PANDORAFMS

Introducción

21-09-2021

Introducción

Volver al Índice de Documentación Pandora FMS

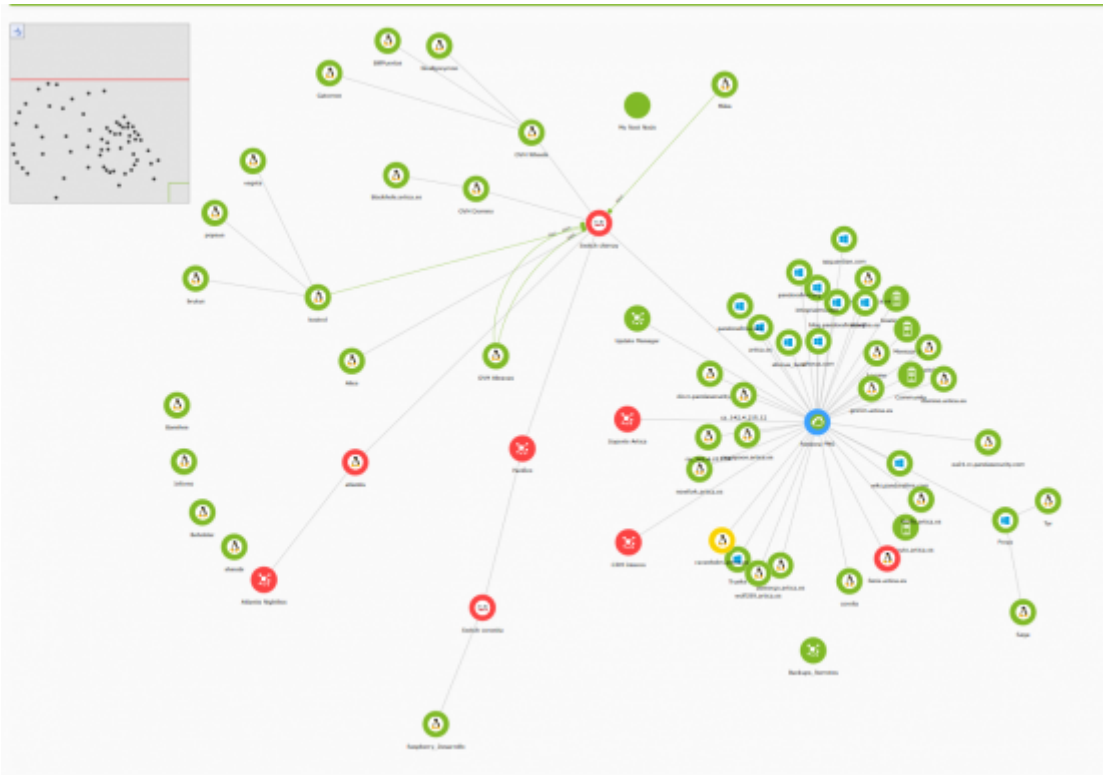
Introducción

¿Qué es exactamente Pandora FMS?

Pandora FMS es un software de monitorización orientado a todo tipo de entornos. Generalizar “monitorización” es algo arriesgado, ya que existen cientos de herramientas, cada una adaptada a un tipo de entorno; no es lo mismo monitorizar impresoras en una pequeña oficina que miles de interfaces de switches y tráfico de red en un centro de datos con miles de servidores.

Pandora FMS está orientado a servir en todo tipo de roles y organizaciones. Su objetivo es ser suficientemente flexible como para gestionar y controlar toda su infraestructura, y que no haga falta invertir tiempo ni dinero en otras herramientas.

FMS es el acrónimo de“**S**istema de **M**onitorización **F**lexible” (en inglés: **F**lexible **M**onitoring **S**ystem). Su propósito es ser capaz de monitorizar tanto herramientas y sistemas complejos de última generación como elementos anticuados, de difícil acceso y poca compatibilidad, todo ello reunido en la misma plataforma.



Pandora FMS dispone a día de hoy de agentes para todos los sistemas operativos “modernos” del mercado, entendiendo “agente” como la pieza de software que se instala en un sistema para extraer información y reportarla al servidor de Pandora FMS.

Por supuesto, Pandora FMS se puede emplear con éxito no solo para monitorizar sistemas, sino también todo tipo de dispositivos de red, ya sea usando SNMP (versiones 1,2,3) o mediante sondas de protocolo TCP (snmp, ftp, dns, http, https, etc), ICMP o UDP.

