Introducción

From:
https://pandorafms.com/manual/!776/
Permanent link:
https://pandorafms.com/manual/!776/es/documentation/pandorafms/introduction/01_introduction
2024/06/10 14:34

Introducción

¿Qué es Pandora FMS?

Pandora FMS es un software de monitorización orientado a todo tipo de entornos. 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 sin invertir tiempo ni dinero en otras herramientas.

FMS es el acrónimo en inglés de “Sistema de Monitorización Flexible”.

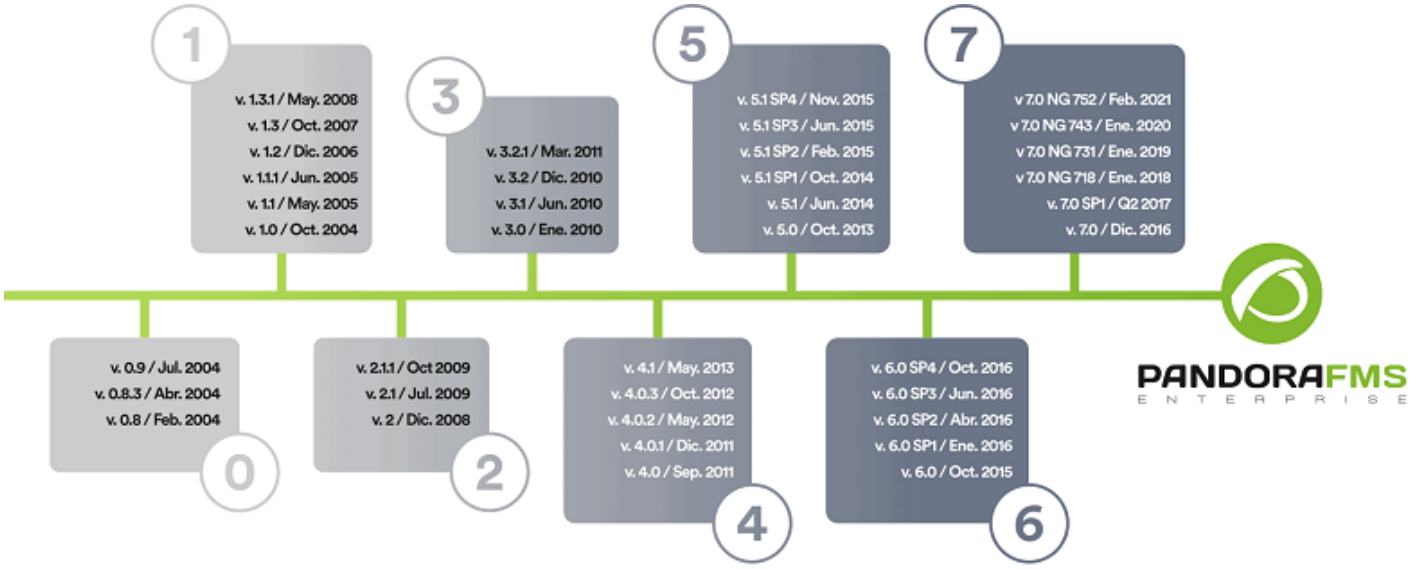
Pandora FMS dispone a día de hoy de agentes para todos los sistemas operativos del mercado. Se puede emplear con éxito no solo para monitorizar sistemas, sino también todo tipo de dispositivos de red, ya sea usando SNMP, mediante sondas de protocolo TCP, ICMP y UDP o Agentes Software.

Acerca de la documentación

- Además de esta documentación oficial existe un foro de usuarios donde puede preguntar sobre dudas.
- Existe un programa de formación oficial con certificación, impartido por parte de las personas que desarrollan Pandora FMS.
- Las guías rápidas ayudan a configurar Pandora FMS e implementar monitorizaciones simples, así como para la instalación de agentes software, tanto para GNU/Linux® como para MS 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. Inicialmente era 100% de código abierto y con los años surgió la necesidad de ofrecer una versión orientada a grandes empresas: Pandora FMS Enterprise, capaz de procesar grandes volúmenes de información por medio de la Metaconsola.

