Introduction à la Supervision

Introduction à la Supervision

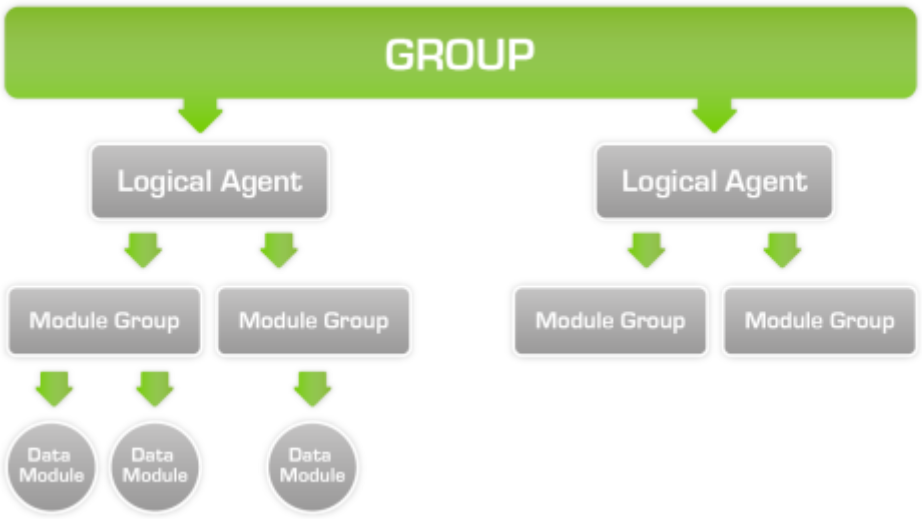
Introduction à la supervision

Toute l'interaction de l'utilisateur avec Pandora FMS se fait via la console web. La console permet l'accès via un navigateur, sans avoir besoin d'installer des applications lourdes, permettant la gestion depuis n'importe quel ordinateur avec un navigateur si le logiciel est compatible avec HTML5.

La supervision est l'exécution de processus sur tous les types de systèmes pour collecter et stocker des informations, effectuer des actions et prendre des décisions sur la base de ces données.

Pandora FMS est un système de surveillance évolutif qui dispose d'une multitude de fonctionnalités permettant d'étendre la portée et le volume des informations collectées, pratiquement sans limites.

Agents logiques sur Pandora FMS



La surveillance effectuée par Pandora FMS est classée dans la catégorie *agents*. Un agent appartient toujours à un *groupe*. Ces agents vont être équivalents à chacun des différents équipements, dispositifs, webs ou applications que nous surveillons.

Les agents définis dans la console Pandora FMS peuvent présenter des informations locales collectées par l'intermédiaire d'un agent logiciel, des informations à distance collectées par le biais de vérifications réseau, ou les deux. Par conséquent, il est important de souligner la différence

entre les agents en tant qu'unité organisationnelle dans la console Pandora FMS, et les agents logiciels en tant que services de collecte de données locales.

Surveillance basée sur des agents software vs. surveillance à distance

Nous pourrions diviser la surveillance en deux grands groupes, selon la façon dont l'information est recueillie :

- La surveillance par agent consiste en l'installation d'un petit logiciel qui reste actif dans le système et en l'obtention d'informations « localement », par l'exécution de commandes et de scripts.
- La supervision à distance consiste à utiliser le réseau pour effectuer des contrôles à distance vers les systèmes, sans qu'il soit nécessaire d'installer un composant supplémentaire dans l'équipement à surveiller.

Comme on peut l'apprécier, la surveillance basée sur des agents logiciels obtiendra l'information par le biais de contrôles locaux, tandis que la supervision à distance obtiendra l'information par le biais de contrôles réseau du serveur Pandora FMS.

Les deux types d'agents partagent la même configuration générale et la même visualisation des données ; la surveillance peut être d'une manière ou d'une autre et aussi combinée, produisant une surveillance mixte.

Configuration de l'agent logique dans la console

Interface d'édition dans la vue normale

- Alias : Pour un fonctionnement correct de toutes les fonctions que Pandora FMS exécute avec ses agents/modules, il est recommandé de ne pas utiliser des caractères comme /, \, |, %, #, & et $ dans le nom d'agent. Lorsque vous traitez avec ces agents, ils peuvent créer une confusion avec l'utilisation des chemins du système ou l'exécution d'autres commandes, causant des erreurs dans le serveur.
- Serveur : Serveur qui va exécuter les contrôles configurés dans la supervision des agents, paramètre spécial en cas de configuration HA dans son installation.
- Primary group : Il permet d'affecter un groupe à l'agent. En cliquant sur l'icône du groupe, vous pourrez accéder à la vue tactique du groupe assigné.
- IP address : Il permet d'attribuer une adresse IP à l'agent. Avec le bouton Check unique IP, vous pouvez vérifier si l'adresse IP saisie est libre, si elle est déjà dans la liste des adresses sauvegardées pour cet agent (elle a une option de suppression) ou si elle est utilisée par un autre agent. Dans le cas où elle est utilisée par un autre agent, lors de la sauvegarde de l'édition, il vous en avertira et vous demandera une confirmation avant d'enregistrer ces données. Dans la General Configuration, vous pouvez configurer le bouton Check unique IP pour qu'il soit utilisé automatiquement pour l'édition de tous les agents.

Interface d'édition dans la vue avancée

- Secondary groups : Paramètre facultatif permettant à un agent d'appartenir à plus d'un groupe (groupes secondaires).
- Cascade protection services : Paramètre permettant d'éviter une avalanche d'alertes. Vous pouvez choisir un agent ou un module d'agent. Dans le premier cas, lorsque l'agent choisi est en situation critique, il ne génère pas d'alertes. Dans le second cas, seulement lorsque le module spécifié est en situation critique, l'agent ne générera pas d'alertes.

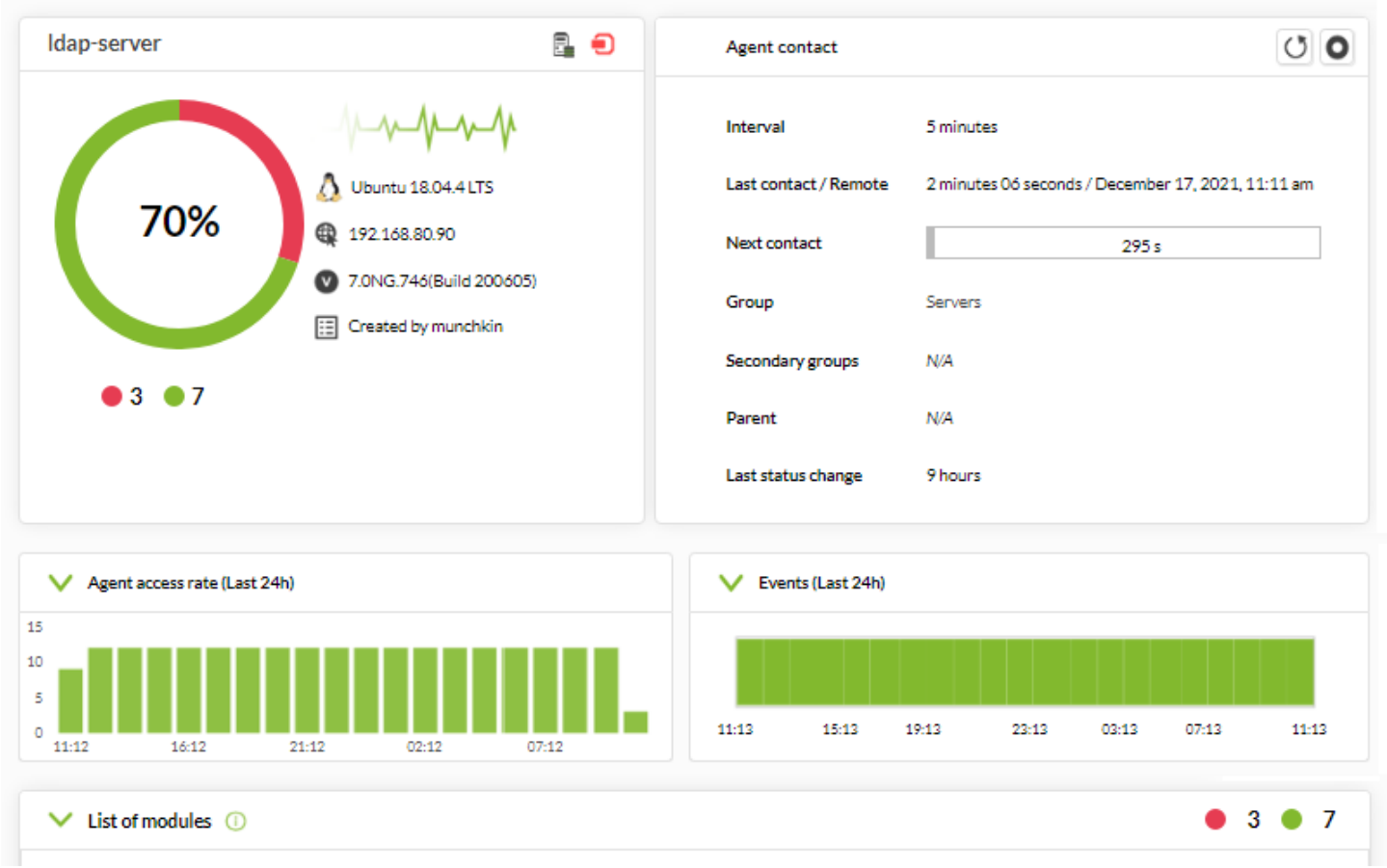
Trois modes de travail peuvent être sélectionnés (Module definition):

- Learning mode : Si XML arrive avec de nouveaux modules, ils seront créés automatiquement (par défaut).
- Normal mode : Si un XML arrive avec de nouveaux modules, ils ne seront créés que s'ils sont déjà déclarés dans la console précédemment.
- Autodisable mode : Identique au mode d'apprentissage, mais si tous les modules passent en mode inconnu, l'agent sera désactivé jusqu'à ce que les informations arrivent à nouveau.