Acerca de la documentación

Toda esta potencia y flexibilidad tiene implícita cierta dificultad inicial. Pese a que la mayoría de la configuración es gráfica, somos conscientes de que aprender a manejar Pandora FMS podría resultar complicado. Por eso hemos estructurado el manual de forma que las más de 800 páginas de documentación están organizadas en varios bloques:

- Parte 1. Entendiendo Pandora FMS.
- Parte 2. Instalación y configuración.
- Parte 3. Monitorización con Pandora FMS.
- Parte 4. Usando y gestionando Pandora FMS.
- Parte 5. Entornos complejos y máximo rendimiento.
- Parte 6. Metaconsola
- Parte 7. Anexos técnicos.
- Parte 8. Referencia técnica.

Además de la documentación oficial existe un foro de usuarios donde puede preguntar, en inglés, español y japonés a otros usuarios. Si necesita formación oficial, existe un programa de formación oficial impartido por parte de las personas que desarrollan Pandora FMS.

Existen unas guías rápidas para ayudar a configurar Pandora FMS e implementar monitorizaciones simples, así como para la instalación de agentes software, tanto para Linux como para Windows.

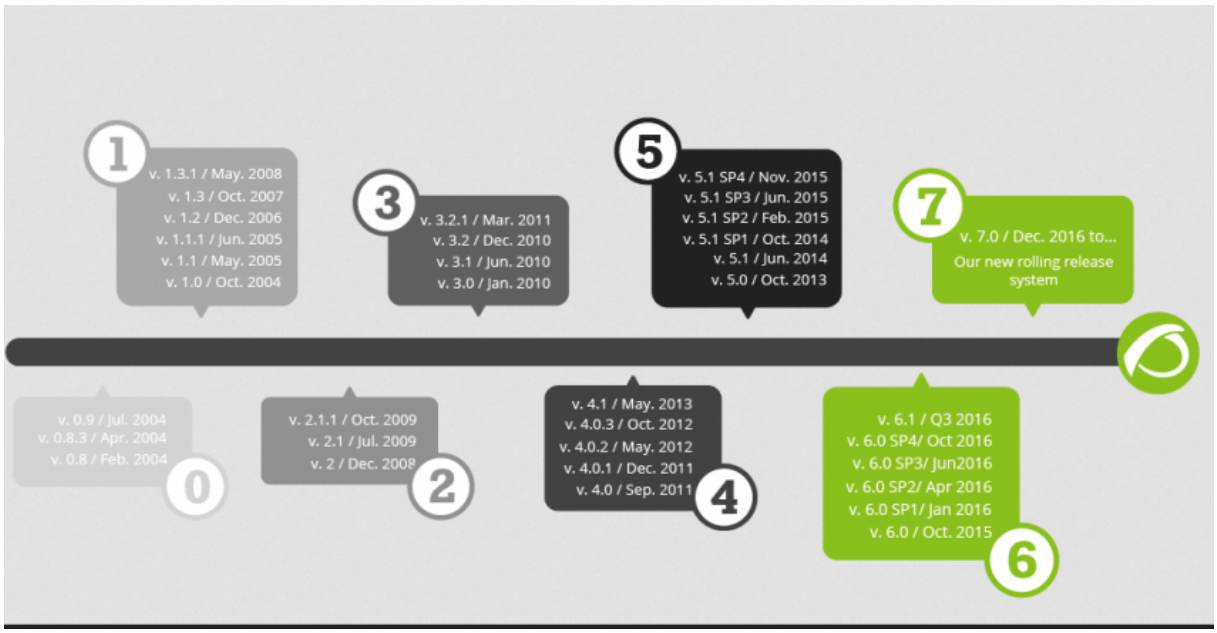
Puede consultar más información en nuestra web: https://pandorafms.com/es

La evolución del proyecto Pandora FMS

Pandora FMS nace de un desarrollo personal de su autor original, Sancho Lerena, en 2003. Desde entonces, ha ido evolucionando sin parar, convirtiéndose en una herramienta robusta y madura.

Aunque inicialmente era 100% de código abierto, con los años surgió la necesidad de ofrecer una versión orientada a grandes empresas: Pandora FMS Enterprise. Esta versión ofrece algunas características específicas para entornos que requieren procesar grandes volúmenes de información y trabajar con miles de dispositivos.

