け取っていません。
- 正常(Normal): データを受け取っており、値が警告や障害の閾値を超過していません。
- 警告(Warning): データを受け取っており、値が警告閾値を超過しています。
- 障害(Critical): データを受け取っており、値が障害閾値を超過しています。
- 不明(Unknown): モジュールは動作していますが、一定期間情報の受け取りが停止しています。

モジュールは、二値、数値、文字列といった、異なるタイプ(種類はこちら)のデータを持ちます。

モジュールのタイプ

Pandora FMS には、いくつかのモジュールのタイプがあります。

- データモジュール(Data module): これは、たとえばデバイスの CPU や空きメモリの使用など、ソフトウエアエージェントがインストールされているシステムでチェックが行われるローカル監視モジュールです。 この種の監視についてもっと知りたい場合は、こちら を参照してください。
- ネットワークモジュール(Network module): これは、エージェントが機能しているかどうか、または特定のポートが開いているかどうかなど、エージェントが指しているデバイスまたはサーバとの接続を確認するために使用されるリモート監視モジュールです。 この種の監視についてもっと知るためには、こちら を参照してください。
- プラグインモジュール(Plugin module): これは、ローカルまたはリモートの監視モジュールで、スクリプトを作成してカスタムチェックを行うことができます。 それらを使って Pandora FMS コンソールからデフォルトの監視機能よりもさらに高度で広範囲なチェックを行うことができます。この種の監視についてもっと知りたい場合は、こちら を参照してください。
- WMI モジュール(WMI module): これは Windows システムに対して、インストールされているサービスのリストや現在の CPU 負荷の取得などができるリモート監視モジュールです。 この種の監視についてもっと知りたい場合は、こちら を参照してください。
- 予測モジュール(Prediction module): これは、監視対象サーバーの平均 CPU 使用率や接続待ち時間の合計など、他の“ 基本 ”モジュールからのデータを参照してさまざまな算術演算を実行する予測監視モジュールです。 この種の監視についてもっと知るためには、こちら を参照してください。
- ウェブサーバモジュール(Webserver module): これは、たとえば Web サイトが停止しているかどうか、または特定の単語が含まれているかどうかを確認するなど Web サイトの状態をチェックしてデータを取得する Web 監視です。この種の監視についてもっと知りたい場合は、こちら を参照してください。
- ウェブ分析モジュール(Web analysis module): これは Web サイトの参照、資格情報の導入、フォームへの準拠など、ユーザの Web 参照のシミュレーションが実行できる Web 監視です。 この種の監視についてもっと知りたい場合は、こちら を参照してください。

状態監視

監視をするとき、システムから、メモリ CPU 筐体温度、接続ユーザ数、eコマースサイトの注文数、その他数値情報をシステムから取得します。時々、我々はデータにのみ興味を持ちますが、一般的に値に対して状態を関連付けたいと考えます。そこで「しきい値」を越えたときに状態が変化し、何が正常か異常かを知らせてくれるようにします。これが監視です。状態の概念について説明します。

Pandora FMS は、データに基づき状態を決定するための しきい値 を定義することができます。3つの可能な状態として、正常 警告 障害があります。しきい値は、ある状態が他の状態に移る値です。モジュールの状態は、それぞれのモジュールの設定において次のパラメータによって指定されたし

きい値に依存します。

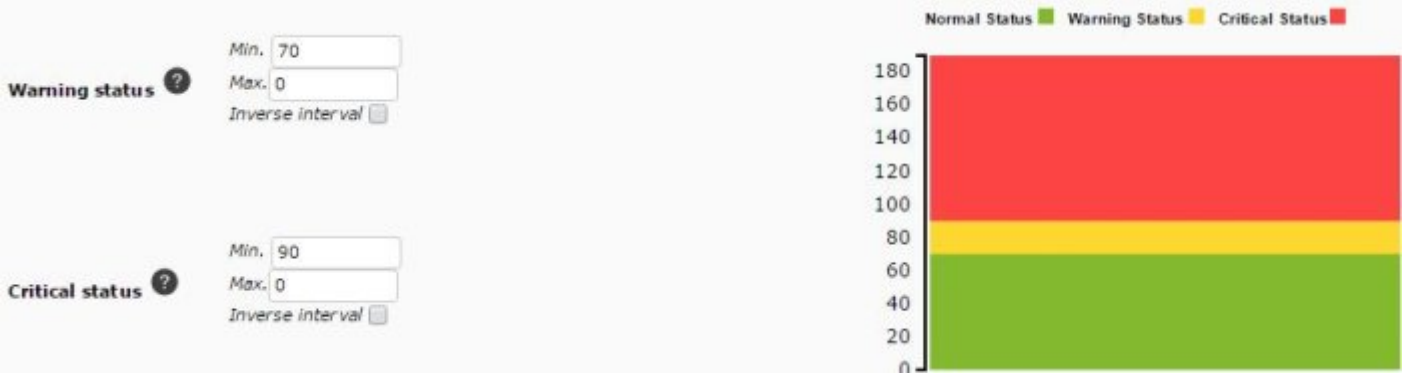
- 警告状態 - 最小 最大(Warning status - Min. Max.): 警告状態の下限と上限です。モジュールの値がこの範囲に入ると、モジュールは警告状態になります。上限を設定しない場合は、無限(下限を超えたすべての値が対象)となります。
- 障害状態 - 最小 最大(Critical status - Min. Max.): 障害状態の下限と上限です。モジュールの値がこの範囲に入ると、モジュールは障害状態になります。上限を設定しない場合は、無限(下限を超えたすべての値が対象)となります。
- 範囲の反転(Inverse interval): 警告と障害のしきい値両方の設定に存在します。有効化すると、モジュールは、値がしきい値に指定した 範囲外 になった場合に状態変化します。文字列モジュールに対しても動作します。文字列が、警告/障害文字列にマッチしなかった場合に状態が変わります。

- パーセンテージ(Percentage): 有効にすると、しきい値はパーセンテージとして解釈されます。 たとえば、最小の 警告閾値 の値が 50 に設定され、パーセンテージ が有効になっている場合、モジュールの値が前の値に対して 50% を下回ると、モジュールは警告状態になります。 最大の 障害閾値 の値が 25 に設定され、パーセンテージ が有効になっている場合、モジュールの値が前の値と比較して 25% 以上増加すると、モジュールは障害状態になります。
- 警告状態 - 文字列(Warning status - Str.): 文字列モジュールに対する正規表現です。マッチするとモジュールは警告状態になります。
- 障害状態 - 文字列(Critical status - Str.): 文字列モジュールに対する正規表現です。マッチするとモジュールは障害状態になります。

“ 警告 ” と “ 障害 ” のしきい値が重なっている場合は、“ 障害 ” しきい値が常に優先されます。

数値しきい値 - ケーススタディ 1

CPU 使用率モジュールは、エージェントのステータスの中で常に緑色です。これは単に 0% と 100% の間の値を報告するためです。 70% に達したときに CPU 使用率モジュールが警告状態(黄色)になり、90% に達したときに障害状態(赤)になるようにするには、次のようにしきい値を設定する必要があります。



そのコンピュータからデータを受信し、データが 70% 未満の場合、データは緑色で正常、70%～89,99% は黄色で警告、90% 以上は赤、障害 となります。 しきい値の動作により、このような場合、上限を設定する必要はありません。これは、下限しきい値のみが設定されている場合、上限しきい値は“ 制限なし ”と見なされ、下限を超える値はすべてしきい値内と見なされるためです。 さらに、しきい値が重複している場合、 障害しきい値が警告しきい値よりも優先されます。

文字列しきい値 - ケーススタディ 2

モジュールが次のような *文字列* としてデータを返すとします。

- OK.
- ERROR connection fail.
- BUSY too many devices.

