Arquitectura

From:
https://pandorafms.com/manual/!783/
Permanent link:
https://pandorafms.com/manual/!783/es/documentation/pandorafms/introduction/02_architecture
2025/10/03 23:41

Arquitectura

Arquitectura de Pandora FMS

El componente vital y donde se almacena casi toda la información es la base de datos MySQL. Todos los componentes de Pandora FMS se pueden replicar y funcionar en un entorno de HA puro (Activo/Pasivo) o en un entorno de grupo o clúster (Activo/Activo con balanceo de carga).

Los Servidores PFMS, con la información generada por ellos mismos o por los Agentes, introducen los datos y la información en la base de datos. La Consola web es la parte encargada de mostrar los datos y de interactuar con el usuario final. Los Agentes Software son aplicaciones que corren en los sistemas monitorizados y recolectan la información para enviarla a los servidores Pandora FMS.

Servidores de Pandora FMS

Los Servidores están integrados en una única aplicación, llamada de forma genérica Pandora Server, que es una aplicación multihilo que ejecuta de forma concurrente diferentes instancias o servidores especializados de Pandora FMS. Estos son los elementos encargados de realizar las comprobaciones existentes pues verifican y cambian el estado de las mismas en función de los resultados obtenidos. También son los encargados de disparar las alertas que se establezcan para controlar el estado de los datos.

Pueden existir servidores simultáneos; uno de ellos es el servidor principal y el resto de los servidores son servidores secundarios. Aunque exista un servidor secundario y uno principal, todos trabajan simultáneamente. La diferencia entre ambos es que cuando un servidor del mismo tipo va fuera de línea (por ejemplo, un Network Server) el servidor principal se encarga de procesar todos los datos que tenía asociado el servidor que está fuera de línea.

Pandora FMS gestiona automáticamente el estado de cada servidor, su nivel de carga y otros parámetros. El usuario puede monitorizar el estado de cada servidor a través de la sección de estado de servidores de la Consola web.

Véase también:

- Export server.
- Sync server.
- SIEM server.
- Monitorización de red con NetFlow y sFlow.
- NCM server.
- Policy Manager.

- MADE server

Data server

Solamente procesa la información enviada por los Agentes Software, los cuales construyen un paquete de información en formato XML y lo entregan en un directorio específico que el servidor de datos procesa primero y luego almacena su resultado en la base de datos.

Se pueden instalar diferentes servidores de datos en diferentes sistemas o en el mismo anfitrión mediante servidores virtuales con múltiples CPU.

A pesar de su sencillez el servidor de datos es uno de los elementos críticos del sistema, ya que procesa toda la información de los agentes y genera alertas y eventos del sistema conforme a esos datos.

Network server

Ejecuta tareas de monitorización remota a través de la red: chequeos ICMP (ej. ping y tiempos de latencia), peticiones TCP y peticiones SNMP. Es muy importante que las máquinas que ejecutan los servidores de red tengan «visibilidad de red» (conexión) a los dispositivos a monitorizar de manera remota.

SNMP trap server

Este servidor utiliza el *daemon* estándar del sistema de recolección de traps, el snmptrapd: Recibe traps SNMP y la Consola SNMP de Pandora FMS los procesa y almacena en la base de datos. También se ocupa de lanzar las alertas asociadas a traps SNMP que hayan sido definidas.

WMI server

WMI es un estándar de Microsoft® para obtener información del sistema operativo y aplicaciones de entornos MS Windows®. Este es el servidor dedicado para monitorizar de forma remota sistemas MS Windows® mediante el protocolo WMI.

Discovery server

Antes denominado Recon server, el Discovery server es empleado para explorar regularmente la red y detectar nuevos sistemas en funcionamiento y aplicar una plantilla de monitorización y comenzar a monitorizar inmediatamente. Utilizando las aplicaciones GNU de sistema nmap, xprobe y traceroute es capaz de detectar los Sistemas Operativos y establecer una topología de red.

