Introducción a la monitorización

Introducción a la monitorización

Introducción a la monitorización

La monitorización consiste en la ejecución de procesos sobre todo tipo de sistemas para recoger y almacenar datos, y posteriormente realizar acciones y tomar decisiones en base a la información obtenida.

Agentes Lógicos en Pandora FMS

La monitorización realizada por Pandora FMS se clasifica en *Agentes Lógicos,* los cuales siempre pertenece a un *Grupo*. Estos equivalen a cada uno de los distintos equipos, dispositivos, webs o aplicaciones que están sometidos a monitorización.

Estos Agentes definidos en la Consola de Pandora FMS pueden presentar datos locales recogidos mediante un Agente Software, datos remotos recogidos mediante chequeos de red, o ambos tipos de datos.

Comparación de la monitorización basada en Agentes Software y en Monitorización Remota

- La monitorización basada en agentes consiste en la instalación de un pequeño programa (Agente Software) que permanece en ejecución en el sistema, obteniendo datos de forma local, mediante la ejecución de comandos y/o guiones (*scripts*).
- La monitorización remota consiste en el uso de la red para ejecutar chequeos remotos hacia los sistemas, sin necesidad de instalar ningún componente adicional en los equipos que se requieren monitorizar.

Configuración de un Agente en Consola

Menú Management → Resources → Manage agents, clic en el nombre de agente, clic en icono Management.

Principales campos de interfaz de edición en vista normal

- Alias: Para un correcto funcionamiento de todas las funciones que realiza Pandora FMS con sus agentes y módulos, evite el uso de los siguientes caracteres /, \, |, %, #, & y $ para el nombrado del agente o módulo. Si estos agentes contienen dichos caracteres, pueden crear confusión con el uso de rutas del sistema o ejecución de otros comandos, provocando errores en el servidor.
- Server: Servidor que va a ejecutar los chequeos configurados en la monitorización del agente, parámetro especial en caso de tener configurado HA en su instalación.
- Primary group: Permite asignar un grupo al agente. Al hacer clic en el icono de grupo podrá acceder a

la vista táctica de grupo asignado.

Principales campos de interfaz de edición en vista avanzada

- Secondary groups: Parámetro opcional para que un agente pueda pertenecer a más de un grupo (grupos secundarios).
- Module definition: Se pueden seleccionar tres modos de trabajo para la definición de módulos.
  - Learning mode: Modo por defecto, si llega un XML con nuevos módulos, se crearán automáticamente; es un comportamiento de aprendizaje.
  - Normal mode: Si llega un XML con nuevos módulos, solamente se crearán si están declarados en la Consola previamente.
  - Autodisable mode: Es igual que el modo de aprendizaje, pero si todos los módulos pasan a desconocido, el agente se deshabilitará hasta que llegue nuevamente información.
- Cascade protection services: Para evitar una avalancha de alertas en cascada. Se puede escoger un agente o un módulo de un agente. En el primer caso, cuando el agente escogido se encuentre en crítico, el agente no generará alertas; en el segundo caso, solo cuando el módulo especificado esté en crítico, el agente no generará alertas.
- Ignore unknown: Esto desactiva el cálculo del estado desconocido en el agente y en cualquiera de sus módulos, por lo que nunca se realizará la transición a desconocido. El estado que refleja es el último estado conocido.

