Eventos

From:
https://pandorafms.com/manual/!current/
Permanent link:
https://pandorafms.com/manual/!current/es/documentation/pandorafms/management_and_operation/02_events
Last update: 2024/03/18 21:07

Eventos

Introducción

El sistema de eventos de Pandora FMS permite ver un registro en tiempo real de todos los acontecimientos que ocurren en los sistemas monitorizados. Por defecto, en la vista de eventos se verá una *instantánea* de lo que está sucediendo en ese momento.

Los eventos son el registro y una parte fundamental de un sistema de monitorización.

Los eventos se clasifican según su severidad :

- 0 Mantenimiento (Blanco/Gris).
- 1 Informativo (Azul).
- 2 Normal (Verde).
- 3 Advertencia (Amarillo).
- 4 Crítico (Rojo).
- 5 Menor (Rosa).
- 6 Mayor (Marrón).

Se pueden realizar las siguientes acciones sobre eventos :

- Cambiar su estado (validado o en progreso).
- Cambiar el propietario.
- Eliminar.
- Mostrar información adicional.
- Añadir un comentario.
- Realizar respuestas personalizables.

Información general

Los eventos se gestionan en el menú Operations → Events → View Events.

En el visor de eventos se muestra un resumen de cada evento y en ocasiones hay otros datos asociados, como el módulo del agente que generó el evento, el grupo, *tags* asociados al módulo, etcétera. También se puede ordenar los eventos por identificador, estado, nombre entre otros campos.

Al hacer clic en el icono de la lupa correspondiente a cada ítem obtendrá más detalles.

- El usuario podrá ver solamente los grupos a los cuales pertenezca, a menos que dicho usuario pertenezca explícitamente al grupo TODOS (ALL).
- Pandora FMS también puede utilizar los eventos para anunciar que se han excedido los

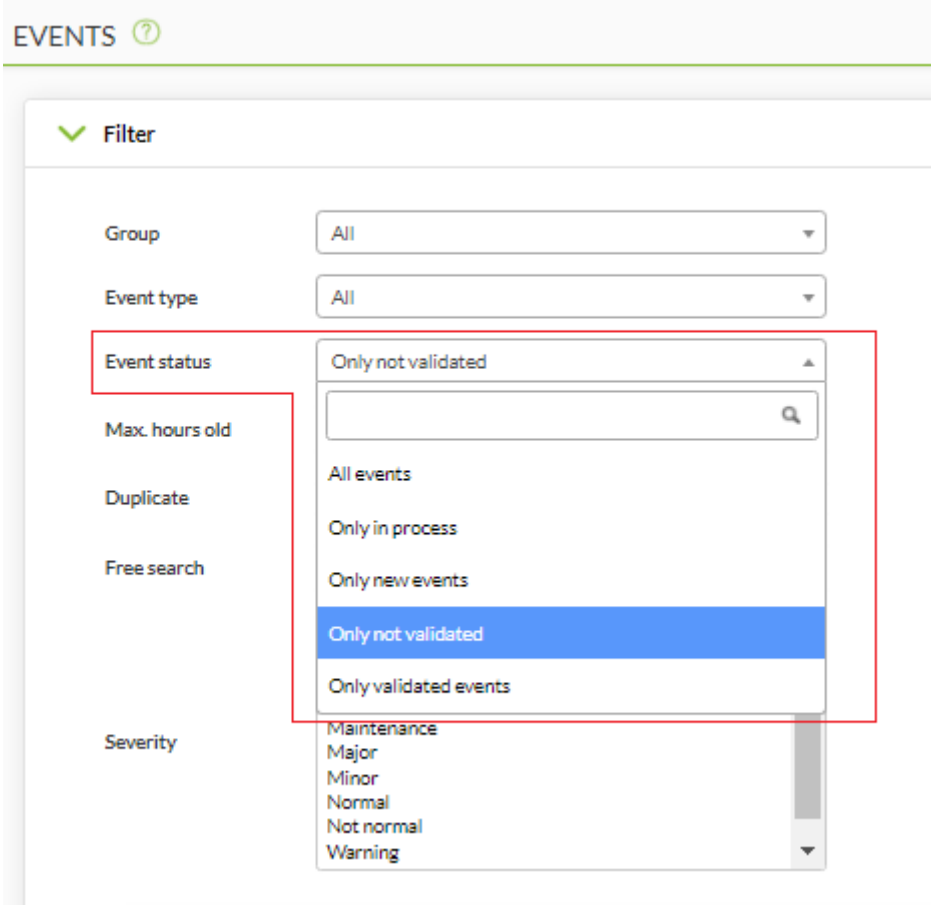
límites impuestos por los usuarios al sistema de monitorización. Por ejemplo, a partir de la versión NG 754 se puede imponer un límite de Agentes en un grupo determinado y al alcanzar dicho límite será mostrado por un evento.

