Supervision prédictive

Supervision prédictive

Introduction

Outre des fonctionnalités telles que la supervision à distance, qu'elle soit Web ou basée sur des agents, Pandora FMS offre des ressources avancées pour améliorer la supervision. Avec ces ressources, vous pouvez effectuer des estimations de l'historique des données ou créer de nouveaux modules basés sur des opérations arithmétiques de modules existants.

Types de supervision prédictive

- Supervision prédictive :
  - *Planification de la capacité* (Capacity planning) : Il fait une prédiction selon la fenêtre de temps spécifié par l'utilisateur, en assumant un comportement plus ou moins linéaire du module cible. Ce type de modules prédictives vous permet de savoir combien de jours il reste avant que le disque devienne complète, ou le nombre de requêtes à la base de données que vous aurez dans un mois si tout continue comme prévu. Ces modules remplacent les modules anciennes de prédiction.
  - *Service* (Service) : Il récupère la valeur d'un service pour pouvoir le montrer dans n'importe quel agent qui soit nécessaire.
- Supervision arithmétique :
  - *Arithmétique synthétique* (Synthetic arithmetic) : Il est possible d'effectuer des opérations arithmétiques (addition, soustraction, multiplication et division) avec des données précédemment obtenues dans d'autres modules.
  - *Moyenne synthétique* (Synthetic average) : Il s'agit d'établir une moyenne avec les données précédemment obtenues dans d'autres modules.
  - *Module de tendance* (Trending module) : Il compare la moyenne actuelle apara rapport à la moyenne de la période précédente et renvoie la différence sous forme de valeur absolue ou de pourcentage. Le Trending module calcule la moyenne de la dérnière période dans l'intervalle indiqué par rapport à la moyenne de la même période du/de la jour/semaine/mois précédent(e). Par exemple si vous sélectionnez une semaine, Trending module calcule la moyenne de la dernière semaine et la compare avec la moyenne de la semaine précédente.

Supervision avec des modules synthétiques

Les modules synthétiques sont des modules fabriqués à partir de données provenant d'autres modules, qui peuvent se trouver dans le même agent ou dans des agents différents. Les opérations pouvant être effectuées sont arithmétiques (additionner, soustraire, multiplier et diviser) entre modules et / ou avec des valeurs absolues.

Les modules synthétiques sont gérés par le serveur de prédiction (Prediction server). Ce sous-composant du serveur Pandora FMS doit être activé et en fonctionnement. Aussi, l'agent qui contiendra les modules synthétiques doit utiliser un Prediction Server. Rappelez-vous que vous pouvez aussi utiliser un Environnement d'haute disponibilité et avoir un équilibrage de charge sur ces serveurs.

Dans la section administration d'un agent, dans l'onglet Modules, accédez en cliquant sur Create module et sélectionnez Create new prediction server module et remplissez les champs demandés.

Pour fonctionner avec d'autres opérations logiques (multiplication, soustraction, division), il vous suffit de prendre en compte l'ordre des opérateurs. Jouez avec l'interface pour voir comment une opération arithmétique peut être effectuée entre différents modules.

Détection des anomalies (MADE)

Introduction au programme MADE

L'objectif final du moteur de détection des anomalies de Pandora FMS (MADE) est la formation et l'utilisation de modèles d'intelligence artificielle pour la détection automatique des anomalies. Pour entraîner ces modèles, de grandes quantités de données d'entrée sont nécessaires, qui sont obtenues à partir de la base de données Pandora FMS. MADE conserve une copie de ces données sur le disque afin d'effectuer des tâches de recyclage et de rééchantillonnage dans un format « feather », conçu pour un stockage efficace des données.

Étant donné que les modèles sont chargés en mémoire et écrits sur le disque relativement fréquemment, les modèles formés sont stockés sur le disque en série avec les données pour des raisons de simplicité et d'efficacité. Le format dans lequel ils sont stockés peut varier en fonction des détails d'implémentation de chaque modèle. Comme nous le verrons plus tard, MADE écrit également des informations relatives aux anomalies et à son propre état dans la base de données.