以下に示すように 警告状態(Warning Status) および 障害状態(Critical Status) フィールドの 文字列(Str.) に正規表現で設定することにより、アラートのしきい値を設定できます。

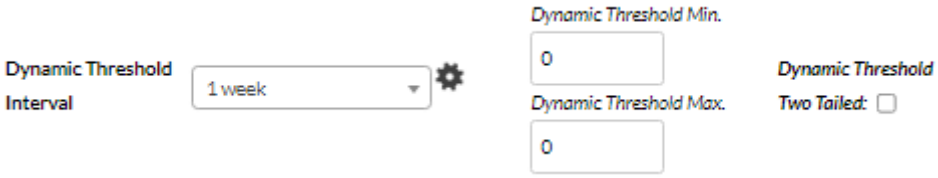
正規表現には注意してください。大文字と小文字が区別されます。

この設定により、モジュールは、データに BUSY という文字列が含まれている場合は警告状態、データに ERROR という文字列が含まれている場合は障害状態となります。

動的監視 (自動しきい値設定)

動的監視は、インテリジェントかつ予測的な方法でモジュールの状態しきい値を自動的かつ動的に調整します。この処理では、しきい値の設定を指定の期間で収集した値から平均および標準偏差を計算することによって行います。

設定可能なパラメータ

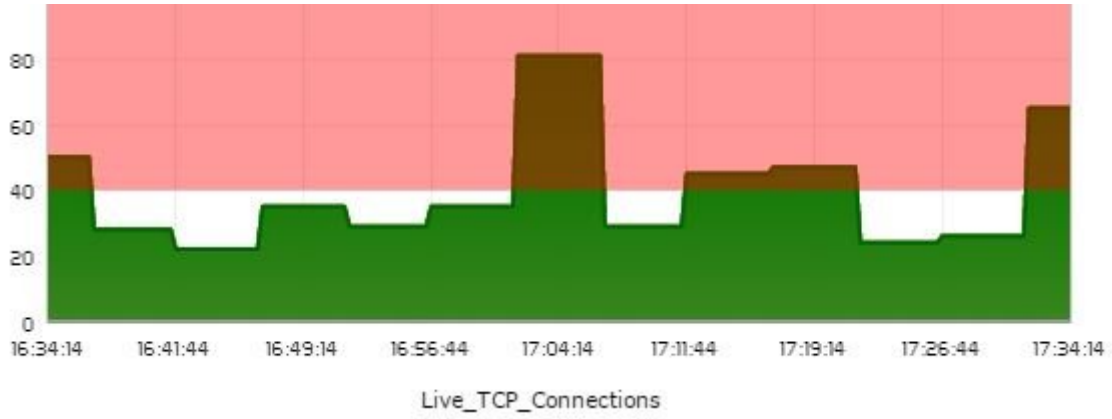


- 動的しきい値の間隔(Dynamic Threshold Interval): しきい値を計算するための時間間隔です。1ヵ月を選択すると、システムは過去1ヵ月間のデータを使ってしきい値を設定します。
- 最大動的しきい値(Dynamic Threshold Max.): パーセンテージの設定で上限を増加させることができます。例えば、平均値が 60前後で障害状態のしきい値が 80のときに、最大動的しきい値を 10 に設定すると、障害状態のしきい値を 10% あげることができます。結果、障害状態しきい値は 88 となります。
- 2つの動的しきい値を使う(Dynamic Threshold Two Tailed): 有効化すると、動的しきい値システムは、平均より *下* のしきい値も設定します。無効化(デフォルト)している場合は、平均値の *上* のみのしきい値を設定します。
- 最小動的しきい値(Dynamic Threshold Min.): *2つの動的しきい値を使う*が有効の場合のみ設定可能です。パーセンテージの設定で下限を下げることができます。例えば、平均値が 60前後で障害状態のしきい値が 40のときに、最小動的しきい値を 10 に設定すると、障害状態のしきい値を 10% 下げることができます。結果、障害状態しきい値は 36 となります。