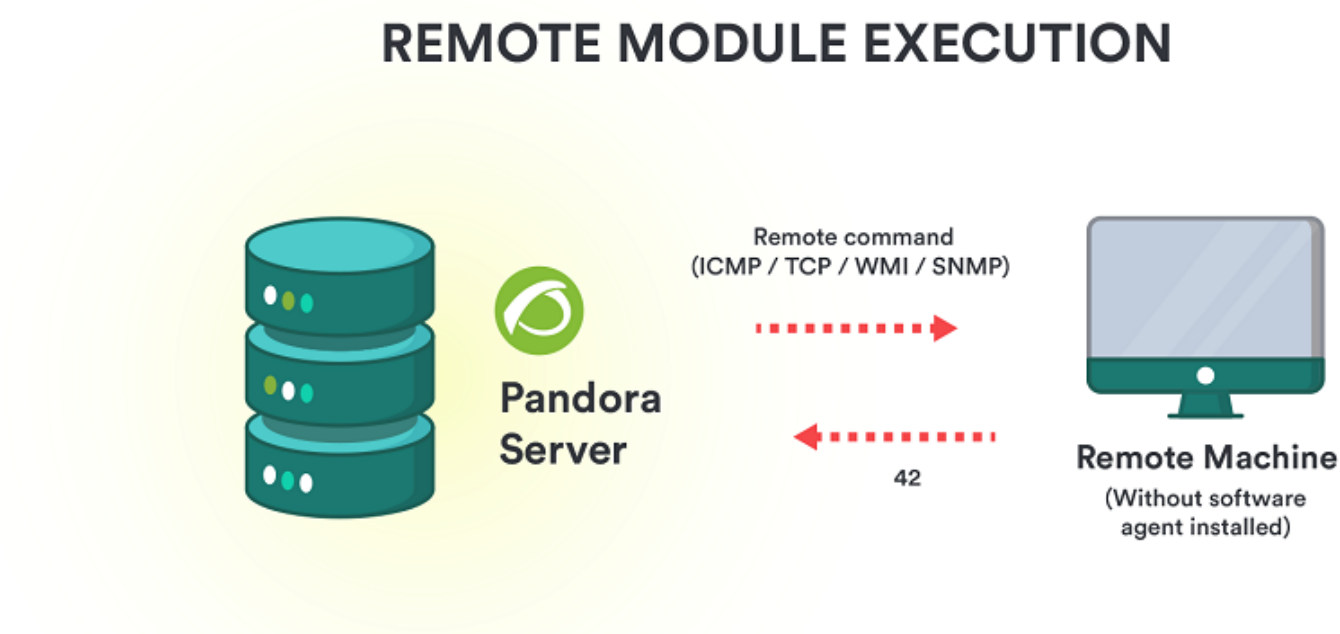


Un vistazo a las funcionalidades de Pandora FMS

- Auto monitorización: Por defecto permite detectar los dispositivos de almacenamiento o las bases de datos (BB.DD.) en un servidor BB.DD., entre otras cosas.
- Auto descubrimiento: Remoto por red se pueden detectar todos sus elementos, catalogarlos según sistema operativo (S.O.) y monitorizar con un perfil asignado.
- Agentes: Pueden obtener información desde la ejecución de un comando hasta la llamada a más bajo nivel de la API de MS Windows®: eventos, *logs*, consumo de memoria, uso de CPU, etcétera. PFMS dispone de una biblioteca de chequeos por defecto para mayor rapidez.
- Controlar: Los propios agentes pueden iniciar servicios, borrar ficheros temporales o ejecutar procesos. En la versión Enterprise se puede hacer desde la Consola web, ejecutando remotamente tareas como detener o iniciar servicios, incluyendo ejecuciones periódicas. Además, se puede usar Pandora FMS para acceder remotamente a sistemas remotos gracias a eHorus (Telnet, VNC o SSH).
- Alertar y notificar: Tan importante como detectar un fallo es avisar del mismo. Con Pandora FMS se dispone de varias formas y formatos de notificación.
- Visualizar y analizar: Aunque monitorizar es recibir un *SNMP trap* o visualizar un servicio interrumpido, también 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.
- 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 autodescubrir, comprobar remotamente, etcétera. También se pueden notificar cambios, como por ejemplo el software desinstalado en un equipo, o utilizarlo para elaborar listados.

Monitorización remota

Cuando se habla de monitorización remota se refiere 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* o monitorización remota.



Generalmente la monitorización remota se utiliza:

- Para comprobar que estén activos y en ejecución.
- Para obtener un valor numérico (por ejemplo medir tráfico de red o 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 y se puede realizar con los protocolos más extendidos, SNMP y WMI (MS Microsoft®).

Cuando es el caso contrario es monitorización asíncrona, y se habla generalmente de *traps SNMP*.

- Para monitorizar entornos de red el protocolo a elegir es SNMP con un explorador 'externo' de dispositivos SNMP, acceso a las colecciones de MIB de los fabricantes de sus dispositivos de red (bibliotecas de OID) y escucha de *traps.* Luego se agregará las colecciones de OID “personalizadas” de cada dispositivo. Para sistemas Unix® y GNU/Linux® se debe tener en cuenta activar las funciones SNMP.
- Para servidores MS Windows® la monitorización remota WMI es muy apropiada y potente ya que se realizan con credenciales de autenticación.

Finalmente, siempre podrá monitorizar elementos de red mediante el uso de pruebas TCP (por ejemplo: protocolo HTTP o protocolo SMTP) o ICMP (por ejemplo: *ping* o tiempo de latencia).

Monitorización local (con agentes software)

Cuando se habla de sistemas y aplicaciones la mejor forma de obtener información es directamente sobre el sistema, ejecutando comandos o consultando las fuentes de datos del sistema desde la propia máquina a monitorizar. Para ejecutar algún tipo de comando, *script* o realizar algún tipo de consulta sobre el sistema o aplicación, se utiliza el Agente Software de Pandora FMS.

Los Agentes Software, 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. Cuando un Agente Software no puede tener contacto directo con el servidor Pandora FMS designado, podrá utilizar una Satellite Server PFMS o un agente *broker.*

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.

- 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: 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, 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.

Procedimientos de actuación

Para poder elaborar procedimientos de actuación se debe tener en cuenta:

- Criticidad del evento: Ser capaz de discriminar algo habitual de algo poco frecuente o crítico.
- Forma de notificar: correo electrónico, SMS, Telegram, alerta sonora, etcétera.
- 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, se aconseja 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.

Modelos de supervisión

- El modelo de supervisión directa implica que hay una o varias personas observando constantemente el sistema. Probablemente pueden ver pequeños cambios, no críticos, y tener mucha más flexibilidad. No es necesario definir alertas para cada caso posible, basta con observar los últimos eventos para qué está ocurriendo en el sistema en ese momento. En grandes entornos se utiliza este modelo.
- El modelo de supervisión indirecta implica el uso de notificaciones automáticas previamente configuradas. Este sistema es adecuado para pocos dispositivos o cuando están muy bien identificados los elementos críticos con su notificación y solución preestablecida.

Volver al índice de documentación de Pandora FMS