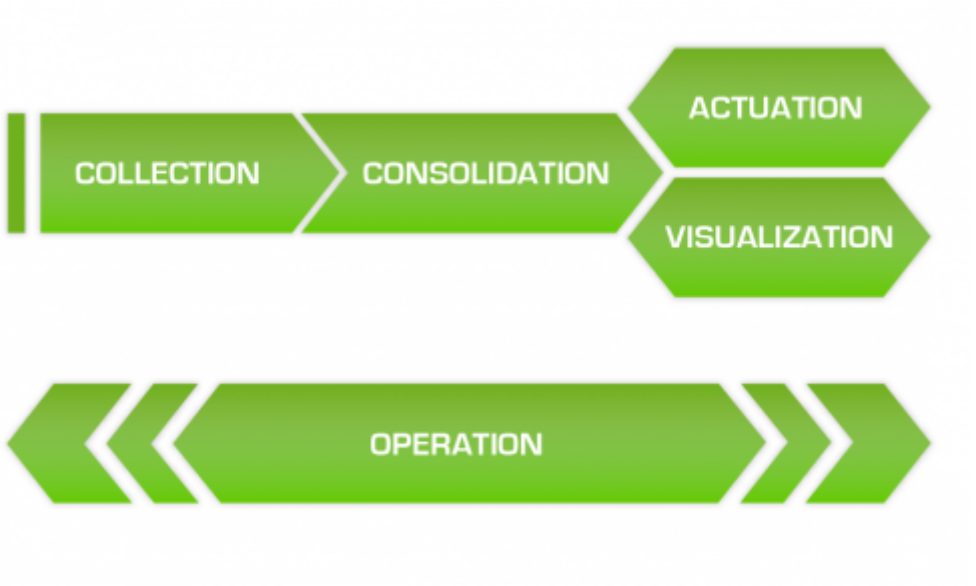
La empresa que se encuentra tras el desarrollo de Pandora FMS y que coordina todo el trabajo de soporte es Ártica Soluciones Tecnológicas, una empresa española, fundada en 2005 por el creador de Pandora FMS.



Pandora FMS se encuentra entre los primeros puestos de Sourceforge y cuenta con miles

de descargas y usuarios satisfechos en todo el mundo. Puede encontrar más información sobre la evolución y el roadmap del proyecto en https://pandorafms.com/es/roadmap-de-pandora/

Un vistazo a las funcionalidades de Pandora FMS



- **Auto monitorización**: La monitorización por defecto de los agentes de Pandora FMS permite detectar los discos duros, las particiones o las bases de datos en un servidor de base de datos, entre otras cosas.
- **Auto descubrimiento**: En remoto, y usando la red, se pueden detectar todos los elementos de la red, catalogarlos según su sistema operativo y,con un perfil asignado, empezar a monitorizarlos. Incluso se puede detectar la topología de la red y construir un esquema de red basado en su enrutamiento.
- **Monitorizar**: Los agentes de Pandora FMS son de los más potentes del mercado. Pueden obtener información desde la ejecución de un comando hasta la llamada a más bajo nivel de la API de Windows: eventos, logs, datos numéricos, estados de un proceso, consumo de memoria o de CPU. Pandora FMS dispone de una biblioteca de chequeos por defecto, pero lo más importante de Pandora FMS es lo **fácil** que es añadir y crear nuevas monitorizaciones.
- **Controlar**: Los propios agentes pueden levantar servicios, borrar ficheros temporales o ejecutar procesos. También se puede hacer desde la consola, ejecutando remotamente tareas como parar o arrancar servicios. Incluso se pueden programar tareas para su ejecución periódica. Además, se puede usar Pandora FMS para acceder remotamente a sistemas remotos gracias a *eHorus*, e incluso emplear herramientas como Telnet o SSH, todo desde una interfaz web.
- **Alertar y notificar**: Tan importante como detectar un fallo es avisar del mismo. Con Pandora FMS se dispone de una variedad casi infinita de formas y formatos de notificación, incluyendo escalados, correlación de alertas y protección en cascada de

alertas.