El Discovery server se emplea también para lanzar tareas programadas y lanzar monitorización específica contra entornos virtuales, bases de datos o todas aquellas aplicaciones o entornos que requieren explorar lo que existe antes de monitorizar.

Plugin server

Ejecuta chequeos complejos de forma remota mediante *scripts* personalizados, gestionándose de forma centralizada. Esto permite a un usuario avanzado definir sus propias pruebas complejas e integrarlas en la aplicación para que se puedan usar de forma cómoda y centralizada desde Pandora FMS.

Prediction server

Un componente de Inteligencia Artificial que implementa una previsión de datos de forma estadística en base a datos pasados con una antigüedad de hasta 30 días, permitiendo predecir valores de un dato con un intervalo de 10 a 15 minutos, y conocer si un dato en el momento actual es anómalo respecto a su historial. Básicamente construye una línea de base dinámica con un perfil semanal.

Web server

Realiza comprobaciones web completas, como el proceso de identificación de un usuario, paso de parámetros por formulario, comprobación de contenidos, navegación por menús, etc. Se utiliza para chequeos de disponibilidad verdadero/falso y para obtener tiempos de latencia de experiencia completa de navegación.

Export server

Permite exportar los datos de un dispositivo monitorizado de una instalación de Pandora FMS a otra, y así tener replicados los datos. Especialmente útil en grandes despliegues con varias instalaciones de Pandora FMS y con necesidad de centralizar.

Inventory server

Obtiene y visualiza información de inventario de los sistemas: Software instalado, modelo de elementos hardware, dispositivos de almacenamiento, servicios en ejecución, etcétera. Puede obtener esta información tanto de forma remota como de forma local.

Event server

Este servidor especial sirve para correlacionar eventos y generar alertas y no ejecuta tareas de monitorización. Este servidor, al contrario que el resto, no dispone de configuración de hilos ni de alta disponibilidad.

ICMP server

Utilizan estrategias avanzadas para ejecutar chequeos ICMP (ping) trabajando con los OID (*Object IDentifier*) previamente validadas, por lo que tiene un rendimiento elevado.

Satellite server

Se instala de forma separada al servidor principal de Pandora FMS y permite el reenvío de ficheros de datos desde los Agentes Software hacia el servidor principal, actuando a modo de *proxy* de agentes en topologías distribuidas. Envía los datos de monitorización como ficheros XML a través de una conexión Tentacle, por lo que no requiere conexión con la base de datos.

WUX server

Combinado con el Grid de Selenium permite realizar transacciones web complejas de forma distribuida. Estas transacciones se ejecutan en un navegador real, su salida se captura y procesa para visualizarla paso a paso, incluyendo capturas de los errores y estadísticas detalladas.

Syslog server

Permite analizar el syslog de la máquina donde está ubicado, analizando su contenido y almacenando las referencias en el servidor OpenSearch correspondiente.

Log server

Permite correlacionar logs y ejecutar sus alertas.

Alert server

Si se activa se encargará de la ejecución de todas las alertas de monitorización, ya que por defecto cada servidor se encarga de sus propias alertas y en algunos casos concretos se pueden producir retrasos en la monitorización si una alerta debe ejecutar alguna tarea y esta tarda más de lo debido en realizarse.

