Collecte et supervision des journaux

Collecte et supervision des journaux

Introduction

La supervision des journaux dans Pandora FMS est établie de deux manières différentes :

1. Basé sur des modules : Elle représente les journaux dans Pandora FMS comme des moniteurs asynchrones, pouvant associer des alertes aux entrées détectées qui répondent à une série de conditions préconfigurées par l'utilisateur. La représentation modulaire des logs permet :
    1. Créez des modules qui comptent les occurrences d'une expression régulière dans un journal.
    2. Obtenir les lignes et le contexte des messages du journal.
2. Basé sur une visualisation combinée : Elle permet à l'utilisateur de visualiser dans une seule console toutes les informations de journal provenant de plusieurs sources qu'il souhaite capturer, en organisant les informations de manière séquentielle, en utilisant l'horodatage dans lequel les journaux ont été traités.

À partir de la version 7.0 NG 774, Pandora FMS intègre OpenSearch pour stocker les informations des journaux. Voir aussi « Installation et configuration d'OpenSearch ».

Comment ça marche

- Les logs analysés par le Agentes Software (eventlog ou fichiers texte), sont transmis au serveur Pandora FMS, sous forme RAW au sein du XML rapport d'agent.
- Le serveur de données Pandora FMS reçoit le XML de l'agent, qui contient à la fois des informations de supervision et de journal.
- Lorsque le serveur de données traite les données XML, il identifie les informations contenues dans les journaux, en enregistrant dans la base de données principale les références de l'agent déclarant et l'origine du journal, puis en envoyant automatiquement les informations à OpenSearch.
- Pandora FMS stocke les données dans des index OpenSearch, générant quotidiennement un index unique pour chaque instance Pandora FMS.
- Le serveur Pandora FMS dispose d'une tâche de maintenance qui supprime les index à l'intervalle défini par l'administrateur système (par défaut, 30 jours).

Collecte de journaux

À partir de la version 7.0 NG 774, Pandora FMS intègre OpenSearch pour stocker les informations des journaux ; vous devez d'abord disposer dudit serveur avant de commencer à collecter les journaux. Voir aussi « Installation et configuration d'OpenSearch ».

Paramètres de la console

Pour activer le système d'affichage des journaux, vous devez activer Management → Setup → Setup → Enterprise. Cliquez sur Activate Log Collector et Update.

Un nouvel onglet appelé Log Collector apparaîtra dans lequel il affiche d'abord l'état de la connexion (OpenSearch status) avec le serveur OpenSearch. Les valeurs suivantes doivent être configurées dans la section OpenSearch options :

1. OpenSearch IP : Adresse IP du serveur OpenSearch à utiliser avec Pandora FMS.
2. Utiliser https : Il doit être activé si l'environnement OpenSearch installé a activé HTTPS pour sa connexion.
3. Port OpenSearch : Le numéro de port TCP.
4. Jours pour purger les anciennes informations : Nombre de jours avant la suppression des données collectées.
5. Authentification de base : (facultatif) Si l'authentification de base a été installée dans OpenSearch (recommandé) l'utilisateur (User) doit être renseigné et mot de passe (Password) défini.

Configuration des agents

La collecte des journaux s'effectue via des agents, à la fois dans l'agent pour Microsoft Windows® et dans les agents Unix® (Linux®, MacOS X®, Solaris®, HPUX®, AIX®, BSD®, etc.). Dans le cas des agents MS Windows®, les informations peuvent également être obtenues à partir de l'observateur d'événements du système d'exploitation, en utilisant les mêmes filtres que dans le module de supervision de l'observateur d'événements.

Exemple sur MS Windows

Pour la version 774 ou supérieure, les lignes qui apparaissent sous `Logs extraction` doivent être *décommentées*:

```
# Log extraction
#module_begin
#module_name X_Server_log
#module_description Logs extraction module
#module_type log
#module_regexp C:\server\logs\xserver.log
#module_pattern .*
#module_end
```

Pour plus d'informations sur la description des modules de type log vous pouvez consulter la section suivante faisant référence aux Directives spécifiques.

```
module_type log
```

En définissant ce type de balise, `module_type log`, il est indiqué qu'elle ne sera pas stockée dans la base de données, mais plutôt qu'elle sera envoyée au collecteur de logs. Tout module avec ce type de données sera envoyé au collecteur, tant qu'il est activé : sinon l'information sera supprimée.