Visualisation de l'agent

Dans cet écran vous pouvez voir une grande quantité d'informations sur l'agent, et il vous offre la possibilité de forcer l'exécution de contrôles à distance et de rafraîchir les données qui arrivent.

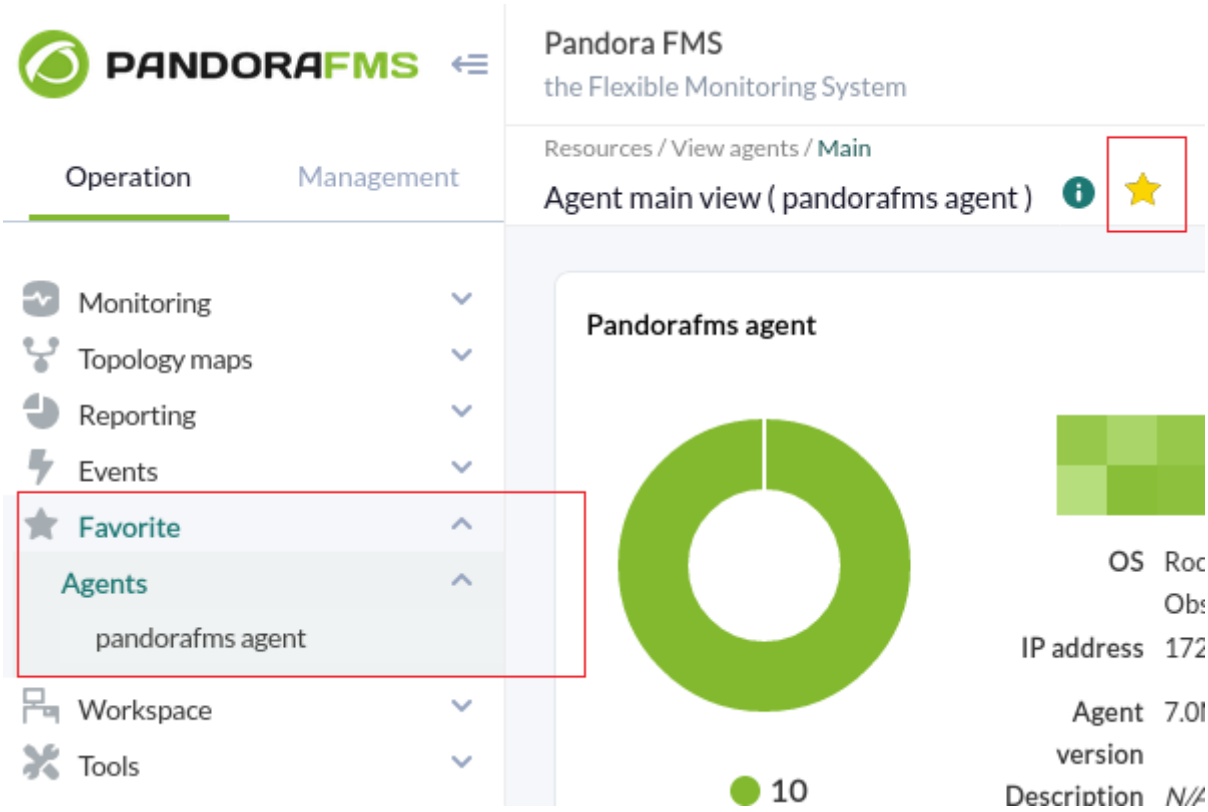
Dans la partie supérieure vous pouvez voir un résumé avec une multitude de données de l'agent, telles que :



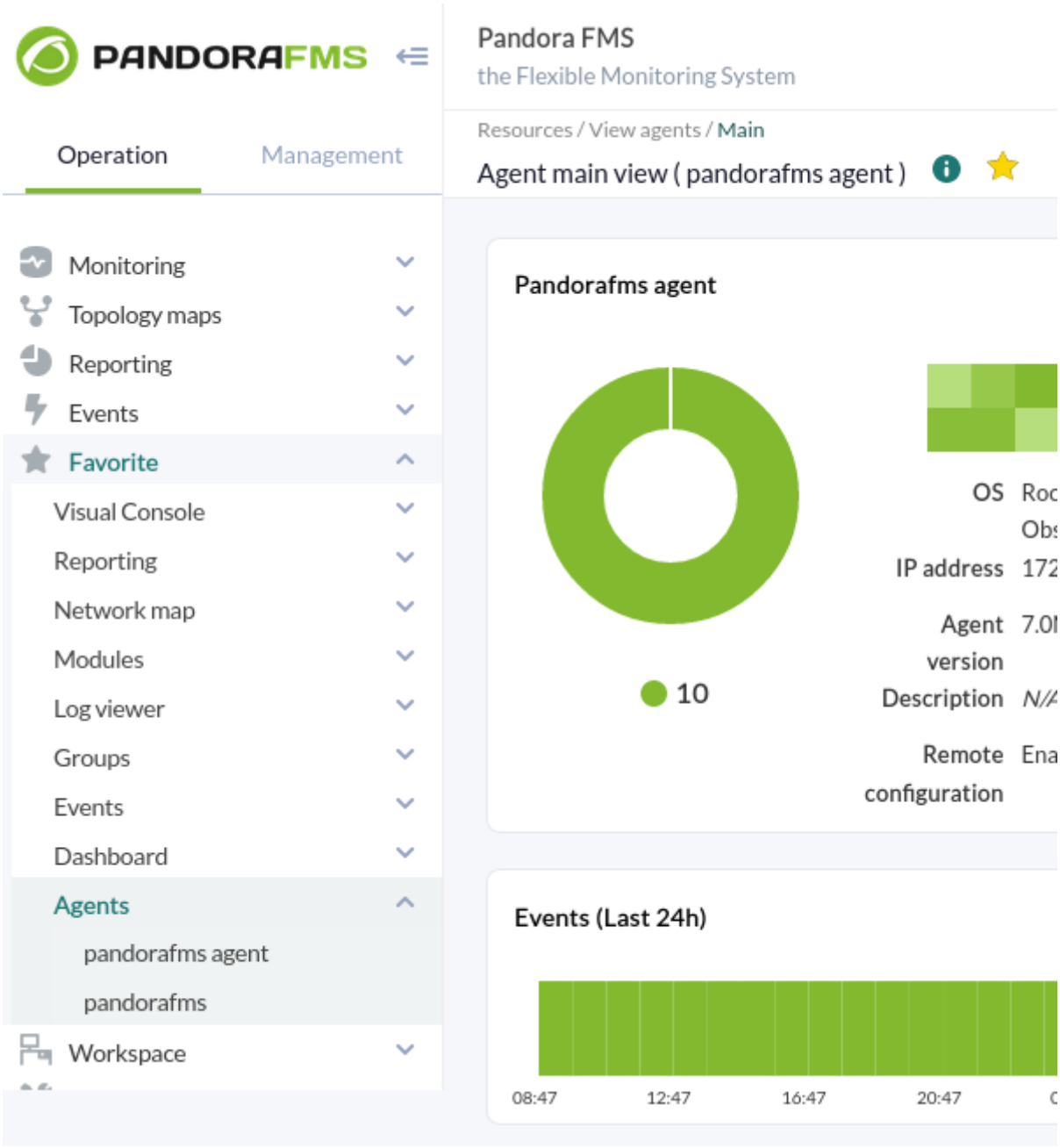
- Total des modules et leur état.
- Événements des dernières 24 heures.
- Information de l'agent.
    - Nom.
    - Version.
    - Accessibilité de l'agent.
    - Groupe.

Version 770 ou supérieure.

En utilisant le système de favoris, vous pouvez ajouter n'importe quel agent à une liste personnalisée pour chaque utilisateur. Cliquez sur le bouton étoile juste à côté du nom de l'agent dans votre vue principale.

