Arquitectura

Volver al Indice

Arquitectura de Pandora FMS

Este capítulo describe de forma general los diferentes componentes de Pandora FMS, su relación entre ellos y cómo utilizar la arquitectura de Pandora FMS para abordar diferentes retos en función de las características de su infraestructura y topología.

Pandora FMS puede ser extremadamente modular y descentralizado o bien sencillo y monolítico. 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 clusterizado (Activo/Activo con balanceo de carga).
Pandora FMS consta de diversos elementos, entre ellos, los que se encargan de recolectar y procesar los datos son los servidores. Los servidores, con la información generada por ellos o por los agentes, introducen los datos en la base de datos. La consola es la parte encargada de mostrar los datos presentes en la base de datos y de interactuar con el usuario final. Los Agentes Software son aplicaciones que corren en los sistemas monitorizados, y recolectan la información para enviársela a los servidores de Pandora FMS.

Servidores de Pandora FMS

En Pandora FMS existen más de diez servidores diferentes ~~especializados~~, encargados de las tareas antes mencionadas. Los servidores están integrados en una única aplicación, llamada de forma genérica "Pandora Server", que es una aplicación multi-hilo que ejecuta de forma concurrente diferentes instancias o servidores especializados de Pandora FMS. A continuación se describe cada uno de los servidores especializados de Pandora FMS.

Los servidores de Pandora FMS son los elementos encargados de realizar las comprobaciones existentes. Ellos las 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.

El servidor de datos de Pandora FMS puede trabajar con alta disponibilidad y/o balanceo de carga. En una arquitectura muy grande, se pueden usar varios servidores de Pandora FMS a la vez para poder manejar grandes volúmenes de información distribuida por diferentes zonas geográficas o funcionales.

Los servidores de Pandora FMS están siempre en funcionamiento y verifican permanentemente si algún elemento tiene algún problema y si está definido como alerta. Si ocurre esto, se ejecutará la acción definida en la alerta, tal como enviar un SMS, un correo electrónico, o activar la ejecución de un script.

Pueden existir servidores simultáneos, uno de ellos es el servidor principal y el resto de los servidores son servidores esclavos. Aunque exista un servidor esclavo y uno maestro, todos trabajan simultáneamente. La diferencia entre ambos es que cuando un servidor del mismo tipo se cae (p.e. Un network server) el servidor maestro se encarga de procesar todos los datos que tenía asociado el servidor que se ha caído.

El servidor que recibe el fichero de datos del agente, o que procesa la información (si esta es de tipo remoto) es el que dispara las alertas asociadas a esos datos que acaba de procesar.

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.

Servidor de datos

Procesa la información enviada por los agentes Software. Los agentes Software recogen información de forma local de los sistemas en los que se encuentran instalados y construyen un paquete de información en formato XML. Estos paquetes en formato XML son enviados al servidor. En el servidor son recibidos en un directorio específico, el servidor procesa todos los archivos que vayan llegando a este directorio de entrada y almacena la información en la base de datos.

