FIM (File Integrity Monitoring)

FIM (File Integrity Monitoring)

Introducción

La monitorización de integridad de ficheros (FIM) permite conocer en un sistema si ficheros críticos e importantes, como por ejemplo de configuración, han sido modificados en algún momento.

Pandora FMS incorpora esta características de monitorización en los Endpoints a partir de la versión 784, tanto para sistemas Linux® como para sistemas MS Windows®.

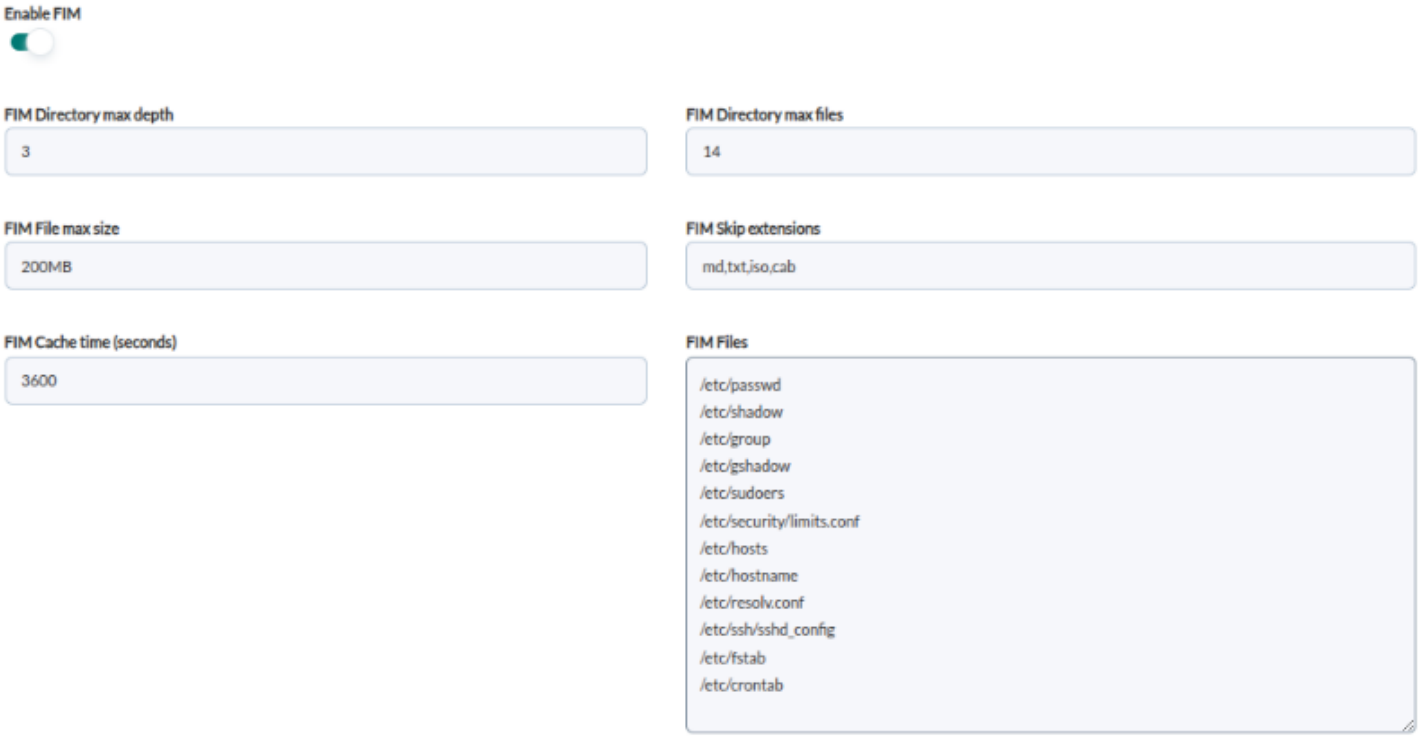
Configuración en un agente

En la pestaña de configuración de seguridad de un agente se puede habilitar o deshabilitar la monitorización FIM:

Management → Resources → Manage agents → Edit → Security → Enable FIM

Al habilitar esta monitorización se permite indicar las rutas a ficheros y directorios que serán comprobados en cada intervalo del EndPoint.

Dentro de la caja de configuración (FIM files) se debe indicar en cada línea la ruta a un fichero o directorio. De acuerdo a cada sistema operativo trae valores por defecto que pueden ser editados, eliminados o agregados, de ser necesario (véase también la configuración de políticas).



Para todas las rutas indicadas se almacenará una caché de tiempo en segundos, FIM Cache time (seconds), para determinar si se ha producido el borrado de algún fichero. Es decir, si un archivo pasa más de los segundos indicados sin ser detectado por el sistema se considerará eliminado.

Para el caso de rutas a directorios, también se podrán indicar algunos parámetros para la detección de cambios en los ficheros que contengan:

- Se podrá indicar la profundidad máxima (número de subdirectorios) dentro del directorio para buscar ficheros.
- También se podrá indicar la cantidad máxima de ficheros a monitorizar en cada directorio, el tamaño máximo de los ficheros dentro del mismo y las extensiones de ficheros que se quieran ignorar.