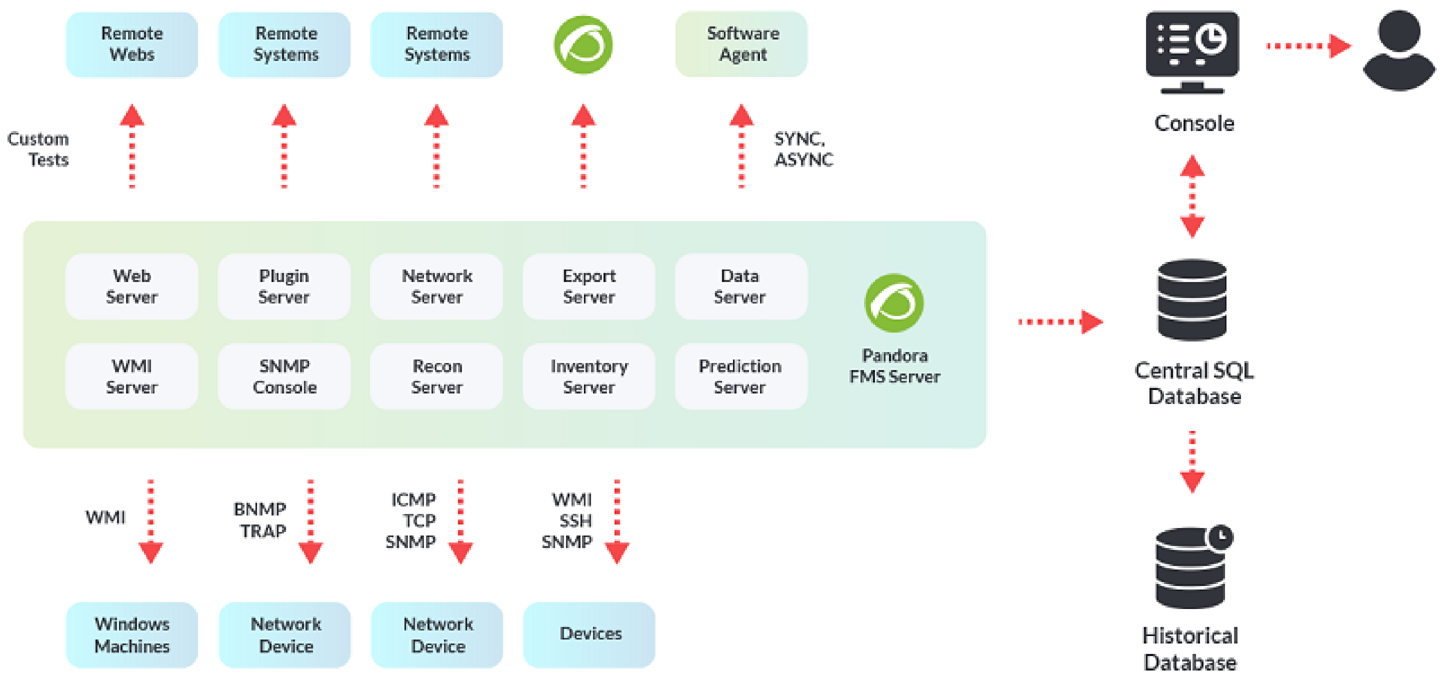
Consola web de Pandora FMS

Es la interfaz de usuario de Pandora FMS. Esta Consola de administración y operación permite a diferentes usuarios, con diferentes privilegios, controlar el estado de los Agentes, ver información estadística, generar gráficas y tablas de datos, así como gestionar incidencias con su sistema integrado. También es capaz de generar informes y definir de forma centralizada nuevos Módulos, Agentes, alertas y crear otros usuarios y perfiles.

Puede ejecutarse en múltiples servidores para repartir carga como para facilitar el acceso por problemas logísticos (grandes redes, numerosos grupos de usuarios diferentes, diferencias geográficas, diferencias administrativas, etcétera).

Base de datos de Pandora FMS

Pandora FMS utiliza una base de datos MySQL en la que almacena toda la información recibida en tiempo real, normalizando todos los datos de las diversas fuentes origen. Actualmente Pandora FMS solamente soporta MySQL, MariaDB y Percona.



Agentes Software de Pandora FMS

Es importante diferenciar dos conceptos: Agente, o Agente en Consola, como contenedor y Agente Software, el cual se ejecuta en un equipo.