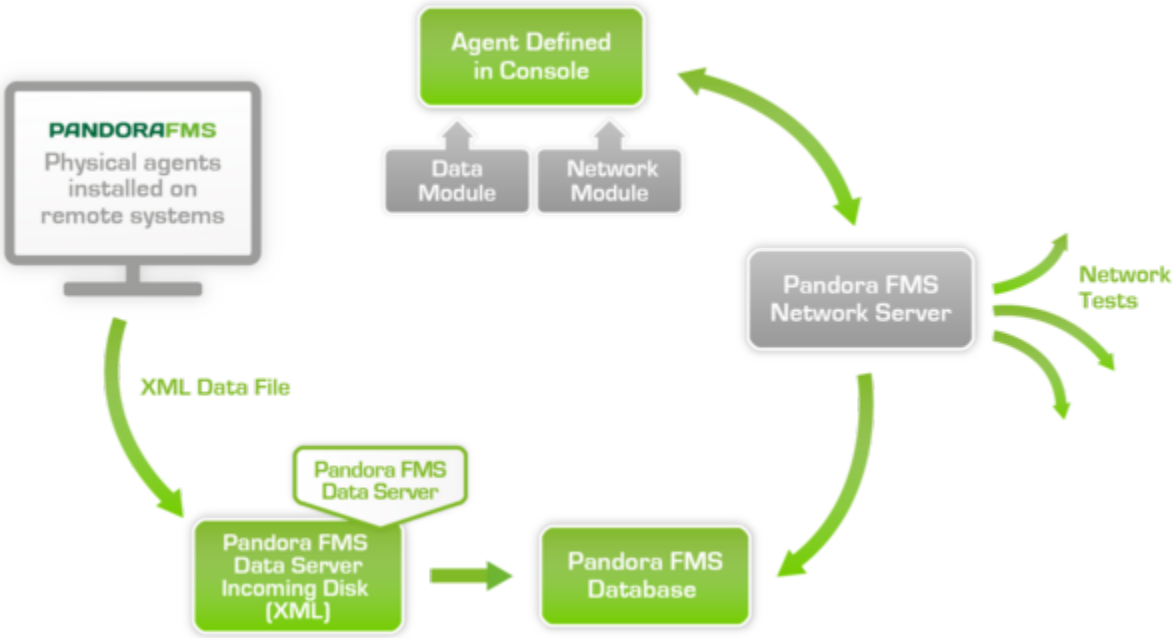
Se pueden instalar diferentes servidores de datos en diferentes sistemas o en el mismo anfitrión (que serán diferentes servidores virtuales). Varios servidores pueden trabajar juntos para entornos muy extensos y que necesiten aprovechar mejor el hardware (p.e. en casos de entornos con multiples CPU).

A pesar de su sencillez y escasa utilización de recursos, 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. El servidor de datos sólo trabaja con los datos que llegan en XML desde los agentes software y no realiza ningún tipo de comprobación remota.

Servidor de red

Ejecuta tareas de monitorización remota a través de la red: chequeos ICMP (Ping, tiempos de latencia), peticiones TCP y peticiones SNMP. Cuando se asigna un agente a un servidor se está especificando el servidor de red que ejecutará los chequeos para ese agente, así que es muy importante que las máquinas que ejecutan los servidores de red tengan «visibilidad de red» para poder ejecutar las tareas de monitorización de red asignadas a los mismos. Es decir, que si va a hacer *pings* a sistemas de una red determinada, el servidor de red pueda llegar a esa red:

Por ejemplo, si se crea un módulo para hacer una comprobación de ping a 192.168.1.1 y se asigna este agente/módulo a un servidor en una red 192.168.2.0/24 sin acceso a la red 192.168.1.0/24 siempre devolverá DOWN ya que no puede contactar con ella.



Consola SNMP

Este servidor, llamado consola de traps SNMP, utiliza el demonio standard del sistema de recoleccion de traps, *snmptrapd*. Este demonio 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 haya definidas.

Servidor WMI

WMI es un estándar de Microsoft para obtener información del sistema operativo y aplicaciones de entornos Microsoft Windows. Pandora FMS tiene un servidor dedicado para monitorizar **de forma remota** sistemas Windows mediante el protocolo WMI.

Servidor de reconocimiento

Utilizado para explorar regularmente la red y detectar nuevos sistemas en funcionamiento. El servidor recon también puede aplicar una plantilla de monitorización para aquellos sistemas detectados recientemente y aplicar automáticamente los módulos por defecto definidos en esa plantilla para comenzar a monitorizar inmediatamente el nuevo sistema. Utilizando las aplicaciones de sistema nmap, xprobe y traceroute es capaz además de detectar los Sistemas Operativos y establecer la topología de red en funcion de los sistemas que ya conoce.

Servidor de complementos (Plugins)

Ejecuta chequeos complejos de forma remota mediante scripts personalizados. Pueden estar desarrollados en cualquier lenguaje e integrados en la interfaz de Pandora FMS, gestionándose de forma centralizada. Esto permite a un usuario avanzado definir sus propias pruebas complejas, desarrolladas por él mismo, e integrarlas en la aplicación para que se puedan usar de forma cómoda y centralizada desde Pandora FMS.