Visualización del agente

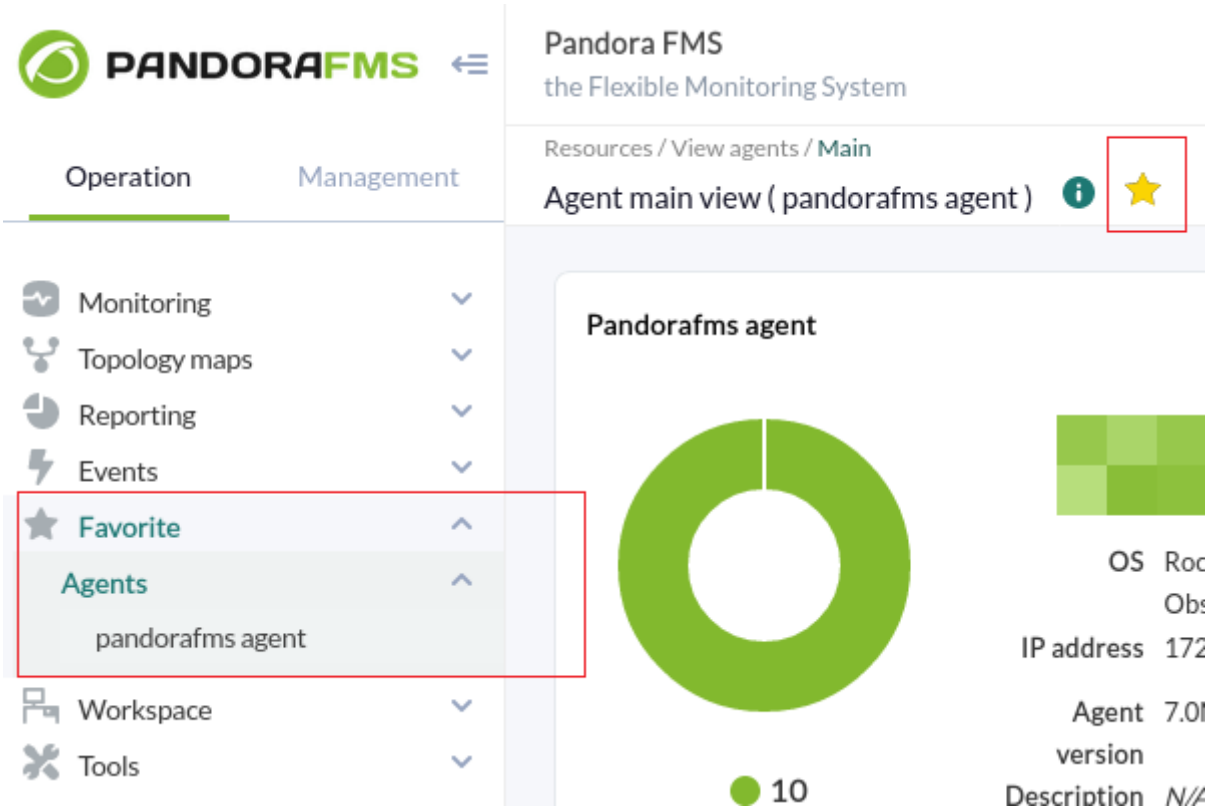
Menú Management → Resources → Manage agents, clic en el nombre de agente.

Esta pantalla ofrece gran cantidad de información referente al agente, con la posibilidad de forzar la ejecución de los chequeos remotos y refrescar datos. En la parte superior muestra un resumen con varios datos del agente.

- Total de módulos y estado de los mismos.
- Eventos en las últimas 24 horas.
- Información del agente.
  - Nombre.
  - Versión.
  - Accesibilidad del agente.
  - Grupo.
- List of modules: pertenecientes al agente y sus respectivos estados (solamente módulos inicializados).
- Lista completa de alertas del agente, con la opción de seleccionar una o varias alertas y validarlas.
- Estado de las fuentes de registro según se hayan configurado en la Recolección de logs.
- Lista con los últimos eventos del agente, con la opción de mostrar solamente los eventos de las últimas 24 horas.

Versión 770 o posterior.

Mediante el sistema de favoritos podrá agregar un agente cualquiera a una lista personalizada para cada usuario. Haga clic en el botón estrella justo al lado del nombre del agente en su vista principal.



Se podrán agregar (o remover) tantos agentes como se necesite, todos estarán siempre a la vista en el apartado Agents del menú Favorite (sección Operation).

Módulos

Los Módulos son unidades de información almacenada dentro de un Agente con los cuales se extrae la información del dispositivo o servidor al que apunta el agente.

Cada Módulo puede almacenar solo un tipo de métrica,
dentro de un agente cada módulo tiene un nombre único.

Estado asociados:

- No iniciado: En espera de recepción de datos.
- Normal: Recibiendo datos con valores comprendidos fuera de los umbrales de advertencia o crítico.
- Advertencia: Datos comprendidos en ese umbral.
- Crítico: Datos comprendidos en ese umbral.
- Desconocido: El módulo ha estado funcionando y ha dejado de recibir información durante un tiempo determinado.

