Recolección y monitorización de logs

Recolección y monitorización de logs

Introducción

La monitorización de *logs* en Pandora FMS está establecida de dos formas diferentes:

1. Basada en módulos: Representa *logs* en Pandora FMS como monitores asíncronos, pudiendo asociar alertas a las entradas detectadas que cumplan una serie de condiciones preconfiguradas por el usuario. La representación modular de los *logs* permite:
    1. Crear módulos que cuenten las ocurrencias de una expresión regular en un *log*.
    2. Obtener las líneas y el contexto de los mensajes de *log*.
2. Basada en visualización combinada: Permite al usuario visualizar en una única Consola toda la información de *logs* de múltiples orígenes que se desee capturar, organizando la información de manera secuencial, utilizando la marca de tiempo en que se procesaron los *logs*.

A partir de la versión 7.0 NG 774, Pandora FMS incorpora OpenSearch para almacenar la información de *logs*. Véase también "Instalación y configuración de OpenSearch".

Cómo funciona

- Los *logs* analizados por los Agentes Software (eventlog o ficheros de texto), son reenviados hacia el servidor de Pandora FMS, en forma RAW dentro del XML de reporte del agente.
- El Data Server Pandora FMS recibe el XML del agente, que contiene información tanto de monitorización como de *logs*.
- Cuando el Data Server procesa los datos del XML identifica la información de los *logs*, guardando en la base de datos principal las referencias del agente que ha reportado y el origen del *log* y luego enviando automáticamente la información a OpenSearch.
- Pandora FMS almacena los datos en índices de OpenSearch generando diariamente un índice único por cada instancia de Pandora FMS.
- El servidor de Pandora FMS dispone de una tarea de mantenimiento que elimina los índices en el intervalo definido por el administrador del sistema (por defecto, 30 días).

Recolección de logs

A partir de la versión 7.0 NG 774, Pandora FMS incorpora OpenSearch para almacenar la información de *logs*, primero se debe disponer de dicho servidor antes de comenzar a recolectar *logs*. Véase también "Instalación y configuración de OpenSearch".

Configuración de la consola

Para activar el sistema de visualización de *logs* debe activar en Management → Setup → Setup → Enterprise. Se debe activar el botón Activate Log Collector y pulsar el botón Update.

Aparecerá una nueva pestaña denominada Log Collector en la cual muestra de primero el estado de conexión (OpenSearch status) con el servidor OpenSearch. Se deberá configurar los siguientes valores en la sección OpenSearch options:

1. OpenSearch IP: Dirección IP del servidor OpenSearch a utilizar con Pandora FMS.
2. Use https: Se debe activar si el entorno OpenSearch instalado tiene habilitado HTTPS para su conexión.
3. OpenSearch Port: Número de puerto TCP.
4. Days to purge old information: Cantidad de días antes de borrar los datos recabados.
5. Basic authentication: (opcional) si se ha instalado la autentificación básica en OpenSearch (recomendado) se deberá colocar el usuario (User) y contraseña (Password) establecidos.

Configuración de los agentes

La recolección de *logs* se hace mediante los agentes, tanto en el agente para Microsoft Windows® como en los agentes Unix® (Linux®, MacOS X®, Solaris®, HPUX®, AIX®, BSD®, etc). En el caso de los agentes MS Windows®, también se puede obtener información del visor de eventos del sistema operativo, utilizando los mismos filtros que en el módulo de monitorización del visor de eventos.

Ejemplo en MS Windows

Para la versión 774 o posterior se deberán descomentar las líneas que aparecen debajo de `Logs extraction` :

```
# Logs 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
```

Para más información sobre la descripción de módulos de tipo *log* puede consultar la siguiente sección referente a Directivas específicas.

```
module_type log
```

Al definir este tipo de etiqueta, `module_type log`, se indica que no almacene en base de datos, sino que se envíe al colector de *log*. Cualquier módulo con este tipo de dato se mandará al colector, siempre y cuando esté habilitado: *en caso contrario se descartará la información.*

Para versiones anteriores a 774:

A partir de la versión 750 esta acción se podrá realizar mediante los plugins de agente activando la opción *Advanced*.