Para indicar el tamaño máximo de los ficheros (FIM File max size) se debe hacer colocando el valor y la unidad. Para indicar la lista de extensiones a ignorar (FIM Skip extensions) se debe hacer separándolas por medio de comas.

Ficheros a incluir en la búsqueda de FIM

Aquí se especifican una lista de ficheros o directorios que se observará con detalle, para detectar, o bien nuevos ficheros en ese directorio, ficheros que desaparecen o son modificados. El parámetro de máxima profundidad y el parámetro de máximo número de ficheros a tratar en un directorio están pensados para que si se introduce un directorio muy genérico, p.e: `c:\Windows\System32`, el agente no tome demasiados recursos del sistema. Se pueden parametrizar a sus necesidades y también personalizar la lista de directorios y ficheros a analizar.

Se dispone también de una forma de excluir algunos directorios y/o ficheros de la búsqueda, por ejemplo:

```
exclude /opt/myapp/*.tmp
```

O simplemente dejar comentarios colocando un numeral al inicio de cada línea, de esta manera no serán tomados en cuenta y se podrán activar en caso de necesidad:

```
#exclude /opt/myapp/*.tmp
```

Se pueden incluir en la búsqueda directorios dinámicos (con *wildcards* tipo asterisco) de la siguiente manera:

```
C:\Users*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\
```

Configuración en políticas de monitorización

La misma configuración que se puede hacer sobre un agente de forma individual se puede aplicar a través de políticas de monitorización.

Cuando la monitorización FIM esté aplicada desde una política no será posible modificar esta configuración directamente en los agentes.

Al editar una política se contará con una pestaña para habilitar esta opción:

Menú Management → Configuration → Manage policies, clic en el nombre de la política a editar, pestaña File Integrity Monitoring → Apply FIM from this policy.

Además de esa opción también habrá que seguir indicando si FIM está habilitado o no para los agentes de la política (opción Enable FIM). Si esto no está habilitado, la configuración FIM de la política no tendrá lugar.

Estas dos últimas opciones funcionan en conjunto para permitir deshabilitar la monitorización FIM sobre un conjunto de agentes desde la propia política. En un caso como ese, Apply FIM from this policy debería estar habilitado y Enable FIM debería estar deshabilitado.

Para el caso de EndPoints instalados en sistemas operativos MS Windows® se deberán sustituir por los siguientes ficheros en el apartado FIM files:

```
%SystemRoot%\System32\config\SAM
%SystemRoot%\System32\config\SYSTEM
%SystemRoot%\System32\config\SECURITY
%SystemRoot%\System32\config\SOFTWARE
%SystemRoot%\System32\config\DEFAULT
%SystemRoot%\System32\winlogon.exe
%SystemRoot%\System32\lsass.exe
%SystemRoot%\System32\services.exe
%SystemRoot%\System32\smss.exe
%SystemRoot%\System32\svchost.exe
%SystemRoot%\System32\csrss.exe
%SystemRoot%\System32\winload.exe
%SystemRoot%\System32\ntoskrnl.exe
%SystemRoot%\System32\drivers\etc\hosts
%SystemRoot%\explorer.exe
%SystemRoot%\System32\cmd.exe
%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe
%SystemRoot%\System32\wscript.exe
%SystemRoot%\System32\cscript.exe
%SystemRoot%\System32\taskmgr.exe
%SystemRoot%\SysWOW64\kernel32.dll
%SystemRoot%\SysWOW64\user32.dll
%SystemRoot%\SysWOW64\advapi32.dll
%SystemRoot%\SysWOW64\gdi32.dll
%SystemRoot%\SysWOW64\ntdll.dll
%SystemRoot%\SysWOW64\ole32.dll
%SystemRoot%\SysWOW64\shell32.dll
%SystemRoot%\SysWOW64\ws2_32.dll
%SystemRoot%\SysWOW64\cmd.exe
%SystemRoot%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
%SystemRoot%\SysWOW64\wscript.exe
%SystemRoot%\SysWOW64\regsvr32.exe
%SystemRoot%\SysWOW64\mshta.exe
```

Por lo demás, la configuración es exactamente la misma que la aplicada directamente sobre un agente.

Resultado de la monitorización FIM

La monitorización FIM genera los siguientes módulos en cada agente que la tenga habilitada:

- `FIM_status`: Monitoriza si se mantiene la integridad de ficheros o no para el agente.
- `FIM_status_last_change`: Fecha del último cambio de estado de la monitorización FIM.
- `FIM_changed`: Monitoriza la cantidad de ficheros cambiados.
- `FIM_deleted`: Monitoriza la cantidad de ficheros eliminados.
- `FIM_new`: Monitoriza la cantidad de ficheros nuevos encontrados.

Además, para cada fichero nuevo, cambiado o eliminado se generarán entradas de *log* que podrán

visualizarse si la recolección de logs está habilitada.

Integración con SIEM

La monitorización FIM también se integra con la monitorización SIEM, ya que Pandora FMS incorpora de manera predeterminada los *decoders* y *rules* para la generación de eventos SIEM (basándose en las entradas de log generadas para la recolección de logs).

Volver al índice de documentación de Pandora FMS