Los eventos se presentan por búsqueda predeterminada de las últimas ocho horas y que *no estén validados* (y también puede ser personalizada), además de agrupar para evitar redundancia. Puede guardar las búsquedas como filtros o bien aplicar un filtro creado previamente.

Operación con eventos

Validación y estados de un evento. Auto validación

Un evento puede estar en cuatro estados:



- En proceso.
- Nuevo.
- No validado.
- Validado.

Autovalidación

Cuando se producen eventos por cambios de estado en módulos, generalmente habrá dos eventos: un primer evento de paso de estado normal a otro estado “incorrecto”, y un evento de

vuelta a estado normal, una vez que la situación problemática esté resuelta. En estos casos los eventos que han pasado a estado incorrecto (ya sea *critical* o *warning*) son validados automáticamente al recuperar la normalidad. Esto es llamado autovalidación de eventos y es una funcionalidad sumamente práctica.

Validación manual

Si se trabaja de manera manual, un evento puede ser validado también: el sistema memorizará la fecha y el usuario que validó el evento, con la posibilidad de grabar un comentario al respecto de la situación, luego la pantalla se refresca y el evento validado es invisibilizado.

Nótese que, además, en las acciones existen más opciones como ejecutar respuestas personalizadas como ping sobre el host, asignar a un usuario, entre otras.

En proceso

Un evento puede ser marcado “en proceso” en la pestaña Responses. De esta manera el evento no se autovalidará y quedará como pendiente.

Individual o procesos por lote

Se puede validar, marcar como “en proceso” o eliminar eventos de manera individual haciendo clic en los iconos correspondientes o aplicarlos de manera masiva a una selección.

En el caso de respuestas personalizadas, el número máximo de eventos a los que aplicar la operación está limitado a diez.

Filtrado de eventos

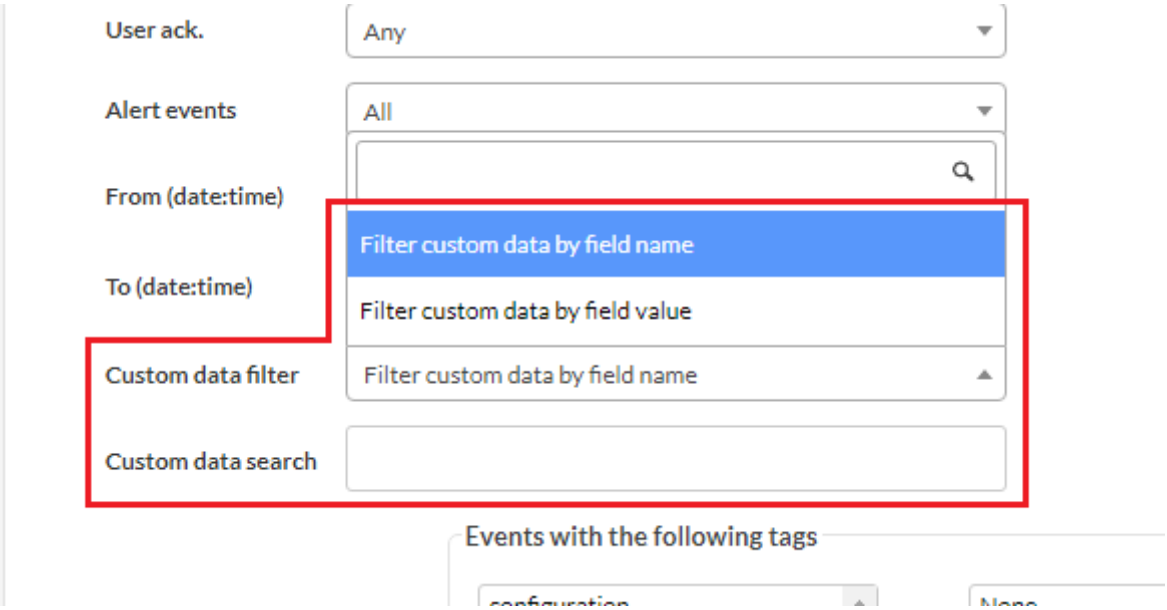
Aspectos importantes de esta funcionalidad:

- Los filtros pueden ser guardados para ser reutilizados en otra oportunidad.
- El máximo de horas de antigüedad (Max. hours old) de los eventos puede ser personalizado.
- Pandora FMS, por defecto, agrupa los eventos repetidos (Duplicate → Group events), sin embargo esta preferencia puede ser cambiada:
    - All events: Muestra todos los eventos individualmente.
    - Group agents: Agrupa los eventos por agente.
    - Group events: El nombre del evento, el ID de agente y el ID de módulo se utilizan para identificar los duplicados.
    - Group Extra IDs: Los eventos se agruparán solamente por Extra ID, ordenado por Timestamp.
- Se puede filtrar por grupo específico. Si utiliza la opción Group recursion también buscará en los subgrupos de dicho grupo. Así mismo si selecciona Search in secondary groups serán incluidos los

eventos de agentes con grupos secundarios asignados. *Estas dos últimas opciones pueden tener repercusión del trabajo en el el servidor PFMS.*

Opciones avanzadas

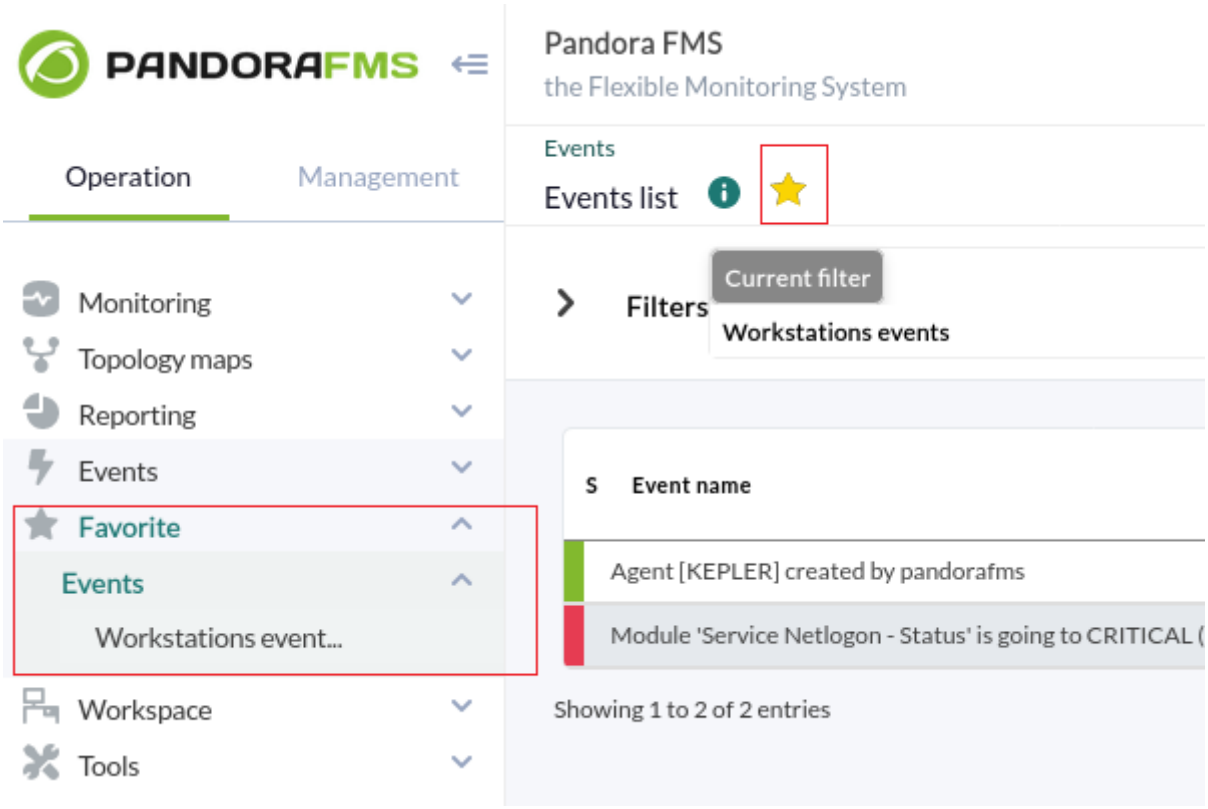
- Puede solicitar los eventos ocurridos en un lapso de tiempo determinado mediante los campos de fecha From (date) y To (date).
- En el campo Free search se puede utilizar una *expresión regular* (por ejemplo, para buscar `Connections` y `Network` se introduce `(Connections|Network)`). La búsqueda es realizada por nombre de agente, nombre de evento, extra ID, fuente, custom data y comentarios.
- Se puede filtrar por campos personalizados mediante los campos Custom data filter, ya sea filtrando el nombre del campo (Filter custom data by field name) o por contenido del campo personalizado (Filter custom data by field value). Dichos campos se mostrarán como columnas en la vista de eventos.



