Monitorización con traps SNMP

Monitorización con traps SNMP

Introducción

Los dispositivos de red que soportan SNMP, como *switches*, *routers*, servidores, impresoras o *Access Panel* pueden enviar alarmas (traps SNMP) cuando suceden determinados eventos, tales como caída de una interfaz, o cuando la carga de la CPU o de la red es muy alta, o si un sistema de alimentación ininterrumpida (SAI o *UPS*) cambia de estado o se llena una partición de disco. Cada dispositivo tiene su propia colección de posibles eventos, que se refleja en una colección, llamaba MIB, en este caso, diferente de la MIB utilizada para hacer consultas al dispositivo.

Los *traps* son enviados solamente cuando sucede algo, de forma asíncrona (no repetitiva en el tiempo) por el dispositivo hacia un receptor de traps SNMP. Pandora FMS tiene una consola de recepción de traps que permite visualizar los traps que envían los objetos monitorizados y añadir alertas a dichos traps. Los traps SNMP se reciben a través del demonio del sistema operativo que el servidor SNMP de Pandora FMS arranca cuando el servidor de Pandora FMS se inicia. Los traps SNMP se almacenan por defecto en:

```
/var/log/pandora/pandora_snmptrap.log
```

La consola SNMP de Pandora FMS *Enterprise* permite crear reglas para renombrar las OID numéricas a OID de tipo alfanuméricas o simples cadenas de texto descriptivas, de forma que sea más intuitivo trabajar con traps SNMP. Pandora FMS también permite cargar los MIB de traps de cualquier fabricante para definir automáticamente esas reglas

Para poder trabajar con traps SNMP, primero modifique el siguiente parámetro en `/etc/pandora/pandora_server.conf` para activar la Consola SNMP:

```
snmpconsole 1
```

Para que los traps SNMP aparezcan traducidos (ya sean los enlaces variables o la cadena Enterprise) se deberá activar los siguientes parámetros:

```
translate_variable_bindings 1
translate_enterprise_strings 1
```

También se debe configurar el archivo `/etc/snmp/snmptrapd.conf` con los parámetros necesarios, por ejemplo:

```
authCommunity log public
disableAuthorization yes
```

Con esta configuración, los traps se crearán para la comunidad public y no requerirán autorización.

SNMPv3

Los traps SNMPv3 son rechazados a menos que el usuario que los envía se añada a `/etc/snmp/snmptrapd.conf` utilizando la directiva ''createUser''. Por ejemplo:

```
disableAuthorization yes
createUser -e 0x0102030405 SNMPv3user SHA mypassword AES
```

Se debe especificar el engineID con la opción `-e`. De lo contrario, sólo se recibirán INFORMs SNMPv3.

Acceso a la consola de recepción de traps

Operation → Monitoring → SNMP → SNMP Console. Mediante el icono de la lupa en la primera columna se puede desplegar toda la información del trap SNMP, otras columnas importantes:

- Status: Cuadrado verde si el trap se ha validado y rojo si no se ha validado.
- SNMP Agent: Agente que ha enviado el trap.
- Enterprise string: OID o Object Identifier (Identificador de Objeto) del trap enviado. Un trap solo puede enviar un dato en este campo.
- Time Stamp: Tiempo que ha transcurrido desde que se ha recibido el trap.

Colores

Además los traps SNMP tienen un color (visto como color de fondo) indicativo de su tipo correspondiente:

- Azul: Tipo mantenimiento.
- Morado: Tipo información.
- Verde: Tipo `normal`.
- Amarillo: Tipo `warning`.
- Rojo: Tipo `critical`.

Validar traps

Con el fin de realizar una gestión efectiva de los traps, es posible validar los mismos para que el administrador pueda discriminar entre los traps que ha visto y por ver. Para validar un trap haga clic sobre el círculo a la izquierda o marcándolos y pulsando el botón Validate.

Borrar traps

Es posible borrar traps una vez que los mismos se han tratado, bien individualmente o mediante selección múltiple y acción Delete.

Para evitar acumulación, existe una opción de configuración que borra automáticamente los traps SNMP transcurridos (pro defecto más de 10 días de antigüedad).