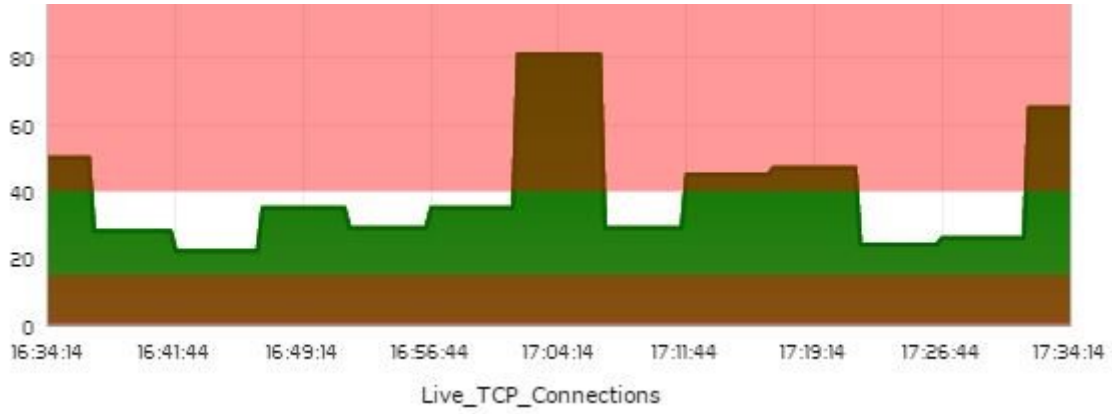
ケーススタディ 1

次の例では、計算された平均値は赤い線の高さ(約30)にあります。

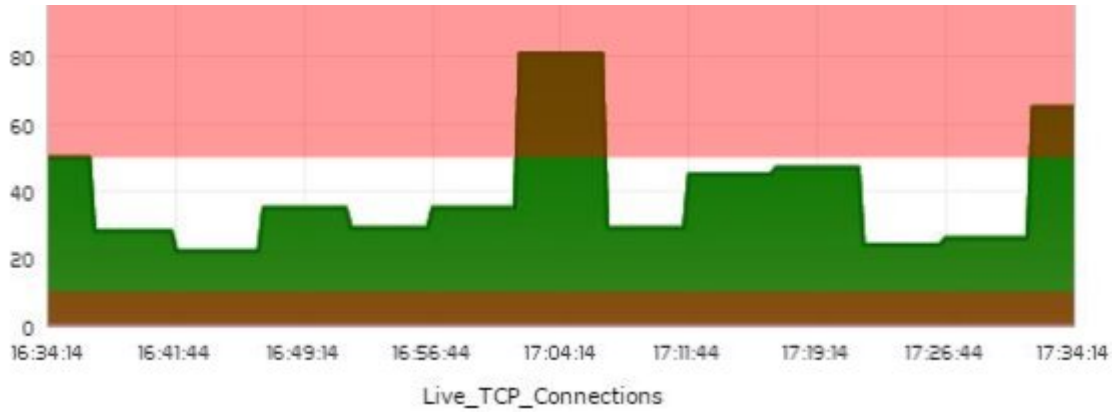
動的しきい値を有効化すると、上限しきい値はこのように設定されます(約45以上)。



パラメータ *2つの動的しきい値を使う(Dynamic Threshold Two Tailed)* が有効化されたため、平均値を下回る障害しきい値も設定されています(約15以下)。

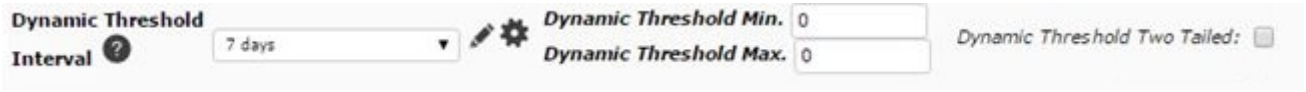


それに応じて、パラメータ *最小動的しきい値(Dynamic Threshold Min.)* および *最大動的しきい値(Dynamic Threshold Max.)* が 20 および 30 に設定されたため、しきい値が拡大され、わずかに許容度が高くなりました。



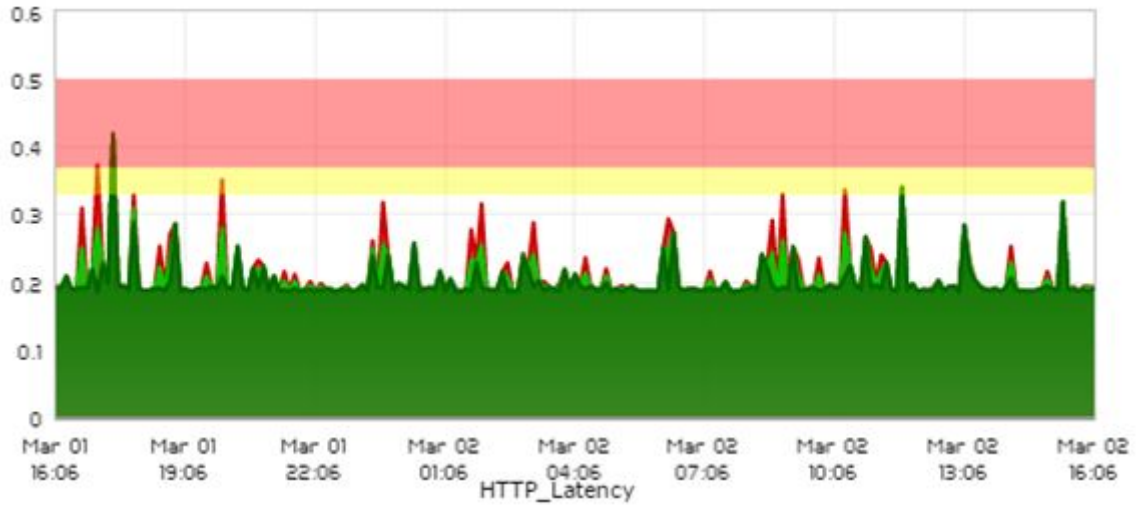
ケーススタディ 2

Web の応答時間モジュールを例にとります。しきい値の計算期間は 1週間です。



設定を保存し、*pandora_db* が実行後されると、しきい値は次のように設定されます。

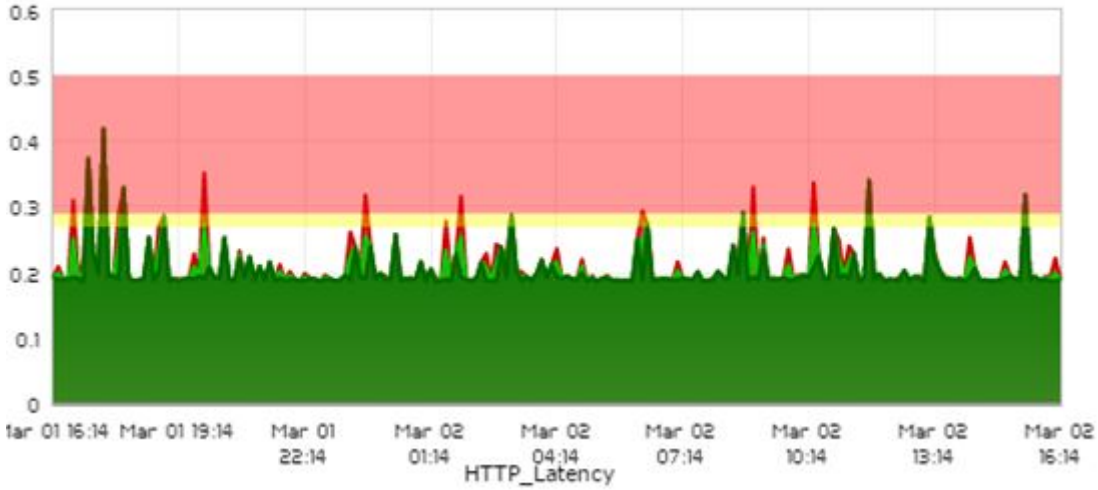
このとき、モジュールは、応答時間が 0.33秒より大きい場合には「警告」ステータスに、0.37秒より大きい場合には「障害」に切り替わります。 グラフは次のようになります。



ここでは、しきい値はやや高いと考えられるため、パラメータ *最小動的しきい値* を使用して最小のしきい値を下げることにしました。 この場合、ある値を超えるものはすべて対象となり、しきい値は最大値を持たないため、 *最大動的しきい値* は使用しません。変更は次のようになります。