Los módulos tienen alguno de los varios tipos de datos: el *booleano*, el numérico o el alfanumérico, entre otros.

Tipos de módulos

- Módulo de datos .
- Módulo de red.
- Módulo de plugin.
- Módulo WMI.
- Módulo de predicción.
- Módulo de webserver.
- Módulo de análisis web.

Monitorización de estados

Cuando se habla de monitorización, se introduce el concepto de estado: es la asociación del "valor relativo" en vez del valor absoluto, de forma que al superar un *umbral* cambie de estado.

Pandora FMS permite definir umbrales para definir el estado que un chequeo tendrá basándose en los datos que haya recogido. Los tres estados posibles son: `NORMAL`, `WARNING` y `CRITICAL` .

- Warning status: Si el valor numérico del módulo se encuentra en los límites inferior y superior. Si no se especifica límite superior todo valor mayor al límite inferior ocasionará el cambio de estado.
- Critical: igual al punto anterior, solo que para el estado `critical`.
- Inverse interval: presente tanto para el umbral `warning` como `critical`, si se encuentra activado, el módulo cambiará de estado cuando sus valores estén fuera del intervalo especificado. También funciona para módulos alfanuméricos.
- Percentage: Si está activado, el valor del umbral se interpreta como un porcentaje. El funcionamiento de los umbrales Percentage es comparar el nuevo valor que reporta el módulo respecto al anterior para ver el porcentaje de variación, y según cumpla o no con los límites de % de incremento (Max.) o decremento (Min.) establecidos cambiará de estado o no.

En caso de que los umbrales *warning* y *critical* se solapen en algún rango, siempre prevalecerá el umbral *critical*.

Opciones básicas

Se debe tener siempre presente que esta interfaz es utilizada tanto por la monitorización local como por la monitorización remota y se presentan parámetros que son válidos en uno o en otro ámbito. *Por ejemplo*, los parámetros Tiempo de espera (*Timeout*) y Reintentos (*Retries*) carecen de utilidad en la monitorización local (chequeos locales) pero son importantes en la monitorización remota.

- Using module component: Al usar un componente de módulo se rellenarán automáticamente con valores de parámetros necesarios para realizar la monitorización, este *token* aparece en todos los tipos de módulos, salvo en los de predicción.
- Module group: Permite asignar el módulo a un grupo de módulo definido.

- Type: Tipo de módulo en función del tipo de dato devuelto. Al seleccionar Using module component el tipo de dato será escogido automáticamente.
- Change to critical status after X intervals in warning status: (*versión 766 o posterior*) Este *token* permite *promover* el cambio de estado a crítico de un módulo si ha estado X veces seguidas (intervalos continuos de monitorización) en estado de advertencia.
    - Por ejemplo, si se coloca un valor de 2: **warning → warning → warning → CRITICAL**.
    - *Importante:* Este *token* trabaja de manera conjunta con FF threshold, por ejemplo Change to critical... a 1 y FF threshold a 1:
        - **normal → normal → warning → warning → CRITICAL**.
- Historical data: Marque esta opción si necesita guardar a largo plazo los valores en la base de datos histórica.
- Target IP y Port: Dirección IP y número de puerto a la cual realizar consultas para obtener valores de monitorización. En algunos casos, como por ejemplo con la monitorización WMI, aparecerán campos de texto adicionales para establecer credenciales de conexión e incluso cadenas de consulta.

Opciones avanzadas

Se debe tener siempre presente que esta interfaz es utilizada tanto por la monitorización local como por la monitorización remota y se presentan parámetros que son válidos en uno o en otro ámbito. *Por ejemplo*, los parámetros Tiempo de espera (*Timeout*) y Reintentos (*Retries*) carecen de utilidad en la monitorización local (chequeos locales) pero son importantes en la monitorización remota.

