PANDORAFMS

Événements

Événements

Introduction

Le système d'événements Pandora FMS vous permet de voir un enregistrement en temps réel de tous les événements qui se produisent dans les systèmes supervisés. Par défaut, dans la vue des événements, vous verrez un instantané de ce qui se passe à ce moment-là.

Les événements constituent un enregistrement et un élément fondamental d'un système de supervision.

Les événements sont classés selon leur gravité :

- 0 Maintenance (blanc/gris).
- 1 Informatif (bleu).
- 2 Normal (vert).
- 3 Avertissement (jaune).
- 4 Critique (rouge).
- 5 Minoritaire (rose).
- 6 Majoritaire (brun).

Les actions suivantes peuvent être effectuées sur les événements :

- Modifier l'état (validé ou en cours).
- Changer de propriétaire.
- Éliminer.
- Afficher des informations supplémentaires.
- Ajouter un commentaire.
- Créer des réponses personnalisables.

Informations générales

Les événements sont gérés dans le menu Opérations → Événements → Afficher les événements.

L'observateur d'événements affiche un résumé de chaque événement et parfois d'autres données associées, telles que le module agent qui a généré l'événement, le groupe, les balises associées au module, etc. Vous pouvez également trier les événements par identifiant, état, nom, entre autres champs.

En cliquant sur l'icône en forme de loupe pour chaque élément, vous obtiendrez plus de détails.

- L'utilisateur ne pourra voir que les groupes auxquels il appartient, sauf si ledit utilisateur

appartient explicitement au groupe TOUS (ALL).
- Pandora FMS peut également utiliser des événements pour annoncer que les limites imposées par les utilisateurs au système de supervision ont été dépassées. Par exemple, à partir de la version NG 754 vous pouvez imposer une limite d'Agents dans un groupe donné et lorsque cette limite est atteinte cela sera signalé par un événement.

Les événements sont présentés par recherche par défaut des huit dernières heures et qui ne sont pas validés (et peuvent également être personnalisés), en plus d'un regroupement pour éviter les redondances. Vous pouvez enregistrer les recherches sous forme de filtres ou appliquer un filtre préalablement créé.

Fonctionnement avec événements

Validation et états d'un événement. Auto-validation

Un événement peut être dans quatre états :

- En procès.
- Nouveau.
- Pas validé.
- Validé.

Auto-validation

Lorsque des événements surviennent du fait de changements d'état dans des modules, il y aura généralement deux événements : un premier événement de passage d'un état normal à un autre état « incorrect », et un événement de retour à un état normal, une fois la situation problématique résolue. Dans ces cas, les événements passés dans un état incorrect (critique ou avertissement) sont automatiquement validés lorsqu'ils reviennent à la normale. C'est ce qu'on appelle l'auto-validation d'événement et c'est une fonctionnalité extrêmement pratique.

Validation manuelle

En travaillant manuellement, un événement peut également être validé : le système mémorisera la date et l'utilisateur qui a validé l'événement, avec la possibilité d'enregistrer un commentaire sur la situation, puis l'écran sera rafraîchi et l'événement validé deviendra invisible.

Notez qu'en outre, dans les actions, il y a plus d'options telles que l'exécution de réponses personnalisées telles que le ping de l'hôte, l'attribution d'un utilisateur, entre autres.

En procès

Un événement peut être marqué « en cours » dans l'onglet Réponses. De cette façon, l'événement ne sera pas auto-validé et restera en attente.

Processus individuels ou par lots

Les événements peuvent être validés, marqués comme « en cours » ou supprimés individuellement en cliquant sur les icônes correspondantes ou appliqués en masse à une sélection.

Pour les réponses personnalisées, le nombre maximum d'événements auxquels l'opération peut être appliquée est limité à dix.