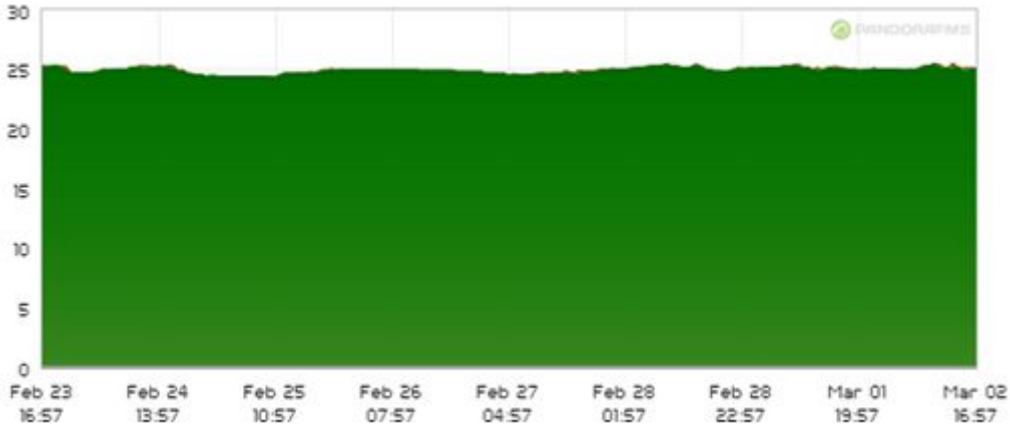
変更を行ったあと *pandora_db* が実行されると、しきい値の設定は次のようになります。

グラフは次のようになります。

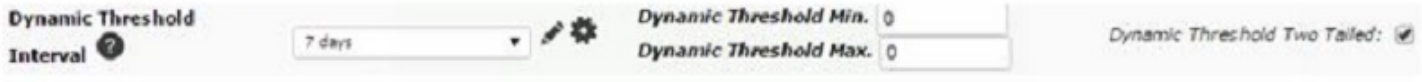


ケーススタディ 3

この例では、制御室または CPD の温度を監視しています。グラフは、わずかなばらつきのある値を示しています。

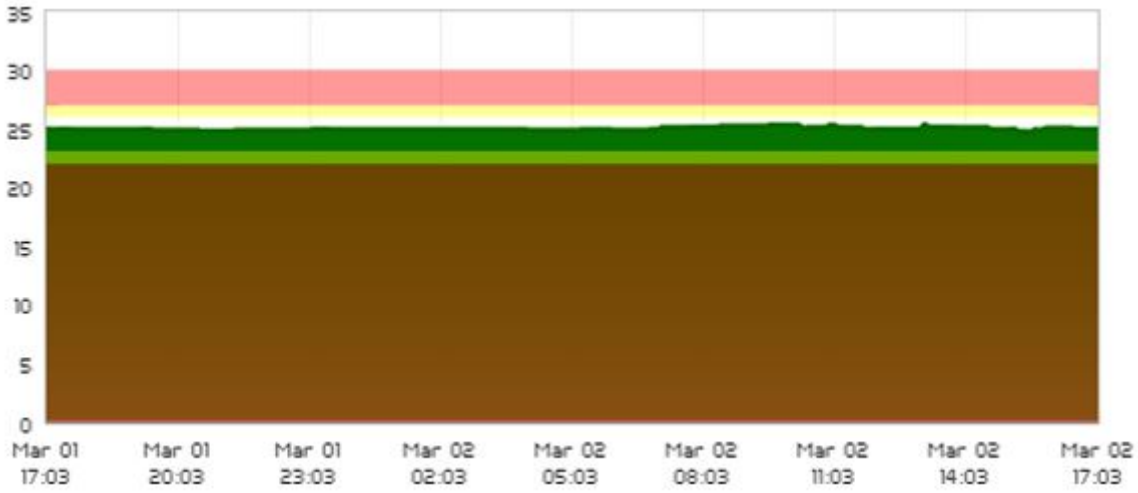


このような状況では、温度は安定した状態で、極端に高い値や極端に低い値になることはあまりありません。そのため、パラメータ *2つの動的しきい値を使う* を設定して、上下両方のしきい値を調整します。 設定は次のとおりです。



自動的に生成されたしきい値は次の通りです。

グラフは以下のようになります。



この場合、23.10 と 26 の間の値は常に正常とみなされます。これが制御室で許容される温度です。必要に応じて“ 最小動的しきい値 ”および“ 最大動的しきい値 ”でしきい値を調整することができます。