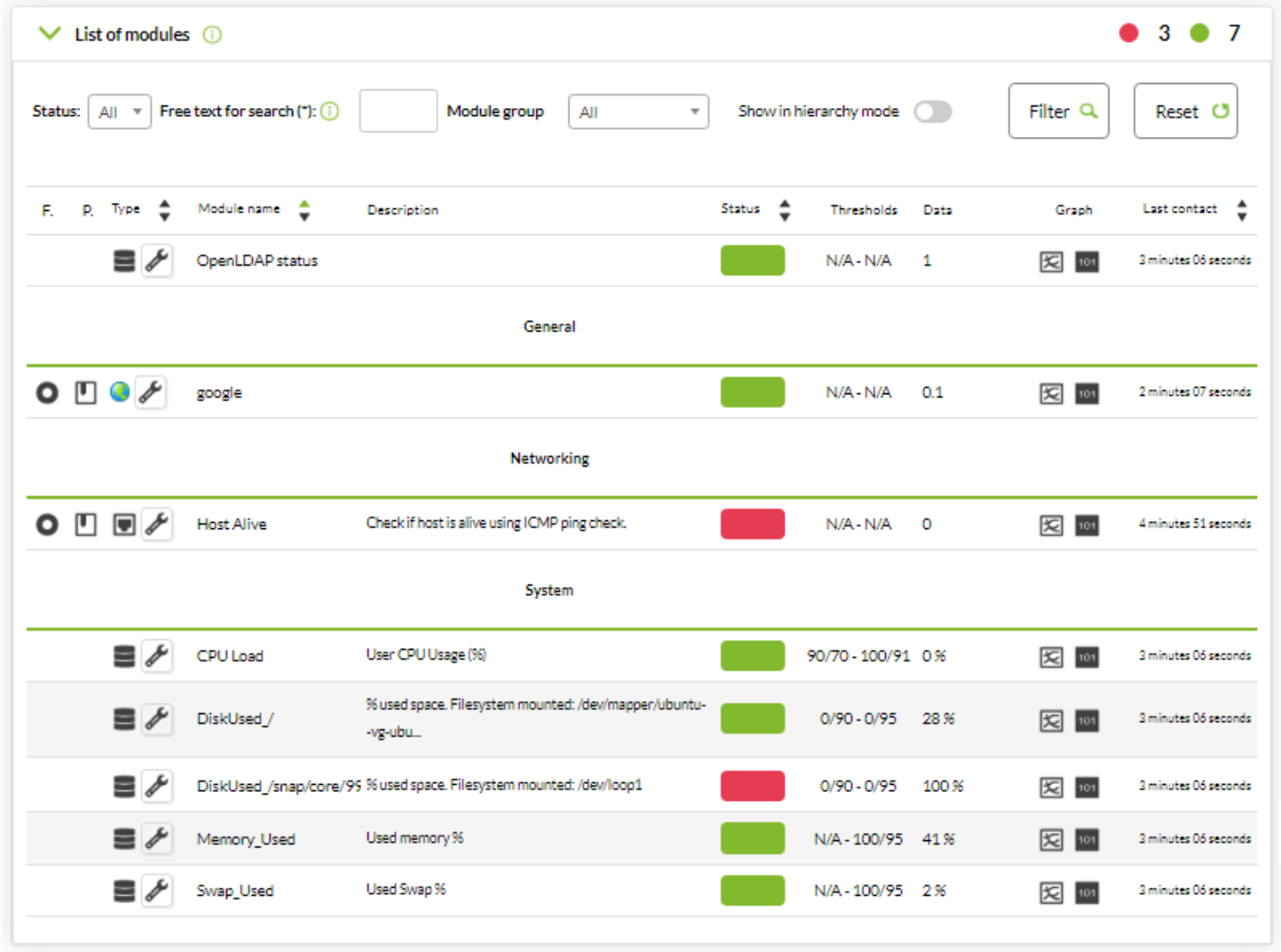


Vous pouvez ajouter (ou supprimer) autant d'agents que vous le souhaitez, tous seront toujours visibles dans la section Agents du menu Favorite (section Operation).

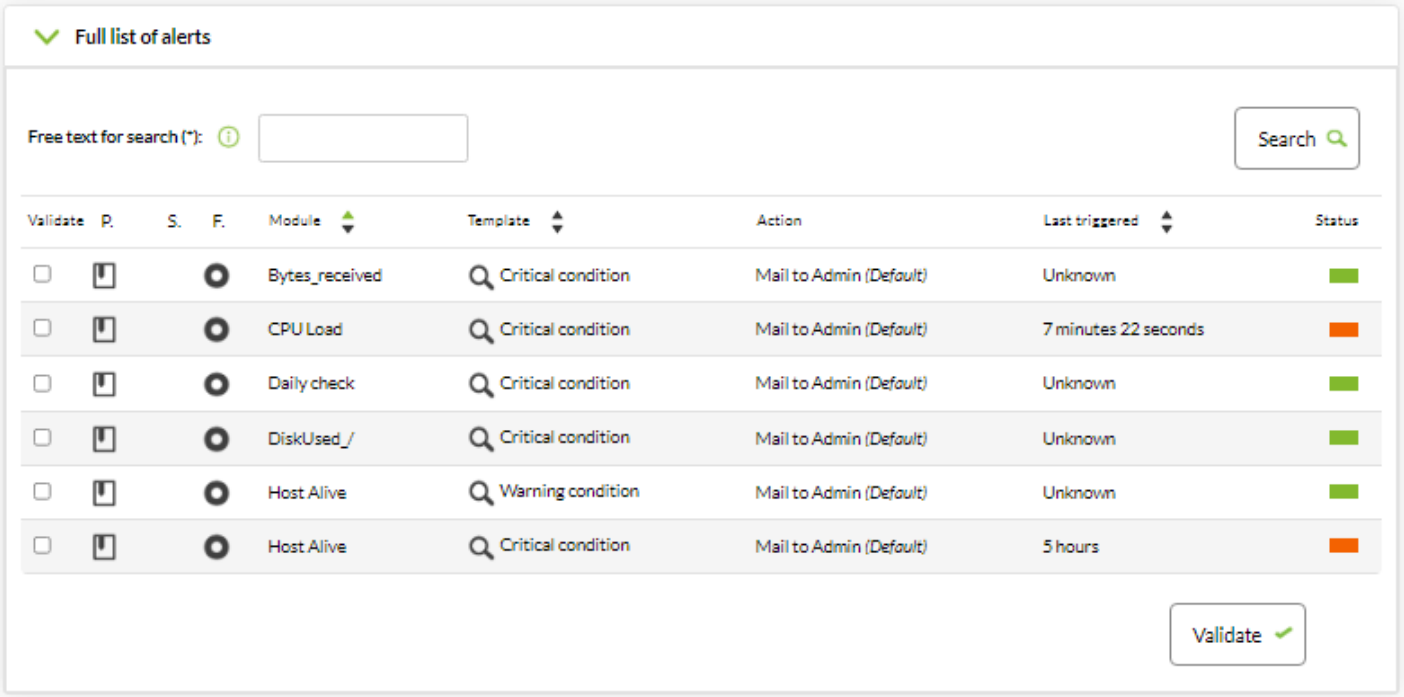


Liste des modules (List of modules) appartenant à l'agent et leurs états respectifs (*Status*).

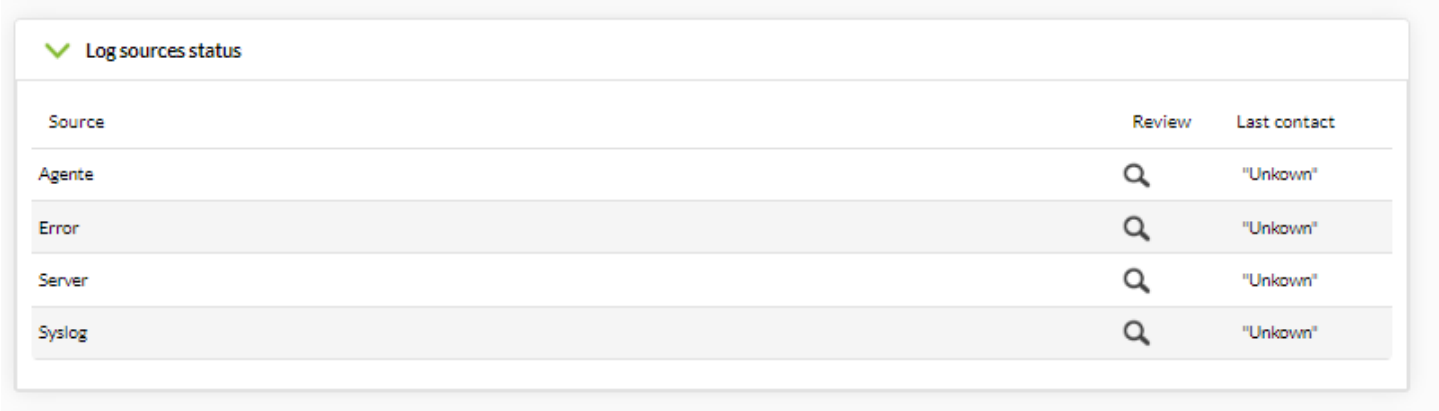
Seuls les modules démarrés sont affichés.



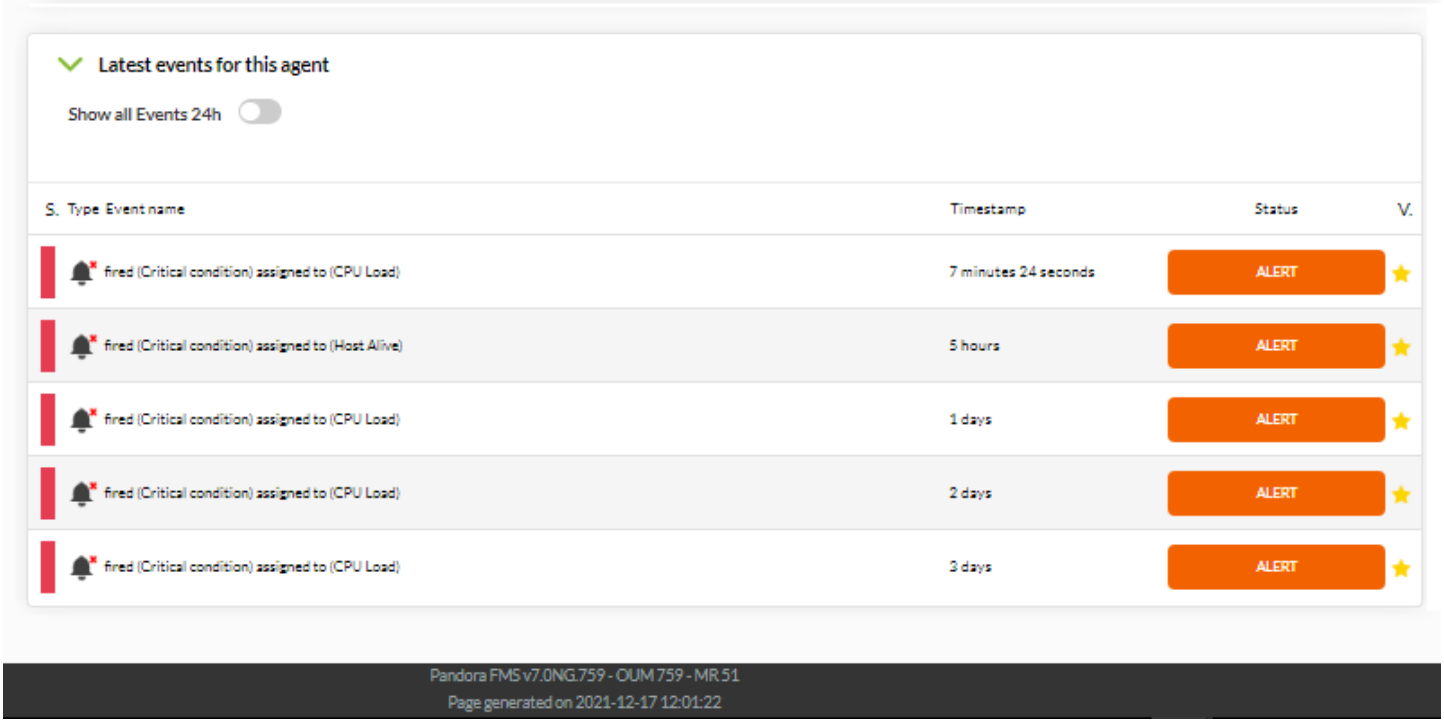
Liste complète des alertes de l'agent (Full list of alerts), avec la possibilité de sélectionner une ou plusieurs alertes et de les valider avec le bouton Validate :



État des sources de journal (Log sources status) tel que configuré dans Log Collection.