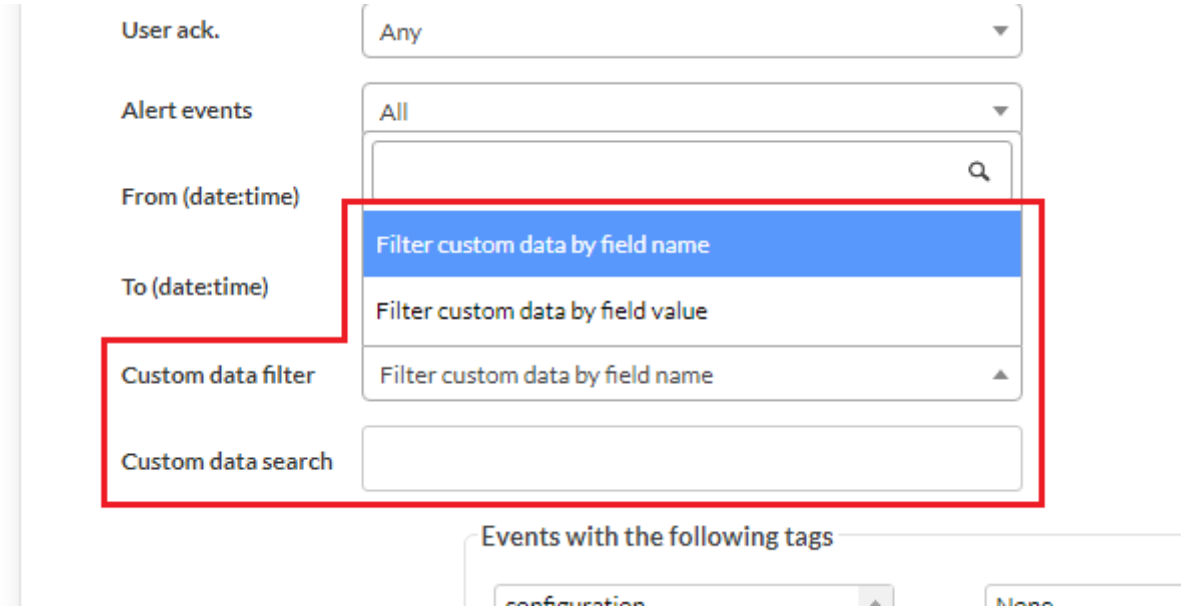
Filtrage des événements

Aspects importants de cette fonctionnalité :

- Les filtres peuvent être enregistrés pour être réutilisés une autre fois.
- L'ancienneté maximale (Max. hours old) des événements peut être personnalisée.
- Pandora FMS, par défaut, regroupe les événements répétés (Dupliquer → Grouper les événements), cependant cette préférence peut être modifiée :
    - Tous les événements : affiche tous les événements individuellement.
    - Grouper les agents : regrouper les événements par agent.
    - Événements de groupe : le nom de l'événement, l'ID de l'agent et l'ID du module sont utilisés pour identifier les doublons.
    - Identifiants supplémentaires de groupe : les événements seront regroupés uniquement par Extra ID, classé par Timestamp.
- Vous pouvez filtrer par groupe spécifique. Si vous utilisez l'option Récursion de groupe, elle recherchera également les sous-groupes de ce groupe. De même, si vous sélectionnez Rechercher dans les groupes secondaires, les événements des agents auxquels des groupes secondaires sont attribués seront inclus. Ces deux dernières options peuvent avoir un impact sur le travail sur le serveur PFMS.