追加設定パラメータ

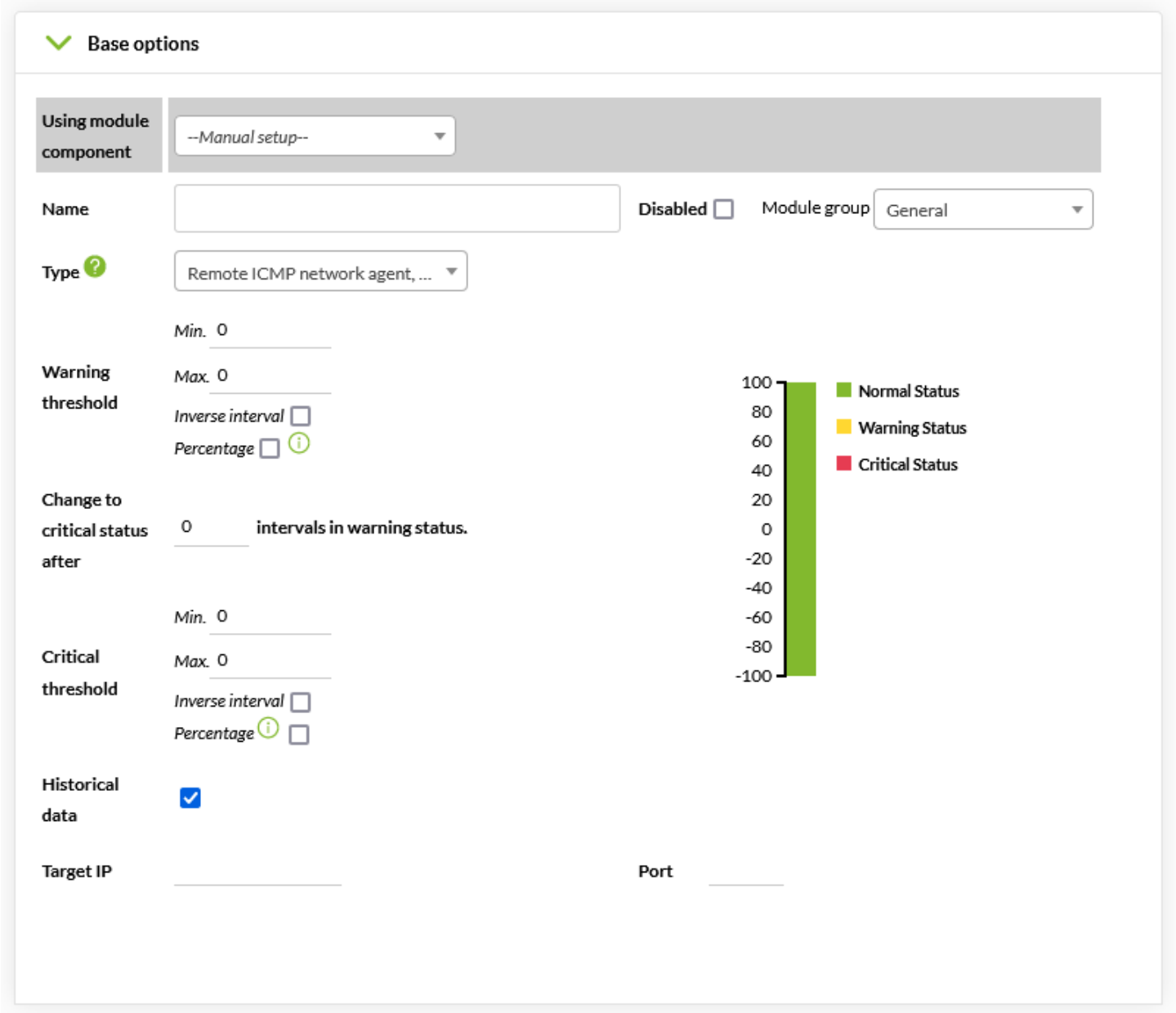
pandora_server.conf に以下を設定可能です。

- dynamic_updates: このパラメーターは、*動的しきい値間隔* で設定された期間中にしきい値が再計算される回数を決定します。デフォルト値は 5です。*動的しきい値間隔* が 1週間で設定されている場合、デフォルトで過去 1週間のデータを集計して、計算は 1回だけ実行されます。1週間が経過した後に処理が再度繰り返されます。 *dynamic_updates* パラメータを変更することで、頻度を減らすことができます。例えば、値が 3の場合、しきい値は 1週間に 3回(または *動的しきい値間隔* で設定された期間)計算されます。
- dynamic_warning: 警告 と障害 のしきい値を区別するパーセンテージです。デフォルト値は 25です。

- dynamic_constant: これは、しきい値の設定に使用される平均の標準偏差を定義します。デフォルトでは 10です。値が高いほど、平均値から離れたしきい値が設定されます。

基本オプション

このインターフェースはローカルモニタリングとリモートモニタリングの両方によって使用され、いずれか一方でのみ有効なパラメーターがあることを常に念頭に置いてください。たとえば、タイムアウト(Timeout) および リトライ(Retries) パラメータは、ローカル監視(ローカルチェック)では役立ちませんが、リモート監視では重要です。

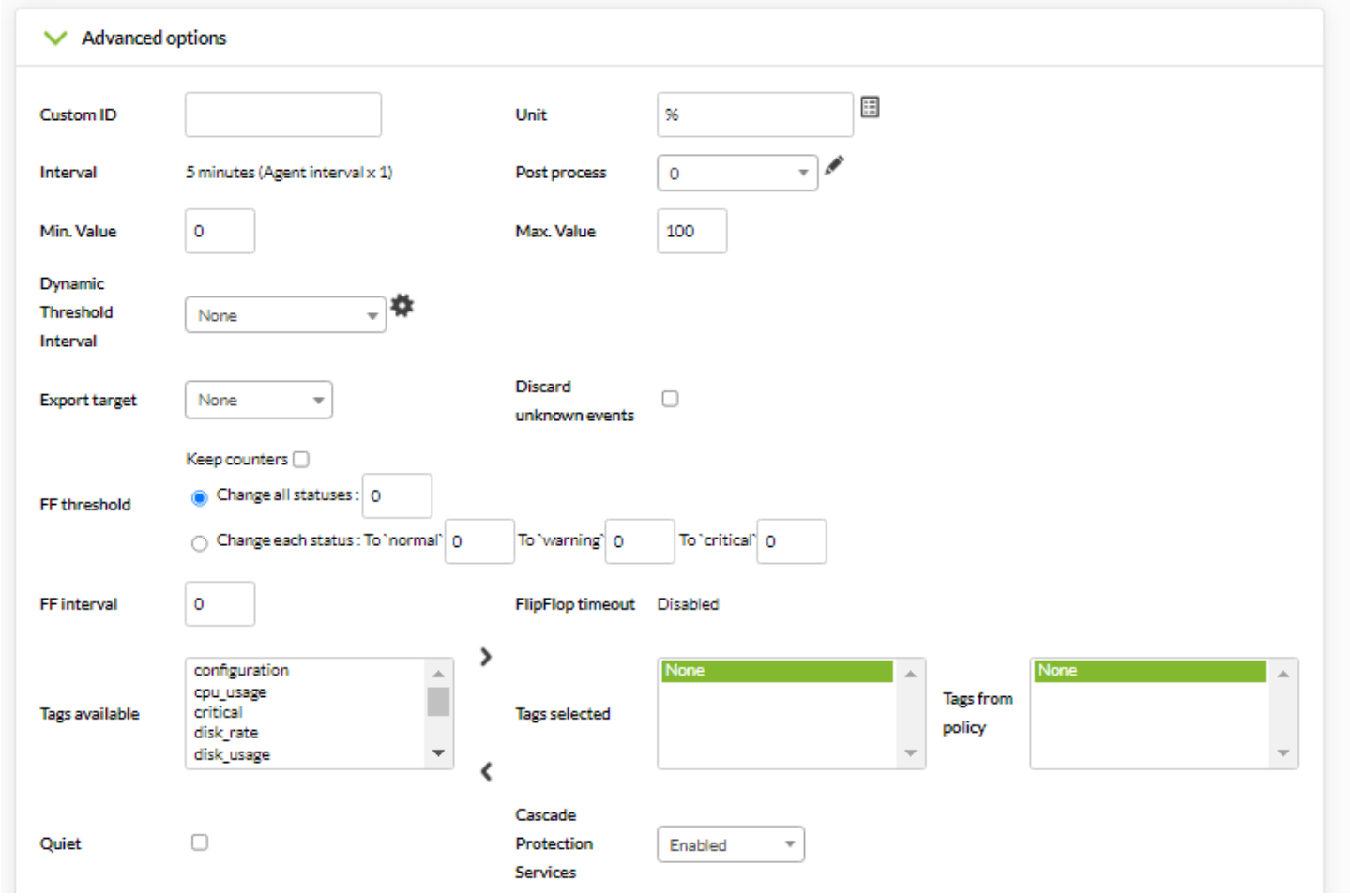


- モジュールコンポーネントの利用(Using module component): Pandora FMS には、使用可能なデフォルトモジュールのレパートリーがあります。 選択したモジュールに応じて、監視を実行するために必要