Agente (Contenedor)

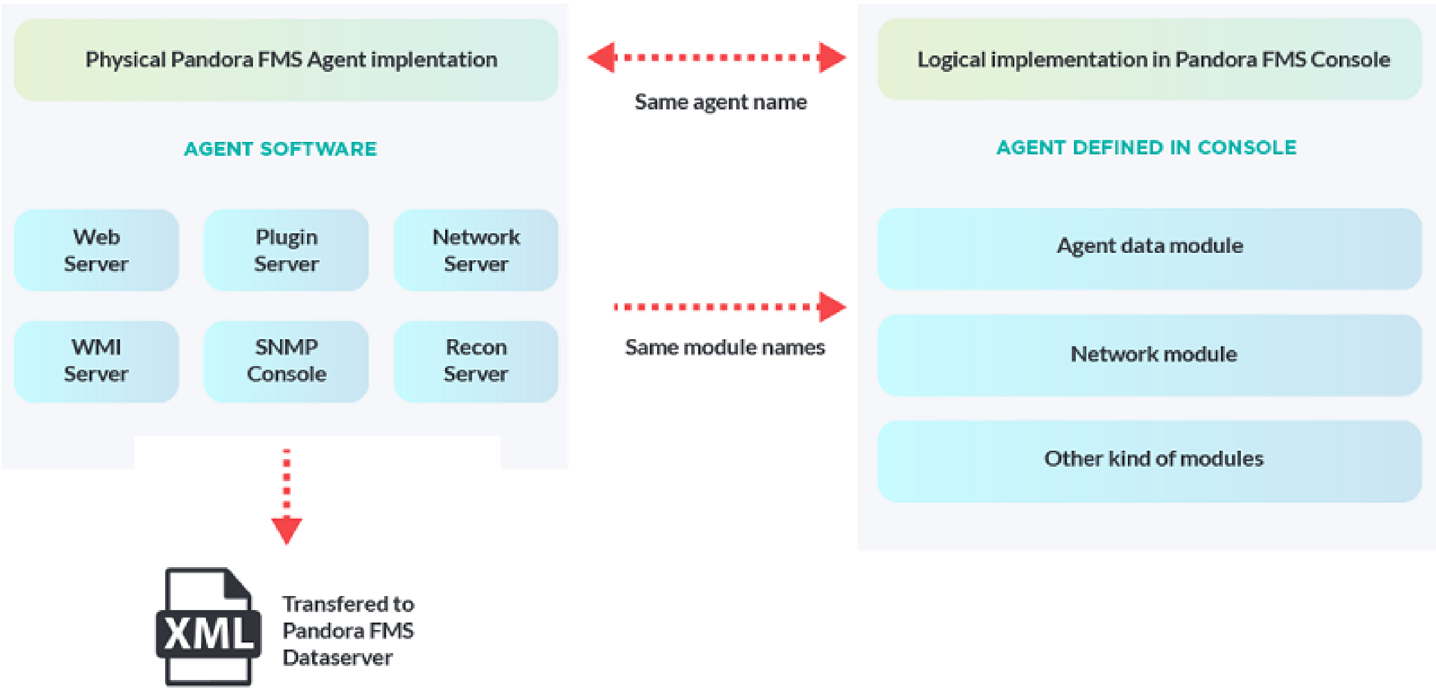
El Agente de Pandora FMS es un elemento organizativo creado en la Consola web de Pandora FMS, asociado a un grupo de Módulos (o elementos individuales de monitorización). Este agente puede tener (opcionalmente) asociadas una o más direcciones IP.

Un Agente puede contener Módulos de tipo remoto o de tipo local. Los Módulos de tipo remoto son ejecutados por aquellos servidores que obtienen información de forma remota (ej. Network server); los módulos de tipo local son ejecutados por los Agentes Software y recolectados y procesados por el Data Server.

Agente Software

Los Agentes Software se instalan en los equipos a monitorizar de manera local, extrayendo la información desde el propio equipo. Se utilizan principalmente en servidores para monitorización de recursos de la máquina (CPU, RAM, discos…) y aplicaciones instaladas (MySQL, Apache, JBoss…). Generalmente, la monitorización de servidores y equipos se llevará a cabo con Agentes Software mientras que la monitorización de equipos de red se hará de forma remota sin la instalación de ningún software.