Pour les versions antérieures à 774 :

A partir de la version 750 cette action peut être réalisée à
l'aide des agent plugins en activant l'option Advanced.

Des exécutions du type présenté ci-dessous peuvent être réalisées :

Module logchannel

```
module_begin
module_name MyEvent
module_type log
module_logchannel
module_source <logChannel>
module_eventtype <event_type/level>
module_eventcode <event_id>
module_pattern <text substring to match>
module_description <description>
module_end
```

Module logevent

```
module_begin
module_name Eventlog_System
module_type log
module_logevent
module_source System
module_end
```

Module regexp

```
module_begin
module_name PandoraAgent_log
module_type log
module_regexp <%PROGRAMFILES%>\pandora_agent\pandora_agent.log
module_description This module will return all lines from the specified logfile
module_pattern .*
module_end
```

Exemple sur les systèmes Unix

Pour la version 774 ou supérieure, les lignes qui apparaissent sous `Logs extraction` doivent être décommentées :

```
# Log extraction
#module_begin
#module_name Syslog
#module_description Logs extraction module
#module_type log
#module_regexp /var/log/logfile.log
#module_pattern .*
#module_end
```

Pour plus d'informations sur la description des modules de type log vous pouvez consulter la section suivante faisant référence à Directives spécifiques.

```
module_type log
```

En définissant ce type de balise, `module_type log`, il est indiqué qu'elle ne sera pas stockée dans la base de données, mais plutôt qu'elle sera envoyée au collecteur de logs. Tout module avec ce type de données sera envoyé au collecteur, à condition qu'il soit activé : sinon l'information sera supprimée.

Pour les versions antérieures à 744 :

```
module_plugin grep_log_module /var/log/messages Syslog \.\*
```

Semblable au plugin d'analyse des journaux (grep_log), le plugin grep_log_module envoie les informations de journal traitées au Log Collector avec le nom « Syslog » comme source. Il utilise l'expression régulière `\.\*` (dans ce cas « tout ») comme modèle pour choisir les lignes à envoyer et celles à ne pas envoyer.

Serveur Syslog Pandora FMS

Ce composant permet à Pandora FMS d'analyser le syslog de la machine où il se trouve, d'analyser son contenu et de stocker les références dans l'OpenSearch correspondant. serveur.

https://www.rsyslog.com/

Le principal avantage de Syslog Server est de compléter l'unification des logs. Pris en charge par

les fonctionnalités d'exportation de Syslog Server depuis les environnements Linux® et Unix®, Syslog Server permet d'interroger les journaux quelle que soit leur origine, en recherchant dans un seul point commun (visualiseur de journaux de la console Pandora FMS).

L'installation de Syslog Server 8.2102 doit être effectuée à la fois sur le client et sur le serveur :

```
dnf install rsyslog
```

Accédez au fichier de configuration `/etc/rsyslog.conf` pour activer les entrées TCP et UDP.

```
  (...)

# Provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# Provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

  (...)
```

Redémarrez le service rsyslog. Une fois le service disponible, vérifiez que le port 514 est accessible avec :

```
netstat -ltnp
```

Sur le client, il est configuré pour qu'il puisse envoyer les logs au serveur Syslog, accéder à rsyslog `/etc/rsyslog.conf` . Localisez et activez la ligne qui vous permet de configurer l'hôte distant (remplacez `remote-host` par l'adresse IP du serveur) :

```
action(type="omfwd Target="remote-host" Port="514" Protocol="tcp")
```

La taille des journaux reçus par rsyslog est de 8 kilo-octets par défaut. Si des journaux plus volumineux sont reçus, de nouvelles entrées sont ajoutées avec le contenu restant jusqu'à ce que le journal complet soit reçu. Ces nouvelles entrées ne contiennent pas le nom de l'hôte qui a envoyé le journal. Ce comportement peut donc entraîner la création de nouvelles sources de journaux indésirables et de nouveaux agents dans la console. Pour éviter cela il est recommandé d'augmenter la taille des logs reçus en ajoutant la ligne suivante :

```
$MaxMessageSize 512k
```

Enregistrez le fichier et quittez l'éditeur de texte.