Liste avec les derniers événements pour l'agent (Latest events for this agent), avec la possibilité de n'afficher que les événements des dernières 24 heures (Show all Events 24h) :



Modules

Les modules sont des unités d'information stockées dans un agent. Il s'agit des éléments de surveillance avec lesquels l'information est extraite de l'appareil ou du serveur vers lequel l'agent pointe.

Chaque module ne peut stocker qu'un seul type de métrique. Dans un même agent il ne peut pas y avoir deux modules avec le même nom.

Dans le même agent, il ne peut pas y avoir deux modules portant le même nom. Tous les modules ont un état associé, qui peut être :

- Non inité : Où aucune donnée n'a encore été reçue.
- Normal : Il reçoit des données dont les valeurs se situent en dehors des seuils d'avertissement ou des seuils critiques.
- Avertissement : Il reçoit des données dont les valeurs se situent à l'intérieur du seuil d'avertissement.
- Critique : Les données sont reçues avec des valeurs inférieures au seuil critique.
- Inconnu : Le module a fonctionné et a cessé de recevoir des informations pendant un certain temps.

Les modules disposent de différents types de données, telles que booléennes, numériques ou alphanumériques entre autres.

Types de modules

Il existe plusieurs types de modules dans Pandora FMS.

- Module de données : est un type de module de surveillance local avec lequel des contrôles sont effectués sur le système dans lequel se trouve l'agent, comme par exemple l'utilisation du CPU de l'appareil ou de sa mémoire libre.
- Module réseau : est un type de module de surveillance à distance avec lequel on vérifie la connexion avec le périphérique ou le serveur vers lequel pointe l'agent, comme par exemple s'il fonctionne ou s'il a un port particulier ouvert.
- Plugin Module : est un type de module de surveillance locale ou à distance avec lequel vous pouvez effectuer des contrôles personnalisés par la création de scripts. Avec eux, des contrôles plus poussés et plus poussés que ceux proposés directement via la console Pandora FMS peuvent être effectués.
- Module WMI : est un type de module de monitoring local avec lequel il est possible de vérifier le système Windows via le protocole WMI, comme par exemple pour obtenir la liste des services installés ou la charge courante du CPU.
- Module de prédiction :est un type de module de surveillance prédictive avec lequel différentes opérations arithmétiques sont effectuées par la consultation de données provenant d'autres modules « de base », comme l'utilisation moyenne du CPU des serveurs surveillés ou la somme des latences de connexion.
- Module Serveur Web : est un type de surveillance Web avec lequel on vérifie l'état d'un site Web et on obtient des données de celui-ci, comme par exemple voir si un site Web est en panne ou s'il contient un mot spécifique.
- Module d'analyse Web : est un type de surveillance Web avec lequel des simulations de la navigation Web d'un utilisateur sont effectuées, comme la navigation vers un site Web, l'introduction d'informations d'identification ou l'exécution de formulaires.

Supevision des états

Lorsqu'on parle de supervision, la notion d'état est introduite : c'est l'association de la « valeur relative » au lieu de la valeur absolue, de sorte que lorsqu'un seuil est dépassé, l'état change.

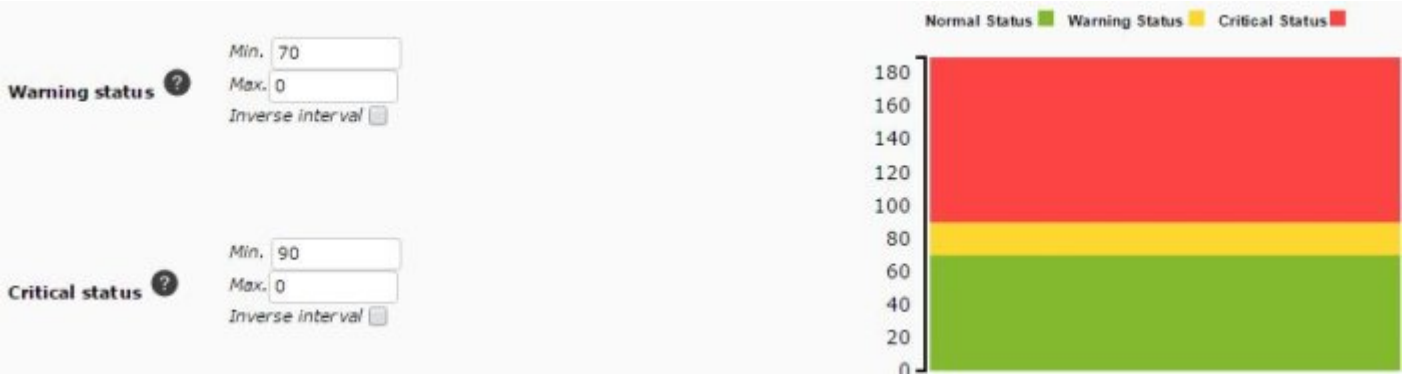
Pandora FMS vous permet de définir des seuils pour définir l'état du contrôle selon les données collectées. Les trois états possibles sont : « NORMAL », « AVERTISSEMENT » et « CRITIQUE ».

- État d'avertissement : Si la valeur numérique du module se situe dans les limites inférieure et supérieure. Si aucune limite supérieure n'est spécifiée, toute valeur supérieure à la limite inférieure entraînera un changement d'état.
- Critique : Pareille au point précédent, mais pour l'état « critique ».
- Intervalle inverse : Présent pour les seuils « avertissement » et « critique », s'il est activé, le module changera d'état lorsque ses valeurs seront en dehors de l'intervalle spécifié. Il fonctionne également pour les modules alphanumériques.
- Pourcentage : Si activé, la valeur du seuil est interprétée sous forme de pourcentage. La façon dont fonctionnent les seuils de Pourcentage est de comparer la nouvelle valeur rapportée par le module par rapport à la précédente pour voir le pourcentage de variation et si elle respecte ou non les limites de pourcentage d'augmentation (Max.) ou de diminution. (Min.) établis, elle changera d'état ou non.

Si les seuils d'avertissement et critiques se chevauchent dans une plage quelconque, le seuil critique prévaudra toujours.

Seuils numériques - Cas pratique 1

Lorsque un module est créé, ses seuils ond par défaut valeur 0. Pour superviser le pourcentage d'utilisation de l'UCT , il faut que son état devienne `warning` (jaune) lorsque le 70 % d'utilisation est atteint et `critical` (rouge) lorsque le 90 % est atteint ; il sera nécessaire d'établir les valeurs suivants :



Ainsi, lorsque la métrique de cet ordinateur est reçue, si la donnée est sous 70 % (`normal`), alors qu'entre 70 % et 89.99 % il apparaîtra en jaune (`WARNING`), et au-dessous de 90 %, rouge `CRITICAL`. En raison du fonctionnement des seuils, il n'est pas nécessaire, dans de tels cas, de fixer des limites supérieures. En effet, si seul le seuil inférieur est fixé, le seuil supérieur sera pris en compte comme « *aucune limite* », de sorte que toute valeur supérieure au seuil inférieur sera prise en compte comme faisant partie du seuil. De plus, si les seuils sont dépassés, le seuil `CRITICAL` prévaudra sur `WARNING`.

Seuils de texte - Cas d'étude 2

Un module peut retourner comme donnée recueillie quelque de ces chaines de caractères (*string*)

:

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

En utilisant des expressions régulières dans le champs Str. des paramètres Warning Status et Critical Status, comme dans l'image, vous pouvez définir des seuils d'alerte.

Faisiez attention aux expressions régulières parce qu'il différencient entre minuscules et majuscules, elles sont *case sensitive*.

Avec cette configuration, le module aura le statut WARNING lorsque les données contiennent la chaîne « BUSY » et son statut sera CRITICAL lorsque les données contiennent la chaîne « ERROR ».

Supervision dynamique (seuils automatiques)

La supervision dynamique consiste en l'ajustement dynamique et automatique des seuils d'état des modules de manière intelligente et prédictive. La méthode de travail consiste à collecter les valeurs d'une période donnée et à calculer une moyenne et un écart-type, qui sont utilisés pour établir les seuils correspondants au niveau du module.

Administration du module

Veuillez aller vers le menu Management → Resources → Manage agents et cliquez sur Modules de chaque agent.

Cette option vous permet d'afficher des informations générales de manière rapide et concise en plaçant le pointeur de la souris sur chacune des icônes des colonnes.

