Sistema de alertas

Sistema de alertas

Introducción

Una alerta es la reacción de Pandora FMS a un valor incorrecto de un Módulo. Dicha reacción es configurable y puede consistir en cualquier cosa que pueda ser desencadenada por un *script* configurado en el Sistema Operativo donde corre el servidor de Pandora FMS que procesa el Módulo, Evento o Log.

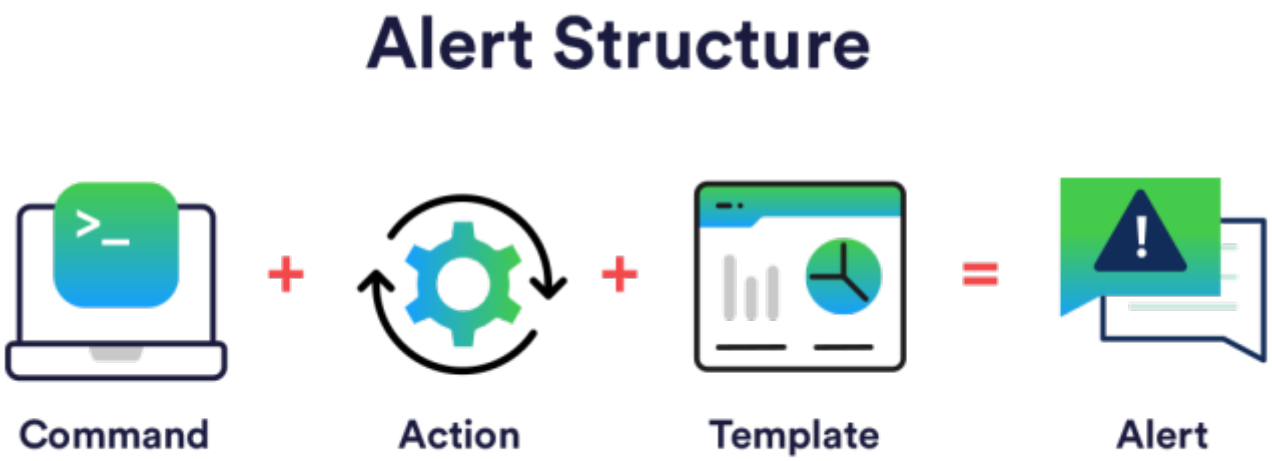
En Pandora FMS, las alertas funcionan mediante la definición de unas condiciones de disparado, unas acciones elegidas para esa alerta, y finalmente la ejecución de unos comandos en el servidor de Pandora FMS, que se encargarán de llevar a cabo las acciones configuradas.

Existen varios tipos de alertas:

- Alertas simples.
- Alertas sobre eventos.
- Alertas sobre traps SNMP.
- Alertas sobre logs.
- Alertas sobre eventos de seguridad (SIEM).
- Alertas sobre inventario.

Pandora FMS también tiene un sistema de gestión de paradas de servicio planificadas o agendadas en el menú Management → Alerts → Scheduled downtime. Este sistema permite desactivar las alertas en los intervalos que existe una parada de servicio.

Estructura de una alerta



- Comandos: Especifican *qué se hará;* será la ejecución que realizará el servidor de Pandora FMS al disparar la alerta.
- Acciones: Especifican *cómo se hará;* son las personalizaciones de los argumentos del comando.
- Plantillas: Especifican *cuándo se hará;* definen las condiciones para disparar la acción o acciones.

Flujo de información en el sistema de alertas

Las plantillas y las acciones tienen una serie de campos genéricos llamados `Field1` , `Field2` , `Field3`, (...) , `Field`*n* los cuales se utilizan para transferir la información desde la *plantilla* a la *acción* y de la acción al *comando*, para finalmente utilizarse como parámetros en la ejecución de dicho comando.

Dicha información se transfiere siempre que el paso siguiente no traiga ya información definida en sus campos `Field`n. Es decir, en caso de solapamiento de campos o parámetros, sobrescribe la acción a la plantilla (por ejemplo, si la plantilla tiene definida `Field1` y la acción también, el `Field1` de la acción *sobrescribe* la acción de la plantilla).

Comando de Alerta

Introducción

Menú Management → Alerts → Commands.

Las acciones que realizará Pandora FMS ante situaciones de alerta se traducirán al final en ejecuciones en el servidor, en forma de comandos.

Para crear comandos de alerta debe acceder como superusuario PFMS.

Creación de un comando para una alerta

Menú Management → Alerts → Commands → Create.

Se recomienda comprobar desde la línea de comandos si la ejecución del comando tiene éxito y que produce el resultado deseado (enviar un correo electrónico, generar una entrada en un fichero de registro, etcétera).

- Command: Comando que se ejecutará al disparar la alerta. Es posible utilizar macros para reemplazar los parámetros configurados en la declaración de las alertas.
- Group: Esto determina a qué grupo de alertas puede asociar el comando. Solamente podrá asignar un grupo al cual pertenezca el usuario que está creando el comando de alerta, a menos que dicho usuario pertenezca explícitamente al grupo TODOS (ALL).
- Field description y Field values:
  - Valores de campo disponibles: Una colección de posibles valores para ese campo. Si este campo está configurado (no está vacío), el campo será un combo de selección en lugar de una caja de texto. El combo necesita para cada posible valor una etiqueta (la opción visible) y un valor (la opción enviada). La sintaxis es la siguiente: valor1,etiqueta1;valor2,etiqueta2;valor3,etiqueta3;valorN,etiquetaN.
  - Hide: Si el campo alberga alguna contraseña, esta opción oculta con asteriscos el contenido.
- Es posible mostrar un editor de código HTML en un campo del comando en la creación o edición de una acción de una alerta si ese campo del comando tiene como valor el *token* especial `_html_editor_` .

Se debe tener en cuenta que los comandos para las alertas ejecutados por el servidor de Pandora FMS se realizan con los mismos privilegios del usuario que ejecuta el servidor de Pandora FMS.

Comandos predefinidos

- eMail: Envía un correo electrónico desde el Pandora FMS Server. Los mensajes de correo electrónico son enviados en formato HTML. Se debe tener en cuenta que el receptor debe poder acceder a los recursos utilizados en la plantilla, como por ejemplo las imágenes.
- Internal audit: Genera una entrada en el sistema de auditoría interna de Pandora FMS. Este se almacena en la base de datos de Pandora FMS y puede revisarse con el visor de eventos desde la consola.
- Monitoring Event: Crea un evento personalizado en la consola de eventos de Pandora FMS.
- Alertlog: Es una alerta predefinida que escribe las alertas en formato de ASCII plano en el fichero `/var/log/pandora/pandora_alert.log` .
- SNMP Trap: Envía un *trap* SNMP parametrizado con los argumentos que se utilicen.

- Syslog: Envía una alerta al registro del sistema por medio del comando del sistema logger.
- Sound Alert: Reproduce un sonido en la consola sonora de eventos cuando ocurre una alerta.
- Jabber Alert: Envía una alerta Jabber a una sala de conversación en un servidor predefinido (primero se debe configurar el fichero `.sendxmpprc`). Coloque en `field1` el alias de usuario, en `field2` el nombre de la sala de chat y `field3` el mensaje de texto.
- SMS Text: Envía un SMS a un teléfono móvil determinado. Primero es necesario definir una alerta y configurar una *gateway* de envío de SMS que sea accesible desde el Pandora FMS Server.
- Validate Event: Valida todos los eventos relacionados con un módulo. Se le pasará el nombre del agente y el nombre del módulo.
- Remote agent control: Envía comandos a los agentes con el servidor UDP habilitado. El servidor UDP se utiliza para ordenar a los agentes (MS Windows® y UNIX®) que *refresquen* la ejecución del agente: es decir, para obligar al agente a ejecutar y enviar datos.
- Generate Notification: Permite enviar una notificación interna a cualquier usuario. Los destinatarios deben ser agregados de memoria y cada usuario borrará su notificación cuando pueda y/o considere conveniente.
- Send report by e-mail y Send report by e-mail (from template): Ambas opciones permiten enviar un informe en distintos formatos (PDF, JSON, CSV) por correo electrónico, la segunda opción permite utilizar una plantilla para dicho informe adjunto.

Cuando se establece una URL pública para una Consola web, los mensajes de correo electrónico que se envíen tendrán ese enlace establecido.