Alertas de Traps SNMP

Introducción

Pandora FMS también dispone de un sistema de alertas para los traps SNMP que recibe. Se basan principalmente en reglas de filtrado, buscando coincidencias en todos los campos posibles de acuerdo a reglas que configure para disparar la alerta.

Añadir una alerta

Las alertas de traps SNMP tienen varios campos que se utilizarán para buscar coincidencias en los traps SNMP recibidos en la consola. Pueden utilizarse de forma opcional los campos que se quieran para crear reglas más generales o más específicas en función de la necesidad. Se accede por el menú Management → Alerts → SNMP alerts → Create. Parámetros importantes:

- Enterprise String: OID principal del trap SNMP. Se buscará la presencia de la cadena, pudiendo incluso ser un trozo del OID; por ejemplo `1.21.34.2.3` en un OID más largo. Se puede emplear del mismo modo en el campo, y realizará la búsqueda como si se tratase de: `*1.21.34.2.3*` (es innecesario emplear asteriscos como caracteres comodines). Para las coincidencias exactas, termine la cadena con el carácter `$` .
- Custom Value/OID: Busca en los campos Value del trap SNMP, así como en los campos Custom OID y Custom Value, es decir, en el resto de campos del TRAP. Aquí funciona la búsqueda por expresión regular. Por ejemplo si tiene un trap SNMP que envía la cadena `Testing TRAP 225` es posible buscar cualquier trap con la subcadena `Testing TRAP` mediante la expresión regular `Testing.*TRAP.*`
- SNMP Agent (IP): Dirección IP del Agente que envía el trap SNMP. *También permite usar una expresión regular o una subcadena*.
- Trap type: Filtra por tipo de trap. La mayoría de los traps generados suelen ser de tipo Other; si no especifica nada, buscará cualquier tipo de trap.
- Single value: Filtra por el valor del trap. Esto solo hace referencia al valor simple del OID principal, no de cualquier OID secundario.
- Variable bindings/Data #1-20: Son expresiones regulares que intentan coincidir con las variables 1 a 20. Si hay un acierto, se dispara la alerta. El valor de la variable se guarda en la macro `_snmp_fx_` correspondiente (`_snmp_f1_`, `_snmp_f2_`, ...). Aunque sólo se puede especificar una expresión regular para veinte variables, las macros `_snmp_fx_` están disponibles para todas ellas

(`_snmp_f11_`, `_snmp_f12_`, ...).
- Alert Action: Combo donde se determina la acción que va a ejecutar la alerta. Si se elige un evento, el evento normal de generación de alerta no se generará.
- Priority: Combo donde se establece la prioridad de la alarma.

Las prioridades de las alertas son diferentes y no tienen nada que ver con la prioridad de los traps SNMP, ni con la de los eventos de Pandora FMS.

Macros de fields en las alertas

Se pueden utilizar las siguientes macros en cualquiera de los campos *field* de las alertas:

- `_data_`: Trap entero.
- `_agent_`: Nombre del Agente.
- `_address_`: Dirección IP.
- `_timestamp_`: Fecha trap SNMP.
- `_snmp_oid_`: OID del trap SNMP.
- `_snmp_value_`: Valor del OID del trap SNMP.

Trabajando en entornos con muchos traps

Protección ante tormenta de traps

Para ello se utilizan los siguientes parámetros de configuración en el fichero `pandora_server.conf` :

- `snmp_storm_protection` : Máximo número de traps procesados en el intervalo de protección.
- `snmp_storm_timeout` : Intervalo en segundos de protección ante tormenta de traps. Durante ese intervalo solo pueden procesarse X traps de la misma fuente (misma dirección IP).
- `snmp_storm_silence_period` : Si es mayor que 0 cada vez que salte el *storm protection* para una fuente concreta, se sumará el tiempo actual más el tiempo de silenciado. Hasta que no pase este tiempo no se registrarán nuevos traps SNMP para la fuente concreta.

La protección ante tormenta de traps, combinada con el filtrado de traps, permite que si se reciben cientos de miles al día, se trabaje con unos pocos miles, evitando los redundantes o inútiles.