MADE génère en conséquence des événements dans Pandora FMS, indiquant qu'il détecte une anomalie dans un moniteur spécifique.

Configuración de MADE

Liens de téléchargement pour MADE, pour EL8 :

https://firefly.pandorafms.com/centos8/pandorafms_made-0.1.0-1.el8.x86_64.rpm

Le serveur Ubuntu :

https://firefly.pandorafms.com/ubuntu/pandorafms-made_0.1.0-2_amd64.deb

Pour activer et personnaliser MADE, vous devez ajouter les options de configuration suivantes au fichier de configuration du serveur Pandora FMS, `/etc/pandora/pandora_server.conf` :

```
# Enable (1) or disable (0) the Monitoring Anomaly Detection Engine (MADE).
madeserver 1

# Directory where models will be stored.
madeserver_path /var/spool/pandora/data_in/models

# Number of server threads for MADE.
madeserver_threads 2

# Model backend: 'prophet' or 'iforest'.
# 'prophet' is better suited for temporal series and supports forecasting.
# 'iforest' is faster and more efficient (cpu, memory...).
madeserver_backend prophet

# MADE will query the Pandora FMS database every madeserver_interval seconds
# to look for new data.
madeserver_interval 10

# Minimum number of data required to train a model (e.g., '7d' for seven days).
madeserver_min_train 7d

# Maximum number of data kept to train models (e.g., '90d' for 90 days).
madeserver_max_history 90d

# Model automatic retraining period (e.g., '7d' for seven days).
madeserver_autofit 7d

# Model sensitivity. A lower value triggers less anomalies.
madeserver_sensitivity 0.1
```

L'aide sur MADE peut être obtenue en exécutant la commande :

```
pandora_made -h
```

MADE fonctionne comme un “daemon” géré par systemd. L'installation du paquet RPM ou DEB active le service, mais pour le démarrer sans redémarrer le serveur, il faut lancer :

```
systemctl start pandora_made.service
```

Ou bien :

```
service pandora_made start
```

Si le système redémarre ou se bloque, systemd redémarre lui-même le service.

Vous pouvez forcer l'entraînement des modèles en utilisant les données précédemment acquises par Pandora FMS avec la commande :

```
pandora_made -c /etc/pandora/pandora_server.conf -t
```

Il est également possible de forcer la formation d'un modèle spécifique, en spécifiant l'identifiant du module Pandora FMS avec `-m` :

```
pandora_made -c /etc/pandora/pandora_server.conf -t -m 1
```