- Console notification: Permite enviar una notificación por Consola web a cualquier usuario. Los destinatarios disponibles se agregarán de manera interactiva. Las notificaciones aparecerán y desaparecerán según se dispare o recupere la alerta correspondiente. Además, los mensajes serán borrados definitivamente según el *token* Max. days before delete old messages. Mediante macros preconfiguradas se mostrará información del agente, módulo, etc. Se debe asegurar de que el destinatario tenga derechos de lectura suficientes sobre los elementos alertados.
- API request: Realiza una consulta API mediante una acción de alerta construida en base a este comando. Se necesitarán, en este orden, los siguientes parámetros:

1. URL: Dirección IP o enlace web al servidor API donde se realizará la consulta.
2. Method: Método a utilizar, de una lista de opciones (GET, POST, PUT, PATCH, DELETE), similares a las utilizadas por la API PFMS (excepto PATCH).
3. Headers: Para incluir formato de solicitud (generalmente en formato JSON), *token* de autorización, etc.
4. Data: La consulta en sí misma y sus parámetros respectivos.
5. SSL: Indica si se utilizará una conexión cifrada para realizar la conexión.

Una solicitud típica incluye código similar a este:

- HEADER:

```
Authorization: Bearer abc123token; Content-Type: application/json; X-Request-ID: 123456
```

- DATA:

```
{'title': 'foo', 'body': 'bar'}
```

Edición de un comando para una alerta

Menú Management → Alerts → Commands → clic sobre el nombre del comando a editar. Una vez se ha modificado la alerta elegida haga clic en el botón Update.

Los siguientes comandos de sistema son inalterables:

- `eMail` (Id. 1).
- `Internal Audit` (Id. 2).
- `Monitoring Event` (Id. 3).
- `Validate Event` (Id. 10).
- `Generate Notification` (Id. 13).
- `Send report by e-mail` (Id. 14).
- `Send report by e-mail (from template)` (Id. 15).
- `Pandora ITSM Ticket` (Id 16).
- `Pandora Telegram` (Id 19, grabar *token* en configuración general).
- `RMM Script` (Id. 22).
- `Console notification` (Id. 23).

Acción

Introducción

Las acciones son los componentes de las alertas en los que se relaciona un comando con las variables genéricas `Field 1`, `Field 2`, ... , `Field 10`.

Las acciones permiten definir *el cómo* lanzar el comando.

Creación de una Acción

Menú Management → Alerts → Actions → Create.

Si se va a crear una acción de alerta basada en alguno de los comandos de alerta predefinidos resulta más práctico copiar la acción de alerta predefinida y luego modificarla.

- Group: El grupo de la acción. Solamente podrá asignar un grupo al cual pertenezca el usuario que está creando el comando de alerta, a menos que dicho usuario pertenezca explícitamente al grupo TODOS (ALL). Si el comando asociado tiene un grupo diferente de *All*, solo se podrá establecer como grupo de la acción el grupo asociado al comando o el grupo *All*. Si por alguna razón esto llega a diferir, verá un mensaje de advertencia para su pronta corrección por parte de un usuario que tenga los derechos necesarios.
- Command: Comando que se usará en el caso de que se ejecute la alerta. Se puede elegir entre los diferentes comandos que hay predefinidos en Pandora FMS.
- Threshold: Una acción de alerta se ejecuta solo una vez dentro de este intervalo de tiempo, independientemente de cuántas veces se active la alerta.
- Command Preview: En este campo, *no editable*, aparecerá automáticamente el comando que se va a ejecutar en el sistema.
- Field 1 ~ Field 10: En caso de ser necesario, en estos campos se define el valor de las macros, de `_field1_` a `_field10_`, que se usarán en el comando. Estos campos pueden ser un campo de texto o un combo de selección si se configura.

Cuando se asigna un valor a los Field en la sección Triggering, de forma predefinida *serán los mismos valores para Recovery, a menos que se asigne un valor diferente*.

Acciones predefinidas de alerta

- Console notification: Este comando le permite generar una notificación al supervisor cuando se activa una alerta. Utiliza el comando predefinido de alerta `Console notification`. Al modificar esta acción predefinida se pueden seleccionar los usuarios que serán notificados.
- Create Pandora ITSM ticket: Al tener activada la integración con Pandora ITSM se podrán crear incidencias de manera automática en dicha aplicación.
- Mail to Admin: Utiliza el comando predefinido `eMail` para enviar mensaje de correo electrónico según se configure en el campo Destination address.
- Monitoring Event: Utiliza el comando del mismo nombre y se pueden configurar los tipos y severidad (disparado y recuperación) de eventos, entre otros detalles.
- Pandora ilert, Pandora Slack, Pandora Telegram, Pandora Vonage: Pandora FMS puede enviar notificaciones, previa configuración, en varias aplicaciones de mensajería instantánea.
- Restart agent: Permite enviar instrucciones (reiniciar por defecto) según comando `Remote agent control` a los EndPoints PFMS.
- Send Report by e-mail y Send Report by e-mail (from template): Para el envío de informes por correo electrónico. Aquí se podrán configurar los destinatarios, informe como tal (o plantilla) y el formato del mismo (PDF, JSON o CSV).

Editar una Acción

Menú Management → Alerts → Actions → clic sobre el nombre de la acción a modificar.

Borrar una acción

Menú Management → Alerts → Actions → clic en icono correspondiente de papelera (columna Delete).

Plantilla de alerta

Introducción a plantillas de alerta

Menú Management → Alerts → Templates.

Las plantillas definen las condiciones de disparo de la alerta (*cuándo* ejecutar la acción). Se asocian a Módulos, de tal manera que en el momento en que se reúnan las condiciones de la plantilla, se ejecutarán la(s) acción(es) asociada(s). Su diseño permite generar un grupo reducido de plantillas genéricas que sirvan para la mayoría de casos posibles en Pandora FMS.

Creación de una Plantilla

Menú Management → Alerts → Templates → Create.

Paso 1: General

- Group: El grupo al cual le será aplicada la plantilla. Solamente podrá asignar un grupo al cual pertenezca el usuario que está creando la plantilla , a menos que dicho usuario pertenezca explícitamente al grupo TODOS (ALL).
- Priority: Campo informativo acerca de la alerta. El evento generado al disparar la alerta heredará esta prioridad, útil para filtrar en búsquedas de alertas.

Paso 2: Condiciones

- Use special days list: Establece el calendario de días especiales que se usará en la plantilla.

- Time Threshold: Tiempo que debe transcurrir para reiniciar el contador de alertas. Define el intervalo de tiempo en el cual se garantiza que una alerta no se va a disparar más veces del número establecido en Max. number of alerts. Pasado el intervalo definido se reiniciará el contador. El reinicio del contador de disparos no se reiniciará si la alerta se recupera al llegar un valor correcto, *salvo que esté activado* el valor Reset counter for non-sustained alerts, en cuyo caso, el contador se reiniciará inmediatamente después de recibir un valor correcto.
- Min number of alerts: Número mínimo de veces que tiene que ocurrir la situación definida en la plantilla (contando siempre a partir del número definido en el parámetro Flip Flop del Módulo) para empezar a disparar una alerta. El valor por defecto es 0, lo que significa que la alerta se disparará cuando llegue el primer valor que cumpla la condición. Funciona como un filtro, útil para ignorar falsos positivos.
- Max number of alerts: Máximo número de alertas que se pueden enviar consecutivamente en el mismo intervalo de tiempo (Time Threshold). Es el valor máximo del contador de alertas. No llegarán más alertas por intervalo de tiempo que las indicadas en este campo.
- Default Action: En esta lista se define la acción por defecto que va a tener la plantilla. Esta es la acción que se creará automáticamente cuando asigne la plantilla al módulo. Coloque una acción o ninguna, sin *embargo no puede colocar varias acciones por defecto*.
- Schedule: Establece los días en los que la alerta podrá dispararse. Es posible ver y configurar cuándo estará activa la alerta cada día de la semana gracias al editor incorporado que se muestra por defecto en modo simple. Además, accediendo al modo detallado se pueden configurar los horarios con mayor precisión.
- Reset counter for non-sustained alerts: Su activación depende de que el número indicado en Min. number of alerts sea mayor que 0. Al activar este *token* se reinicia el contador de alertas cuando no se repita la condición indicada de manera consecutiva. Por ejemplo, si el campo Min. number of alerts tiene un valor de 2, significará que el módulo tiene que pasar 3 veces por el estado asignado en Condition type para disparar la alerta. Hay dos escenarios con este último *token*:
- Si el *token* de reinicio está marcado será necesario que el número de estados críticos sea consecutivo, de lo contrario el contador se reiniciará.

```
normal -> critical -> critical -> critical
```