L'envoi de journaux génère un agent conteneur avec le

nom du client, il est donc recommandé de créer les agents avec « alias as name » en le faisant correspondre au nom d'hôte du client, évitant ainsi la duplication dans les agents.

Pour activer cette fonctionnalité dans Pandora FMS Server, activez dans le fichier `pandora_server.conf` le contenu suivant :

```
# Enable (1) or disable (0) the Pandora FMS Syslog Server
syslogserver 1

# Full path to syslog's output file.
syslog_file /var/log/messages

# Number of threads for the Syslog Server
syslog_threads 2

# Maximum number of lines queued by the Syslog Server's
# producer on each run.
syslog_max 65535
```

N'oubliez pas que vous devez modifier la configuration de votre appareil pour que les journaux soient envoyés au serveur Pandora FMS.

Filtres au niveau du serveur PFMS

Sur le serveur Pandora FMS, à l'aide du token syslog_whitelist, vous pouvez admettre uniquement les logs qui correspondent à une expression régulière ou regexp, qui est sensible à la casse (par exemple, `windows` n'est pas la même chose que `Windows`) et ignorer tout le reste.

Avec le token syslog_blacklist vous pouvez refuser les logs qui correspondent à l'ensemble regexp (et laisser tout le reste dans).

Les deux jetons sont désactivés par défaut.

- syslog_whitelist : L'activation de ce jeton laissera entrer uniquement les journaux conformes à la regexp et le reste sera supprimé.
  - Si ce token est activé et que vous avez le filtre par défaut `.*`, tout sera accepté.
  - Important : Si ledit token est activé SANS regexp, RIEN ne sera admis.
- Le filtrage des mots-clés autorisés est effectué en premier, cela réduit le travail pour l'étape suivante.
- syslog_blacklist : Placer une regexp supprimera tout ce qui y est conforme (si ce token est activé mais laissé SANS regexp, RIEN ne sera bloqué.).
- Le filtrage par syslog_blacklist est effectué en dernier.

Interface OpenSearch

NG version 774 ou ultérieure.

Visualisation et recherche

Dans un outil de collecte de logs, deux caractéristiques sont principalement intéressantes : pouvoir rechercher des informations - filtrage par date, sources de données et/ou mots-clés, etc. - et pouvoir visualiser ces informations (menu Operation → Monitoring → Log viewer) dessiné en occurrences par unité de temps.

Le champ le plus important - et le plus utile - sera la chaîne de recherche à saisir dans la zone de texte Search en combinaison avec les trois types de recherche disponibles (Search mode) :

- Exact match : La recherche de chaîne littérale, le journal contient une correspondance exacte.
- All words : La recherche qui contient tous les mots indiqués, quel que soit l'ordre dans la même ligne de journal.
- Any word : La recherche qui contient l'un des mots indiqués, quel que soit l'ordre.
- Si vous cochez l'option pour voir le contexte du contenu filtré, vous obtiendrez un aperçu de la situation avec les informations d'autres lignes de journal liées à la recherche.

Affichage et recherche avancés

Avec cette fonctionnalité, vous pouvez afficher les entrées de journal sous forme graphique, en classant les informations en fonction de modèles de capture de données.

Ces modèles de capture de données sont essentiellement des expressions régulières et des identifiants qui vous permettent d'analyser les sources de données et de les afficher sous forme de graphique.