Servidor de predicción

Es un pequeño componente de Inteligencia Artificial que implementa una previsión de datos de forma estadística en base a datos pasados con una profundidad de hasta 30 días en cuatro referencias temporales permitiendo predecir los valores de un dato con un intervalo de 10-15 minutos, y conocer si un dato en el momento actual es anómalo respecto a su historial. Básicamente tendremos que construir una baseline dinámica con un perfil semanal.

Este servidor, también gestiona el cálculo de la monitorización de servicios (BPM) a partir de la versión 5.0 de Pandora FMS.

Servidor de chequeos WEB (Goliat)

Servidor de chequeos WEB (Goliat), el Servidor de exportación, el Servidor de inventario, el Servidor de correlación de eventos y el Servidor de red enterprise soloestáan disponibles en la versión Enterprise de Pandora FMS.

El servidor de chequeos WEB sirve para hacer pruebas de carga. Realiza comprobaciones web completas, desde 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 (funciona, no funciona) y para obtener tiempos de latencia (en segundos) de experiencia completa de navegación, incluyendo recursos asociados a la página (imágenes, textos completos, etc).

Servidor de exportación

(Sólo versión Enterprise)

El servidor de exportación de Pandora FMS permite exportar los datos de un dispositivo monitorizado de una instalación de Pandora FMS a otra, y así tener replicados los datos. Esto es especialmente útil cuando se tiene una gran despliegue, con varias instalaciones de Pandora FMS, y se quiere tener cierta información crítica centralizada en uno solo.

Servidor de inventario

(Sólo versión Enterprise)

El servidor de inventario obtiene y visualiza información de inventario de los sistemas: software instalado, modelo de elementos hardware, discos duros, servicios corriendo en el sistema, etc. Puede obtener esta información tanto de forma remota como de forma local, a través de los Agentes Software.

Servidor de correlación de eventos

(Sólo versión Enterprise)

Este servidor especial sirve para correlar eventos y generar alertas, no ejecuta tareas de monitorización. Al igual que los otros, se puede especificar en la configuración para su arranque o no. Este servidor al contrario que el resto no dispone de configuración de hilos ni de alta disponibilidad.

Servidor de red enterprise SNMP e ICMP

(Sólo versión Enterprise)

Son dos servidores adicionales que utilizan estrategias avanzadas para ejecutar chequeos ICMP (ping) y SNMP (polling) de forma que producen un rendimiento muy superior a la version opensource, a cambio de unos requisitos bastante delicados (especialmente SNMP), ya que trabajan con OID's previamente validadas por el servidor open.

Servidor Satélite

(Sólo versión Enterprise)

Este componente se instala de forma separada al servidor principal de Pandora FMS. Permite explorar y detectar nuevos sistemas, monitorizar de forma remota con ICMP y SNMP de alta velocidad, ejecuta plugins remotos y permite el reenvío de ficheros de datos desde los agentes software hacia el servidor principal, actuando a modo de proxy de agentes. Envía los datos de monitorización como XMLs a través de una conexión tentacle, por lo que no requiere conexión con la base de datos.

Existe un capítulo específico dedicado a la monitorización de Topologías distribuidas con Satellite Server

Servidor WUX

Es un servidor, que combinado con el Grid de Selenium permite realizar transacciones WEB complejas de forma distribuida. Se diferencia de los chequeos de WEB sencillos (Goliat) en que estas transacciones se ejecutan en un navegador real, y su salida se captura y procesa para visualizarla paso a paso, incluyendo capturas de los errores, así como estadísticas detalladas de todas las peticiones WEB.