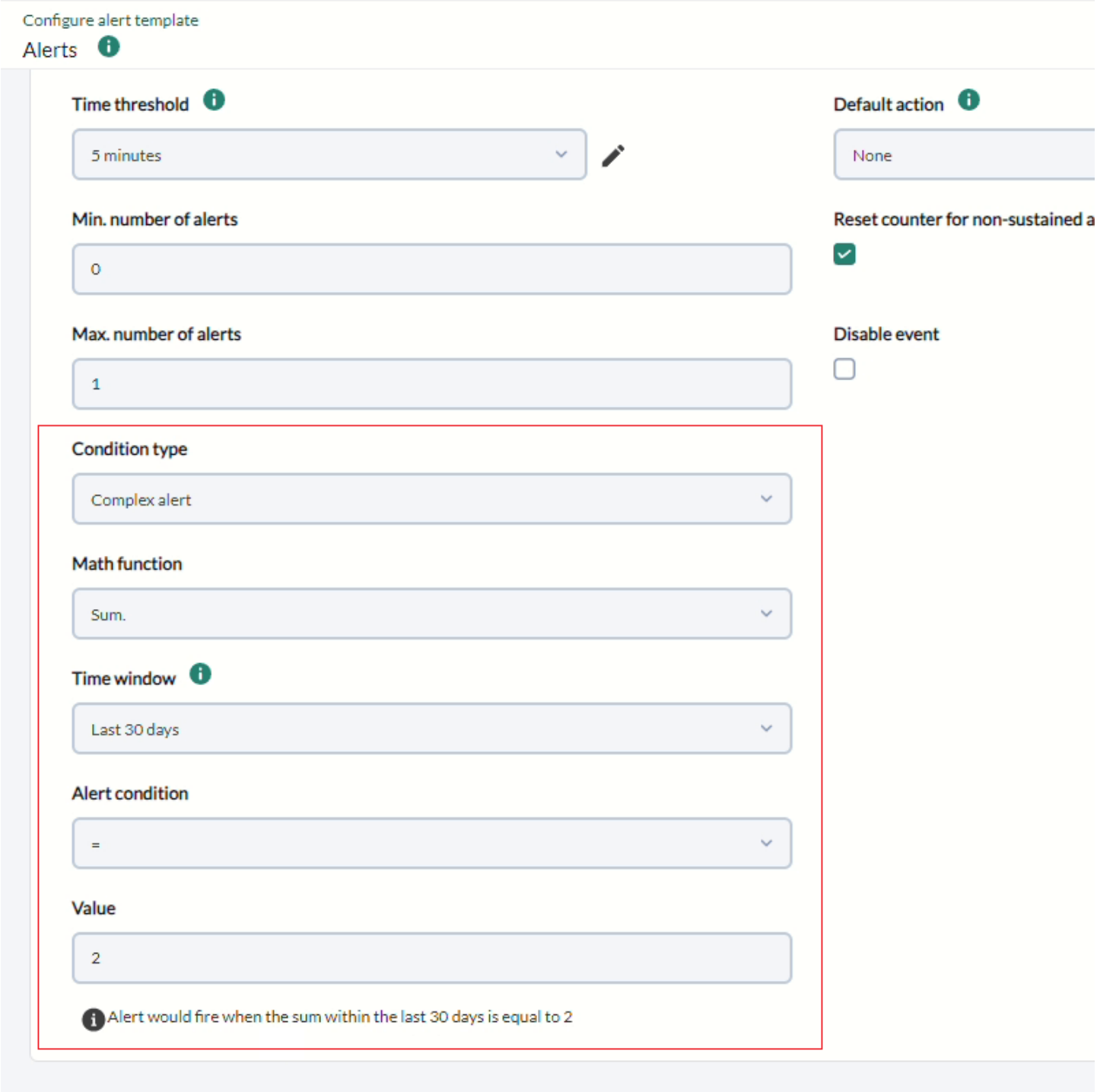
- Si no se marca el *token* de reinicio, la alerta se disparará tras una secuencia alternativa o continua de estados críticos:

```
normal -> critical -> normal -> critical -> normal -> critical
```

Para comprobar de forma periódica los módulos en estado desconocido (Unknown status) bien puede activar el *token* `unknown_updates` en la configuración del servidor PFMS.

- Disable event: Marcando este *token*, el evento generado en la vista de eventos de disparo de alerta no se creará.
- Condition type: Permite especificar el elemento que desencadenará la alerta, como por ejemplo que esté en estado crítico (Critical estatus) o que simplemente sea distinto al estado normal (Not normal status). También se pueden establecer alertas complejas (Complex alerts), por ejemplo que la suma

sea exactamente igual a dos en los últimos treinta días:



Paso 3: Campos avanzados

- Alert recovery: Combo donde puede definir si habilita o no la recuperación de alertas. En el caso de que la recuperación de alerta esté habilitada, cuando el módulo deje de cumplir las condiciones indicadas por la plantilla, se ejecutará la acción asociada con los argumentos especificados por los campos `field` definidos en esta columna.
- En todas las instancias de los campos `field1` ... `field10` (tanto en la plantilla de alerta, como en el comando y en la acción) se pueden emplear las definidas en la lista de macros.

Una vez se ha completado la configuración finalice haciendo clic en el botón Finish.

Plantillas de alerta predefinidas

Plantillas que vienen creadas por defecto:

1. Critical condition: Configurado con una *severidad crítica*, un tipo de condición en *estado crítico*, con acción por defecto el envío de mensaje de correo electrónico al administrador y con recuperación de alerta activada.
2. Manual alert: Esta es una plantilla usada para disparar alertas manuales, *la condición definida aquí nunca será ejecutada*. Se utiliza esta plantilla para asignar a las acciones y comandos utilizados para hacer la gestión remota (reinicio del EndPoint, ejecutar comandos en el servidor, etcétera).
3. Warning condition: Configurado con una *severidad de advertencia*, un tipo de condición en *estado de advertencia*, con acción por defecto el envío de mensaje de correo electrónico al administrador y con recuperación de alerta activada.
4. Unknown condition: Configurado con una *severidad de advertencia*, un tipo de condición en estado desconocido, con acción por defecto el envío de mensaje de correo electrónico al administrador y con recuperación de alerta activada.
5. Default critical condition: Las cuatro plantillas anteriores pueden ser personalizadas, esta plantilla es de solamente lectura (plantilla de sistema) y es una copia de la plantilla Critical condition. Se incluye así dada la importancia del estado de criticidad.

Asignar Plantillas de alerta a los módulos

Gestión de Alertas desde el submenú de Alertas

Asignación de Alertas desde el submenú de Alertas

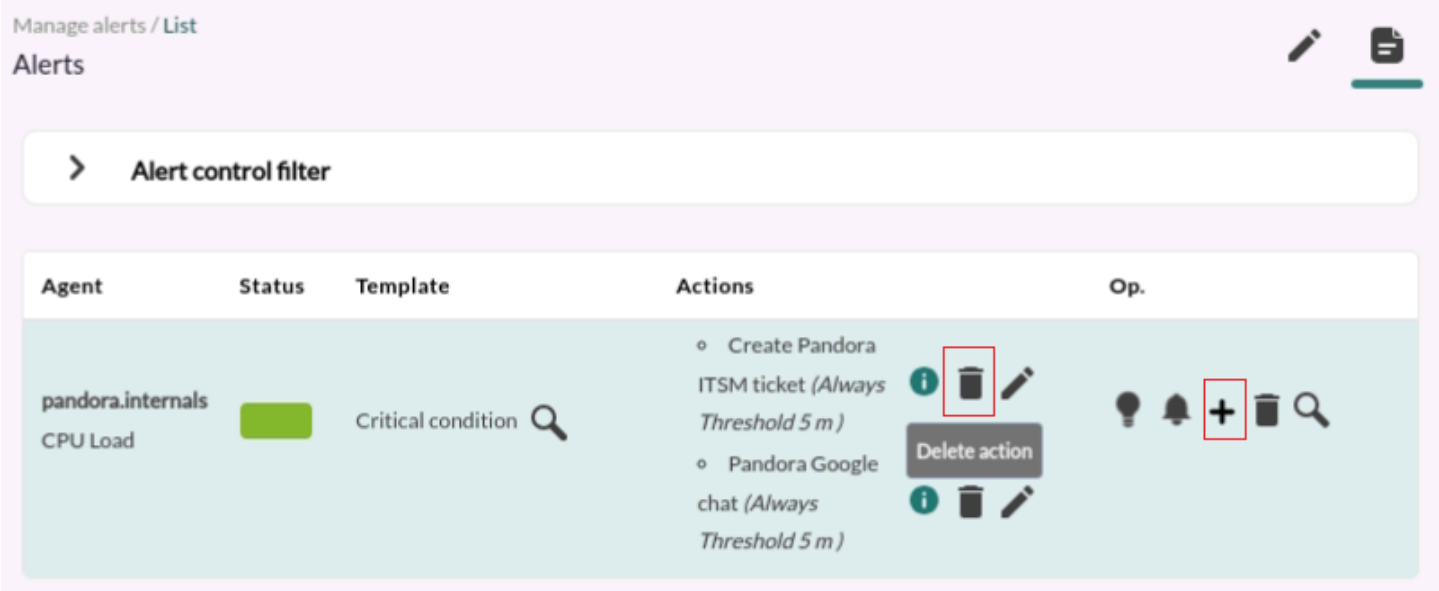
Menú Management → Alerts → Module Alerts → clic en el icono de lápiz Builder alert.