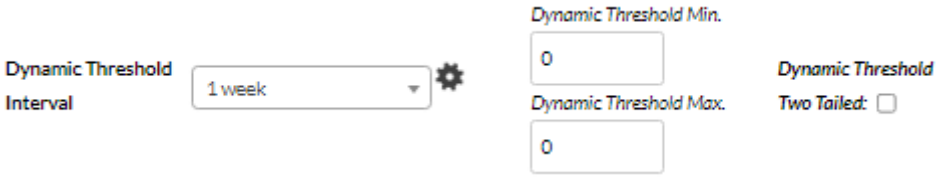
Vous pouvez également effectuer des actions telles que la modification du module en cliquant sur son nom. La colonne des actions (Actions) contient, de gauche à droite :

- Activer ou désactiver le module.
- Dupliquer un module (le préfixe lui sera ajouté) copy of ...)
- Normaliser les valeurs : Cette action est irréversible et une confirmation sera effectuée avant la suppression de ces valeurs extrêmes.

- Supprimer un module.

En outre, chaque élément contient une case à cocher permettant d'effectuer des opérations de masse (activer, désactiver, supprimer) sur les modules sélectionnés.

Paramètres possibles

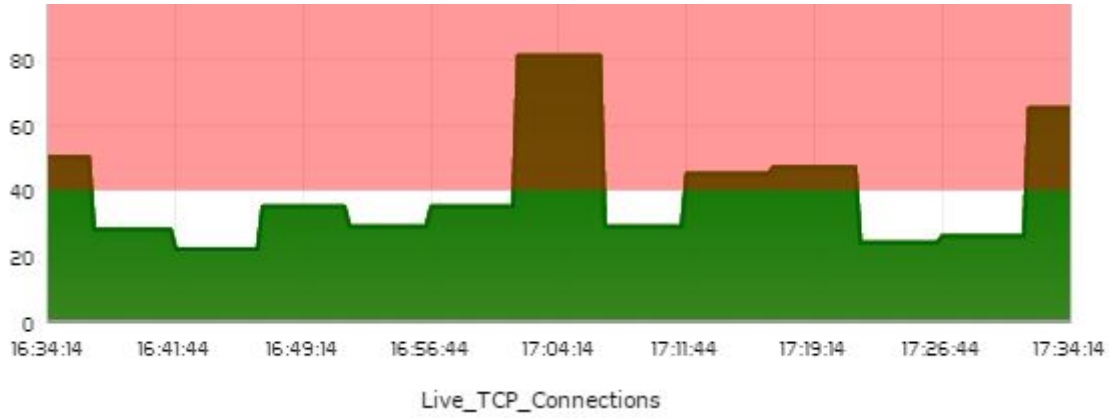


- Dynamic Threshold Interval : Intervalle de temps qui sera considéré pour effectuer le calcul des seuils. Si nous choisissons 1 mois, le système prendra toutes les données existantes du dernier mois et construira les seuils en fonction de ces données et des seuils avec des valuers au dessus de la moyenne seront établies.
- Dynamic Threshold Max. : Valeur maximale du seuil dynamique critique, si vous décidez d'établir un pourcentage pour ça. Par exemple : si les valeurs moyennes sont autour de 60 et que le seuil critique a été établi à partir de la valeur 80, si nous établissons la valeur *Dynamic threshold Max : 10*, nous allons augmenter ce seuil critique de 10%, le laissant à 88.
- Dynamic Threshold Two Tailed : (désactivé par défaut), ils sont des intervalles de seuils dynamiques, si cette option est activé, le système de seuils dynamiques aussi établira les seuils sous la moyenne.
- Dynamic Threshold Min. : Il permet de réduire la limite inférieure du pourcentage que nous indiquons. Par exemple, si les valeurs moyennes sont autour de 60 et que le seuil critique inférieur a été fixé à 40, si nous fixons la valeur *Dynamic Threshold Min: 10*, nous réduirons ce seuil critique de 10%, le laissant à 36.

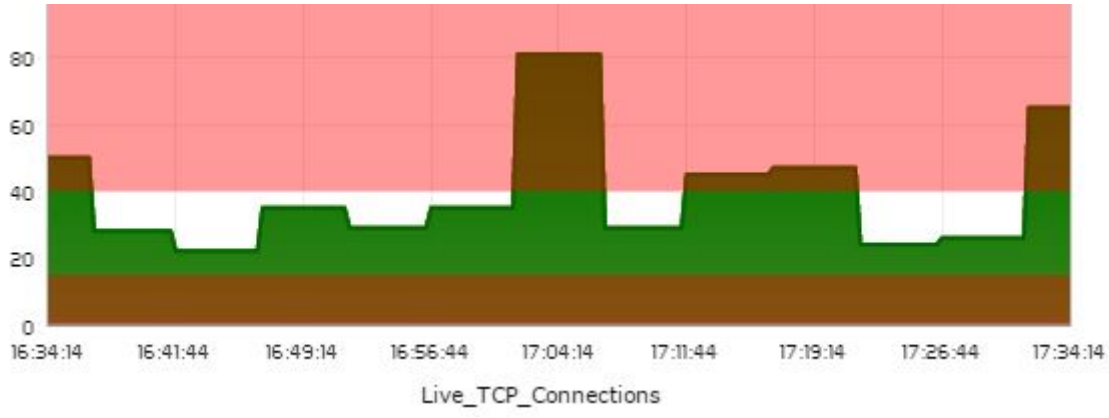
Cas pratique

Dans l'exemple suivant, la valeur moyenne calculée est à la hauteur de la ligne rouge (environ 30) :

Lors de l'activation des seuils dynamiques, le seuil supérieur (env. 45 et plus) a été réglé de cette manière :

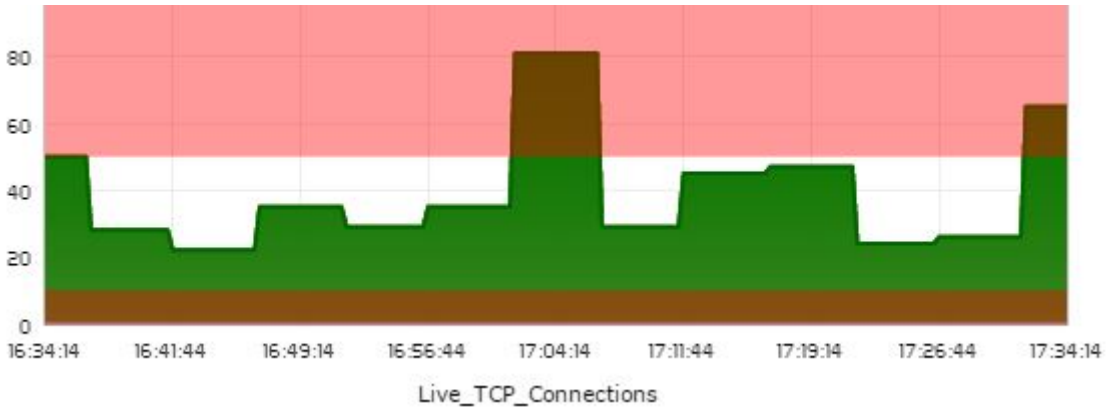


Nous avons activé le paramètre *Dynamic Threshold Two Tailed*, de sorte qu'un seuil critique a également été fixé en dessous des valeurs moyennes (environ 15 et en dessous) :



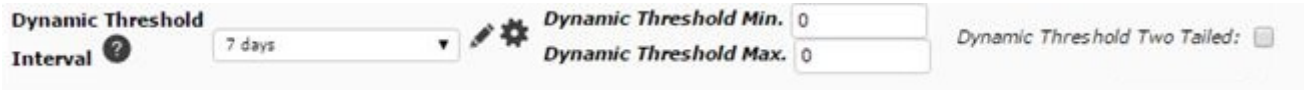
Nous avons maintenant réglé les paramètres *Dynamic Threshold Min.* et *Dynamic Threshold Max.* sur 20 et 30 respectivement, de sorte que les seuils ont été ouverts, étant légèrement plus

permissifs :



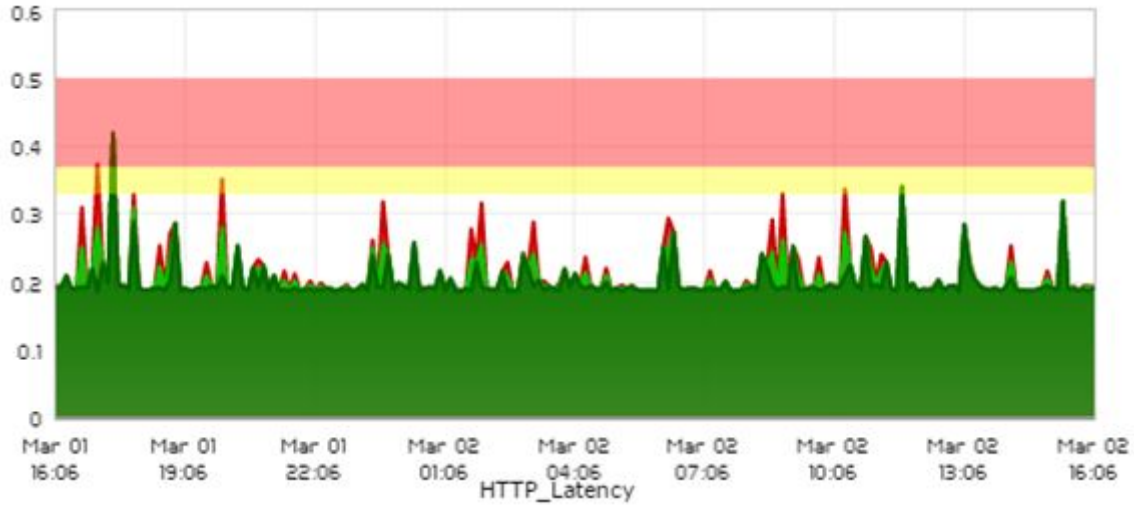
Cas pratique 2

Nous partons d'un module de latence web. La configuration de base que nous avons utilisée tient compte d'un intervalle d'une semaine :