Consola web de Pandora FMS

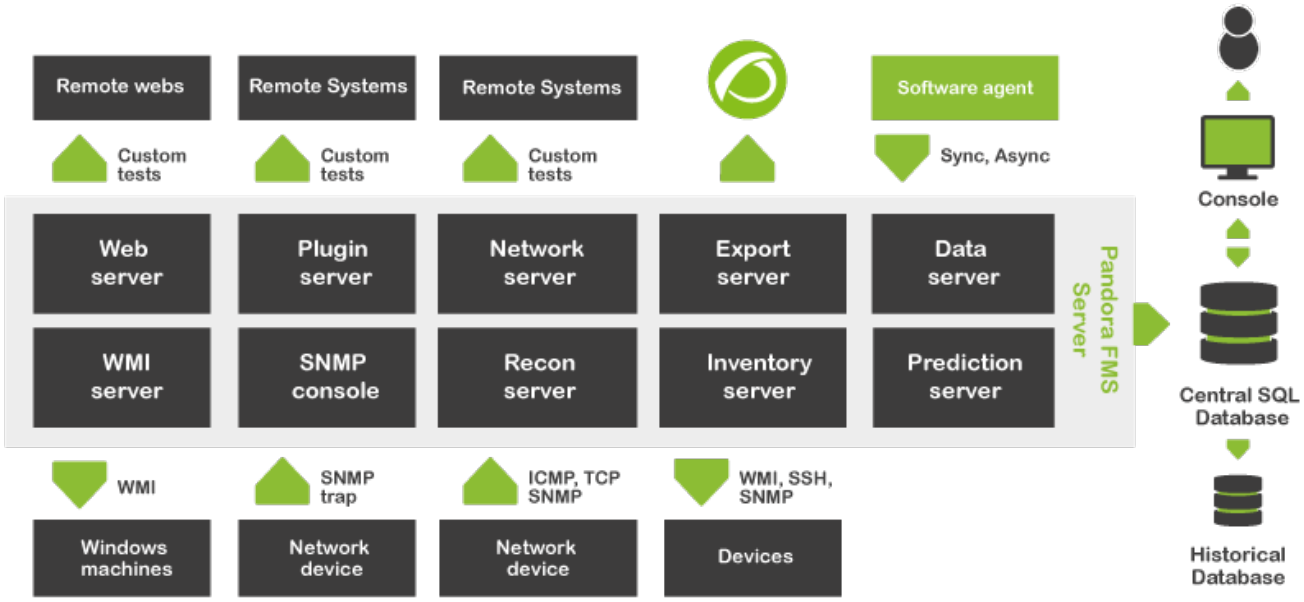
Es la interfaz de usuario de Pandora FMS. Esta consola de administración y operación permite a diferentes usuarios, con diferentes privilegios, controlar el estado de los agentes, ver información estadística, generar gráficas y tablas de datos así como gestionar incidencias con su sistema integrado.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

La consola web está programada en PHP y no requiere por parte del usuario final la instalación de ningún software adicional. Puede accederse desde cualquier plataforma moderna que soporte HTML y CSS. Se recomienda Firefox 2.x o Chrome. La experiencia de usuario con navegadores como Internet Explorer 6 es muy pobre, y podrían perderse funcionalidades imprescindibles de la consola.

La consola web a su vez, puede ejecutarse en múltiples servidores, esto es, podemos tener tantas consolas web como queramos, tanto para repartir carga como para facilitar el acceso por problemas logísticos (grandes redes, numerosos grupos de usuarios diferentes, diferencias geográficas, diferencias administrativas, etc.). Su único requisito es poder acceder al contenedor de datos donde Pandora FMS almacena todo: la base de datos, y en el caso de la versión Enterprise, acceder al repositorio de configuraciones de los agentes de forma sincronizada (via NFS).

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. Conforma el componente más importante y crítico de toda instalación de Pandora FMS, conteniendo no solo la información e histórico de datos, sino todas las configuraciones realizadas a lo largo del tiempo. En el pasado soportamos PostgreSQL y Oracle, pero actualmente sólo soportamos MySQL/MariaDB/Percona.



La base de datos es el núcleo de Pandora FMS

Estos datos se gestionan automáticamente desde Pandora FMS, llevando a cabo un mantenimiento periódico y automático de la base de datos, no siendo necesaria ningún tipo de tarea de administración de base de datos ni proceso manual asistido por un operador o administrador. Esto se realiza por medio de una purga periódica de los datos pasada una fecha.

Agentes Software de Pandora FMS

Cuando nos referimos a un agente en Pandora FMS es importante diferenciar dos conceptos:

- Agente, o agente en consola, como contenedor.
- Agente Software, como software que se ejecuta en un equipo.