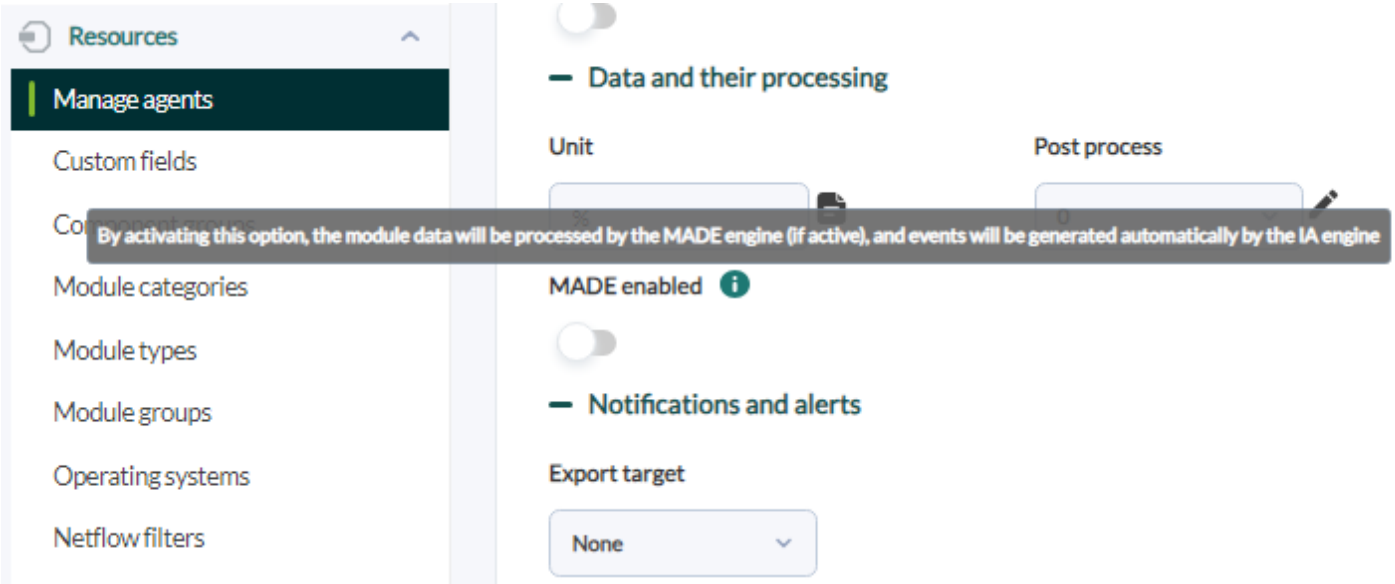
Lors du réentraînement d'un modèle, MADE l'évalue et compare ses performances avec le modèle actuel, en conservant toujours le meilleur modèle. Vous pouvez forcer la suppression des anciens modèles avec la commande :

```
pandora_made -c /etc/pandora/pandora_server.conf -d
```

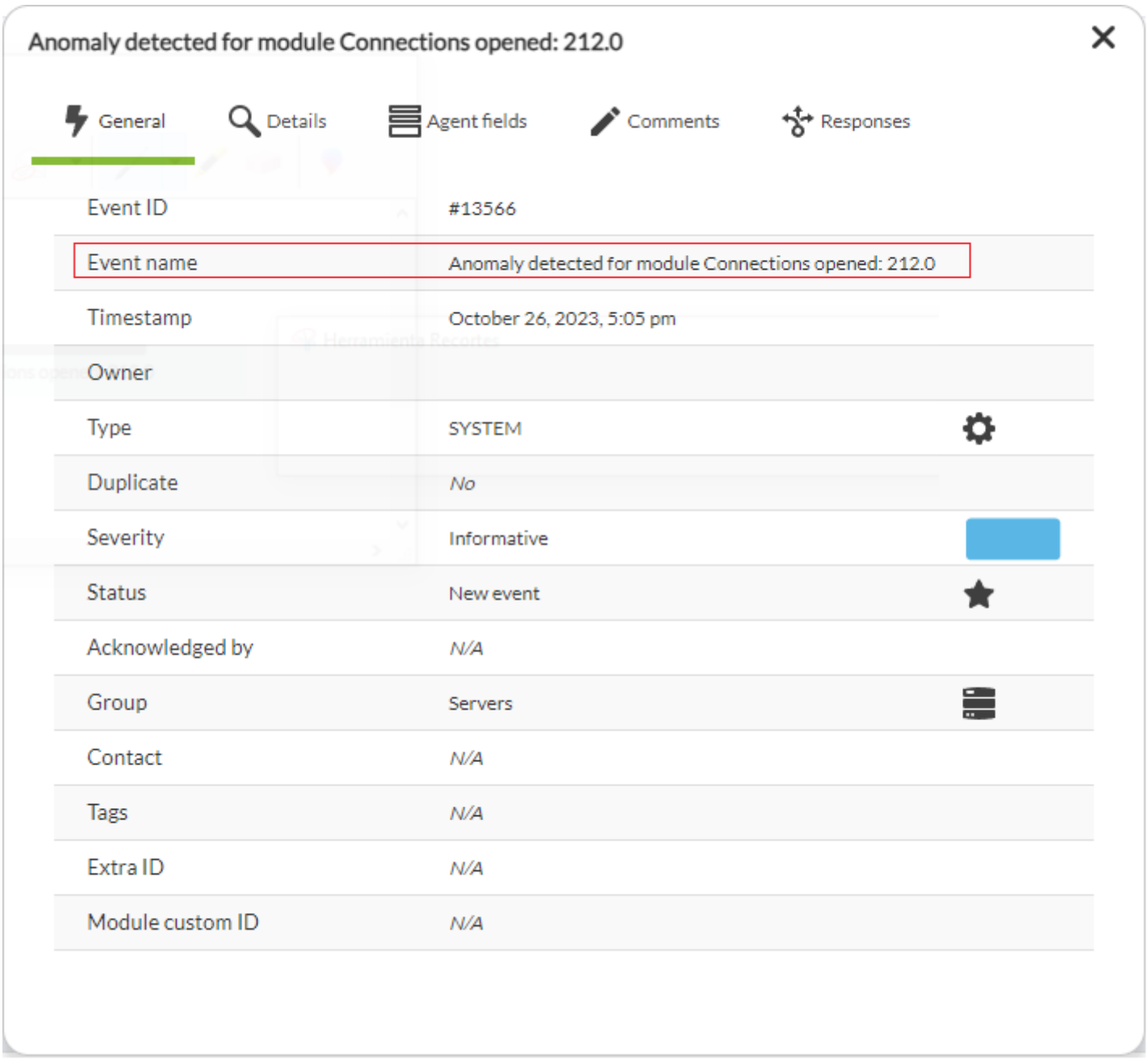
Il peut s'avérer pratique d'exécuter périodiquement cette commande à partir de cron.