- Agent: Autocompletado para elegir el Agente.
- Module: Listado de módulos del Agente anteriormente seleccionado.
- Actions: Acción que se ejecutará al disparar la alerta. Si la plantilla ya tiene una acción por defecto puede dejarse en Default.
- Template: Plantilla que contendrá las condiciones de disparo de la alerta.
- Threshold: Una acción de alerta no será ejecutada más de una vez cada `action_threshold` segundos, a pesar del número de veces que la alerta sea disparada. Este umbral tiene prioridad sobre la configuración del umbral de la acción.

Modificar alertas desde el submenú de Alertas

Una vez que se ha creado una alerta, solamente será posible modificar las acciones que se hayan añadido a la acción que tiene la plantilla.

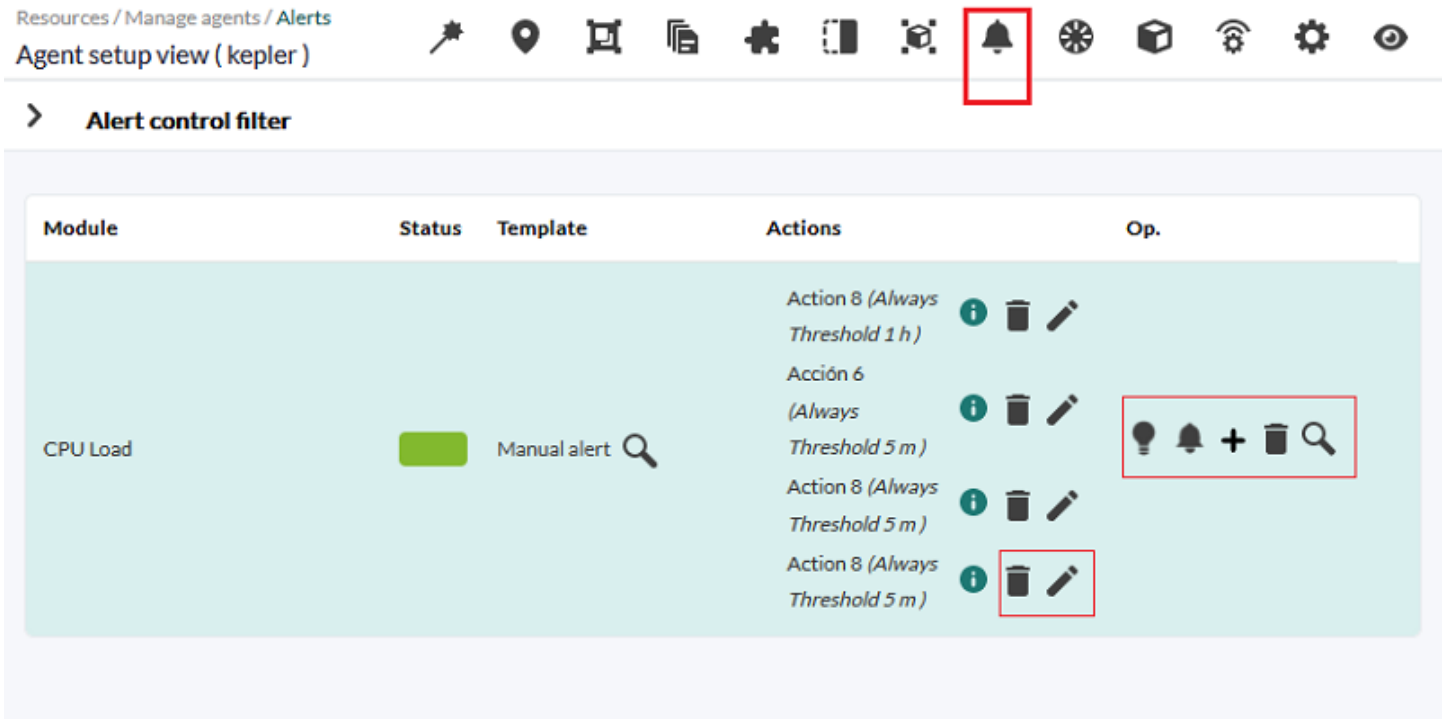
También es posible suprimir la acción que fue seleccionada cuando se creó la alerta haciendo clic en el icono de papelera gris que está a la derecha de la acción, o añadir nuevas acciones haciendo clic en el botón +.



A partir de la versión 781 la acción por defecto solamente es mostrada si es la única existente.

Gestionar alertas desde el agente

Desde la sección de administración del agente puede añadir nuevas alertas navegando a la solapa correspondiente:



Allí se podrá:

- Editar o borrar todas y cada una de las acciones de cada alerta asignada al agente (columna Actions).
- De la columna de opciones (Op.):

- Podrá deshabilitar o habilitar.
- Podrá colocar la alerta en modo *standby* .
- Podrá agregar una acción.
- Podrá borrar por completo la alerta.
- Podrá visualizar en detalle la alerta.

Visión general de una alerta

- Definir umbral crítico y de advertencia en módulo.
- Asociar la alerta al módulo, para ello vaya a la solapa de alertas dentro del Agente donde está el Módulo.

De ser necesario se puede crear una acción nueva y/o plantilla nueva, al hacer clic en esos botones se redirigirá a las secciones correspondientes. Una vez se haya(n) creado los nuevos componentes, se debe regresar al paso anterior.

- Con el botón Add alert se guarda la nueva alerta.
- *Escalado de alertas:* Un escalado de alertas son acciones adicionales que se ejecuten si la alerta se repite una cierta cantidad de veces de forma consecutiva.
    - Únicamente se necesita añadir las acciones adicionales y determinar entre cuáles repeticiones consecutivas (Number of matching alerts) de la alerta va a ejecutar esta acción.
    - Cuando una alerta se recupera, todas las acciones que se hayan ejecutado hasta ese momento se volverán a ejecutar, no solo las que correspondan a la configuración de Number of alerts match from actual.
    - De manera adicional se puede colocar un Threshold como segundo parámetro, por el cual no

podrá lanzarse una alerta más de una vez durante dicho intervalo.
- Finalmente se puede configurar envío de mensajes de alerta por medio de mensajería instantánea como Telegram, por ejemplo.

Alertas en Standby

Las alertas pueden estar activadas, desactivadas o en modo de espera (*standby*). La diferencia entre las alertas desactivadas y las que están en *standby* es que las desactivadas simplemente no funcionarán y por lo tanto no se mostrarán en la vista de alertas. En cambio, las alertas en *standby* se mostrarán en la vista de alertas y funcionarán pero solamente a nivel de visualización. Esto es, se mostrará si están o no disparadas *pero no realizarán las acciones que tengan programadas ni generarán eventos*.

Las alertas en *standby* son útiles para poder visualizarlas sin que molesten en otros aspectos.

Protección en cascada

La protección en cascada es una característica de Pandora FMS que permite evitar un bombardeo masivo de alertas cuando un grupo de Agentes no es accesible, debido a una conexión principal que falla.

Este tipo de cosas ocurren, por ejemplo, cuando un elemento de la red intermedio como un *router* o un *switch* fallan, y deja inaccesible a una gran parte de la red gestionada con Pandora FMS. Debido a que los chequeos de red fallarían en este escenario, comenzarían a dispararse alertas por dispositivos caídos sin ello ser cierto.

Para que funcione el agente con protección en cascada activada debe tener correctamente configurado el Agente padre (Advanced options, *token* Parent), del cual depende.

Si el Agente padre tiene en ese momento alguna alerta de Módulo en estado crítico disparada, *el agente inferior con protección en cascada solamente ejecutará sus alertas de módulos en estado* `warning` o `unknown`.

La protección en cascada se activa desde la configuración del Agente, sección Advanced options, haga clic en la opción Cascade protection modules y/o Cascade protection services.

