Monitorización predictiva

Monitorización predictiva

Introducción

Además de las características como la monitorización remota, basada en Agentes o web, Pandora FMS ofrece recursos avanzados para mejorar la monitorización. Con estos recursos puede realizar estimaciones sobre el histórico de datos o crear nuevos Módulos basados en operaciones aritméticas de Módulos existentes.

Tipos de monitorización predictiva

- Monitorización predictiva:
  - *Planificación de la capacidad* (Capacity planning): Realiza una predicción basándose en la ventana de tiempo especificada por el usuario, asumiendo un comportamiento más o menos lineal del módulo objetivo. Este tipo de módulos predictivos nos permite saber cuántos días nos quedan hasta que el disco se llene, o el número de peticiones a la base de datos que tendremos dentro de un mes, de seguir como hasta ahora. Estos módulos reemplazan a los antiguos módulos de predicción.
  - *Servicio* (Service): Rescata el valor de un servicio para poder mostrarlo en cualquier Agente en el que sea necesario.
- Monitorización aritmética:
  - *Aritmética sintética* (Synthetic arithmetic): Se trata de poder realizar operaciones aritméticas (suma, resta, multiplicación y división) con datos obtenidos previamente en otros Módulos.
  - *Media sintética* (Synthetic average): Se trata de sacar una media con de datos obtenidos previamente en otros Módulos.
  - *Tendencia* (Trending module): Compara la media actual con la media del periodo anterior y devuelve la diferencia en valor absoluto o como porcentaje. El Trending module hace la media del último período en la periodicidad indicada versus la media del mismo período un día/semana/mes anterior. Por ejemplo si selecciona una semana, Trending module calcula la media de la última semana y la compara con la media de la semana anterior.

Monitorización con módulos sintéticos

Los Módulos sintéticos son Módulos fabricados a partir de datos de otros Módulos, que pueden estar en el mismo Agente o en Agentes diferentes. Las operaciones que se pueden realizar son aritméticas (sumar, restar, multiplicar y dividir) entre Módulos y/o con valores absolutos.

Los Módulos sintéticos son gestionados por el servidor de predicción (Prediction Server). Dicho subcomponente del servidor de Pandora FMS debe estar activo y en funcionamiento. Así mismo, el Agente que contendrá los

Módulos sintéticos debe usar un Prediction Server.
Recuerde que usted también puede utilizar un Entorno de Alta Disponibilidad y tener un balanceo de carga en dichos servidores.

En la sección de administración de un Agente en la solapa de Módulos, se accede haciendo clic en Create module y se selecciona Create new prediction server module y se completan los campos solicitados.

Para otras operaciones lógicas (multiplicación, resta, división) se ha de tener en cuenta el orden de los operadores. Pruebe con la interfaz para aprender cómo se puede hacer cualquier operación aritmética entre diferentes Módulos.

Detección de anomalías (MADE)

Introducción a MADE

El propósito final del motor de detección de anomalías de Pandora FMS (MADE) es el entrenamiento y uso de modelos de Inteligencia Artificial para la detección automática de anomalías. Para entrenar dichos modelos, se necesitan grandes cantidades de datos de entrada, que son obtenidos de la base de datos de Pandora FMS. MADE mantiene una copia de estos datos en disco para llevar a cabo tareas de reentrenamiento y remuestreo en formato *feather*, diseñado para el almacenamiento eficiente de datos.

Dado que los modelos se cargan en memoria y se escriben a disco con relativa frecuencia, los modelos entrenados se almacenan en disco serializados junto a los datos por simplicidad y eficiencia. El formato en el que se almacenan puede variar según los detalles de implementación de cada modelo. Como veremos más adelante, MADE además escribe información relacionada con anomalías y con su propio estado en la base de datos.

MADE genera como resultado eventos en Pandora FMS, indicando que detecta una anomalía en un monitor específico.

Configuración de MADE

Enlaces de descarga de MADE, para EL8:

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

Para Ubuntu server:

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

Para activar y personalizar MADE, hay que añadir las siguientes opciones de configuración al fichero de configuración del servidor de 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
```

Se puede obtener ayuda sobre MADE ejecutando el comando:

```
pandora_made -h
```

MADE se ejecuta como un *daemon* gestionado por systemd. Al instalar el paquete RPM o DEB se habilita el servicio, pero para arrancarlo sin reiniciar el servidor es necesario ejecutar:

```
systemctl start pandora_made.service
```

O bien:

```
service pandora_made start
```

Si el sistema se reinicia o se produce algún fallo, el propio systemd se encarga de volver a arrancar el servicio.

Se puede forzar el entrenamiento de modelos utilizando datos previamente adquiridos por Pandora FMS con el comando:

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

También es posible forzar el entrenamiento de un modelo específico, especificando el identificador del módulo de Pandora FMS con `-m`:

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

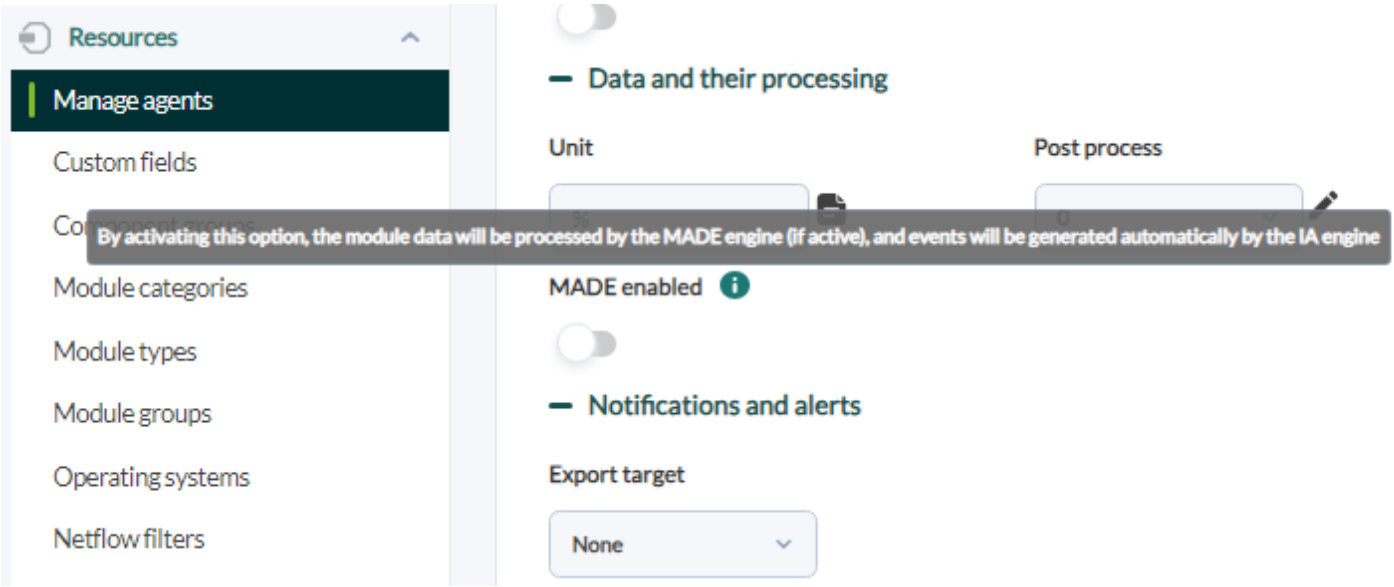
Al reentrenar un modelo, MADE lo evalúa y compara su rendimiento con el modelo actual, quedándose siempre con el mejor modelo. Se puede forzar el borrado de modelos antiguos con el comando:

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

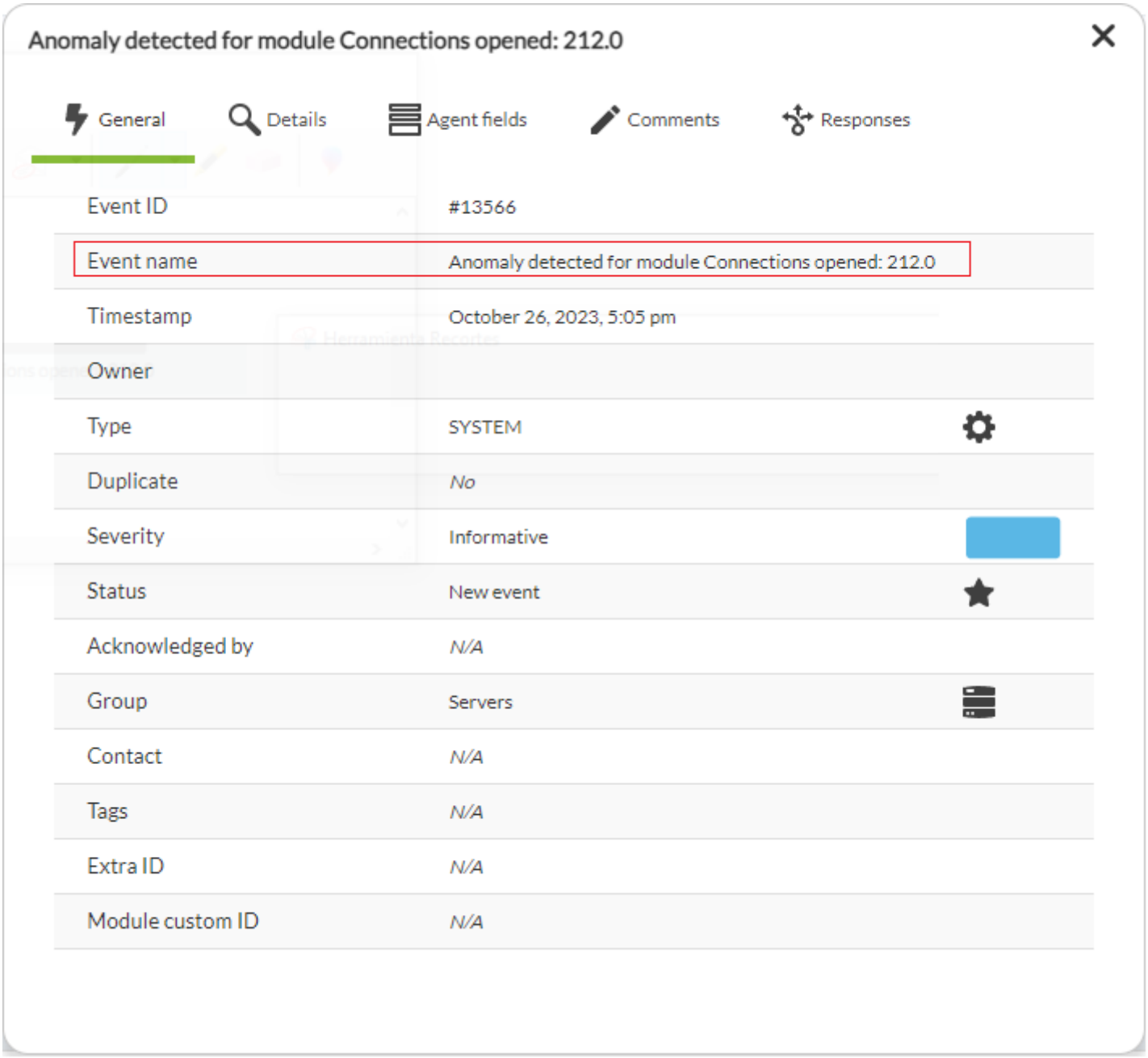
Puede resultar conveniente ejecutar este comando de forma periódica desde cron.

Configuración de MADE a nivel de módulo

Una vez instalado y configurado MADE a nivel general, en cada módulo de índole numérico tendrá el siguiente selector para agregar dicho módulo al trabajo de procesar los datos:



Una vez pasado cierto tiempo y al detectar una anomalía, MADE publicará sus propios eventos en una categoría específica:



Véase también el sistema de alertado para eventos.

Detección de anomalías

Una vez instalado y arrancado el servicio, MADE funciona de forma automática. MADE lee los datos de Pandora FMS, los *remuestrea* y rota cuando es necesario, entrena modelos cuando tiene suficientes datos, los reentrena de forma periódica, y genera eventos cuando detecta anomalías.

Se deberá indicar en cuáles módulos desea activar la detección de anomalías. No precisará más configuración que activarlo en cada módulo, en la sección de configuraciones avanzadas:

El sistema es *inteligente* y realizará el entrenamiento del modelo para cada serie de datos y generará un evento de anomalía detectada.

Dichos eventos podrán ser capturados como cualquier otro evento de PFMS para generar notificaciones personalizadas a través de las alertas de eventos.

Consideraciones sobre los diferentes modelos IA aplicados

MADE resulta una herramienta útil para llamar la atención sobre determinados patrones que serían muy complicados de detectar o predecir por un administrador.

El modo *Prophet* permite entrenar modelos más robustos, que tienen en cuenta las características temporales de las series de datos y permiten realizar predicciones en el futuro, pero puede resultar costoso de entrenar en entornos muy grandes. Es el *backend* que se recomienda utilizar por defecto.

El modo *IsolationForest* es mucho más eficiente en el uso de recursos y ha generado resultados satisfactorios durante las pruebas, pero esto último puede variar en función del entorno y los datos. Se recomienda su uso cuando el modo *Prophet* provoque pérdidas de rendimiento por falta de recursos hardware.

Volver al índice de documentación de Pandora FMS