Configuration de MADE au niveau du module

Une fois que MADE a été installé et configuré au niveau général, dans chaque module numérique vous aurez le sélecteur suivant pour ajouter ce module au travail de traitement des données :



Après un certain temps et en cas de détection d'une anomalie, MADE publiera ses propres événements dans une catégorie spécifique :



Voir aussi le système d'alerte pour les événements.

Détection des anomalies

Une fois le service installé et démarré, MADE fonctionne automatiquement. MADE lit les données de Pandora FMS, les ré-échantillonne et les fait pivoter si nécessaire, entraîne les modèles lorsqu'il dispose de suffisamment de données, les ré-entraîne périodiquement et génère des événements lorsqu'il détecte des anomalies.

Vous devez indiquer dans quels modules vous souhaitez activer la détection d'anomalies. Aucune

autre configuration n'est nécessaire, si ce n'est l'activation dans chaque module, dans la section des configurations avancées :

Le système est intelligent et effectue l'apprentissage du modèle pour chaque série de données et génère un événement d'anomalie détecté.

Ces événements peuvent être capturés comme n'importe quel autre événement de PFMS afin de générer des notifications personnalisées par le biais d'alertes d'événements.

Considérations sur les différents modèles d'AI appliqués

MADE est un outil utile pour attirer l'attention sur certains modèles qui seraient très difficiles à détecter ou à prévoir pour un administrateur.

Le mode *Prophet* permet d'entraîner des modèles plus robustes, qui prennent en compte les caractéristiques temporelles de la série de données et permettent de faire des prédictions dans le futur, mais il peut être coûteux à entraîner dans des environnements très vastes. C'est le mode *backend* qu'il est recommandé d'utiliser par défaut.

Le mode *IsolationForest* est beaucoup plus économe en ressources et a généré des résultats satisfaisants lors des tests, mais ces derniers peuvent varier en fonction de l'environnement et des données. Son utilisation est recommandée lorsque le mode *Prophet* entraîne des pertes de performances dues à un manque de ressources matérielles.

Revenir à l'index de la documentation Pandora FMS