Toda la información de los chequeos realizados se plasma en un único fichero de datos en formato XML, que es enviado a través del protocolo Tentacle al servidor de Pandora FMS en un intervalo predeterminado de 300 segundos. También es posible transmitir los paquetes usando SSH o FTP.



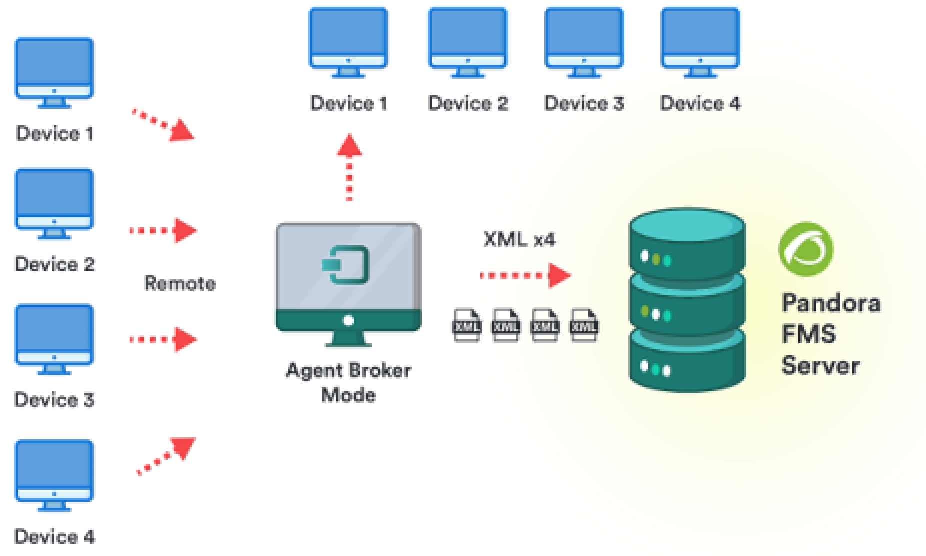
Topologías, esquemas y modelos de monitorización

Redes accesibles

- Red accesible para monitorización remota centralizada: donde, desde el servidor de Pandora FMS, se puede acceder a todas las máquinas y/o dispositivos para sondear remotamente.
- Red accesible para monitorización basada en Agentes: donde, desde los Agentes Software instalados en las máquinas monitorizadas, pueden llegar sin problemas al servidor de Pandora FMS.

Redes con dificultad de acceso

- Red remota no alcanzable por los chequeos remotos de Pandora FMS: Utiliza la modalidad *broker agent.*



- Agentes Software que no tienen acceso al servidor de Pandora FMS: Este caso utiliza la característica de *proxy* de los Agentes Software o un Satellite server como *proxy* de agentes software.

- Necesidad de monitorizar redes diferentes para monitorización remota con el servidor: En este caso también se puede hacer uso del *Satellite Server* o varios servidores diferentes de Pandora FMS conectados a la misma base de datos.

Características especiales organizativas

- Dualidad de reporte: Adicionalmente, puede configurar Agentes para que reporten a dos servidores de Pandora FMS diferentes, aunque solo podrá ser gestionado por uno de ellos.
- Gestión fragmentada: Se necesita delegar la administración de parte de los equipos a diferente personal, con diferentes accesos. Esto, más que un problema de arquitectura, es un problema de gestión. Se soluciona con los permisos asignados sobre políticas.

Grandes entornos con Pandora FMS

- Red numerosa: Cuando no pueden ser centralizadas en un único servidor se utilizan servidores en modo *broker*, que distribuyen la carga de los chequeos remotos.
- Servidores redundantes: Por seguridad, dado el caso fallar el hardware primario, un servidor en modo HA puede automáticamente reubicar y delegar la carga de trabajo de monitorización.

Volver al índice de documentación de Pandora FMS