Filtrado de traps en el servidor

Algunos sistemas reciben un número elevado de traps SNMP de los cuales sólo interesa monitorizar un pequeño porcentaje. Desde Monitoring → SNMP → SNMP Filters se pueden definir distintos filtros. Se pulsa el botón Create, se agrega una descripción y tantos filtros como necesite

con el botón +.

Personalizar Traps SNMP

Las siguientes características son de la versión Enterprise únicamente.

Renombrado y personalización de traps

Tenga en cuenta que todos los traps anteriores no cambiarán su aspecto, esto entrará en funcionamiento con los nuevos traps que entren en el sistema a partir de este momento.

Editar un trap SNMP es el proceso para *personalizar* el aspecto que tiene un trap SNMP en la Consola web. Para editar un trap se utiliza el menú Operation → Monitoring → SNMP → SNMP trap editor.

El Custom OID es una expresión regular compatible con lenguaje Perl que se comparará con la parte de la cadena del trap SNMP que contiene los variable *bindings*. No suele ser necesario para traducir un trap.

Custom OID no está pensado para contener la cadena de variable *bindings* completa, que puede ser más larga que la máxima longitud que soporta, sino una expresión regular que encaja con una o más variables.

Subir las MIB del fabricante

Esta opción sirve para subir MIB y ampliar la base de datos interna de traducción de Pandora FMS, de forma que cuando llegue un trap SNMP, sea automáticamente traducido por su descripción. Se accede por medio del menú Operation → Monitoring → SNMP → MIB uploader.

Asociar un trap al resto de alertas de Pandora FMS

Esta es una característica *Enterprise* y se configura en Management → Setup → Setup → Enterprise → Forward SNMP traps to an agent (if it exists).

Si se cambia esta opción, hay que reiniciar el servicio del servidor de Pandora FMS para que empiece a actuar.

Esta opción (general al servidor) reenvía el trap SNMP a un Módulo especial del Agente llamado SNMPTrap como cadena de texto, si y solo si, la dirección IP origen del trap SNMP está definida como IP de un agente. Cuando esto ocurre, el trap SNMP llega como una línea de texto al Agente dentro de ese Módulo, que es un Módulo que se define solo cuando llega el primer trap SNMP.

Sobre ese Módulo se pueden especificar alertas de texto, siendo estas completamente estándar, como las de cualquier módulo. Esto permite personalizar la monitorización SNMP para que ciertos traps, de ciertos orígenes puedan ser tratados como un módulo más, y así integrarlo en el resto de la monitorización, incluyendo la correlación de alertas.

Otra solución es montar una alerta sobre el trap SNMP que active un módulo de un agente. Por ejemplo, el trap SNMP consiste escribir en un fichero de *logs*, y se tiene un agente que lee ese fichero y se ejecute cuando hay un 1 escrito. De esta forma, el módulo saltará cuando se reciba el trap SNMP deseado y se podrá establecer la correlación en base al trap recibido.

Gestor externo de traps SNMP

La consola de SNMP está limitada a recibir traps SNMP, ya que solo procesa TRAP como ente individual, pero un trap SNMP puede contener mucha información.

A veces ocurre que la única monitorización que se puede hacer está basada en traps SNMP.

Para ello se puede optar por procesar de nuevo la información recogida en un trap SNMP a través de un *script* externo, que actúa a modo de *plugin*.

Para ello se debe crear un comando de alerta que ejecute dicho *script* para postprocesar el trap SNMP recibido.

La aplicación de esta tecnología es sumamente amplia por ello cada *script* debe ser particularizado ya que puede tener una estructura muy dinámica. En muchos sistemas la información que se recibe, no solo es de texto, si no también numérica, con lo que puede alimentar a módulos de información numéricos y así representar gráficas etc. Siempre habrá que tener en cuenta que los datos generados en el XML deberían ser siempre de tipo asíncrono.

SNMP trap forwarding

Con Pandora FMS es posible habilitar el reenvío de traps SNMP a un *host* externo habilitando el snmp_forward_trap en el *token* en el fichero de configuración de Pandora.