なパラメータが自動的に入力されます。 この設定は予測モジュールを除くすべてのタイプのモジュールにあります。
- 名前(Name): モジュール名。
- 無効化(Disable): モジュールを無効化できます。
- モジュールグループ(Module group): 定義済のモジュールグループにモジュールを割り当てることができます。
- タイプ(Type): 返されるデータのタイプに応じたモジュールのタイプです。モジュールコンポーネントの利用Using module component) を選択すると、データタイプは自動的に選択されます。
- 警告閾値(Warning threshold) および 障害閾値(Critical threshold): モジュールの状態が警告状態または障害状態に変更される値のしきい値。条件の反転(Inverse interval) を使うと、*範囲外*の場合に警告/障害状態になるように定義できます。
- 警告状態 X 回後に障害状態に変更(Change to critical status after X intervals in warning status): Pandora FMS バージョン 766 以降では、モジュールが連続して N 回警告状態が続いた場合(継続的な監視間隔)に、モジュールを障害状態へ変更することができます。連続抑制回数 との主な違いは、それがステータスの変更を遅らせるのに対し、障害状態への変更 を優先することです。 両方のオプションが相互に連携して機能することを常に念頭に置いてください。
- データの保存(Historical data): データを保存する場合にチェックします。
- 対象IP(Target IP) および ポート(Port): 監視対象の IP アドレスとポート番号。場合によっては、たとえば WMI 監視の場合のように、接続認証情報やクエリ文字列を設定するために追加のテキストフィールドが表示されます。

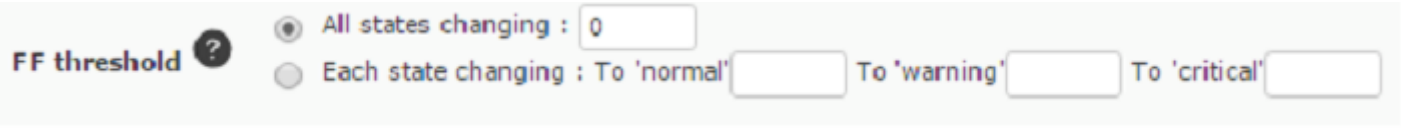
高度なオプション

このインターフェースはローカルモニタリングとリモートモニタリングの両方によって使用され、いずれかの範囲で有効なパラメーターを設定することを常に念頭に置いてください。 たとえば、タイムアウト(Timeout) および リトライ(Retries) パラメーターは、ローカル監視(ローカルチェック)では役立ちませんが、リモート監視では重要です。



- **カスタム ID(Custom ID): カスタム ID を指定するフィールドです。**
- 単位(Unit): **モジュールが受信するデータの単位を選択できるようにするパラメータで、デフォルトは空です。特定の単位(Timeticks, Bytes, Entries, など) または、鉛筆アイコン をクリックすることにより設定します。**
- Interval: Period in which the module should return data. If a module does not receive data during more than two intervals, it will go into in unknown state.
- 間隔(Interval): **モジュールがデータを返す間隔を定義するパラメータです。モジュールがデータを受信しない状態が 2周期以上続くと、不明状態になります。**
  - **リモートモジュールの場合、これはリモートチェックが実行される期間です。**
  - **データモジュールの場合、それは定義されたエージェント間隔の N倍を表し、その期間にローカルチェックを実行する数値です。**
- 保存倍率(Post process): **モジュールの受信データの保存時の倍率です。デフォルトは 0 で無効状態です。次の変換を実行できます。**
  - Seconds to months.
  - Seconds to weeks.
  - Seconds to days.
  - Seconds to minutes.
  - Bytes to Gigabytes.
  - Bytes to Megabytes.
  - Bytes to Kilobytes.
  - Timeticks to weeks.
  - Timeticks to days.
  - 鉛筆アイコン **をクリックすることにより、カスタム設定ができます。**
- 最小値(Min. Value) **および** 最大値(Max. Value): **モジュールがとりうる最小および最大値を設定できます。**
- 動的しきい値間隔(Dynamic Threshold Interval): 動的監視(動的しきい値)**のための予約フィールドです。**
- **エクスポートターゲット**(Export target): **エクスポートサーバを設定した場合に設定することができます。**

- 不明イベントの破棄(Discard unknown events): 不明イベントを破棄できます。
- 連続抑制しきい値(FF threshold): 連続障害検知抑制のしきい値を設定できます。監視における一般的な現象として状態が正常・異常の間で頻繁に変化する現象があります。これが発生するような場合は、N間隔を超えて状態が変化したままの状態になっていることで本来の状態を判断する必要があります。 *連続抑制しきい値*は、頻繁にイベント生成や状態が変わることを 'フィルタリング' するために使用されます。これにより Pandora FMS は、状態が変わった後、同じ状態が少なくとも N回継続した場合に初めて状態が変化したと認識しますN回未満の場合は変更されたとは見なされません。
  - 連続抑制時の間隔(FF interval): 連続抑制が有効で状態変化がある場合、次の実行でモジュールの間隔が変更されます。
  - 連続抑制タイムアウト(FlipFlop timeout): 非同期モジュールでのみ使用できるパラメータです。連続抑制による状態変化を有効にするためには、指定された間隔内に連続してデータを受信しなければなりません。



連続抑制回数 (FF Threshold: FF は FlipFlop を意味します) パラメータは、イベントや状態の連続的な変化をフィルタするために利用します。オリジナルの状態から変化した状態が連続して X 回を超えて続かないと、変化が発生したと Pandora FMS が認識しないようにすることができます。以下に例を見てみましょう。あるホストへの ping でパケットロスがあります。このような場合、次のような結果になります。

```
1
1
0
1
1
0
1
1
1
```

しかし、ホストは稼働しています。連続抑制回数を 2に設定し、少なくとも 3回連続でダウン状態にならないとPandora にダウンと認識し通知して欲しくないとすると、上記の例はダウンと見なさないパターンに該当します。逆に以下のような場合にダウンと認識します。

```
1
1
0
1
0
0
0
```

最後の状態になったときに、ダウンと認識し、それ以前はダウンではありません。

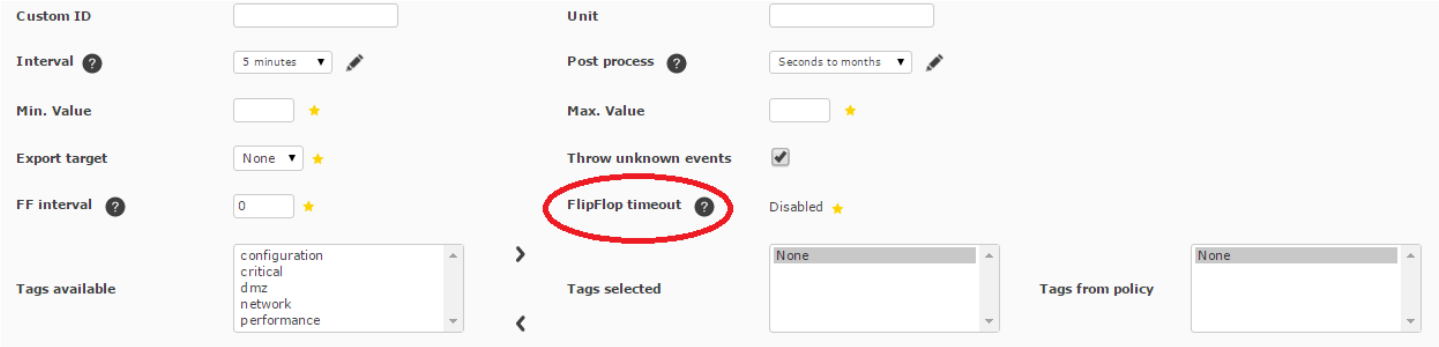
連続抑制回数は、このような不安定な変動を避けるために便利です。すべてのモジュールにおいて実装されており、状態の変化を避けるのに利用します (*proc モジュールの場合は、設定された制限