- **Visualizar y analizar**: Monitorizar no solo es recibir un trap o visualizar un servicio caído, es presentar informes de tendencias, gráficas resumen de datos recopilados durante meses, generar portales de usuarios, delegar informes a terceros o definir sus propias gráficas y tablas. Pandora FMS incorpora todo ello desde su interfaz WEB.
- **Inventariar**: Al contrario que otras soluciones, donde el concepto de CMDB es la base, para Pandora FMS esto es opcional. El inventario es flexible y dinámico, se puede auto-descubrir, comprobar remotamente, etc. Se pueden notificar cambios (por ejemplo software desinstalado en un equipo) o simplemente utilizarlo para elaborar listados.

Introducción a la monitorización

Desde el principio, cada manual técnico de un paquete de software nos informa sobre la configuración, los archivos de texto, las bases de datos, los protocolos, etc. Muy a menudo aprendemos a configurar a nivel básico, pero ignoramos todo el potencial del software que estamos utilizando, lo que se puede hacer con él y en qué situaciones. El propósito de este apartado es explicar de forma breve pero sistemática la "teoría" que hay detrás de la monitorización como tal, independientemente del software que se vaya a usar para monitorizar, antes de comenzar a hablar de temas puramente técnicos.

Tipos de monitorización

Cuando hablamos de "saber cómo está" un determinado elemento, sea este un servidor, una base de datos, un elemento de red o una nevera, podemos plantearnos varias cuestiones:

1. ¿Cómo obtenemos la información?, ¿existe algo en el dispositivo que se encarga de ello o tenemos que "ir y venir" preguntando?
2. ¿Nos interesa estar preguntando constantemente o esperar a que "ocurra algo"?
3. ¿Qué tipo de información nos aporta? ¿Es algo que se pueda dibujar en una gráfica y ver su progresión?

Estas preguntas responden a tres cuestiones clave que condicionan toda la forma de plantear nuestro modelo de monitorización.

La primera pregunta responde a si nosotros vamos a utilizar una monitorización basada en agentes, que se ejecutan dentro del dispositivo que vamos a controlar, o por el contrario todo se hace de forma externa, utilizando una conexión de red. Existen sistemas de monitorización que funcionan de una u otra forma, y dispositivos que solo se pueden monitorizar de una forma y no de la otra. Pandora FMS soporta todos los modelos.

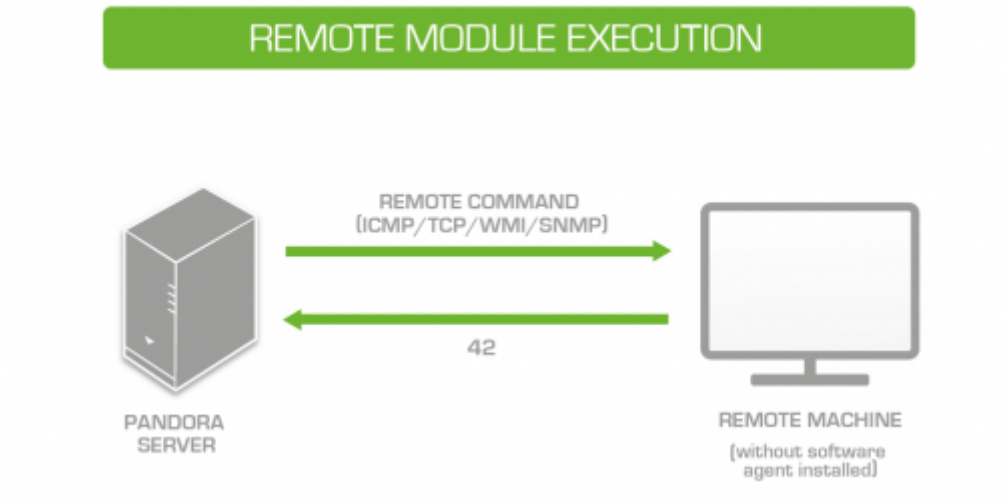
La segunda pregunta responde a si la monitorización es síncrona (cada X segundos se pregunta, independientemente de que la información haya cambiado o no) o bien asíncrona (solo me llega información cuando algo relevante ha ocurrido). Si utilizo monitorización síncrona con 10 millones de elementos y cada 5 minutos recojo datos, la carga será considerable; sin embargo, si lo hago cada 50 minutos, será más manejable, pero si ocurre algo puedo tardar 50 minutos en enterarme. Si utilizo monitorización asíncrona (por ejemplo con traps SNMP o con logs) ahorro muchos recursos, pero no podré trazar gráficas ni hacer históricos, salvo de los sucesos ocurridos. Muchas herramientas se basan solo en el primero de los modelos (a veces se conocen como herramientas de "rendimiento" o "capacity"); también existen herramientas basadas en el modelo de gestión de "eventos" y muchas veces no sirven para ambas cosas. Pandora FMS soporta ambas aproximaciones.