- Custom ID: Campo para almacenar un valor de identificación personalizado.
- Unit: Elección de la unidad de los datos recibidos por el módulo, por defecto vacío. Bien puede elegir una unidad específica (*Timeticks*, *Bytes*, *Entries*, etcétera) o hacer clic en el icono de lápiz para establecer unidades personalizadas.
- Interval: Periodo en que el módulo debería devolver datos. Si un módulo pasa más de dos intervalos sin recibir datos, entrará en estado desconocido.
    - Si son módulos remotos: periodo en el cual se realiza el chequeo remoto.
    - Si son módulos de datos: valor numérico que representa X veces el intervalo del agente definido, realizando el chequeo local en ese periodo.
- Post process: Permite establecer una conversión del dato recibido por el módulo (posprocesado del valor). Por defecto deshabilitado (0). Existen opciones predefinidas al instalar Pandora FMS y también puede establecer conversiones personalizadas al hacer clic en el icono de lápiz.
- Min. Value y Max. Value: Permite establecer un valor mínimo y un valor máximo esperados para el módulo.
- Dynamic Threshold Interval: Campos reservados a la Monitorización dinámica (Umbrales dinámicos).
- Export target: Dado el caso haya configurado un servidor de exportación, podrá establecer uno.
- Discard unknown events: Permite descartar eventos desconocidos.
- FF threshold: Permite fijar umbrales para la protección FlipFlop. Se conoce por *FlipFlop* (FF) a un fenómeno usual en monitorización, cuando un valor oscila frecuentemente entre valores alternativos (MAL/BIEN). Cuando esto ocurre se suele emplear un “umbral”, de forma que para considerar que algo ha cambiado de estado tiene que “permanecer” más de X intervalos seguidos en un estado sin alterarse. *FF Threshold* se utiliza para “filtrar” los cambios continuos de estado en la generación de eventos/estados: así Pandora FMS “sabe” que hasta que un elemento no esté al menos X veces en el

mismo estado, después de cambiar desde un estado original, no lo considere como que ha cambiado.
    - FF Interval: Si está activado el Umbral FlipFlop y ocurre un cambio de estado, el intervalo del módulo se cambiará para la siguiente ejecución.
    - FlipFlop timeout: Tiempo de espera solo utilizado en módulos asíncronos. Para que un cambio de estado por FF sea efectivo se tienen que recibir datos consecutivos iguales dentro del intervalo especificado.

Para el cálculo de los Acuerdos de nivel de servicio (SLA), si no se colocan umbrales SLA, Pandora FMS tomará en cuenta los FF threshold.

- Tags available y Tags from policy: Son características de la versión Enterprise. Se detallan en la siguiente sección "Tags".
- Quiet: El módulo seguirá recibiendo información, pero no se generará ningún tipo de evento ni alerta (modo “silencioso”).
- Cascade Protection Services: *Servicio de protección en cascada*, parámetro por el cual la generación de eventos y alertas pasaría al servicio al que pertenece, en caso de estar habilitada esta funcionalidad de eventos en cascada.
- Critical instructions, Warning instructions y Unknown instructions: Contienen las instrucciones a seguir si el estado del módulo pasa a crítico, advertencia o desconocido. Útil en el uso de Plantillas y componentes.
- Cron: Se puede especificar periodos de tiempo en los cuales se ejecutará el módulo. Tiene la nomenclatura: Minuto, Hora, Día del Mes, Mes, Día de la semana. Existen tres posibilidades distintas:
    - Cron from: Tiene establecido por defecto en todos sus campos Any (_Cualquiera_), sin restricción alguna de tiempo para la monitorización.
    - Si Cron from → algún valor específico y Cron to todos en Any: se ejecutará únicamente cuando coincida con el número estipulado. Ej: `15 20 * * *`, solo se ejecutará todos los días a las 20:15.
    - Cron from → algún valor específico y Cron to → → algún valor específico: se ejecutará durante el intervalo expuesto. Ej: `5 * * * *` y `10 * * * *`, se ejecutará cada hora entre los minutos 5 y 10 (esto es equivalente a `5-10 * * * *`).
    - Timeout: Tiempo que espera el agente a la ejecución del módulo, expresado en segundos.
    - Retries: Establece el número de reintentos para la ejecución del módulo.
- Category: Esta categorización no tiene efectos desde la interfaz de usuario normal. Está pensada para usarse en conjunto con la Metaconsola.
- Module parent: Se utiliza para establecer jerarquía en la protección en el servicio de protección en cascada (Cascade Protection Services).
- Custom macros (Macros personalizadas): Se puede definir cualquier número de macros de módulo. El formato recomendado para los nombres de macros es el siguiente: `_macroname_` .