Se podrán realizar ejecuciones del tipo de las que se muestran a continuación:

Módulo 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
```

Módulo logevent

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

Módulo 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
```

Ejemplo en sistemas Unix

Para la versión 774 o posterior se deberán descomentar las líneas que aparecen debajo de `Logs extraction`:

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

Para más información sobre la descripción de módulos de tipo *log* puede consultar la siguiente sección referente a Directivas específicas.

```
module_type log
```

Al definir este tipo de etiqueta, `module_type log`, se indica que no almacene en base de datos, sino que se envíe al colector de *log*. Cualquier módulo con este tipo de dato se mandará al colector, siempre y cuando esté habilitado: *en caso contrario se descartará la información.*

Para versiones anteriores a 744:

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

Similar al plugin de *parseo* de *logs* (grep_log), el *plugin* grep_log_module envía la información procesada del *log* al Colector de logs con el nombre de "Syslog" como origen. Utiliza la expresión regular `\.\*` (en este caso "*todo*") como patrón a la hora de elegir qué líneas enviamos y cuáles no.

Pandora FMS Syslog Server

Este componente permite a Pandora FMS analizar el syslog de la máquina donde está ubicado, analizando su contenido y almacenando las referencias en el servidor OpenSearch correspondiente.

https://www.rsyslog.com/

La ventaja principal del Syslog Server consiste en complementar la unificación de *logs*. Con apoyo de las características de exportado de Syslog Server de los entornos Linux® y Unix®, Syslog

Server permite la consulta de *logs* independientemente del origen, buscando en un único punto común (visor de *logs* de la consola de Pandora FMS).

La instalación de Syslog Server 8.2102 se debe realizar tanto en cliente como en servidor:

```
dnf install rsyslog
```

Acceda al fichero de configuración `/etc/rsyslog.conf` para habilitar el *input* de TCP y 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")

 (...)
```

Reinicie el servicio rsyslog. Una vez el servicio esté disponible, compruebe que el puerto 514 está accesible con:

```
netstat -ltnp
```

En el cliente se configura para que pueda enviar los *logs* al Syslog Server, acceda al rsyslog `/etc/rsyslog.conf` . Localice y habilite la línea que permite configurar el *host* remoto (cambie `remote-host` por la dirección IP del servidor):

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

El tamaño de los *logs* recibidos por rsyslog es de 8 kilobytes por defecto. Si se reciben *logs* con un tamaño mayor se añaden nuevas entradas con el contenido restante hasta recibir el *log* completo. Estas nuevas entradas no contienen el nombre del *host* que envió el *log*, por lo que este comportamiento puede causar que se creen tanto nuevos orígenes de *logs* indeseados como nuevos agentes en la consola. Para evitar esto se recomienda aumentar el tamaño de los *logs* recibidos añadiendo la siguiente línea:

```
$MaxMessageSize 512k
```

Guarde el fichero y salga del editor de texto.

El envío de *logs* genera un agente contenedor con el nombre del cliente por lo que se recomienda crear los

agentes con “alias as name” haciendo que coincida con el *hostname* del cliente, así se evitará duplicidad en los agentes.

Para activar esta funcionalidad en Pandora FMS Server, habilite en el archivo `pandora_server.conf` el siguiente contenido:

```
# Enable (1) or disable (0) the Pandora FMS Syslog Server
#  (PANDORA FMS ENTERPRISE ONLY).
syslogserver 1