Options avancées

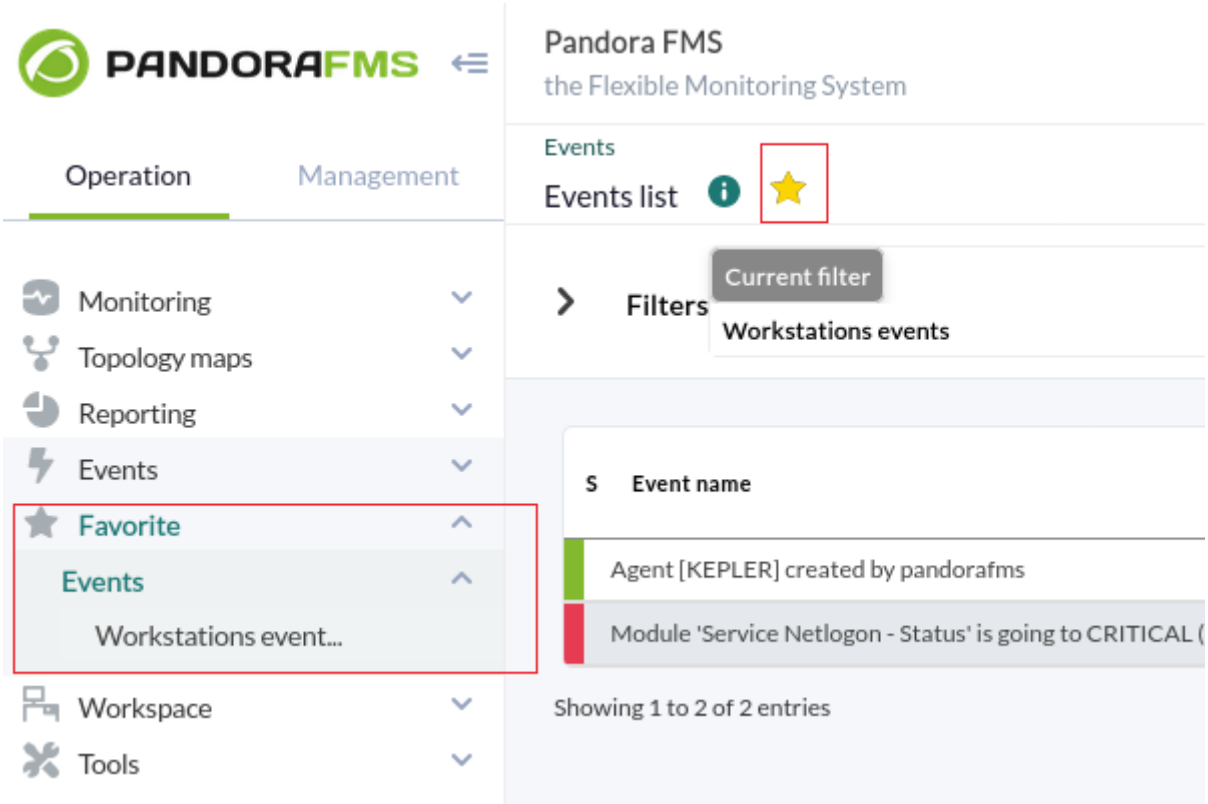
- Vous pouvez demander des événements qui se sont produits dans une période donnée en utilisant les champs de date Du (date) et Au (date).
- Dans le champ Free search, vous pouvez utiliser une expression régulière (par exemple, pour rechercher « Connexions » et « Réseau », vous saisissez « (Connexions|Réseau) »). La recherche est effectuée par nom d'agent, nom d'événement, ID supplémentaire, source, données personnalisées et commentaires.
- Vous pouvez filtrer par champs personnalisés à l'aide des champs Filtre de données personnalisé, soit en filtrant le nom du champ (Filtrer les données personnalisées par nom de champ), soit par le contenu du champ personnalisé (Filtrer les données personnalisées données par valeur de champ). Ces champs seront affichés sous forme de colonnes dans la vue des événements.



Filtres favoris

Version 770 ou ultérieure

Les filtres d'événements considérés comme plus fréquemment utilisés peuvent être ajoutés à la section Événements du menu Favoris (menu Opération). Ceci est réalisé en cliquant sur l'icône étoile qui apparaîtra lors du chargement d'un filtre enregistré (Filtre actuel). Un nouveau clic vous permettra de décocher l'icône et de la supprimer du favorite system.



Suppression d'événements

Les événements peuvent être supprimés individuellement (manuellement) et/ou automatiquement : dans le menu Gestion → Setup → Setup → Max. jours avant la suppression des événements, la période à conserver est spécifiée en jours.

Dans la version Entreprise, activer Activer l'historique des événements dans Gestion → Configuration → Configuration → Base de données historique, il est possible de les conserver dans le but de créer des rapports spéciaux.