La tercera pregunta hace referencia a que a veces nos interesa una cadena de texto (un evento descriptivo), a veces un número (para poder pintar gráficas), o simplemente un estado (caído, vivo). Poder trabajar con diferentes tipos de datos aporta más flexibilidad. Pandora FMS soporta todos estos tipos de datos.

Estos tres "paradigmas" condicionan mucho su entorno y la herramienta que debe elegir para monitorizarlo. Sea consciente de la información que necesita y piense cuál es la mejor forma de obtenerla. Planifique qué elementos de información dispone y cómo pretende monitorizarlos.

Monitorización remota

Cuando hablamos de monitorización remota nos referimos a que el servidor de Pandora FMS es quien sondea, de forma regular o **síncrona** los dispositivos que desea monitorizar. Este proceso de sondeo síncrono se conoce como "polling". Cuando hablamos de este modelo, no hacemos referencia a la monitorización "local" o basada en agentes instalados sobre los dispositivos que deseamos observar.



Generalmente, cuando hacemos una monitorización remota se realiza para dos propósitos diferentes:

- Comprobar que están vivos (por ejemplo interfaz o sistema activo).
- Obtener un valor numérico (por ejemplo medir el tráfico de red o el número de conexiones activas).

Esta monitorización, cuando es síncrona, siempre se realiza en el mismo sentido: desde el servidor de monitorización hacia el elemento monitorizado.

A veces puede interesarnos lo contrario, que el dispositivo “nos avise” cuando algo ocurre. Esto es monitorización **asíncrona**, y en el caso de monitorización remota se habla generalmente de “traps SNMP”.

La monitorización síncrona se suele realizar usando el protocolo SNMP, que es el más extendido en equipamiento de red. No obstante también se puede hacer mediante WMI, un protocolo similar pero propietario de Microsoft.

Ambos protocolos funcionan de forma parecida; básicamente un servidor “pregunta” por la red para un elemento concreto de configuración del “agente SNMP” o “Servicio WMI” que escucha en el dispositivo. Ese elemento concreto en SNMP se llama OID, y en WMI se identifica mediante una query WQL. Puede ser la memoria libre del sistema, el nº de conexiones del router o el tráfico en una interfaz determinada.

Si su monitorización está orientada sobre todo a entornos de red, **necesita** conocer SNMP en detalle y será la parte que más le interese usar de su herramienta de monitorización. La monitorización asíncrona mediante traps SNMP también es vital. Necesitará, además de una herramienta de monitorización, un explorador 'externo' de dispositivos SNMP, acceso a las colecciones de MIBS de los fabricantes de sus dispositivos de red (que son sus bibliotecas de OID's) y, por supuesto, mucha paciencia para investigar, ya que cada dispositivo tiene generalmente su propia colección de OID's y solo le interesarán algunos elementos dentro de los miles de que dispone cada dispositivo.

Si su monitorización está orientada a servidores Windows y no le interesa instalar agentes en las máquinas, la monitorización remota WMI es también muy apropiada y potente. La interfaz WMI es aún más potente que la de SNMP. Mediante WMI podrá obtener prácticamente cualquier dato, estado o evento de sus servidores Windows.

Los sistemas Unix y Windows también pueden ser sondeados mediante SNMP, pero la información que devuelven es considerablemente menor. Además, necesitará activar y configurar los agentes SNMP del sistema operativo, cosa que puede resultar más complicada que simplemente instalar un agente de monitorización de Pandora FMS.

Finalmente, siempre podrá monitorizar elementos de red mediante el uso de pruebas TCP o ICMP. El ICMP se usa básicamente para:

- Saber si un sistema responde (ping).
- Saber el tiempo de latencia (respuesta) de ese dispositivo (en milisegundos).

Mediante las pruebas TCP se puede saber si un servidor WEB responde adecuadamente, o si un servidor de correo (SMTP) envía bien los correos. Este tipo de pruebas no busca simplemente que el servicio mantenga el puerto abierto, sino que responda como debe; es decir, que el comando de enviar correo reciba un OK o la respuesta del servidor WEB sea “200 OK” (respuesta válida en protocolo HTTP).