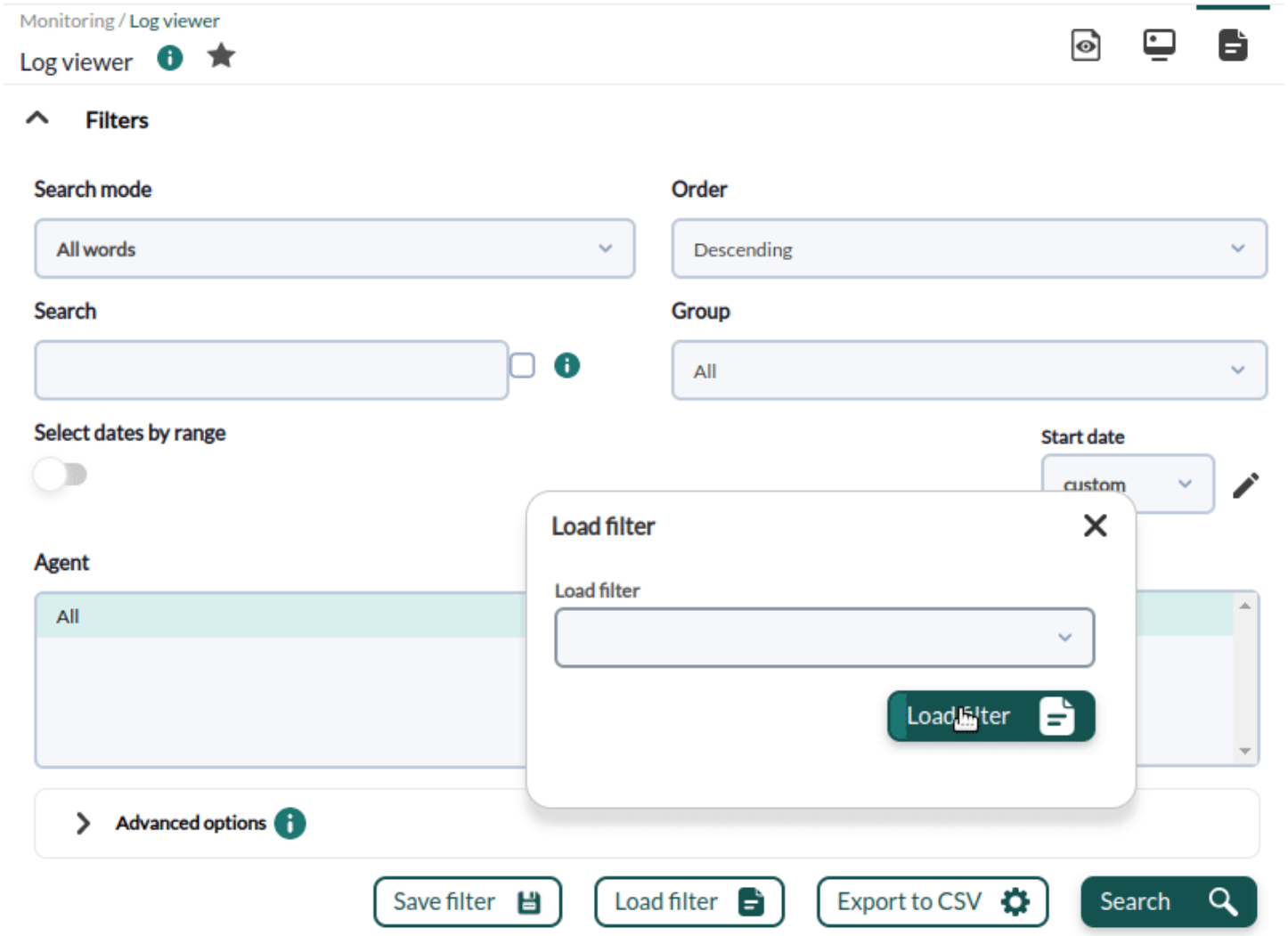
Pour accéder aux options avancées, cliquez sur Advanced options. Un formulaire s'affichera dans lequel vous pourrez choisir le type d'affichage des résultats :

- Afficher les entrées du journal (texte brut).
- Afficher le graphique du journal.
- À l'aide de l'option d'affichage du graphique du journal (Display mode), vous pouvez sélectionner le modèle de capture (Use capture model).
- Le modèle par défaut, *Apache log model*, offre la possibilité de traiter ou d'analyser les logs Apache au format standard (access_log), pouvant extraire des graphiques comparatifs de temps de réponse, regroupés par page visitée et code de réponse :
- Vous pouvez appuyer sur le bouton Modifier ou sur le bouton Créer pour créer un nouveau modèle de capture.