# Full path to syslog's output file (PANDORA FMS ENTERPRISE ONLY).
syslog_file /var/log/messages

# Number of threads for the Syslog Server
#  (PANDORA FMS ENTERPRISE ONLY).
syslog_threads 2

# Maximum number of lines queued by the Syslog Server's
#   producer on each run (PANDORA FMS ENTERPRISE ONLY).
syslog_max 65535
```

Recuerde que es necesario que modifique la configuración de su dispositivo para que los *logs* se envíen al servidor de Pandora FMS.

Filtros a nivel de PFMS server

En el servidor de Pandora FMS, por medio del *token* syslog_whitelist, se pueden admitir solamente los registros que coincidan con una expresión regular o regexp, la cual es sensible a mayúsculas y minúsculas (por ejemplo, `windows` no es igual a `Windows`) *y descartar todo lo demás* .

Con el *token* syslog_blacklist se pueden denegar registros que coincidan con la regexp establecida (*y dejar entrar todo lo demás*).

Ambos *token* vienen desactivados por defecto.

- syslog_whitelist: Al activar dicho *token* solamente dejará entrar los *logs* que cumplan con la regexp y se descarta el resto.
  - Si dicho *token* está activado y se tiene el filtro que viene por defecto `.*`, se admitirá todo.
  - Importante: Si dicho *token* está activado SIN regexp, NADA será admitido.
- El filtrado de palabras clave permitidas se realiza primero, esto reduce el trabajo para el siguiente paso.
- syslog_blacklist: Al colocar una regexp se descartará todo lo que cumpla con ello (si se activa este *token* pero se deja SIN regexp, NADA será bloqueado.).

- El filtrado por syslog_blacklist se realiza de último.

Interfaz de OpenSearch

Versión NG 774 o posterior.

Visualización y búsqueda