Existe una serie de plugins por defecto para chequeos TCP, pero puede implementar fácilmente sus propios chequeos, adaptando sus propios scripts o desarrollando otros nuevos. La integración con Pandora FMS no requiere “API”, estructuras complejas o librerías propietarias.

La monitorización transaccional web, aunque es monitorización remota, recibe un capítulo específico para ello por su importancia.

Monitorización local (con agentes software)

Cuando se habla de sistemas y aplicaciones, sin duda la mejor forma de obtener información es directamente sobre el sistema, esto es, ejecutando comandos o consultando las fuentes de datos del sistema desde la propia máquina que se quiere monitorizar. Esto supone que hay que ejecutar algún tipo de comando, script o realizar algún tipo de consulta sobre el sistema o la aplicación, para lo que utilizaremos el agente software de Pandora FMS.

En la nomenclatura que usa Pandora FMS se habla de agente para referirse a la “entidad” contenedora de información. Por ello, definimos “agente software” como la pieza de software que se instala en un sistema para extraer información y reportarla al servidor de Pandora FMS. El agente software se ejecuta constantemente sobre el sistema (como servicio) y reporta información cada X tiempo.

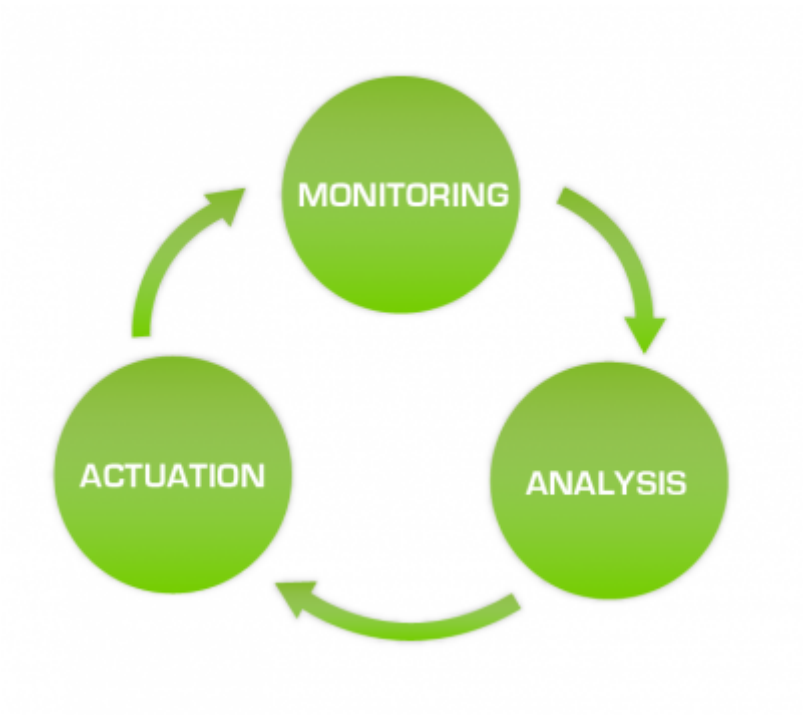
Los agentes, además de su función esencial de obtener información mediante comandos, incluyen otra serie de funciones avanzadas, como obtener información de inventario. También se pueden configurar para que actúen de forma proactiva en caso de problema o fallo, interactuando automáticamente con el sistema, borrando algún fichero temporal o ejecutando algún comando.

Para obtener información *precisa* y *específica* de lo que nos interesa muchas veces tendremos que consultar la documentación de la aplicación que queremos monitorizar, ya que, aunque dispongamos de monitores genéricos, la monitorización interna de aplicaciones conlleva cierta complejidad adicional y elementos específicos.

En Windows existe una variedad casi infinita de accesos a la información: WMI, Perfcounters, Eventlog, logs del sistema, registro, comandos, scripts de powershell, API de NT, etc. De hecho, la arquitectura de Microsoft es de las más fáciles, potentes y mejor documentadas a la hora de obtener información del sistema. En sistemas Unix/Linux la capacidad del agente software para ejecutar cualquier comando nos permite aprovechar toda la potencia de la shell.