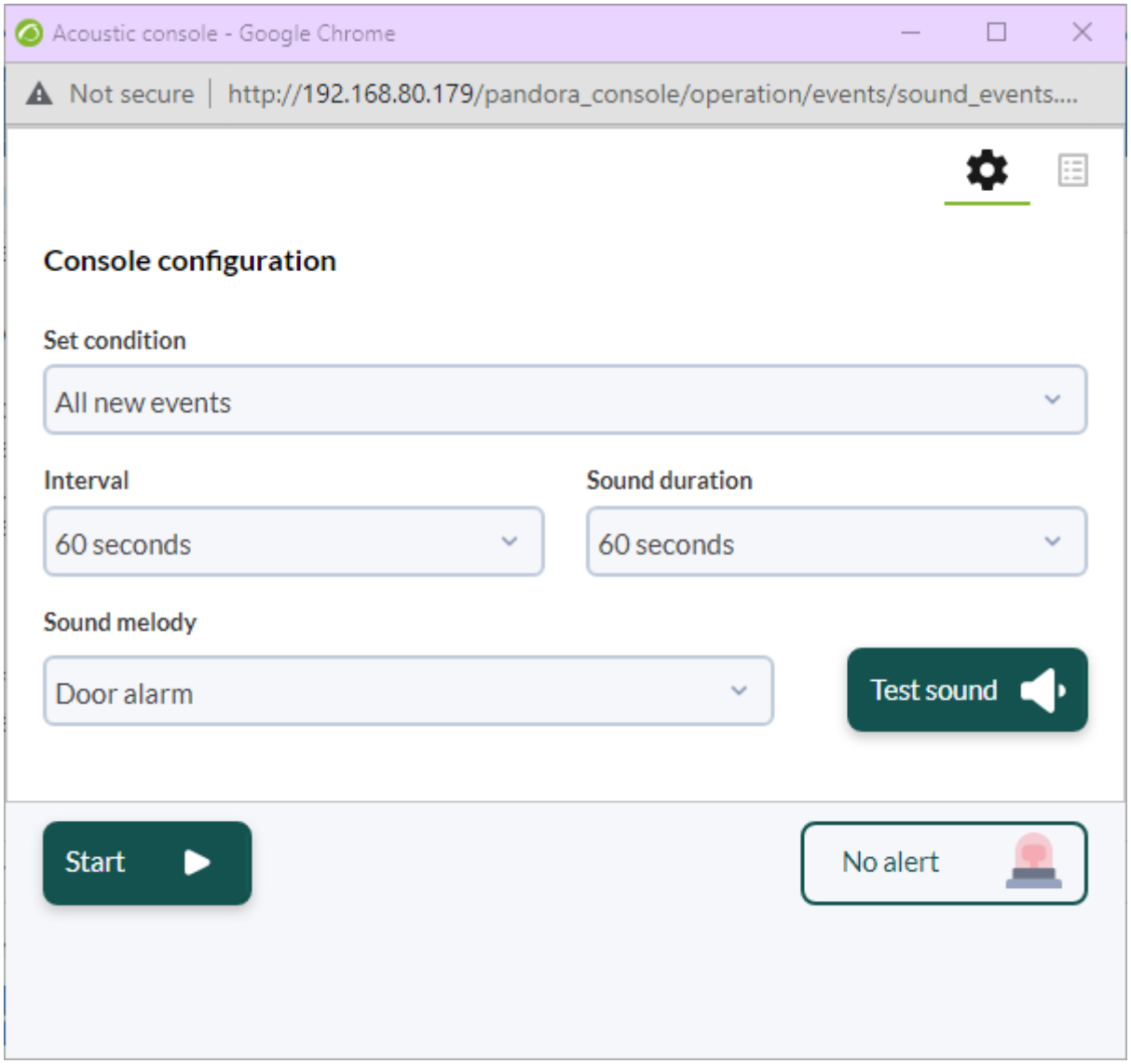
Événements en RSS

- Afin d'accéder au flux RSS des événements, il est nécessaire de configurer les adresses IP autorisées à accéder dans le champ Liste IP avec accès API dans Setup.
- Vous aurez également besoin d'un lecteur RSS tel que Inoreader, Selfoss ou de votre lecteur RSS préféré.

Pour voir les événements sur une chaîne d'information, accédez à Opération → Événements → RSS et avec ce lien, abonnez-vous depuis le lecteur d'actualités de votre choix.