もしくは自動制限により制限されます)。

バージョン 5.1 からは、連続抑制回数には 2つのモードがあります。

- 全状態変化(All state changing): 正常、警告、障害すべての状態変化に対して、同じ値を利用します。
- 個別状態変化(Each state changing): 正常、警告、障害への状態変化ごとに異なる値を設定できます。

非同期モジュールでは、タイムアウト(連続抑制タイムアウト)も設定できます。短時間に複数回、警告や障害のデータを受信した場合にのみ障害通知をしたい場合に便利です。 データを受信する間隔がタイムアウト値を超えた場合は、連続抑制回数のカウンタがリセットされます。



たとえば、エージェントから 5分以内に 2回障害データが送られた場合にのみ通知をしたい場合(5分を超える間隔でデータが送られてきても障害通知したくない場合)は、連続抑制回数に 1、連続抑制タイムアウトに 300 を設定します。

- *カウンタ維持*

これは、連続抑制の高度なオプションで、モジュールの状態を制御します。“ カウンタ維持 ” によって、値ではなく、受け取った値を持つモジュールの状態に応じて、あるステータスから別のステータスに移行するためのいくつかのカウンタ値が設定されます。

どのように動作するか例を以下に示します。

次のようなモジュールがあると仮定します。

```
間隔: 5分
しきい値:
 障害: 90 - 100;
 警告: 80 - 90;

連続抑制:
  正常: 0;
  警告: 3;
  障害: 2;

現在の状態: **正常**;
```

そして、以下のようなデータ/状態を受け取ります。

データ	状態
81	警告
83	警告
95	障害
89	警告
98	障害
81	警告
86	警告

例からわかるように、データから状態は警告と障害になりますが、連続抑制の定義にマッチしないため現在の状態は正常です。

カウンタ維持パラメータを設定することにより、カウンタは維持され、結果、状態の変化は以下のようになります。

データ	データの状態	モジュールの状態
81	警告	正常
83	警告	正常
95	障害	正常
89	警告	警告
98	障害	警告
81	警告	警告
86	警告	警告

別の例を見てみます。

次のようなモジュールがあると仮定します。

```
間隔: 5分
しきい値:
 障害: 90 - 100;
 警告: 80 - 90;

連続抑制:
  正常: 2;
  警告: 3;
  障害: 2;

現在の状態: **正常**;
```

状態カウンタは、正常状態と障害状態が連続して到着した場合にのみ累積します。一方で、警告状態は連続して到着しなくてもカウンタを累積することがあります。

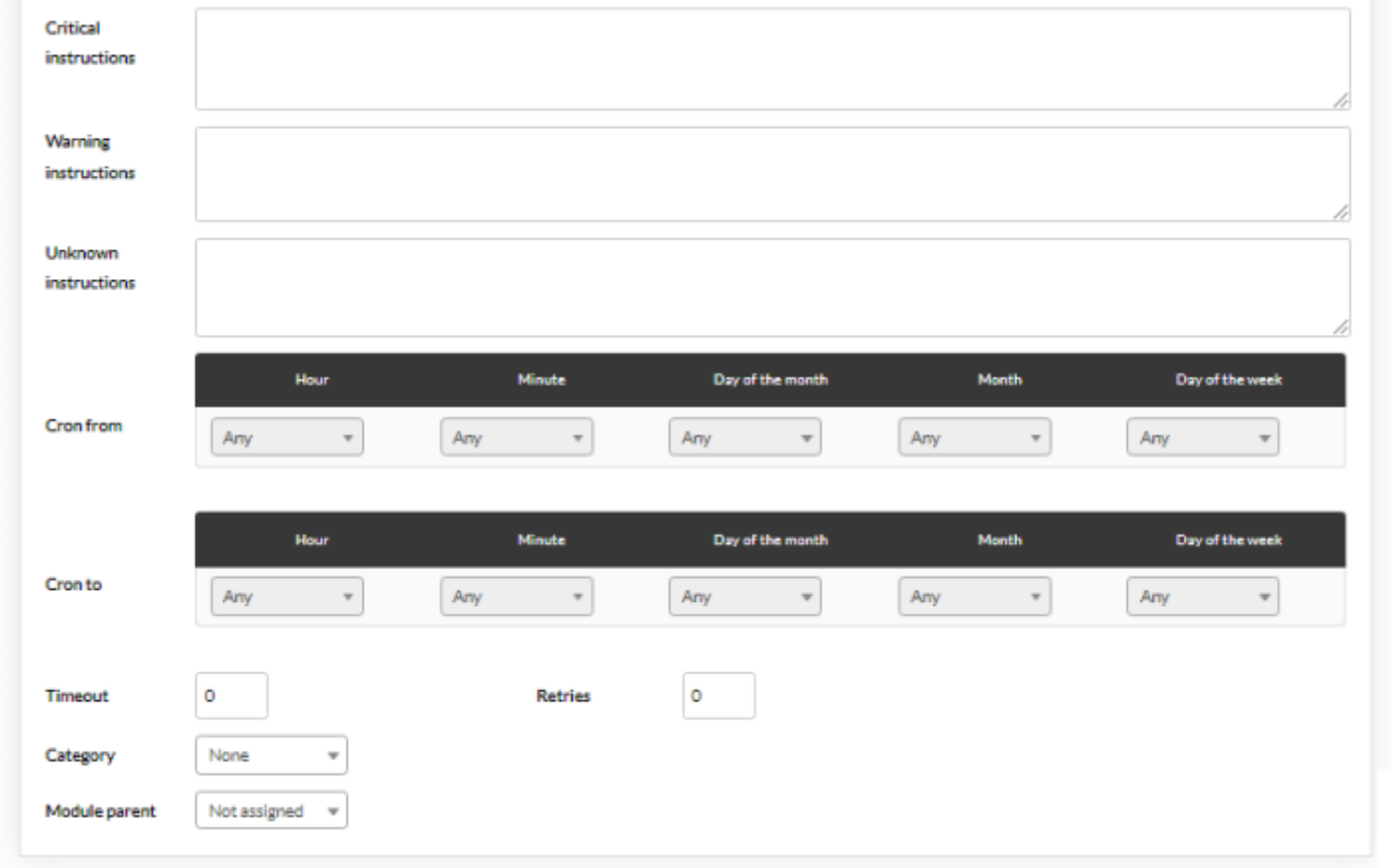
状態カウンタは、以下のような場合にリセットされます。 - 値の状態が現在の状態と一致する値が到着した場合 - “ カウンタ維持 ” の状態にマッチし、状態が変更された場合