Filtros favoritos

Versión 770 o posterior

Los filtros de eventos que se consideren más frecuentes en su uso, podrán ser agregados a la sección Events en el menú Favorite (menú Operation). Esto se logra haciendo clic en el icono de estrella que aparecerá al cargar un filtro guardado (Current filter). Al hacer clic de nuevo podrá desmarcar el icono y retirarlo del sistema de favoritos.



Borrado de eventos

Los eventos pueden ser borrados de manera individual (manualmente) y/o de manera automática: en el menú Management → Setup → Setup → Max. days before events are deleted se especifica, en días, el período a mantener.

E En la versión Enterprise, activando Enable event history en Management → Setup → Setup → Historical database, se cuenta con la opción de conservarlos con el propósito de crear informes especiales.

Eventos en RSS

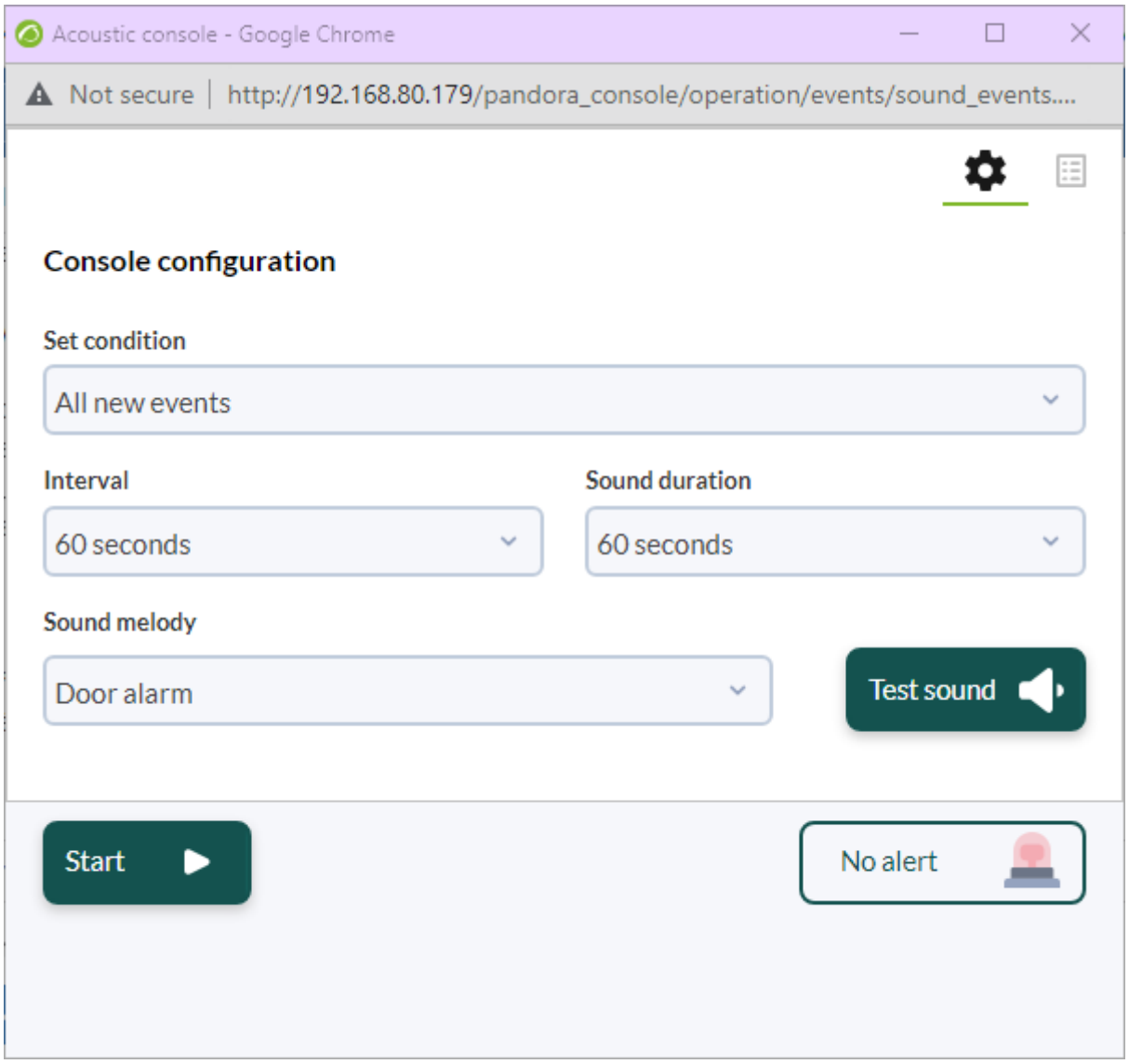
- Para poder acceder al *feed RSS* de los eventos es necesario configurar las direcciones IP que tienen permitido el acceso en el campo IP list with API access dentro de Setup.
- También necesitará de un lector RSS como Inoreader, Selfoss o su lector RSS favorito.