Filtres communs

Version 771 ou ultérieure

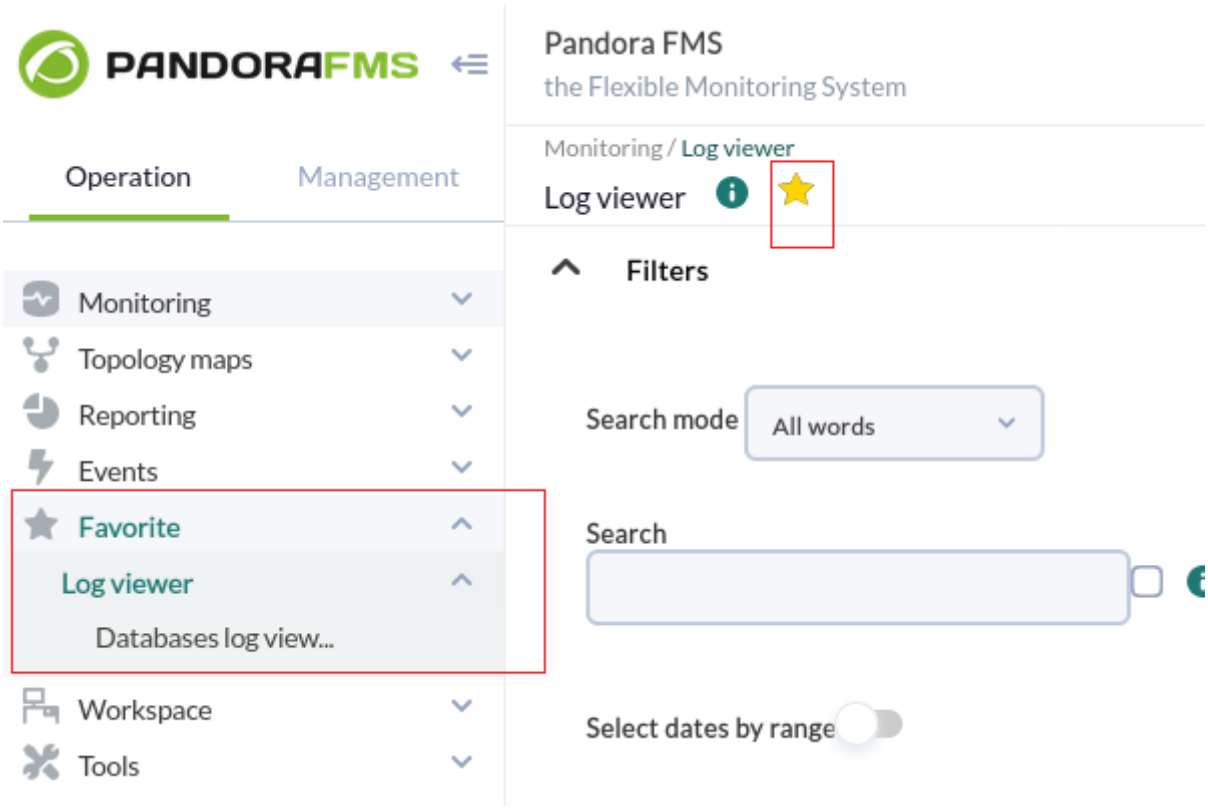
Grâce à cette option, vous pouvez enregistrer les préférences de filtrage fréquemment utilisées, créant ainsi une liste de filtres fréquents. Lorsque vous avez configuré toutes les valeurs du filtre, cliquez sur le bouton Save filter, attribuez un nom et cliquez sur Save. À tout autre moment, vous pouvez charger ces préférences en utilisant le bouton Load filter, puis affichez la liste des filtres enregistrés, sélectionnez-en un et cliquez sur Load filter.



Filtres enregistrés comme éléments favoris

Version 770 ou ultérieure.

À l'aide du système de favoris de PFMS, vous pouvez enregistrer un raccourci pour le Log viewer avec des préférences de filtrage en cliquant sur l'icône en forme d'étoile dans le titre de la section.



Log source dans la vue Agent

À partir de la version 749 de Pandora FMS, une boîte appelée Log sources status a été ajoutée à la vue de l'agent, dans laquelle apparaîtra la date de la dernière mise à jour des journaux par cet agent. Lorsque vous cliquez sur l'icône en forme de loupe Review, vous redirigez vers la vue Log Viewer filtrée par ce log.

Version 774 ou ultérieure : par défaut, les données affichées dans les deux vues sont limitées aux dernières 24 heures et peuvent être modifiées si nécessaire.

Retour à l'index de la documentation Pandora FMS