Procedimientos en la monitorización

Antes de comenzar una etapa de despliegue es importante plantear cuáles son los puntos críticos y de mayor importancia de la plataforma tecnológica que se va a monitorizar. De este modo, antes de tener información de datos concretos sobre los sistemas se puede saber qué hacer con ellos y cómo explotar toda la utilidad sin perder tiempo en investigaciones o detalles más triviales.



En su caso, ¿cuál cree que describe mejor su necesidad de monitorización?

- Sirve para evitar pérdidas → Disponibilidad.
- Analizar degradaciones → Rendimiento.
- Evaluar crecimientos → Planificación de capacidad.

Cada uno de los casos se enfoca en unos aspectos concretos:

Disponibilidad: Interesa sobre todo la monitorización basada en eventos, y probablemente con monitorización remota sea suficiente; es más rápida de desplegar y se podrán obtener resultados de forma breve. Los informes de SLA serán los de mayor utilidad en este caso.

Rendimiento: En este caso, son las gráficas y los números; se puede obtener esa información tanto con agentes como con chequeos remotos, pero probablemente se necesiten agentes para obtener información pormenorizada de los sistemas. Los informes agrupados y las gráficas combinadas son prioritarias.

Planificación de capacidad: Mucho más especializada; se necesita obtener datos, como en el segundo caso, pero jugar con ellos, con monitores de tipo predictivo e informes de proyección, muy específicos. Establecer alertas tempranas será de mucha ayuda, y se necesitará conocer bien los conceptos de estados WARNING y CRITICAL, además de elaborar una serie de políticas de gestión de eventos que permitan prever el problema antes de que suceda, sin duda el caso más complejo e interesante.

Ahora que ya conoce estos modelos, ¿ya se ha planteado qué hará cuando el sistema le diga que X servicio se ha caído?. O peor aún: ¿Qué sucederá cuando la capacidad de sus

servidores llegue al límite el próximo viernes?

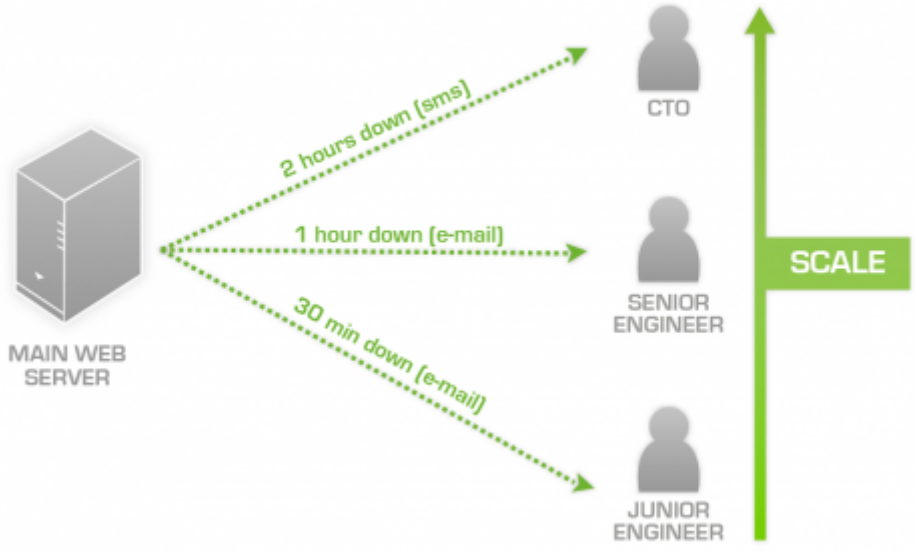
Necesita pensar en procedimientos de actuación.

Procedimientos de actuación

Para poder elaborar procedimientos de actuación será necesario tener en cuenta varios factores:

- **Criticidad del suceso**: Ser capaz de discriminar algo habitual de algo poco frecuente o crítico.
- **Forma de notificar**: email, sms, Telegram, alerta sonora…
- **Escalado**: Diferentes formas de aviso tras la reiteración de un problema. Un caso habitual es la notificación a un responsable tras cierto tiempo sin resolver un problema.