Para ver los eventos en un canal de noticias se accede en Operation → Events → RSS y con ese enlace suscríbase desde el lector de noticias de su preferencia.

Consola sonora de eventos

Permite difundir las distintas alertas sonoras cuando se produce un evento. La melodía se oirá

continuamente hasta que pause el evento sonoro o pulse el botón de OK.



Lista de eventos que generan sonido, por defecto (y pueden ser personalizados):

- El disparo de cualquier alerta.
- El paso de un módulo a estado warning.
- El paso de un módulo a estado critical.
- El paso de un módulo a estado unknown.

Vaya a la opción Operation → Events → Acoustic console . Esta acción abre una ventana emergente de control de todos los eventos sonoros. Usted debe configurar el navegador web para que permita abrir ventanas emergentes.

Minimizar la ventana de la Consola Acústica causará que
no trabaje como se espera.

Los eventos sonoros se exploran cada 10 segundos de forma asíncrona, al suceder un evento la ventana comenzará a parpadear en rojo y vibrar y además, dependiendo de la configuración de su

navegador y/o sistema operativo, la ventana mantendrá el foco y se posicionará por delante del resto de ventanas abiertas.

Solamente se va a alertar con sonido aquellos eventos que se produzcan desde y mientras que la ventana anterior permanezca abierta, coincidan con los seleccionados y que tengan una alerta sonora configurada.

Configuración avanzada

Para agregar nuevas melodías, copie dichos ficheros en formato WAV, al directorio:

```
/var/www/pandora_console/include/sounds/
```

Exportar eventos en CSV

Para exportar los eventos a formato CSV pulse Operation → Events → View events → Export to CSV File.

Alertas de eventos. Correlación de eventos

Para la versión 741 o superior existe la gestión de alertas relacionadas con eventos, tema tratado en capítulo aparte.

Eventos desde línea de comandos

Creación y validación de eventos

La API externa de Pandora FMS se utiliza haciendo llamadas remotas (via HTTPS) sobre el fichero `/include/api.php`. Este es el método que se ha definido en Pandora FMS para integrar aplicaciones de terceros con Pandora FMS. Básicamente consiste en un llamada con los parámetros formateados para recibir un valor o una lista de valores que después dicha aplicación usará para realizar operaciones.

Los tres puntos principales para activar la API PFMS:

1. Active el acceso a la IP desde la que va a ejecutar el comando.
2. Establezca una contraseña general para la API.
3. Defina un usuario específico con su contraseña que solo pueda conectar vía API.

La herramienta dedicada para crear o validar eventos por la API de Pandora FMS puede ser copiada de:

```
/usr/share/pandora_server/util/pandora_revent.pl
```

Al ser ejecutada en el dispositivo cliente, sin parámetros, podrá ver la sintaxis completa.