En una herramienta de recolección de *logs* interesan principalmente dos características: el poder buscar información -filtrando por fecha, fuentes de datos y/o palabras clave, etcétera- y poder visualizar esa información (menú Operation → Monitoring → Log viewer) dibujada en ocurrencias por unidad de tiempo.

El campo más importante -y útil- será la cadena a buscar a introducir en el cuadro de texto Search en combinación con los tres tipos de búsqueda disponibles (Search mode):

- Exact match: Búsqueda de cadena literal, el *log* contiene una coincidencia exacta.
- All words: Búsqueda que contenga *todas* las palabras indicadas, independientemente del orden en una misma línea de *log*.
- Any word: Búsqueda que contenga *alguna* de las palabras indicadas, independientemente del orden.
- Si marca la opción de ver el contexto del contenido filtrado, obtendrá una vista general de la situación con información de otras líneas de *logs* relacionadas con la búsqueda.

Visualización y búsqueda avanzadas

Con esta característica se puede mostrar de manera gráfica las entradas de *log*, clasificando la información en base a modelos de captura de datos.

Estos modelos de captura de datos son básicamente expresiones regulares e identificadores que permiten analizar los orígenes de datos y mostrarlos como un gráfico.

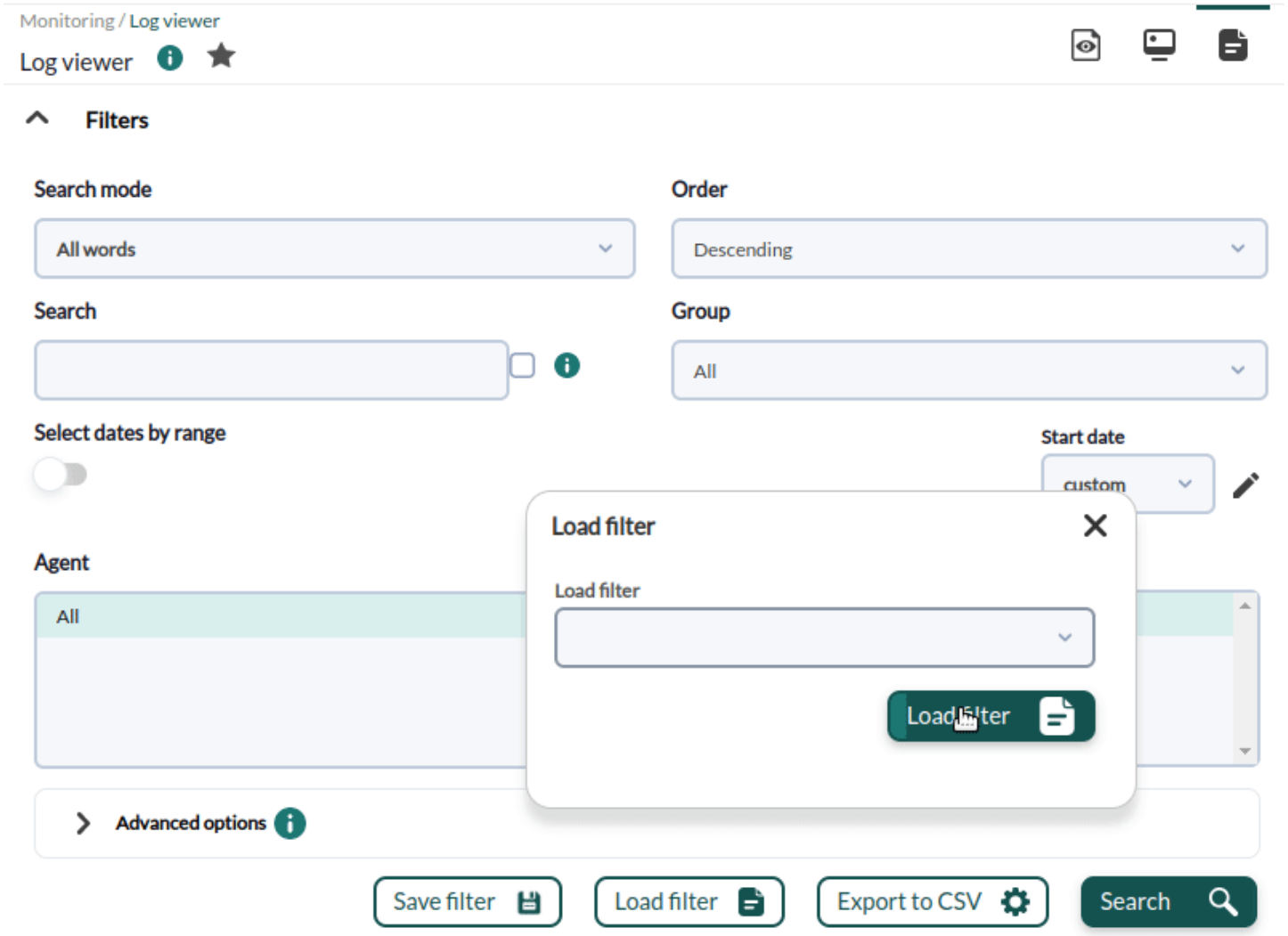
Para acceder a las opciones avanzadas pulse en Advanced options. Se mostrará un formulario donde podrá elegir el tipo de vista de resultados:

- Mostrar entradas de *log* (texto plano).
- Mostrar gráfica de *log*.
- Mediante la opción *mostrar gráfica de log* (Display mode) podrá seleccionar el modelo de captura (Use capture model).