Console d'événements sonores

Il permet de diffuser les différentes alertes sonores lorsqu'un événement survient. La mélodie sera entendue en continu jusqu'à ce que vous mettiez l'événement sonore en pause ou que vous appuyiez sur le bouton OK.



Liste des événements qui génèrent du son, par défaut (et personnalisables) :

- Le déclenchement de toute alerte.
- La transition d'un module vers l'état avertissement.
- Le passage d'un module à l'état critique.
- La transition d'un module vers le statut inconnu.

Accédez à l'option Opération → Événements → Console acoustique. Cette action ouvre une fenêtre contextuelle contrôlant tous les événements sonores. Vous devez configurer votre navigateur Web pour autoriser l'ouverture des fenêtres contextuelles.

Si vous réduisez la fenêtre Acoustic Console, elle ne fonctionnera pas comme prévu.

Les événements sonores sont analysés toutes les 10 secondes de manière asynchrone, lorsqu'un événement se produit, la fenêtre commencera à clignoter en rouge et à vibrer et également, selon la configuration de votre navigateur et/ou système d'exploitation, la fenêtre conservera le focus et sera positionnée en devant le reste des fenêtres ouvertes.

Seuls les événements qui se produisent depuis et pendant que la fenêtre précédente reste ouverte, correspondent à ceux sélectionnés et pour lesquels une alerte sonore est configurée seront alertés avec du son.

Paramètres avancés

Pour ajouter de nouvelles mélodies, copiez ces fichiers au format WAV, dans le répertoire :

```
/var/www/pandora_console/include/sounds/
```

Exporter les événements au format CSV

Pour exporter les événements au format CSV, appuyez sur Opération → Événements → Afficher les événements → Exporter vers un fichier CSV.

Alertes d'événement. Corrélation des événements

Pour la version 741 ou supérieure il existe la gestion des alertes liées aux événements, sujet abordé dans un chapitre séparé.

Événements de la ligne de commande

Création et validation d'événement

La API externe Pandora FMS est utilisé en effectuant des appels à distance (via HTTPS) vers le fichier `/include/api.php`. C'est la méthode qui a été définie dans Pandora FMS pour intégrer des applications tierces à Pandora FMS. Fondamentalement, il s'agit d'un appel avec les paramètres formatés pour recevoir une valeur ou une liste de valeurs que l'application utilisera ensuite pour effectuer des opérations.

Les trois points principaux pour activer l'API PFMS :

1. Activez l'accès à l'IP à partir de laquelle vous exécuterez la commande.
2. Définissez un mot de passe général pour l'API.
3. Définissez un utilisateur spécifique avec son mot de passe qui ne peut se connecter que via API.

L'outil dédié à la création ou à la validation d'événements via l'API Pandora FMS peut être copié depuis :

```
/usr/share/pandora_server/util/pandora_revent.pl
```

Lorsqu'il est exécuté sur l'appareil client, sans paramètres, vous pourrez voir la syntaxe complète.

Les options pour valider un événement sont :

```
./pandora_revent.pl -p <chemin_vers_consoleAPI> -u <informations
d'identification> -validate_event <options> -id <event_id>
```

Pour que les champs de déclaration « inconnu », « critique » ou « avertissement » apparaissent dans les détails de l'événement généré, l'événement doit être de type « going_unknown », « going_down_critical » ou `going_down_warning`, respectivement.

Dans certaines occasions, peut-être pour des raisons de sécurité, vous devez uniquement avoir la possibilité de créer des événements, pour cela vous pouvez copier « pandora_revent_create.pl » sur l'appareil client. Il est situé à :

```
/usr/share/pandora_server/util/pandora_revent_create.pl
```

Cet outil partage des caractéristiques similaires avec `pandora_revent.pl`.