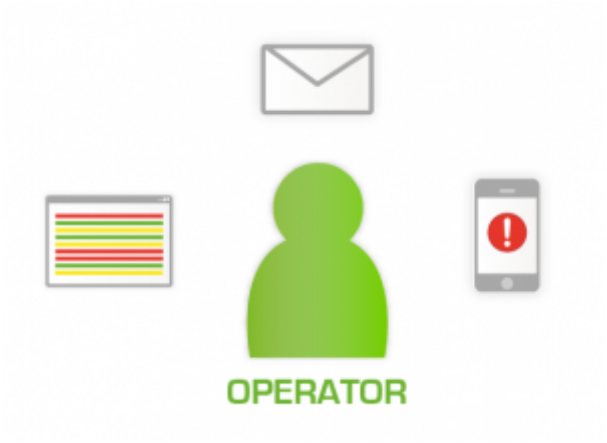
Antes de entrar en configuraciones, es aconsejable tener claros estos conceptos, elaborar esquemas con los elementos críticos, forma de monitorizarlos, qué hacer con toda la información recogida y cómo notificar los problemas que aparezcan.



Si primero se centra en lo más crítico, ya tiene el punto de partida sobre **qué** es lo más importante para su organización. Una vez sepa qué es lo más crítico, ya descubrirá **cómo** monitorizarlo, y mientras tanto pensará en **quién** es el responsable del mantenimiento de esos sistemas y cómo notificarlo.

Modelos de supervisión

Por supervisión entendemos el hecho de que un sistema de monitorización está diseñado para reportar información y funcionar de forma automática, pero que, de hecho, es vigilado por un ser humano de forma directa o indirecta. Esta persona a menudo recibe el nombre de “operador”, y es la persona que observa la pantalla o recibe los eventos de cualquier otra manera, que puede ser mediante un dispositivo “smartphone” o similar, o mediante correos o registros log recogidos con otra herramienta. El sistema no importa, lo importante es el concepto de que hay alguien a cargo y pendiente del sistema.



Por otro lado, existe una serie de personas, que generalmente podemos denominar “administradores de sistemas” o “personal de infraestructura”, que son los que, cuando algo sucede, reciben una llamada del operador: “Oye, tenemos un problema”. O directamente reciben una notificación automática por parte del sistema mediante, por ejemplo, SMS o correo electrónico.

Aquí ya vemos una gran diferencia:

- El **modelo de supervisión directa** implica que hay una o varias personas observando constantemente el sistema, y si sucede algo crítico será detectado en el acto. Probablemente pueden ver pequeños cambios, no críticos, y tener mucha más flexibilidad. No es necesario definir alertas para cada caso posible, basta con mirar los eventos (últimos sucesos) para qué está ocurriendo en el sistema en ese momento. Se pueden definir muchas pantallas, y además definir alertas para apoyar esa supervisión. En grandes entornos se usa este modelo, ya que por mucho que definamos una política de alertas no se puede nunca garantizar una supervisión “autónoma y perfecta”.
- El **modelo de supervisión indirecta** implica que no hay una persona permanentemente observando la pantalla. Por ello es necesario definir de antemano qué notificaciones automáticas van a utilizarse, ya que ni los eventos ni las gráficas estarán bajo supervisión continua. Este sistema es adecuado cuando tenemos pocos dispositivos o tenemos muy bien identificados los elementos críticos y sabemos

como abordar el problema (notificación y solución).

Para trabajar en equipo, cuando intervienen operadores, administradores y personal de tercer nivel son muy útiles las herramientas de las que dispone Pandora FMS, como marcado de eventos, creación de incidencias, escalado de notificaciones, mensajería interna, tablón de avisos y chat entre usuarios de Pandora FMS.

¿ Y ahora qué ?

En los siguientes capítulos trataremos exclusivamente de Pandora FMS. Hasta ahora, hemos contemplado cosas generales que es importante que sepamos antes de seguir explorando la herramienta. Probablemente nuestros usuarios ya sepan muchas cosas y hayan probado otros programas de monitorización. Quizás hayan oído que tal o cual aplicación se monitoriza de una determinada manera en todas partes y que su forma es la mejor.

Puede, pero en nuestra experiencia, cada cliente hace las cosas de una manera. Y por mucho que sepamos de monitorización, no creemos que sepamos más que el propio usuario de cómo tiene montada su infraestructura. Monitorizar cosas sencillas es fácil; lo difícil es adaptar la monitorización a un negocio sin adaptar el negocio a la monitorización. Tenemos más de 800 páginas por delante para descubrir la mejor manera de monitorizar una organización con Pandora FMS. Todo un reto.

Volver al Índice de Documentación Pandora FMS