Gestión independiente del demonio snmptrapd

Es posible que por alguna razón se prefiera gestionar el demonio snmptrapd de forma independiente a Pandora FMS (para detenerlo o iniciarlo de forma independiente al *daemon* principal de Pandora FMS). Para ello, debe tener en cuenta varias cosas:

1. Debe activar igualmente el parámetro `snmpconsole` en el servidor de Pandora FMS.

2. Los *logs* configurados en el servidor de Pandora FMS deben ser los mismos que se generen en la llamada independiente a snmptrapd

3. La llamada a snmptrapd debe tener un formato específico ya que la llamada al demonio estándar del sistema es inválida. La llamada debe ser como esta (el parámetro `-A` es especialmente importante):

```
/usr/sbin/snmptrapd -A -t -On -n -a -Lf /var/log/pandora/pandora_snmptrap.log -p
/var/run/pandora_snmptrapd.pid --format1=SNMPv1[**]%4y-%02.2m-
%l[**]%02.2h:%02.2j:%02.2k[**]%a[**]%N[**]%w[**]%W[**]%q[**]%v\n --
format2=SNMPv2[**]%4y-%02.2m-%l[**]%02.2h:%02.2j:%02.2k[**]%b[**]%v\n
```

4. Debe configurar en el fichero de configuración del servidor, el *token*:

```
snmp_trapd manual
```

5. Cuando establezca este funcionamiento debe realizar la siguiente operación:

- Cambiar la configuración en `/etc/pandora/pandora_server.conf`.
- Detener el servidor de Pandora FMS.
- Finalizar el proceso snmptrapd.
- Arrancar snmptrapd manualmente (con el formato indicado arriba).
- Arrancar el servidor de Pandora FMS.

Gestión del fichero de log de traps

El proceso *snmptrapd* puede ser parado y arrancado sin necesidad de parar y arrancar el proceso de Pandora FMS server, siempre y cuando los ficheros `pandora_snmptrap.log.index` y `pandora_snmptrap.log` no sean modificados. Si estos ficheros son modificados, es preciso reiniciar el servidor de Pandora FMS. Si necesita rotar de forma externa el *log* de traps, deberá

reiniciar el servidor de Pandora FMS después de borrar los ficheros anteriormente mencionados.

Buffering de traps SNMP

Es más eficiente que la consola SNMP procese directamente los traps desde el fichero de *log* de snmptrapd. Esta configuración se recomienda sólo si la fiabilidad o la conectividad directa son motivo de preocupación.

Si los traps SNMP se envían a un manager externo a través de una conexión poco fiable se perderá parte de la información. Pandora FMS le permite, en vez de eso, reenviar los traps desde un snmptrapd local a su servidor de Pandora FMS de una forma fiable.

Prerrequisitos:

- Un snmptrapd local que está recibiendo traps.
- Un agente de Pandora FMS local.
- Una instalación de Pandora FMS.

snmp_extlog puede ser cualquier fichero en el que el servidor de Pandora FMS pueda escribir, pero tiene que ser distinto de snmp_logfile (también definido en `/etc/pandora/pandora_agent.conf`).

Generador de Traps

Esta herramienta permite generar traps SNMP personalizados que posteriormente puede observar en la consola SNMP. Se accede por el menú Operation → SNMP → SNMP trap generator.

En el SNMP Type escoja un tipo de SNMP entre las siguientes opciones:

- Cold Start: Indica que el agente se ha iniciado o reiniciado.
- Warm Start: Indica que la configuración del agente ha sido modificada.
- Link down: Indica que la interfaz de comunicación está fuera de servicio (inactiva).
- Link up: Indica que una interfaz de comunicación se ha activado.
- Authentication failure: Indica que el agente recibió una solicitud de un NMS no autorizado (controlado por la comunidad).
- EGP neighbor loss: Indica que en los sistemas donde los enrutadores que usan el protocolo EGP, un *host* cercano está fuera de servicio.
- Enterprise: En esta categoría se encuentran todos los traps SNMP nuevos, incluidos los de proveedores.

Volver al índice de documentación de Pandora FMS