Agente (Contenedor)

El agente de Pandora FMS es simplemente un elemento organizativo creado en la consola web de Pandora FMS y que está asociado a un grupo de módulos (o elementos individuales de monitorización). Además, este agente puede tener (opcionalmente) asociadas una o más direcciónes IP.

El agente puede tener asociados módulos remotos, obtenidos a través de servidores de Red, WMI, Plugin, etc.

- Verificación de si el motor está conectado o en línea (PING).
- Verificación de si un puerto determinado está abierto o cerrado.
- Verificación de si una entidad de red, alojada en un puerto específico del hardware, está respondiendo correctamente.
- Verificación de si una entidad de red, alojada en un punto específico del hardware, tiene el contenido deseado.
- Verificación (es) de hardware por SNMP (determinación de la MIB).
- Verificación del tiempo de latencia entre el nodo y los servidores de Pandora FMS.

El agente también puede tener asociados módulos de tipo "local", que son los que están definidos en la configuración del agente Software y que también se deben definir en el Agente de la consola WEB. Cuando un paquete de datos llega por primera vez desde un agente software, por defecto se creará de forma automática el nuevo agente, con su grupo de módulos ejecutados de forma local, en la consola web.

Por tanto, 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 (network server, recon server...), y los módulos de tipo local son ejecutados por los agentes software y recolectados y procesados por el servidor de datos (Data Server).

Agente Software

Los agentes software se instalan en los equipos que desean monitorizarse localmente, 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.

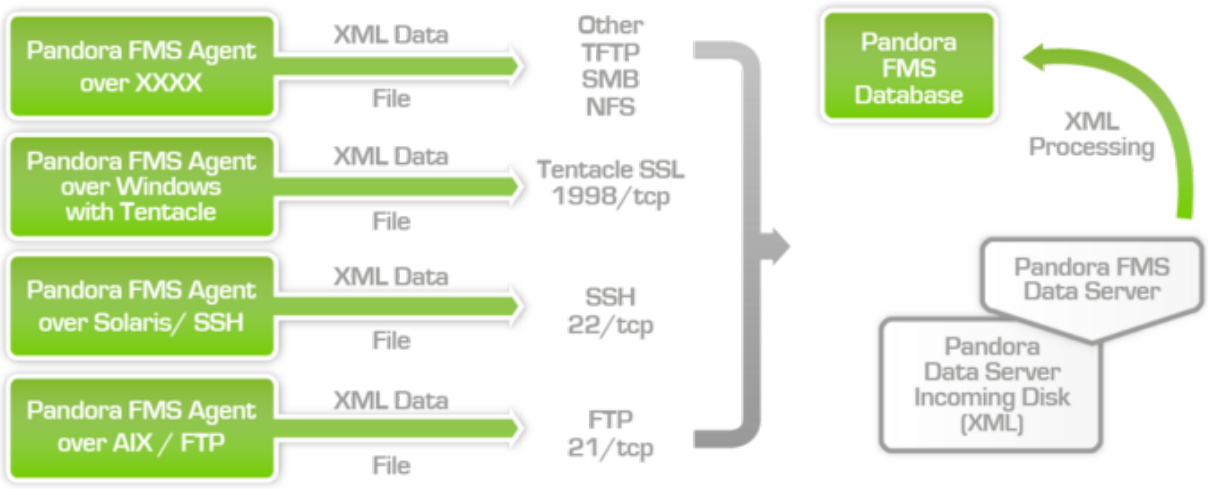


Ilustración: Recolección de datos locales en Pandora FMS

Cada agente software realiza varios chequeos, llamados módulos, que corresponden cada uno a un dato concreto, como puede ser uso de CPU. Toda la información de los chequeos realizados se plasma en un único fichero de datos en formato XML que es enviado al servidor de Pandora FMS.

El proceso de copia del paquete de datos del agente al servidor se realiza de forma regular (Síncrona) cada cierto tiempo, este **intervalo** es definido en el agente software, que es quien inicia las comunicaciones con el servidor.