Utilisation de champs personnalisés dans les événements

Les événements avec des champs personnalisés peuvent être générés via la Pandora FMS CLI. Exemple:

```
perl pandora_manage.pl \
             /etc/pandora/pandora_server.conf \
             --create_event 'Événement personnalisé' Pare-feu système \
             'localhost' 'module' 0 4 '' 'admin' '' '' '' '' \
             '{"Emplacement": "Bureau", "Priorité": 42}'
```

Paramètres d'événement

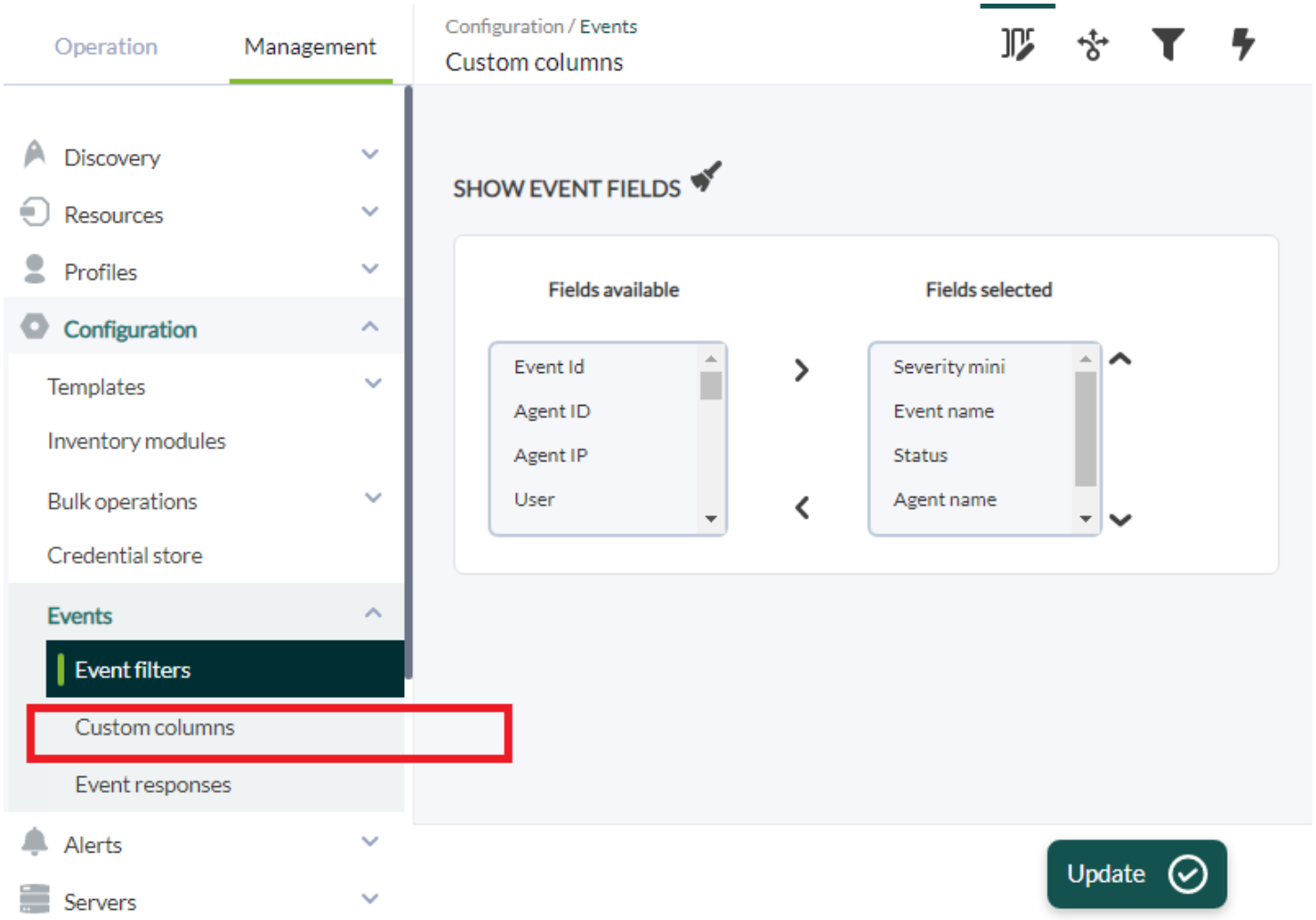
Grâce à Gestion → Configuration → Événements, il est possible de configurer :

- Colonnes personnalisées.
- Réponses.