Lors de l'enregistrement des modifications, après avoir lancé pandora_db, les seuils ont été définis de cette façon :

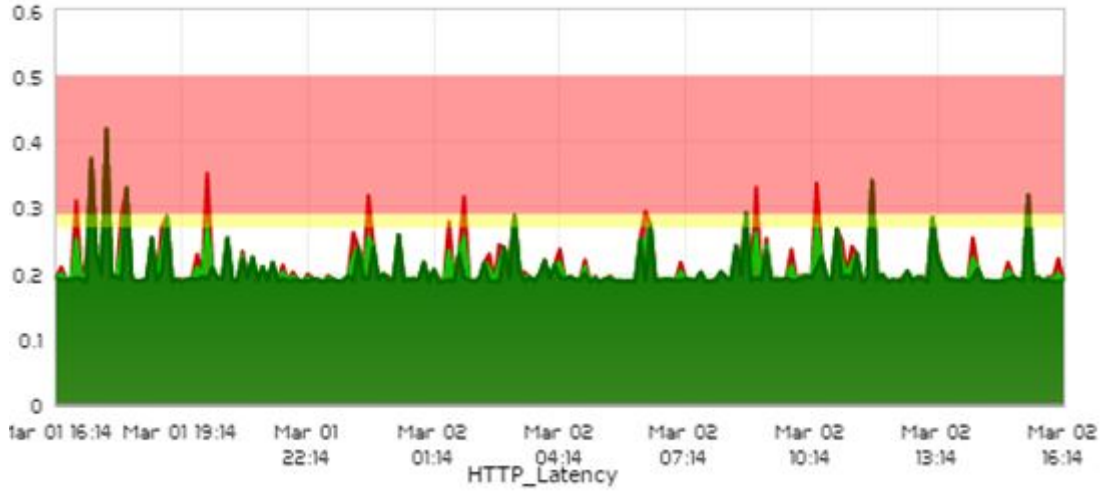
Le module passe donc à l'état *warning* lorsque la latence est supérieure à 0'33 secondes, et à l'état *critical* lorsqu'elle est supérieure à 0'37 secondes. Le graphique le montre comme suit :



Il a été considéré que le seuil est quelque peu permissif, c'est pourquoi il a été décidé d'utiliser le paramètre *Dynamic Threshold Min.* pour réduire les seuils minimaux. Comme dans ce cas, le seuil n'a pas de valeurs maximales car toute valeur supérieure à une certaine valeur sera considérée comme incorrecte, nous n'utiliserons pas *Dynamic Threshold Max.*. La modification apportée est la suivante :

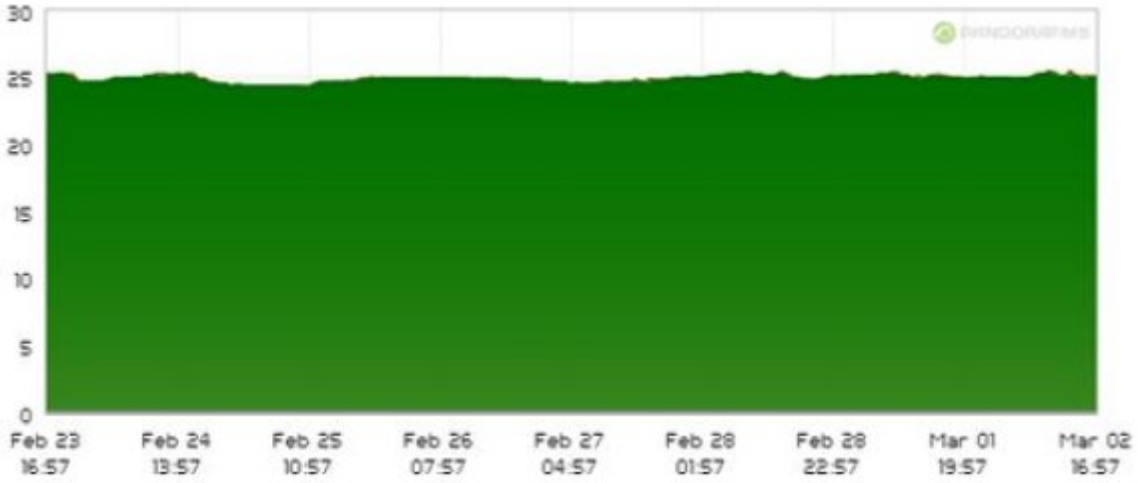
Après l'application des changements et l'exécution de *pandora_db*, les seuils sont fixés comme suit :

Et le graphique ressemblera à ceci :

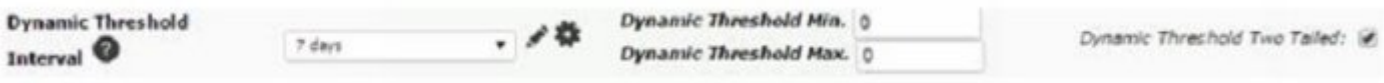


Cas pratique 3

Dans cet exemple nous supervisons la temperature d'un salle de contrôle ou un CPD. La graphique représente les valeurs avec peu de variation :

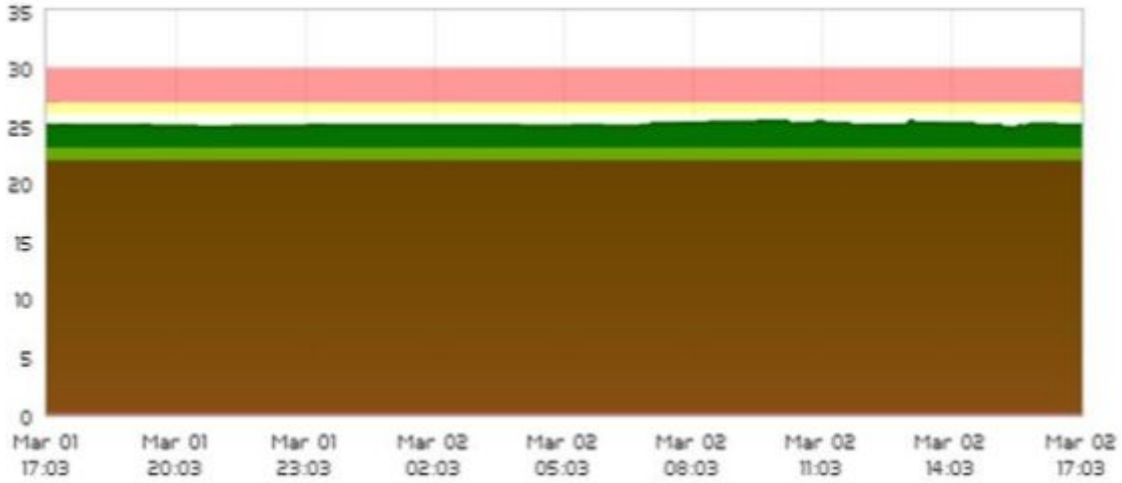


Dans cette situation, il est fondamentale que la température soit estable dans un intervalle précis, donc on utilisera le paramètre *Dynamic Threshold Two Tailed* pour délimiter les seuils sous et au dessus. La configuration est la suivante :



Les seuils générés automatiquement sont les suivants :

Las graphique les montre ainsi :



DeAinsi ils seront considérés normales tous les valeurs entre 23'10 *et 26'0*, puisque c'est la température acceptable dans l'environnement à superviser. Si vous en avez besoin, vous pourriez utiliser les paramètres *Dynamic Threshold Min.* et *Dynamic Threshold Max.* une autre fois pour établir les seuils.