Protección en cascada basada en servicios

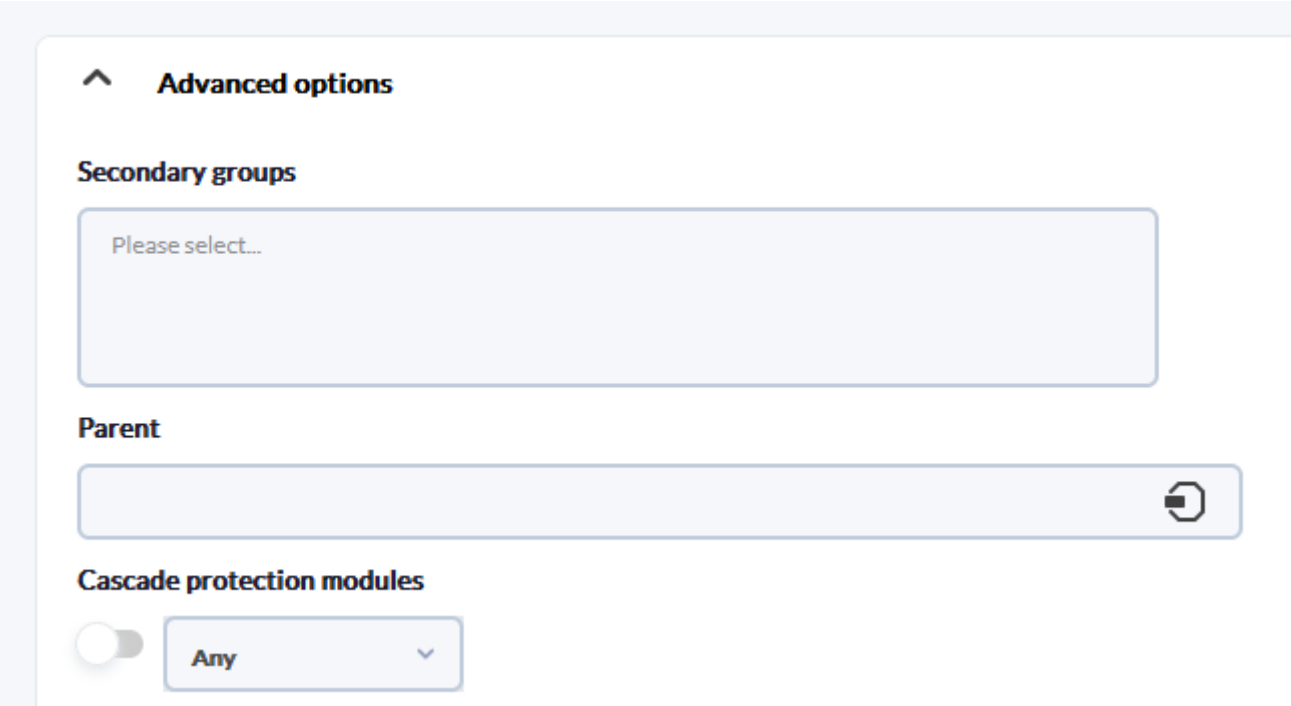
La Protección en cascada basada en servicios evita que los elementos de un servicio disparen sus alertas si se dispara la alerta del servicio al que pertenecen.

Para habilitar esta funcionalidad, se debe activar el *token* Cascade protection services en la configuración avanzada de los agentes a los cuales se necesite el tener este comportamiento, y activar el *token* Cascade protection enabled en la configuración del servicio al que pertenezcan dichos agentes.

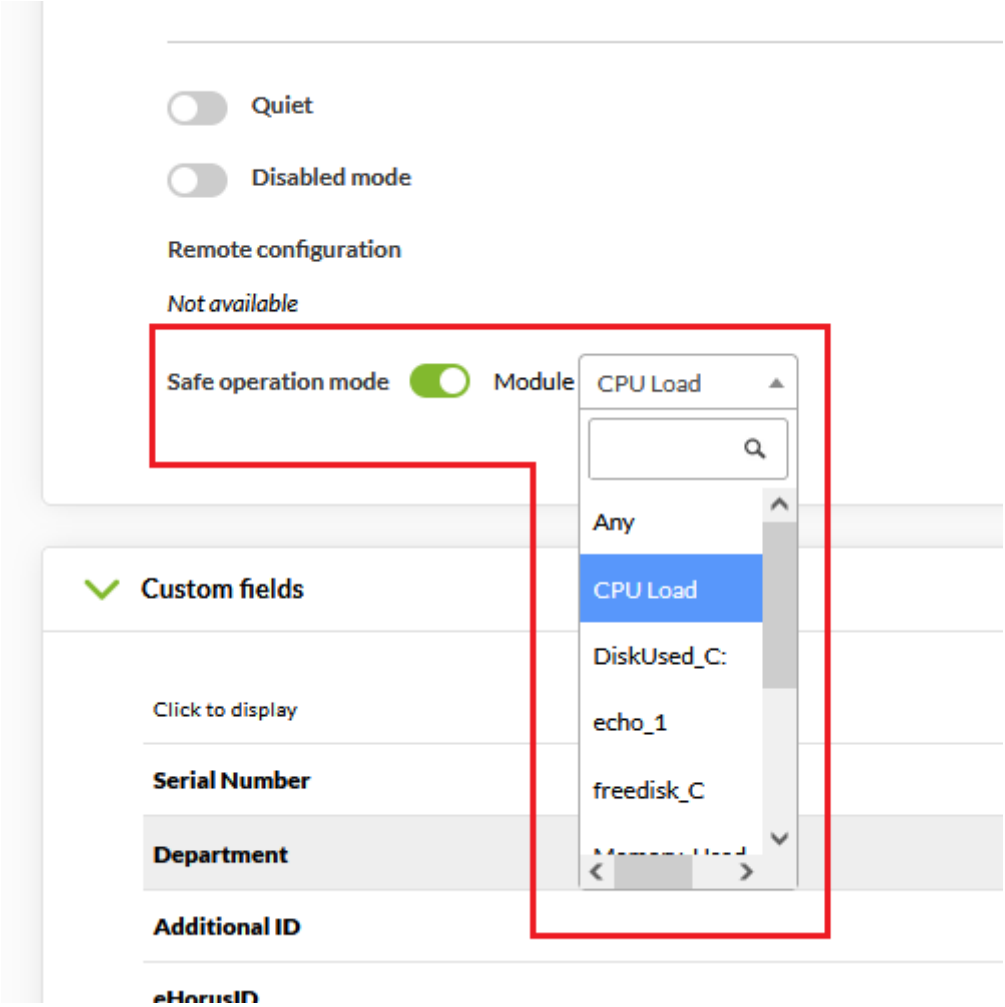
Cuando se dispare la alerta del servicio se podrá enviar en la alerta la información de cuales elementos del servicio están en crítico con la macro `_rca_` que indicará la causa raíz del estado del servicio.

Protección en cascada basada en módulos

Se puede usar el estado de un Módulo de un Agente padre para evitar que envíen alertas del Agente en caso de que pase a estado crítico.



Modo de operación seguro

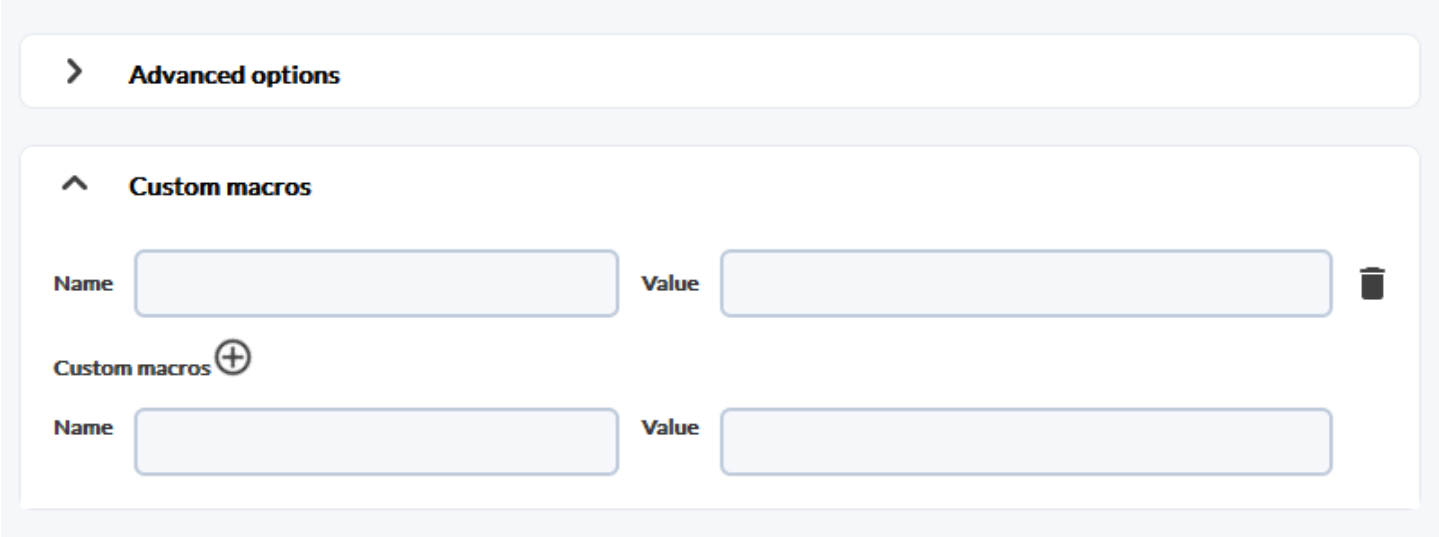


El modo de operación seguro se puede habilitar en las opciones de configuración avanzadas de un Agente.