- Paramètres de filtre.

Personnalisation de la vue des événements

Il est possible de personnaliser les champs que l'observateur d'événements affiche par défaut ; Pour cela, depuis Événements → Voir les événements, cliquez sur Gérer les événements → Colonnes personnalisées et choisissez les champs à afficher.



Les champs affichés par défaut sont au nombre de cinq, mais il y a d'autres champs à ajouter :

- Event ID.
- Agent name.
- User.
- Group.
- Event type.
- Module name.
- Alert.
- Severity.
- Comment.
- Tags.

- Source.

- Extra ID.
- Owner.
- ACK Timestamp.
- Instructions.
- Server name.
- Data.
- Module status.
- Module custom ID.

Création de filtres d'événements

Menu Gestion → Configuration → Événements → Filtres d'événements.

Vous permet de créer, supprimer et modifier les filtres appliqués à la vue des événements. Après avoir enregistré, vous pouvez accéder à Afficher les événements et charger le filtre approprié.

Event Responses

Introduction

Une réponse à un événement est une action personnalisée qui peut être exécutée sur un événement, telle que la création d'un ticket Pandora ITSM avec les informations pertinentes sur l'événement. Vous pouvez obtenir plus d'informations sur Pandora ITSM dans la documentation de Pandora FMS.

Entrez un nom de représentant, une description, les paramètres à utiliser séparés par des virgules, la commande à utiliser (cette dernière permet l'utilisation de macros), le type et le serveur qui exécutera la commande. Dans les Parameters, vous pouvez en saisir autant que vous le souhaitez, en les séparant par des virgules. Lors de la réponse, une boîte de dialogue apparaîtra pour remplir chacun d'entre eux et l'ajouter ainsi à l'événement.

Event Responses macros

Les macros acceptées sont les suivantes :

_agent_address_

Adresse de l'agent.

_agent_alias_

Alias de l'agent.

_agent_id_

Identifiant de l'agent.

_agent_name_

Nom de l'agent.

_alert_id_

Identifiant de l'alerte associée à l'événement

_command_timeout_

Temps de réponse de la commande (secondes).

_current_user_

Identifiant de l'utilisateur qui exécute la réponse.

_current_username_

Nom complet de l'utilisateur qui exécute la réponse.

_customdata_json_

Extrait les informations des données personnalisées au format JSON.

_customdata_text_

Sortir toutes les données personnalisées en mode texte (avec des sauts de ligne).

_customdata_X_

Extrait un champ particulier des données personnalisées, en remplaçant le X par le nom du champ.

_event_date_

Date dans laquelle s'est produit l'événement.

_event_extra_id_

Identifiant extra.

_event_id_

Identifiant de l'événement.

_event_instruction_

Instructions de l'événement.

_event_severity_id_

Identifiant de la criticité de l'événement.

_event_severity_text_

Criticité de l'événement (traduit par la console Pandora FMS).

_event_source_

Source de l'événement.

_event_status_

État de l'événement (Nouveau, validé ou événement en processus).

_event_tags_

Étiquettes de l'événement séparées par des virgules.

_event_text_

Texte complet de l'événement.

_event_type_

Type d'événement (Système, Changeant à l'état inconnu...).

_event_utimestamp_

Date dans laquelle s'est produit l'événement sous format utimestamp.

_group_id_

Identifiant du groupe.

_group_name_

Nom du groupe dans la base de données.

_group_contact_

Informations de contact pour un groupe d'agents.

_module_address_

Adresse du module associé à l'événement.

_module_id_

Identificant du module associé à l'événement.

_module_name_

Nom du module associé à l'événement.

_node_id_

Pour Metaconsole et Node: renvoie l'identifiant du nœud.

_node_name_

Pour Metaconsole et Node: renvoie le nom du nœud.

_owner_user_

Utilisateur proprietaire de l'événement.

_owner_username_

Nom complet de l'utilisateur proprietaire de l'événement.

_user_id_

Identifiant de l'utilisateur.

Retour à l'index de documentation du Pandora FMS