Paramètres de configuration additionnels

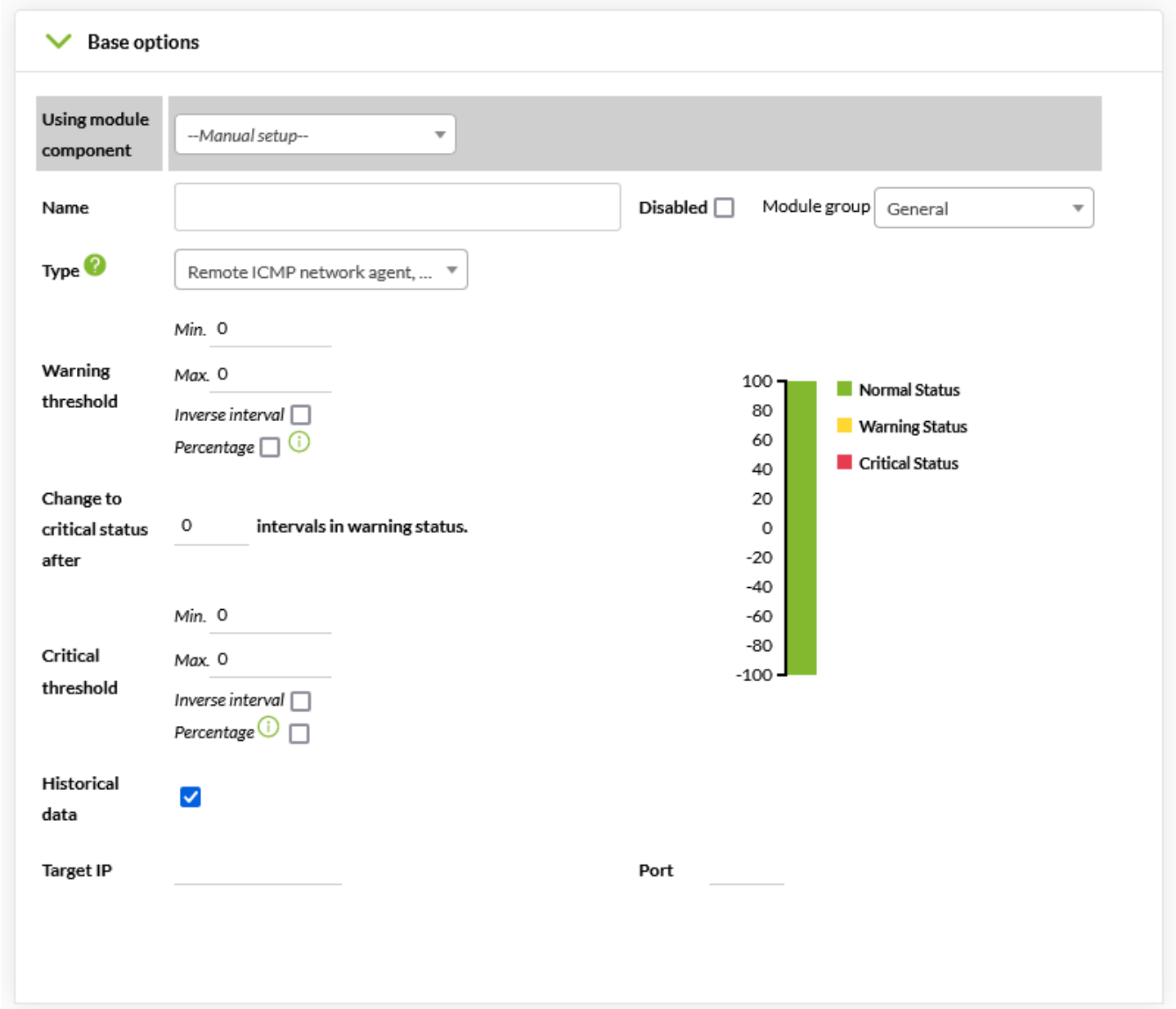
Il y a aussi plusieurs paramètres de configuration supplémentaires dans le fichier pandora_server.conf.

- dynamic_updates : Ce paramètre détermine combien de fois les seuils sont recalculés pendant la période définie dans *Intervalle seuil dynamique*. Si nous configurons l'intervalle de seuil dynamique avec une valeur de 1 semaine, par défaut les données sont collectées à partir d'une semaine en arrière et le calcul est fait une seule fois, en répétant le processus après une semaine. Si nous modifions le paramètre *dynamic_updates* nous pourrions augmenter cette fréquence. Par exemple, si vous configurez le paramètre avec une valeur de 3, les seuils seront recalculés jusqu'à trois fois au cours d'une semaine (ou la période que nous avons configurée dans *Dynamic Threshold Interval*) Sa valeur par défaut est 5.
- Dynamic_warning : différence entre le seuils `warning` et `critical`, en pourcentage. Sa valeur par défaut est 25.
- dynamic_constant : détermine l'écart de la moyenne qui sera utilisée pour établir les seuils ; des

valeurs plus élevées éloignent les seuils des valeurs moyennes. Sa valeur par défaut est 10.

Options de base

Gardez toujours à l'esprit que cette interface est utilisée à la fois par la surveillance locale et la surveillance à distance et qu'elle présente des paramètres qui sont valables dans l'un ou l'autre domaine. Par exemple, les paramètres Timeout et Retries ne sont pas utiles pour la supervision locale (contrôles locaux) mais sont importants pour la supervision à distance.



- Using module component : Lors de l'utilisation d'un composant de module, les paramètres nécessaires seront remplis automatiquement pour effectuer la supervision. Ce token apparaît dans

tous les types de modules, à l'exception des modules de prédiction.
- Name : Nom du module.
- Disabled : Il permet de désactiver le module.
- Module group : Il permet d'affecter le module à un groupe de modules défini.
- Type : Type de module en fonction du type de données renvoyées. En sélectionnant Using module component, le type de données sera choisi automatiquement.
- Warning threshold et Critical threshold : Seuils qui, lorsqu'ils sont atteints par la valeur renvoyée, font le module devenir en état d'avertissement. (Warning) ou état critique (Critical). Vous pouvez utiliser l'Inverse interval pour définir que l'état d'avertissement/critique *est toute valeur en dehors de cette plage*.
- Change to critical status after X intervals in warning status : À partir de la version 766 de PFMS, il existe la possibilité de *favoriser* le passage d'un module à l'état critique s'il a été en état d'avertissement le même nombre de fois de suite (intervalles de supervision continue) en état d'alerte. La principale différence avec le seuil FF est que cette fonctionnalité retarde le changement d'état alors que le Change to critical status after après le favorise. Gardez toujours à l'esprit que les deux options fonctionnent en conjonction l'une avec l'autre.
- Historical data : Cochez cette option si vous devez stocker des valeurs dans la base de données historique à long terme.
- Target IP y Port : Adresse IP et numéro de port à interroger pour les valeurs de supervision. Dans certains cas, comme pour la supervision WMI, des champs de texte supplémentaires apparaissent pour définir les informations d'identification de la connexion et même les chaînes de requête.

Options avancées

Gardez toujours à l'esprit que cette interface est utilisée à la fois par la surveillance locale et la surveillance à distance et qu'elle présente des paramètres qui sont valables dans l'un ou l'autre domaine. Par exemple, les paramètres Timeout et Retries ne sont pas utiles pour la surveillance locale (contrôles locaux) mais sont importants pour la surveillance à distance.

- Custom ID: Champ permettant de stocker une valeur d'identification personnalisée.
- Unit: Election de l'unité des données reçues par le module, par défaut désactivé (*none*). Vous pouvez soit choisir une unité spécifique (*Timeticks*, *Bytes*, *Entries*, etc.) ou cliquez sur l'icône du crayon pour définir des unités personnalisées.
- Interval: Période dans laquelle le module doit renvoyer les données. Si un module passe plus de deux intervalles sans recevoir de données, il entrera dans un état inconnu:

1. Dans le cas des modules distants: Il s'agit de la période pendant laquelle le contrôle à distance est effectué.
2. Dans le cas des modules de données: Il s'agit d'une valeur numérique qui représente X fois l'intervalle d'agent défini, effectuant le contrôle local pendant cette période.
3. Dans le cas des agents de courtage via la console Web, à partir de la version 776, leur intervalle n'est pas affiché afin d'éviter des changements non désirés.

- Post process: Paramètre par lequel les données reçues par le module peuvent être converties. Par défaut, il est désactivé avec la valeur 0. Vous pouvez également définir des conversions personnalisées en cliquant sur l'icône en forme de crayon.

- Min. Value et Max. Value: Permet de définir une valeur minimale et maximale attendue pour le module.
- Dynamic Threshold Interval: Champs réservés à la surveillance dynamique (seuils dynamiques).
- Export target: Si vous avez configuré un serveur d'exportation, vous pouvez en créer un.
- Discard unknown events: Permet d'écarter les événements inconnus.
- FF threshold: connu sous le nom de Flip-Flop (FF), il est un phénomène courant dans la supervision, quand une valeur oscille fréquemment entre des valeurs alternatives (MAL/BIEN), ce qui la rend difficile à interpréter. Dans ce cas, on utilise généralement un « seuil », de sorte que pour considérer que quelque chose a changé d'état, il doit « rester » plus de X intervalles consécutifs dans un état non modifié. *FF Threshold* est utilisé pour « filtrer » les changements continués d'état dans la génération d'événements / états: ainsi Pandora FMS « sait » qu'un état n'est pas considéré comme changé jusqu'à ce que l'élément soit au moins X fois sur le même état après avoir changé son état original.
    - FF Interval: Permet de spécifier un intervalle de temps plus court pour le prochain contrôle si un seuil de basculement est activé dans le module. Lorsque FF est activé et qu'un changement d'état est détecté qui répond aux conditions de contrôle définies, l'intervalle du module pour la prochaine exécution sera ajusté. Ce réglage permet d'accélérer les contrôles lorsque des conditions spécifiques sont requises, en définissant une valeur inférieure à l'intervalle du module principal.
    - FlipFlop timeout: Temps d'attente pour les modules asynchrones. Pour qu'un changement d'état par bascule soit efficace, des données consécutives égales doivent être reçues dans l'intervalle spécifié.

Pour le calcul des Accords de niveau de service (SLA), si aucun seuil SLA n'est défini, Pandora FMS prendra en compte les seuils FF.

- Tags available et Tags from policy: Elles sont détaillées dans la section suivante "Tags".
- Quiet: Le module continuera à recevoir des informations, mais aucun type d'événement ou d'alerte ne sera généré.
- Cascade Protection Services: Paramètre par lequel la génération d'événements et d'alertes passerait au service auquel il appartient, si cette fonctionnalité est activée.
- Critical instructions, Warning instructions et Unknown instructions: Contient les instructions à suivre si l'état du module devient critique, avertissement ou inconnu. Utile dans l'utilisation des modèles et des composants.
- Cron: Vous pouvez spécifier des périodes de temps dans lesquels le module sera exécuté ; il a la nomenclature: minute, heure, jour du mois, mois, jour de la semaine et il y a de différentes possibilités :
    - Cron from → Il n'y a aucune restriction de surveillance (par défaut), il a Any établi par défaut dans tous les champs.
    - Cron from → valeur spécifique et Cron to → tous dans Any: il sera exécuté seulement lorsqu'il coincide avec le numéro établi. Exemple: 15 20 * * *, fonctionnera tous les jours à 20:15
    - Cron from → valeur spécifique et Cron to → valeur spécifique: il sera exécuté pendant l'intervalle. Exemple: 5-10 * * * * , fonctionne toutes les heures entre les minutes 5 et 10.
    - Timeout: Temps d'attente de l'agent pour l'exécution du module, exprimé en secondes.
    - Retries: Définit le nombre de tentatives pour l'exécution du module.
- Category: Cette catégorisation n'a aucun effet depuis l'interface utilisateur normale. Elle est destinée à être utilisée en conjonction avec la Métaconsole.
- Module parent: Utilisé pour établir la hiérarchie de la protection dans le service de protection en cascade (Cascade Protection Services).
- Custom macros (Macros personnalisées): N'importe quel nombre de macros de module peut être

défini. Le format recommandé pour les noms de macros est le suivant `_macroname_`.