Las opciones para validar un evento son:

```
./pandora_revent.pl -p <path_to_consoleAPI> -u <credentials> -validate_event
<options> -id <id_event>
```

Para que los campos de las instrucciones `unknown`, `critical` o `warning` aparezcan en los detalles del evento generado, dicho evento debe ser de tipo `going_unknown`, `going_down_critical`, o bien `going_down_warning`, respectivamente.

En algunas ocasiones, tal vez por motivos de seguridad, se debe contar únicamente con la opción de la creación de eventos, para ello puede ser copiado `pandora_revent_create.pl` al dispositivo cliente. Está ubicado en:

```
/usr/share/pandora_server/util/pandora_revent_create.pl
```

Esta herramienta comparte similares características con `pandora_revent.pl`.

Uso de campos personalizados en eventos

Se pueden generar eventos con campos personalizados a través del CLI de Pandora FMS. Ejemplo:

```
perl pandora_manage.pl \
             /etc/pandora/pandora_server.conf \
             --create_event 'Custom event' system Firewalls \
             'localhost' 'module' 0 4 '' 'admin' '' '' '' '' \
             '{"Location": "Office", "Priority": 42}'
```

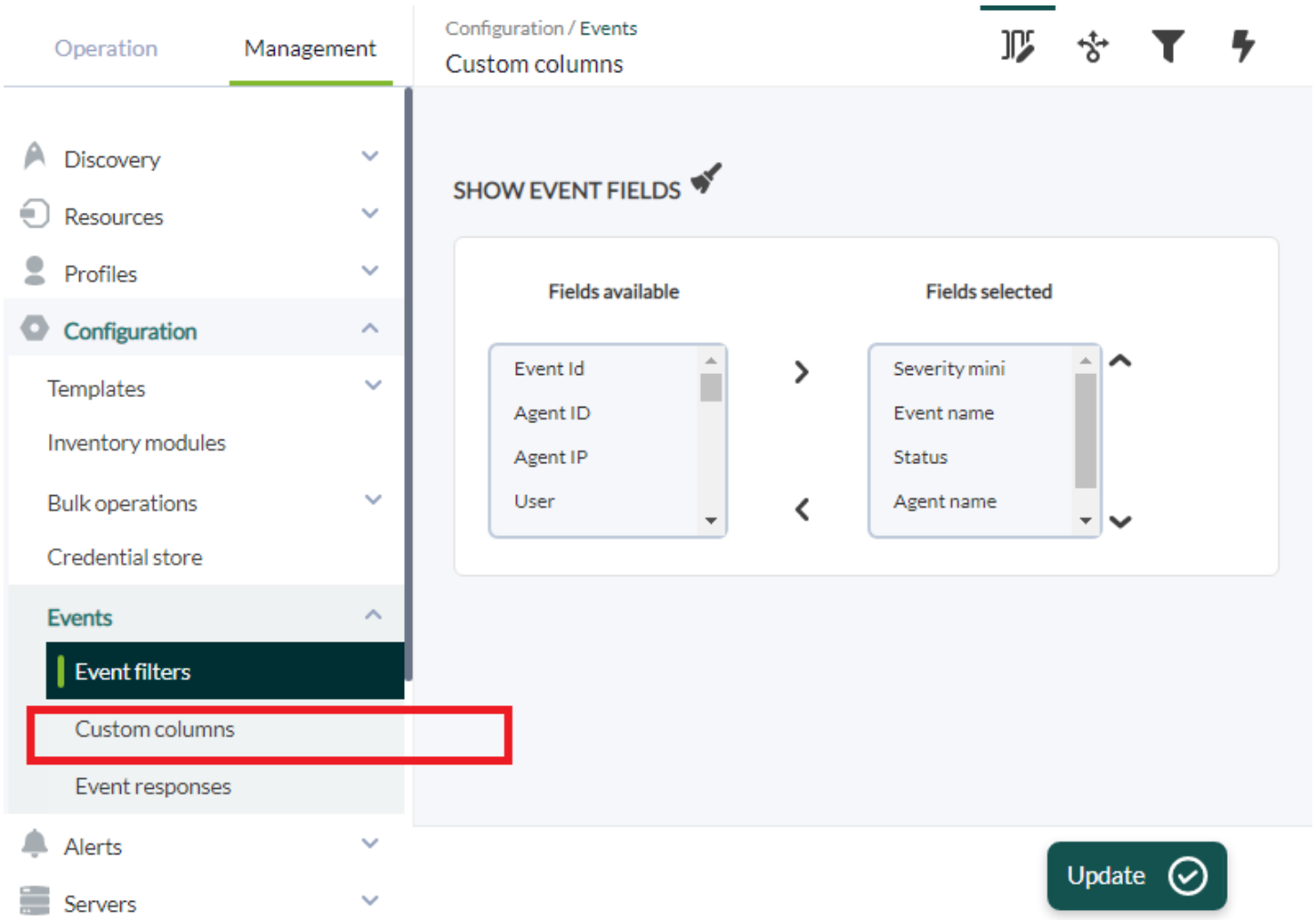
Configuración de eventos

Por medio de Management → Configuration → Events es posible configurar:

- Columnas personalizadas.
- Respuestas.
- Configuración de filtros.

Personalización de la vista de eventos

Es posible personalizar los campos que muestra por defecto el visor de eventos; para ello, desde Events → View events, haga clic en Manage events → Custom columns y elija los campos a mostrar.



Los campos que se muestran por defecto son cinco, sin embargo existen más campos para añadir:

- Event ID.
- Agent name.
- User.
- Group.
- Event type.
- Module name.
- Alert.
- Severity.

- Comment.
- Tags.

- Source.
- Extra ID.
- Owner.
- ACK Timestamp.
- Instructions.
- Server name.
- Data.
- Module status.
- Module custom ID.

Creación de filtros de evento

Menú Management → Configuration → Events → Events filters.

Permite crear, eliminar y editar los filtros aplicados a la vista de eventos. Luego de guardar se puede ir a View events y cargar el filtro adecuado.

Event Responses

Introducción

Una respuesta de evento es una acción personalizada que se puede ejecutar sobre un evento, como por ejemplo la creación de un *ticket* en Pandora ITSM con la información relevante del evento. Puede obtener más información acerca de Integria IMS en la documentación de Pandora FMS.