Estas macros se pueden utilizar en las alertas de módulos y son especialmente útiles en Monitorización WUX y Monitorización de Usuario. Si el módulo es de tipo análisis de módulo web:

Las macros dinámicas tendrán un formato especial que empieza por @ y tendrán estas posibles sustituciones:

- `@DATE_FORMAT` (fecha/hora actual con formato definido por el usuario)
- `@DATE_FORMAT_nh` (horas)
- `@DATE_FORMAT_nm` (minutos)

- @DATE_FORMAT_nd (días)
- @DATE_FORMAT_ns (segundos)
- @DATE_FORMAT_nM (mes)
- @DATE_FORMAT_nY (años)

Donde "n" puede ser un número sin signo (positivo) o negativo y FORMAT sigue el estándar de strftime de perl.

- Module relations: Utilizado para sustituir el módulo, ya sea de forma directa (Direct) o en conmutación por error (Failover), a efectos de cálculo de SLA.
- Ignore unknown: Esto desactiva el cálculo del estado desconocido en el módulo, por lo que nunca se realizará la transición a desconocido. El estado que refleja es el último estado conocido.

Module tags

Menú Management → Profiles → Module tags.

Las *tags* son etiquetas asociadas a cada módulo que luego se propagarán a los eventos que este módulo genere y se podrán usar en las alertas de eventos de este módulo. Permiten ser usados como filtros en informes, vistas de eventos e incluso tienen vistas específicas para ellas y se puede emplear en las alertas, ya que están disponibles como macro.

Se pueden utilizar, además, para otorgar permisos de acceso específicos a un módulo, de forma que un usuario pueda acceder únicamente a un módulo del agente, sin tener acceso al resto de módulos.

Monitorización dinámica (Umbrales dinámicos)

La monitorización dinámica consiste en el ajuste dinámico y de forma automática de los umbrales de estados de los módulos de una forma predictiva. El modo de funcionamiento es recoger los valores de un periodo determinado y calcular una media y una desviación estándar, que son utilizadas para establecer los umbrales correspondientes a nivel de módulo. Los parámetros están ubicado en las opciones avanzadas de los módulos:

- Dynamic Threshold Interval: Intervalo de umbral dinámico o cantidad de tiempo que considerará para realizar el cálculo de umbrales. Si se elige un mes, el sistema tomará todos los datos existentes en el último mes y construirá los umbrales en base a esos datos y se establecerán umbrales con valores por encima de la media.
- Dynamic Threshold Max.: Máximo valor del umbral dinámico crítico, si se decide establecer un margen de tolerancia (en porcentaje) para ello; por ejemplo, si los valores promedio se encuentran alrededor del 60 y el umbral crítico ha sido establecido a partir del valor 80, si se establece el valor *Dynamic Threshold Max: 10*, se aumentará un 10% este umbral crítico, por lo que quedaría en un valor de 88 .
- Dynamic Threshold Min.: Permite reducir el límite inferior en el porcentaje que se indique. Por ejemplo, si los valores promedio se encuentran alrededor del 60 y el umbral crítico inferior ha sido establecido en un valor 40, si se establece el valor *Dynamic Threshold Min: 10*, se reducirá un 10%

este umbral crítico, por lo que quedaría en un valor de 36.
- Dynamic Threshold Two Tailed: Son intervalos de umbrales dinámicos, inactivos por defecto. Si se activa esta opción el sistema de umbrales dinámicos también establecerá umbrales por debajo de la media.

Biblioteca de módulos

Disponible a partir de la versión 744. Para acceder a la biblioteca de módulos desde el menú se necesitarán permisos de *Agent Read* (AR).

Acceda a Management → Module library → View para acceder a la vista principal. También puede agrupar por categorías (bases de datos, virtualización, etcétera) o busque el *plugin* por su nombre en el cuadro de texto Search.

Los enlaces de descarga de los módulos Enterprise de Pandora FMS solo serán visibles en estos casos:

- El usuario y la contraseña que se haya configurado en el *setup* deben coincidir con el de soporte de Integria IMS.
- La versión de Pandora FMS es Enterprise.
- El usuario de Pandora FMS tiene permiso AW.

Volver al índice de documentación de Pandora FMS