- El modelo por defecto, *Apache log model*, ofrece la posibilidad de procesar o parse logs de Apache en formato estándar (access_log), pudiendo extraer gráficas comparativas de tiempo de respuesta, agrupando por página visitada y código de respuesta:
- Bien puede pulsar el botón de editar o el botón de crear para realizar un nuevo modelo de captura.

Filtros frecuentes

Versión 771 o posterior

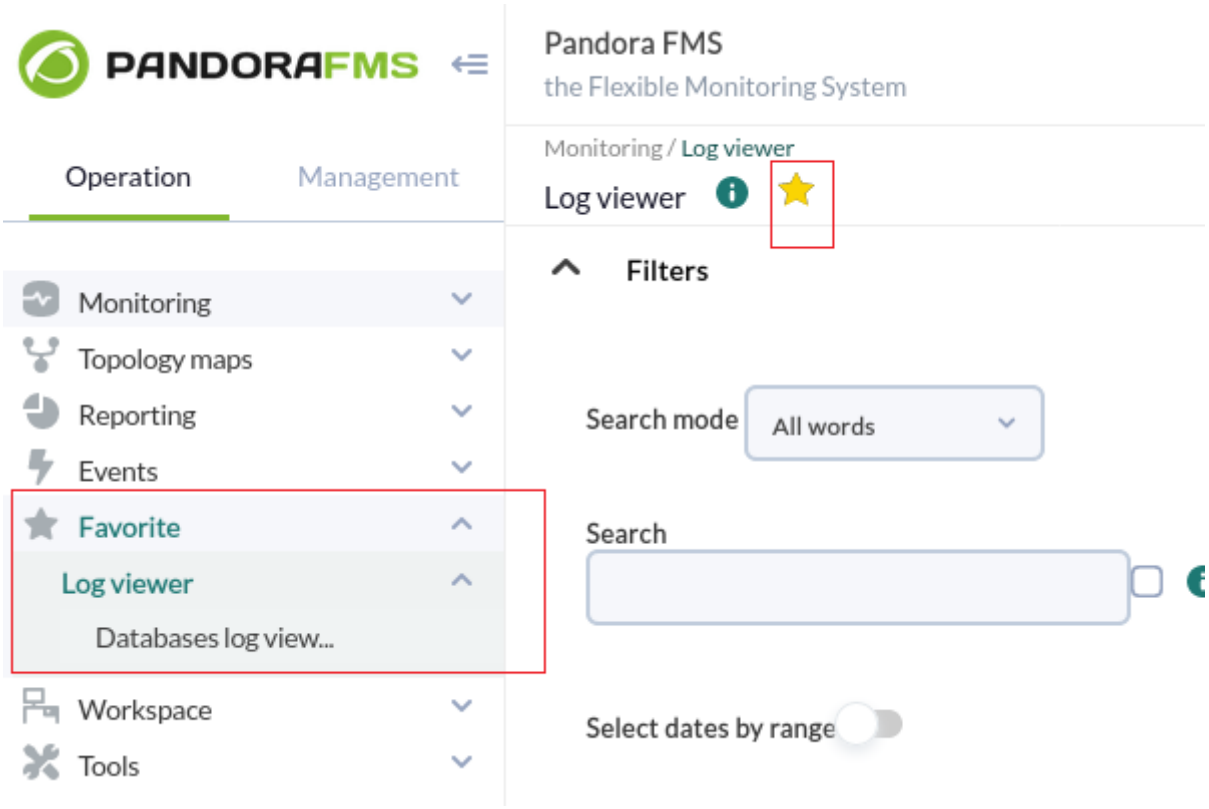
Por medio de esta opción podrá guardar las preferencias de filtrado de uso frecuente, creando así una lista de filtros frecuentes. Cuando haya configurado todos los valores de filtrado, pulse en el botón Save filter, asigne un nombre y pulse Save. En cualquier otra oportunidad podrá cargar dichas preferencias por medio del botón Load filter, luego descuelgue la lista de filtros guardados, seleccione uno de ellos y pulse Load filter.



Filtros guardados como elementos favoritos

Versión 770 o posterior.

Mediante el sistema de favoritos en PFMS se podrá guardar un acceso directo para el Log viewer con las preferencias de filtrado si hace clic en el icono con forma de estrella situado en el título de la sección.



Log Source en la Vista de Agentes

A partir de la versión 749 de Pandora FMS, se ha añadido en la Vista del agente un cuadro llamado Log sources status, en el cual aparecerá la fecha de la última actualización de los *logs* por parte de ese agente. Al pulsar en el icono de la lupa de Review, redirige a la vista del Log Viewer filtrada por ese *log*.

Versión 774 o posterior: Por defecto los datos mostrados en ambas vistas están delimitados a las últimas 24 horas, pudiendo ser cambiado según se necesite.

Volver al índice de documentación de Pandora FMS