正常カウンタと障害カウンタには特別な動作があり、連続していない場合はこれらのカウンタのみがリセットされます。

この場合、次のようなデータを受け取ります。

データ	データの状態	障害カウンタ	警告カウンタ	正常カウンタ	モジュールの状態
81	警告	0	1	0	正常
83	警告	0	2	0	正常
95	障害	1	2	0	正常
89	警告	0	0	0	警告
警告カウンタが 3 になったとき、状態が警告に変更されカウンタはリセットされます。					
50	正常	0	0	1	警告
98	障害	1	0	0	警告
正常カウンタと障害カウンタが増え続けるには、連続している必要があります。障害状態の値を受信したとき、正常カウンタは 0 になります。					
91	障害	0	0	0	障害
障害カウンタが 2 に達すると、状態は障害に変更されカウンタはリセットされます。					
30	正常	0	0	1/td>	障害
31	正常	0	0	0/td>	正常
正常カウンタが 2 に達すると、状態は正常に変更されカウンタはリセットされます。					
81	警告	0	1	0/td>	正常
83	警告	0	2	0/td>	正常
12	正常	0	0	0/td>	正常
受け取ったデータが正常状態で、かつ現在の状態と同じであれば、カウンタはリセットされます。					

- タグの存在(Tags available) および ポリシーからのタグ(Tags from policy): これらは Enterprise 版の機能です。詳細に関しては、"タグ" の章 を確認してください。
- 静観(Quiet): モジュールが情報を受信し続けますが、イベントや警告は生成されません。
- サービス関連障害検知抑制(Cascade Protection Services): これが有効になっている場合、イベントおよびアラートの生成はそれが属するサービスによります。



- 障害時手順(Critical instructions), 警告時手順(Warning instructions) および 不明状態時手順(Unknown instructions): モジュールの状態が、障害、警告、または不明になった際の手順です。テンプレートとコンポーネント の利用で便利です。
- Cron: 分、時間、日、月、曜日でモジュールの実行を指定することができます。3つの設定があります。
  - Cron 開始: すべてのフィールドが 任意(any) の場合は実行制限はありません。
  - Cron 開始: *特定*Cron 終了: *任意(any)* : 特定のタイミングにマッチした場合に実行します。例: 15 20 * * * は、毎日 20:15 に実行します。
  - Cron 開始: *特定*Cron 終了: *特定*: 特定の期間で実行します。例: `5 * * * *` および `10 * * * *` の場合は、毎時 5 から 10分に実行します。
- タイムアウト(Timeout): エージェントがモジュールの実行を待つ時間(秒単位)。
- リトライ(Retries): モジュール実行の再試行回数を設定します。
- カテゴリ(Category): これは通常のユーザーインターフェイスの設定では何の影響もありません。 メタコンソールと組み合わせて使用することを目的としています。
- モジュールの親(Module parent): 関連障害検知抑制での階層を設定するために使用します。
- カスタムマクロ(Custom macros): 任意の数のカスタムモジュールマクロが定義できます。マクロのフォーマットは次の通りです。

```
_macroname_
```

例:

```
    _technology_
    _moduleprioritY_
    _contactperson_
```

これらのマクロは、モジュールのアラートで利用でき、特に ユーザエクスペリエンス監視 で便利です。 モジュールが Web 分析モジュールタイプの場合:

動的マクロは @ で始まる特別なフォーマットを持ち、これらは置換されます。

```
@DATE_FORMAT (ユーザが指定したフォーマットでの現在日時)
@DATE_FORMAT_nh (時間)
@DATE_FORMAT_nm (分)
@DATE_FORMAT_nd (日)
@DATE_FORMAT_ns (秒)
@DATE_FORMAT_nM (月)
@DATE_FORMAT_nY (年)
```

ここで"n" は符号やマイナスを含まない数値です。フォーマットは perl strftime に従います。

モジュールタグ

管理(Management) メニュー → プロファイル(Profiles) → モジュールタグ(Module tags)

タグは、各モジュールに関連付けられたタグで、このモジュールが生成するイベントに伝播され、このモジュールからのイベントアラートで使用できます。 これらはレポートやイベント表示でフィルターとして使用でき、マクロ として利用できるため、特定のビューを持つこともでき、アラートで使用することもできます。

また、モジュールに特定のアクセス許可を付与するために使用することもできます。これにより、ユーザはエージェントの一つのモジュールのみにエージェントの一つのモジュールのみにアクセスでき、残りのモジュールにはアクセスできないようにすることができます。

動的監視 (動的しきい値)

動的監視は、予測的な方法でのモジュール状態しきい値の動的かつ自動調整を行います。 動作は、指定された期間の値を収集し、モジュールレベルで対応するしきい値を設定するために使用される平均と標準偏差を計算することで行われます。 パラメータはモジュールの詳細オプションにあります。

- 動的しきい値間隔(Dynamic Threshold Interval): しきい値の計算を実行するために考慮される動的なしきい値の間隔または時間。 月が選択された場合、システムは先月の既存のすべてのデータを取得し、そのデータに基づいてしきい値を構築し、平均を上回る値でしきい値が確立されます。
- 最大動的しきい値(Dynamic Threshold Max.): 障害状態動的しきい値の最大値（許容範囲が（パーセンテージで）設定されている場合）。 たとえば、平均値が約 60 で障害状態しきい値が 80 に設定されている場合に、このパラメータが 10 に設定されていると、この障害状態しきい値は 10% 増加し、値 88 となります。
- 最小動的しきい値(Dynamic Threshold Min.): 指定された割合で下限を減らすことができます。 たとえば、平均値が約 60 で、下限障害状態しきい値が 40 に設定されている場合、このパラメータに 10 が設定されていると、この障害状態しきい値は 10% 減少するため、 値は 36 となります。
- 2つの動的しきい値を使う(Dynamic Threshold Two Tailed): これらは動的なしきい値間隔であり、デフォルトでは無効になっています。 このオプションを有効にすると、動的しきい値システムは平均値を下回るしきい値も設定します。

モジュールライブラリ

バージョン 744 からあります。メニューからモジュールライブラリへアクセスするには、エージェント参照 (AR) 権限が必要です。

管理(Management) → モジュールライブラリ(Module library) → 表示(View) にアクセスして、メイン画面にアクセスします。 カテゴリ (データベース、仮想化など) でグループ化したり、検索(Search) テキスト ボックスで名前でプラグインを検索したりすることもできます。

Pandora FMS の Enterprise モジュール のダウンロードリンクは、次の場合にのみ表示されます。

- セットアップで設定されている ユーザとパスワード が Integria IMS サポートのものとマッチしている。
- Pandora FMS バージョン が Enterprise である。
- Pandora FMS ユーザが AW 権限を持っている。

Pandora FMS ドキュメント一覧に戻る