Si el estado del Módulo seleccionado pasa a `critical`, el resto de Módulos del Agente se deshabilitan hasta que vuelva a `normal` o `warning` de nuevo. Esto permite, por ejemplo, deshabilitar Módulos remotos si se pierde la conectividad.

Macros personalizados de alerta de módulo

Estas macros especificas se pueden añadir expandiendo la sección de macros de cualquier módulo.



- Se definen en el Módulo.
- Almacenan los datos en la base de datos.
- Pueden tener cualquier nombre, por ejemplo `_myMacro`.
- No se reflejan en la configuración local (`.conf`).
- Se usan exclusivamente para las alertas.
- No se pueden definir a nivel de componente.
- Se pueden definir en las políticas de monitorización.
- Los valores establecidos pueden ser utilizados como parte de los campos en la definición de alertas.

Configuración de correos para alertas en Pandora FMS

Pandora FMS por sí sola tiene la facultad de enviar correos electrónicos tal como se explica en la configuración general de la Consola. Sin embargo su flexibilidad permite el envío de correo electrónico con diferentes plataformas de correo. Una vez se hayan establecido ambos mecanismos se podrá configurar la acción de envío y crear su alerta.

Alertas en eventos

Menú Management → Alerts → Event Alerts.

Se pueden construir alertas basándose en los eventos recibidos. Estas alertas pueden ser sencillas o complejas, en base a un conjunto de reglas con relaciones lógicas.

Este tipo de alertas permite trabajar desde una perspectiva mucho más flexible, ya que no se generan alertas en función del estado de un Módulo específico, sino sobre un evento que puede haber sido generado por varios Módulos diferentes e incluso de distintos Agentes.

A la hora de definir alertas sobre eventos es imprescindible indicar los parámetros

agente, módulo y evento.

En entornos de Command Center las alertas de eventos no están centralizadas. Cada nodo deberá tener configuradas sus reglas de evento ya que las reglas configuradas en el Command Center solamente dispararán las alertas de los eventos de la propia Command Center.

Cada alerta de evento se configura para saltar ante un determinado tipo de evento; cuando se cumple la ecuación lógica definida por las reglas y sus operadores, la alerta se disparará.

Dado el elevado número de eventos que puede llegar a albergar la base de datos de Pandora FMS, el servidor trabaja sobre una ventana de eventos máxima, parámetro event_window, que se define en el fichero de configuración `pandora_server.conf`. Los eventos que se hayan generado fuera de esta ventana de tiempo no serán procesados por el servidor.

Creación de alertas de eventos

Para que funcionen las alertas de eventos hay que activar el servidor de eventos con el parámetro `eventserver 1` en el fichero de configuración del servidor de Pandora FMS.

Menú Management → Alerts → Event Alerts.

Con el botón Create se agrega una nueva alerta de evento y el proceso es similar a la creación de una plantilla de alerta. Existen cinco pasos para la creación completa de una alerta de evento, algunos aspectos importantes son:

- Paso 1, Configure: Contiene los datos básicos como nombre, grupo de agentes al que pertenecerá la alerta de evento y su severidad.
- Paso 2, Conditions: Paso donde se asignará una plantilla de alerta, una lista de días especiales, la opción Disable event (el evento generado en la vista de eventos de disparo de alerta no se creará si se marca este *token*) y *un modo de evaluación de reglas*:

Cuando existen dos o más alertas de eventos se evalúan una a una siguiendo el orden cronológico de creación y, si se necesita, estableciendo una jerarquía.

Cada alerta de evento tiene para ello dos parámetros de configuración específicos:

- Rule evaluation mode: Puede ser Pass o Drop. El primero significa que, en caso de que un evento cumpla con las reglas de una alerta, se sigan evaluando el resto de alertas a continuación. Es el comportamiento por defecto. Drop, de otra manera, significa que cuando un evento cumpla con una alerta, dejen de evaluarse el resto de alertas.

- Grouped by: Permite agrupar las reglas por Agente, Grupo, Módulo o Alerta de módulo. Así, si se configura una regla para que se dispare cuando se reciban dos eventos críticos y se agrupa por Agente, deberán llegar dos eventos críticos de un mismo Agente.

- Paso 3, Rules: Reglas dentro de una alerta de evento.
- Paso 4, Fields: Campos dentro de una alerta de evento
- Paso 5, Triggering: Disparado dentro de una alerta de eventos.

Al finalizar la creación y regresar a la vista global se tendrá la lista de alertas de eventos registradas y la información sobre ellas, además de opciones sobre ellas (operar con la acción deshabilitada, en modo standby, añadir más acciones, editar o eliminar la alerta de evento correspondiente). También se podrá cambiar el orden entre sí de las diferentes alertas de eventos.

Reglas dentro de una alerta de evento

Las alertas de eventos se basan en reglas de filtrado que emplean los siguientes operadores lógicos:

- `and`
- `nand`
- `or`
- `nor`
- `xor`
- `nxor`

Estos operadores lógicos sirven para buscar eventos y/o expresiones que coincidan con las reglas de filtrado configuradas y si se encuentran coincidencias se disparará la alerta. Para definir las reglas del alertado será necesario arrastrar los elementos de la parte izquierda al drop area de la parte derecha para construir su regla.

Solamente guardará los cambios cuando pulse el botón para avanzar al siguiente paso (botón Next).

Elementos de configuración disponibles:

Estos elementos se irán habilitando para guiar al usuario en el cumplimiento de la gramática de la regla. A continuación se explica de manera simplificada la gramática a utilizar:

```
S → R | R + NEXO +R

R → CAMPO + OPERADOR + C | CAMPO + OPERADOR + C + MODIFICADOR

C → VARIABLE
```

Donde S es el conjunto de reglas definidas para la alerta de evento.

Para limpiar y deshacer todos los cambios se dispone de dos botones: Cleanup y Reset.

Los bloques tienen simultaneidad a la hora de cumplir la condición:

(A and B)

Obliga a que el elemento analizado (evento) cumpla simultáneamente A y B.

A and B

Obliga a que ambas reglas (A) y (B) se cumplan en la ventana de evaluación. Esto quiere decir que deben existir entradas que satisfagan ambas reglas en los últimos segundos (definido por el parámetro `event_window`).

En los operadores de comparación == y `!=` se comparan literalmente las cadenas de texto. Para mayor flexibilidad considere utilizar el operador REGEX el cual emplea Expresiones Regulares.

Campos dentro de una alerta de evento

Se deben configurar `Field2` , `Field3`, (...) , `Field`*n*, los cuales se utilizan para transferir la información desde la *plantilla* a la *acción* y de la acción al *comando*, para finalmente utilizarse como parámetros en la ejecución de dicho comando.

Dicha información se transfiere siempre que el paso siguiente no traiga ya información definida en sus campos `Field`n. Es decir, en caso de solapamiento de campos o parámetros, sobrescribe la acción a la plantilla (por ejemplo, si la plantilla tiene definida `Field1` y la acción también, el `Field1` de la acción *sobre escribe* la acción de la plantilla).

Versión 764 o posterior: Las macros relacionadas con módulos y agentes no están disponibles en los campos de la sección Alert recovery ya que la recuperación de estas alertas se ejecuta cuando el threshold termina y carece de un evento de recuperación para obtener dicha información.

Disparado dentro de una alerta de eventos

En esta sección debe configurar las acciones que va a realizar cuando se dispare la alerta e indicar en qué intervalos y cada cuánto tiempo se va a ejecutar dicha acción.