Les macros dynamiques auront un format spécial commençant par @ et auront ces substitutions possibles:

- `@DATE_FORMAT` (date/heure actuelle avec format défini par l'utilisateur)
- `@DATE_FORMAT_nh` (heures)
- `@DATE_FORMAT_nm` (minutes)
- `@DATE_FORMAT_nd` (jours)
- `@DATE_FORMAT_ns` (secondes)
- `@DATE_FORMAT_nM` (mois)
- `@DATE_FORMAT_nY` (années)

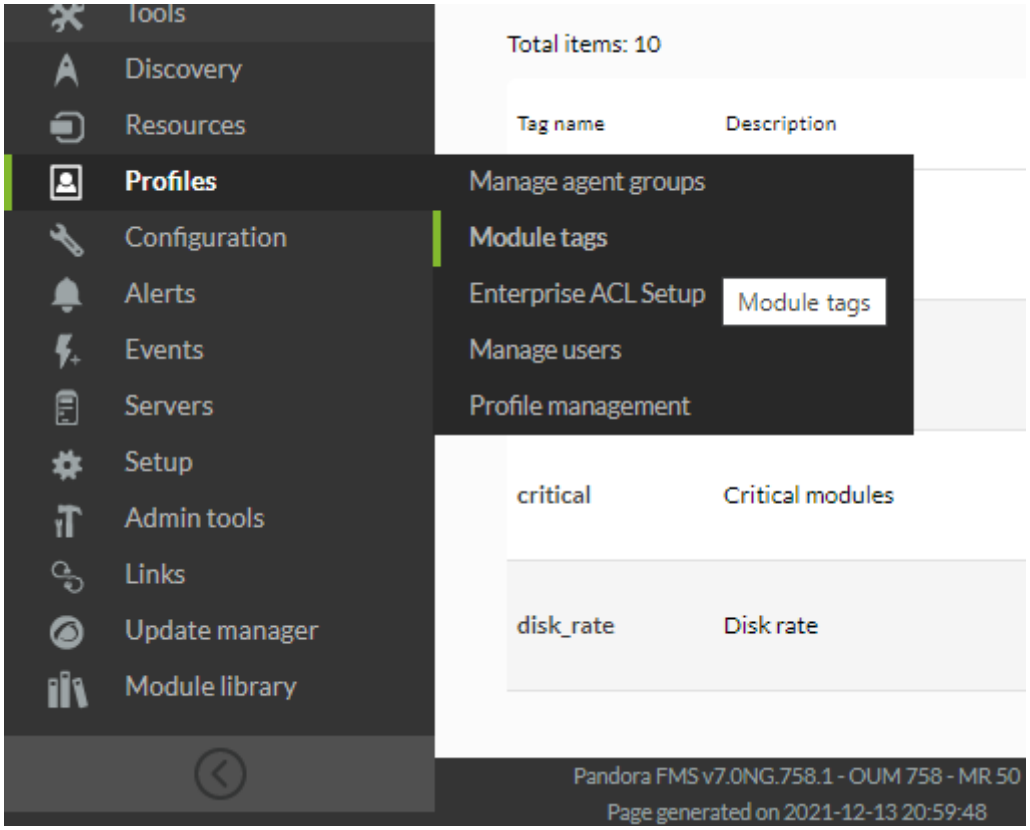
Où « n » peut être un nombre sans signe positif ou négatif et FORMAT strftime de Perl.

- Module relations: Utilisé pour remplacer le module, soit directement (Direct) ou en cas de basculement (Failover), dans le but de calculer les SLA.
- Ignore unknown: Cela désactive le calcul de l'état inconnu dans le module, de sorte que la transition vers l'état inconnu n'a jamais lieu. L'état qu'il reflète est le dernier état connu.

Tags

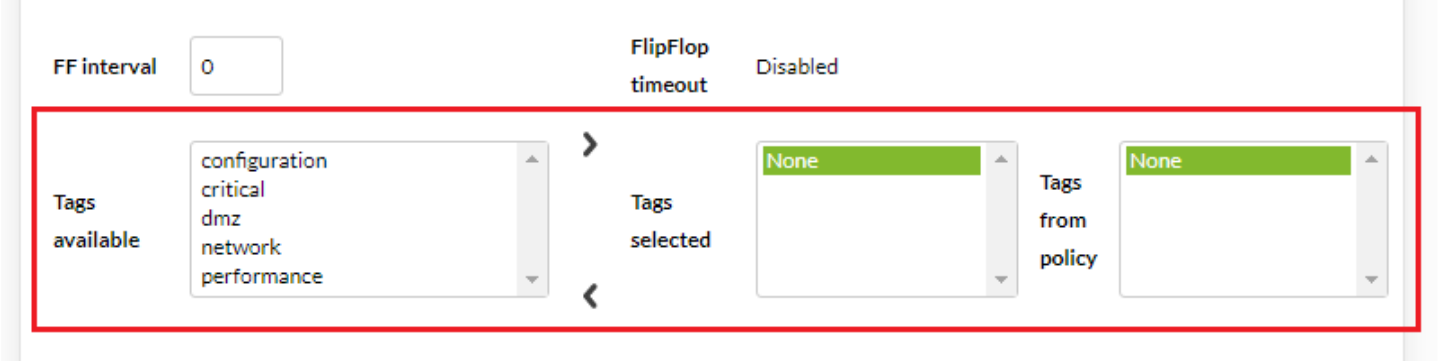
Les *tags* sont des étiquettes associées à chaque module qui seront propagées aux événements générés par ce module et peuvent être utilisées dans les alertes d'événements de ce module. Les tags sont utiles car ils permettent de les utiliser comme filtres dans les rapports, les vues d'événements et même d'avoir des vues spécifiques pour eux. Les informations complémentaires du *tag* (URL, *email*, téléphone) peuvent être utilisées dans les alertes, car elles sont disponibles sous forme de macro.

Pour créer ou modifier un tag, cliquez sur Module tags :



Le *tag* permet de définir un nom, une description et éventuellement une URL complète, *email* ou téléphone associé à ce *tag*. Il est à noter que vous pouvez associer un ou plusieurs *tags* à chaque module. Pour ce faire, ils doivent d'abord être créés comme décrit ci-dessus. Une fois créés, ils seront disponibles pour être assignés à chaque module.

Dans les options avancées d'un module, les *tags* disponibles seront affichées dans la colonne de gauche et dans la colonne de droite les *tags* déjà associées au module :



Les tags peuvent également être utilisées pour accorder des permissions d'accès spécifiques à un module, de sorte qu'un utilisateur ne peut accéder qu'à un seul module de l'agent, sans avoir accès au reste des modules. Ceci peut être vu dans la section profil des utilisateurs dans gestion et administration.

Supervision dynamique (seuils dynamiques)

La supervision dynamique consiste en l'ajustement dynamique et automatique des seuils d'état des modules de manière prédictive. Le mode de fonctionnement consiste à collecter les valeurs pour une période donnée et à calculer une moyenne et un écart type, qui servent à établir les seuils correspondants au niveau du module. Les paramètres se situent dans les options avancées des modules :

- Dynamic Threshold Interval : L'intervalle de seuil dynamique ou durée qui sera prise en compte pour effectuer le calcul du seuil. Si un mois est choisi, le système prendra toutes les données existant au cours du dernier mois et construira les seuils en fonction de ces données et les seuils seront établis avec des valeurs au-dessus de la moyenne.
- Dynamic Threshold Max. : La valeur maximale du seuil dynamique critique, s'il est décidé d'établir une marge de tolérance (en pourcentage) pour celui-ci ; Par exemple, si les valeurs moyennes sont autour de 60 et que le seuil critique a été établi à partir de la valeur 80, si la valeur Dynamic Threshold Max: 10 est définie, ce seuil critique sera augmenté de 10 %, il restera donc à une valeur de 88.
- Dynamic Threshold Min. : Il permet de réduire la limite inférieure du pourcentage indiqué. Par exemple, si les valeurs moyennes sont autour de 60 et que le seuil critique inférieur a été fixé à une valeur de 40, si la valeur Dynamic Threshold Min: 10 est définie, ce seuil critique sera réduit de 10 %, donc il reste à une valeur de 36.
- Dynamic Threshold Two Tailed : Il s'agit d'intervalles de seuil dynamiques, inactifs par défaut. Si cette option est activée, le système de seuils dynamiques également fixera des seuils en dessous de la moyenne.

Librairie de modules

Pour y accéder depuis le menu, vous devrez avoir *Agent Read* (AR) permis.

Accédez à Management → Module library → View pour accéder à la vue principale. Vous pouvez également effectuer des regroupements par catégories (bases de données, virtualisation, etc.) ou rechercher le plugin par son nom dans la zone de texte Search.

Les liens de téléchargement seront visibles dans ces cas :

- L'utilisateur et le mot de pass que vous configurez dans le *setup* doivent coïncider avec celui du support d'Pandora ITSM.
- L'utilisateur Pandora FMS a permis AW.

Pour plus d'informations sur comment accéder à la librairie, visitez la section de la Configuration de la console.

Retour à l'index de documentation du Pandora FMS