Introduzca un nombre representativo, descripción, los parámetros a utilizar separados por comas, el comando a usar (estos últimos permiten el uso de macros), el tipo y el servidor que ejecutará el comando. En Parameters se podrá colocar tantos como se necesite, separados por medio de comas. Al realizar la respuesta aparecerá un cuadro de diálogo para rellenar cada uno de ellos y agregarlo así al evento.

Event Responses macros

_agent_address_

Dirección del agente.

_agent_alias_

Alias del agente.

_agent_id_

Identificador del agente.

_agent_name_

Nombre del agente.

_alert_id_

Identificador de la alerta asociada al evento.

_command_timeout_

Tiempo de respuesta del comando (segundos).

_current_user_

Identificador del usuario que ejecuta la respuesta.

_current_username_

Nombre completo del usuario que ejecuta la respuesta.

_customdata_json_

Saca la información de custom data en formato JSON.

_customdata_text_

Saca toda la información de custom data en modo texto (con saltos de linea).

_customdata_X_

Saca un campo concreto de custom data, sustituyendo la X por el nombre del campo.

_event_date_

Fecha en la que se produjo el evento.

_event_extra_id_

Identificador extra.

_event_id_

Identificador del evento.

_event_instruction_

Instrucciones del evento.

_event_severity_id_

Identificador de la criticidad del evento.

_event_severity_text_

Gravedad del evento (traducido por la consola de Pandora FMS).

_event_source_

Procedencia del evento.

_event_status_

Estado del evento (Nuevo, validado o evento en proceso).

_event_tags_

Etiquetas del evento separadas por comas.

_event_text_

Texto completo del evento.

_event_type_

Tipo del evento (Sistema, Cambiando a estado desconocido...).

_event_utimestamp_

Fecha en la que se produjo el evento en formato *utimestamp*.

_group_id_

Identificador del grupo.

_group_name_

Nombre del grupo en base de datos.

_group_contact_

Información de contacto de un grupo de agentes.

_module_address_

Dirección del módulo asociado al evento.

_module_id_

Identificador del módulo asociado al evento.

_module_name_

Nombre del módulo asociado al evento.

_node_id_

Para Metaconsola y Nodo: devuelve el identificador de nodo.

_node_name_

Para Metaconsola y Nodo: devuelve el nombre de nodo.

_owner_user_

Usuario propietario del evento.

_owner_username_

Nombre completo del usuario propietario del evento.

_user_id_

Identificador del usuario.

Volver al Índice de Documentación Pandora FMS