- Actions: Acción que se necesita ejecutar.

- Threshold: Intervalo de tiempo que tiene que pasar para que se vuelva a ejecutar la acción una vez se dispare la alarma.

Una vez seleccionados los parámetros anteriores se pulsa el botón Add y después se puede elegir y visualizar la lista de acciones configuradas (sección Select the desired action and mode to view the Triggering fields for this action).

La información acerca de el último disparado de alerta será presentada de acuerdo a como se tenga configurado (Timestamp, time comparison, or compact mode).

Macros para alerta de evento

Las macros que se pueden utilizar dentro de la configuración de una alerta de evento están en la lista de macros.

Alertas de logs

Menú Management → Alerts → Log Alerts.

Se pueden construir alertas basándose en los logs recibidos. Estas alertas pueden ser sencillas o complejas, en base a un conjunto de reglas con relaciones lógicas.

Este tipo de alertas permite trabajar desde una perspectiva mucho más flexible, ya que no se generan alertas en función del estado de un Módulo específico, sino sobre un log que puede haber sido generado por varios Módulos diferentes e incluso de distintos Agentes.

Cada alerta de log se configura para dispararse ante un determinado tipo de evento; cuando se cumple la ecuación lógica definida por las reglas y sus operadores, la alerta saltará.

Dado el elevado número de logs que se pueden llegar a albergar en Pandora FMS, el servidor trabaja sobre una ventana de eventos máxima, parámetro log_window, que se define en el fichero de configuración `pandora_server.conf`. Los logs que se hayan generado fuera de esta ventana de tiempo no serán procesados por el servidor.

Creación de alertas de logs

Para que funcionen las alertas de logs se debe activar el servidor de logs con el

parámetro `logserver 1` en el fichero de configuración del Pandora FMS server. Se recomienda cambiar dicho valor por medio de la interfaz gráfica de configuración remota.

Luego se debe activar el Log collector en el menú Management → Settings → System Settings → Log collector → Activate Log Collector.

Menú Management → Alerts → Log Alerts.

Con el botón Create se agrega una nueva alerta de log y el proceso es similar a la creación de una plantilla de alerta. Existen cinco pasos para la creación completa de una alerta de log, algunos aspectos importantes son:

- Paso 1, Configure: Contiene los datos básicos como el grupo de agentes al que pertenecerá la alerta de log, nombre de la alerta y su severidad.
- Paso 2, Conditions: Paso donde se asignará una plantilla de alerta, alguna lista de días especiales, la opción Disable event (el evento generado en la vista de eventos de disparo de alerta no se creará si se marca este *token*) y un modo de evaluación de reglas:

Cuando existen dos o más alertas de *logs* se evalúan una a una siguiendo el orden cronológico de creación y, si se necesita, estableciendo una jerarquía.

Cada alerta de log tiene para ello dos parámetros de configuración específicos:

- Rule evaluation mode: Al elegir Pass significa que, en caso de que un log cumpla con las reglas de una alerta, se sigan evaluando el resto de alertas de log a continuación. Es el comportamiento por defecto. En el caso de elegir Drop, cuando un log cumpla con una alerta se dejarán de evaluar el resto de alertas de log.
- Grouped by: Permite agrupar las reglas por Agente, Grupo, Módulo o Alerta de módulo. Así, si se configura una regla para que se dispare cuando se reciban dos eventos críticos y se agrupa por Agente, deberán llegar dos eventos críticos de un mismo Agente.

En las alertas que contengan reglas de *logs*, solo afectará a la agrupación por Agente. Si elige una agrupación diferente, las alertas basadas en entradas de *log* no se cumplirán nunca.

- Paso 3, Rules: Reglas dentro de una alerta de log.
- Paso 4, Fields: Campos dentro de una alerta de log
- Paso 5, Triggering: Disparado dentro de una alerta de log.

Al finalizar la creación y regresar a la vista global se tendrá la lista de alertas de logs registradas y la información sobre ellas, además de opciones sobre ellas (operar con la acción deshabilitada, en modo standby, añadir más acciones, editar o eliminar la alerta de log correspondiente). También se podrá cambiar el orden entre sí de las diferentes alertas de *logs*.

Reglas dentro de una alerta de log

Las alertas de eventos se basan en reglas de filtrado que emplean los siguientes operadores lógicos:

- `and`
- `nand`
- `or`
- `nor`
- `xor`
- `nxor`

Estos operadores lógicos sirven para buscar logs y/o expresiones que coincidan con las reglas de filtrado configuradas y si se encuentran coincidencias se disparará la alerta.

Para definir las reglas del alertado será necesario arrastrar los elementos de la parte izquierda al drop area de la parte derecha para construir su regla.

Solamente guardará los cambios cuando pulse el botón para avanzar al siguiente paso (botón Next).

Elementos de configuración disponibles:

Estos elementos se irán habilitando para guiar al usuario en el cumplimiento de la gramática de la regla. A continuación se explica de manera simplificada la gramática a utilizar:

```
S → R | R + NEXO +R

R → CAMPO + OPERADOR + C | CAMPO + OPERADOR + C + MODIFICADOR

C → VARIABLE
```

Donde S es el conjunto de reglas definidas para la alerta de log.

Para limpiar y deshacer todos los cambios se dispone de dos botones: Cleanup y Reset.

Los bloques tienen simultaneidad a la hora de cumplir la condición:

(A and B)

Obliga a que el elemento analizado (log) cumpla simultáneamente A y B.

A and B

Obliga a que ambas reglas (A) y (B) se cumplan en la ventana de evaluación. Esto quiere decir que deben existir entradas que satisfagan ambas reglas en los últimos segundos (definido por el parámetro `log_window`).

En los operadores de comparación == y `!=` se comparan literalmente las cadenas de texto. Para mayor flexibilidad considere utilizar el operador REGEX el cual emplea Expresiones Regulares.

Campos dentro de una alerta de log

Se deben configurar `Field2` , `Field3`, (...) , `Field`*n*, los cuales se utilizan para transferir la información desde la *plantilla* a la *acción* y de la acción al *comando*, para finalmente utilizarse como parámetros en la ejecución de dicho comando.

Dicha información se transfiere siempre que el paso siguiente no traiga ya información definida en sus campos `Field`n. Es decir, en caso de solapamiento de campos o parámetros, sobrescribe la acción a la plantilla (por ejemplo, si la plantilla tiene definida `Field1` y la acción también, el `Field1` de la acción *sobre escribe* la acción de la plantilla).

Versión 764 o posterior: Las macros relacionadas con módulos y agentes no están disponibles en los campos de la sección Alert recovery ya que la recuperación de estas alertas se ejecuta cuando el threshold termina y carece de un evento de recuperación para obtener dicha información.

Disparado dentro de una alerta de log

En esta sección debe configurar las acciones que va a realizar cuando se dispare la alerta de log e indicar en qué intervalos y cada cuánto tiempo se va a ejecutar dicha acción.

- Actions: Acción que se necesita ejecutar.

- Threshold: Intervalo de tiempo que tiene que pasar para que se vuelva a ejecutar la acción una vez se dispare la alarma de log.

Una vez seleccionados los parámetros anteriores se pulsa el botón Add y después se puede elegir y visualizar la lista de acciones configuradas (sección Select the desired action and mode to view the Triggering fields for this action).

La información acerca de el último disparado de alerta será presentada de acuerdo a como se tenga configurado (Timestamp, time comparison, or compact mode).

Macros para alerta de evento

Las macros que se pueden utilizar dentro de la configuración de una alerta de evento están en la lista de macros.

Alertas SIEM

Estas alertas son evaluadas por el servidor de eventos SIEM en el momento de su generación, por lo que para su correcto funcionamiento se deberá habilitar y configurar la monitorización SIEM.

Gestión de alertas SIEM

Menú Management → Alerts → SIEM Alerts.

En esta sección es posible crear, editar y eliminar alertas SIEM. Es necesario el permiso LW para acceder a esta sección.

Estas alertas se basan en el sistema de filtros de las vistas de eventos SIEM, de manera que cualquier evento que fuese mostrado con las condiciones de filtro configuradas serán los que disparen la alerta.

Por ejemplo, si se configura una alerta SIEM con un filtro de eventos críticos, justo antes de que el servidor de eventos SIEM genere uno con esa condición la alerta se disparará.

Las alertas SIEM, igual que el resto de alertas, cuentan con las opciones de configuración globales para su disparo.

Operación de alertas SIEM

Menú Operation → SIEM → Alerts.

En esta sección es posible ver, habilitar/deshabilitar y cambiar el modo *standby* de las alertas SIEM disponibles en el entorno. Es necesario el permiso LM para acceder a esta sección.

Lista de macros

Las Macros de comandos, Macros de acciones y Macros alerta de evento son comunes entre sí con algunas excepciones especificadas en cada descripción:

Macro	Descripción
address	Dirección IP del Agente que disparó la alerta.
_addressn_n_	La dirección IP del Agente que corresponde a la posición indicada en n: addressn_1_ , addressn_2_, ...
agent	Alias del Agente que disparó la alerta. Si no tiene asignado alias, se usa el nombre del Agente.
agentalias	Alias del Agente que disparó la alerta.
_agentcustomfield_n_	Campo personalizado número n del Agente: _agentcustomfield_9_.
agentcustomid	Identificador personalizado del Agente.
agentdescription	Descripción del Agente que disparó la alerta.
agentgroup	Nombre del grupo del Agente.
agentname	Nombre del Agente que disparó la alerta.
agentos	Sistema operativo del Agente.
agentstatus	Estado actual del Agente.
_alert_critical_instructions_	Instrucciones contenidas en el Módulo para un estado critical.
_alert_description_	Descripción de la alerta.
_alert_name_	Nombre de la alerta.
_alert_priority_	Prioridad numérica de la alerta.
_alert_text_severity_	Prioridad en texto de la alerta (Maintenance, Informational, Normal, Minor, Warning, Major, Critical).
_alert_threshold_	Umbral de la alerta.
_alert_times_fired_	Número de veces que se ha disparado la alerta.
_alert_unknown_instructions_	Instrucciones contenidas en el Módulo para un estado unknown.
_alert_warning_instructions_	Instrucciones contenidas en el Módulo para un estado warning.
_all_address_	Todas las direcciones del Agente que disparó la alerta.

Macro	Descripción
_critical_threshold_min_	Umbral mínimo de crítico.
_critical_threshold_max_	Umbral máximo de crítico.

Macro	Descripción
data	Dato que hizo que la alerta se disparase.

Macro	Descripción
dataunit	Muestra el tipo de unidad especificado en el campo Unit (ubicada en la sección Advanced options del módulo de un agente).

Macro	Descripción
_email_tag_	Buzones de correo electrónico asociados a los tags de Módulos.
_event_cf_text_	Solamente para alertas de evento: Saca toda la información de *custom data* en modo texto (con saltos de linea).
_event_cf_json_	Solamente para alertas de evento: Saca la información de *custom data* en formato JSON.
_event_cfX_	Solamente para alertas de evento: Clave del campo personalizado (X) del evento que disparó la alerta. De esta manera, si hay un campo personalizado cuya clave es IPAM, se puede obtener su valor usando la macro _event_cfIPAM_.
_event_description_	Solamente para alertas de evento: Descripción textual del evento de Pandora FMS.
_event_extra_id_	Solamente para alertas de evento: Identificador extra.
_event_id_	Solamente para alertas de evento: Identificador del evento que disparó la alerta.
_event_text_severity_	Solamente para alertas de evento: Prioridad en texto de el evento que dispara la alerta (Maintenance, Informational, Normal Minor, Warning, Major, Critical).
eventTimestamp	Timestamp en el que se creó el evento.

Macro	Descripción
fieldX	Campo X definido por el usuario.

Macro	Descripción
_group_contact_	Información de contacto del grupo. Se configura al crear el grupo.
groupcustomid	Identificador personalizado del grupo.
groupother	Otra información sobre el grupo. Se configura al crear el grupo.

Macro	Descripción
homeurl	Es un enlace de la URL pública que debe configurarse en las opciones generales de la configuración.

Macro	Descripción
_id_agent_	Identificador del Agente, útil para construir un URL de acceso a la Consola web de Pandora FMS.
_id_alert_	Identificador de la alerta, útil para correlacionar la alerta en herramientas de terceros.
_id_group_	Identificador del grupo de Agente.
_id_module_	Identificador del Módulo.
interval	Intervalo de la ejecución del Módulo.

Macro	Descripción
lastdatatimestamp	Última fecha y hora de chequeo recibida por un módulo (útil para alertas de paso a desconocido).
lastdatatime	Última fecha y hora de chequeo recibida (en formato Unix time) por un módulo (útil para alertas de paso a desconocido).
logTimestamp	*Timestamp* en el que se creó el *log*.
logSource	Origen del *log* que disparó la alerta.

Macro	Descripción
module	Nombre del Módulo.
modulecustomid	Identificador personalizado del Módulo.

Macro	Descripción
_moduledata_X_	Con esta macro (X es el nombre del Módulo en cuestión) es posible recoger el último dato del Módulo. Si es numérico lo devuelve formateado con los decimales especificados en la configuración de la Consola web y con su unidad (si la tiene). Se puede enviar así información adicional (y quizás muy relevante) de otros módulos del mismo Agente. Si X contiene espacios, estos deben ser colocados como una entidad HTML: . Se puede ver una lista de entidades HTML en Wikipedia.
moduledescription	Descripción del Módulo.
_modulegraph_nh_	Solamente para alertas que usen el comando eMail: Devuelve una imagen codificada en base64 de una gráfica del Módulo con un periodo de n horas. Requiere de una configuración correcta de la conexión del servidor a la consola vía API, la cual se realiza en el fichero de configuración del servidor.
_modulegraphth_nh_	Solamente para alertas que usen el comando _email_tag_: Misma operación que la macro _modulegraph_nh_ con la diferencia de incluye los umbrales crítico y de advertencia del Módulo, en caso de que estén definidos.
modulegroup	Nombre del grupo del Módulo.
modulestatus	Estado del Módulo.
modulelaststatuschange	Solamente para Macros de comando: *Timestamp* en el que se produjo el último cambio de estado del Módulo.
modulelaststatustime	Solamente para Macros de comando: Fecha y hora en el que se produjo el último cambio de estado del Módulo.
moduletags	Las URL asociadas a los tags de módulos.

Macro	Descripción
_name_tag_	Nombre de los tags asociados al Módulo.

Macro	Descripción
_phone_tag_	Teléfonos asociados a los tags de módulos.
_plugin_parameters_	Puede ser insertada tanto en el asunto como en el cuerpo de la notificación por correo electrónico de una alerta. Una vez allí será sustituida (en formato JSON) por los valores hallados en tagent_modulo.macros para el *plugin* en cuestión.
policy	Nombre de la política a la que pertenece el Módulo (si aplica).
prevdata	Dato previo antes de disparase la alerta (revisar nota al respecto).

Macro	Descripción
rca	Cadena de análisis de causa raíz (únicamente para Servicios).

Macro	Descripción
secondarygroups	Solamente para macros de comandos y macros de acciones: Muestra los grupos secundarios del Agente.
_server_ip_	Dirección IP del servidor al que el Agente está asignado.
_server_name_	Nombre del servidor al que el Agente está asignado.
statusimagetag	Macro utilizada en acciones de alertas con notificaciones por correo electrónico para indicar visualmente el estado al momento del envío. Genera un elemento HTML de tipo img.

Macro	Descripción
_target_ip_	Dirección IP del objetivo del Módulo.
_target_port_	Puerto del objetivo del Módulo.

Macro	Descripción
telegramtoken	Se sustituye por el *token* configurado en Management → Settings → System settings → General setup → Alerts configuration → Telegram configuration.
timestamp	Hora y fecha en que se disparó la alerta.
_time_down_human_	Esta macro solo funciona para alertas de recuperación: Tiempo fuera de servicio o fuera de línea en formato largo, tal como: “1day 10h 35m 40s”.
_time_down_seconds_	Esta macro solo funciona para alertas de recuperación: Tiempo fuera de servicio, o fuera de línea, en segundos.
timezone	Zona horaria que se representa en _timestamp_.

Macro	Descripción
_warning_threshold_max_	Umbral máximo de advertencia.
_warning_threshold_min_	Umbral mínimo de advertencia.

Nota:

Para la macro _prevdata_ es necesario *descomentar* la siguiente sección en el fichero de configuración del servidor de Pandora FMS:

```
# Default texts for some events. The macros _module_ and _data_ are supported.
text_going_down_normal Module '_module_' is going to NORMAL (_data_) with
previous data (_prevdata_)
#text_going_up_critical Module '_module_' is going to CRITICAL (_data_)
#text_going_up_warning Module '_module_' is going to WARNING (_data_)
#text_going_down_warning Module '_module_' is going to WARNING (_data_)
#text_going_unknown Module '_module_' is going to UNKNOWN
```

Se debe reiniciar el proceso del servidor para que se apliquen los nuevos cambios.

Volver al índice de documentación de Pandora FMS