El intervalo predeterminado es de 300 segundos. Valores inferiores a 100 segundos no se recomiendan de forma general ya que podrían afectar al rendimiento del sistema anfitrión, además de cargar excesivamente la base de datos y el propio servidor de Pandora FMS.

Hay que recordar que **Pandora FMS no es un sistema de tiempo real**, es un sistema de monitorización general de aplicaciones y sistemas en entornos cuya criticidad no sea el tiempo real. No obstante si se puede adaptar Pandora FMS para que opere en entornos de tiempos de respuesta en torno a 3-5 segundos.

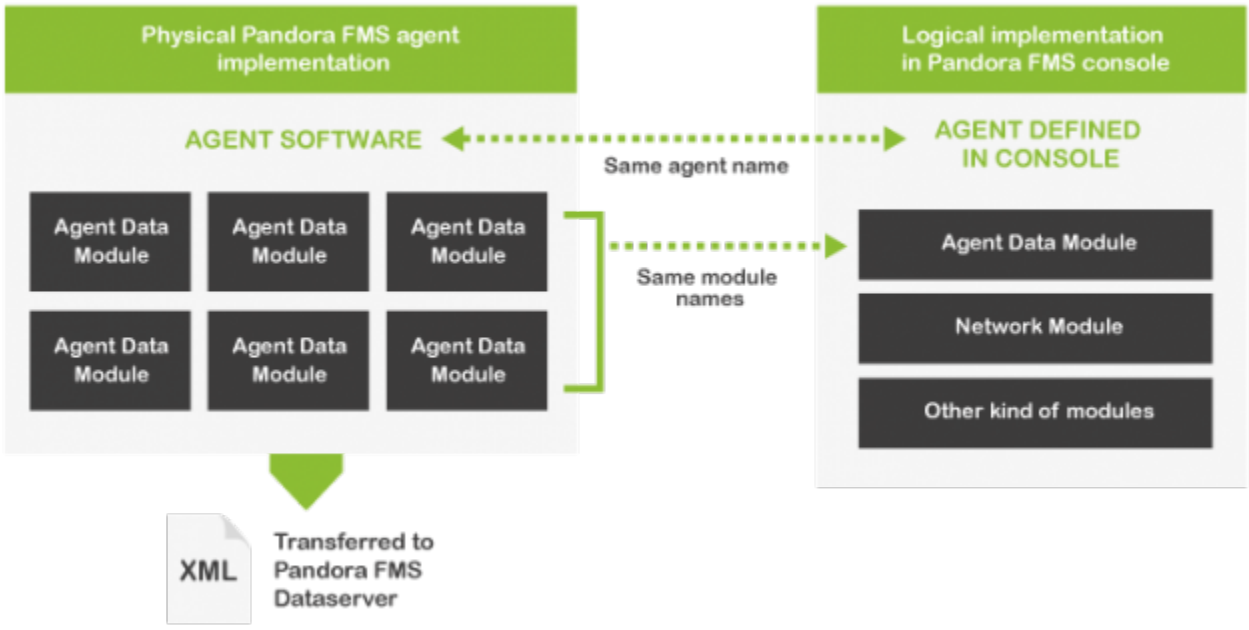


Ilustración: Esquema lógico de un agente / agente fisico

Las transferencias de paquetes XML se hace generalmente a través del protocolo Tentacle, aunque también es posible transmitir los paquetes usando SSH o FTP.

Tanto con SSH como con Tentacle se puede hacer que el proceso sea totalmente seguro ya que no viajan contraseñas por la red ni datos confidenciales sin cifrar, se asegura la confidencialidad, integridad y autenticación de las conexiones entre el agente y el servidor. En la documentación sobre la instalación y configuración de los Agentes y el Servidor se detalla el proceso de generación de claves para poder hacer la transferencia SCP (SSH) de forma automática y también mediante el protocolo Tentacle.

También se puede realizar la transferencia mediante FTP o cualquier otro sistema de transferencia de ficheros, aunque se eligió Tentacle por la seguridad que ofrece este sistema, por su facilidad para el usuario y por sus múltiples opciones (SSL).

Consultar los anexos a la documentación para configurar transferencias a través de otros protocolos.

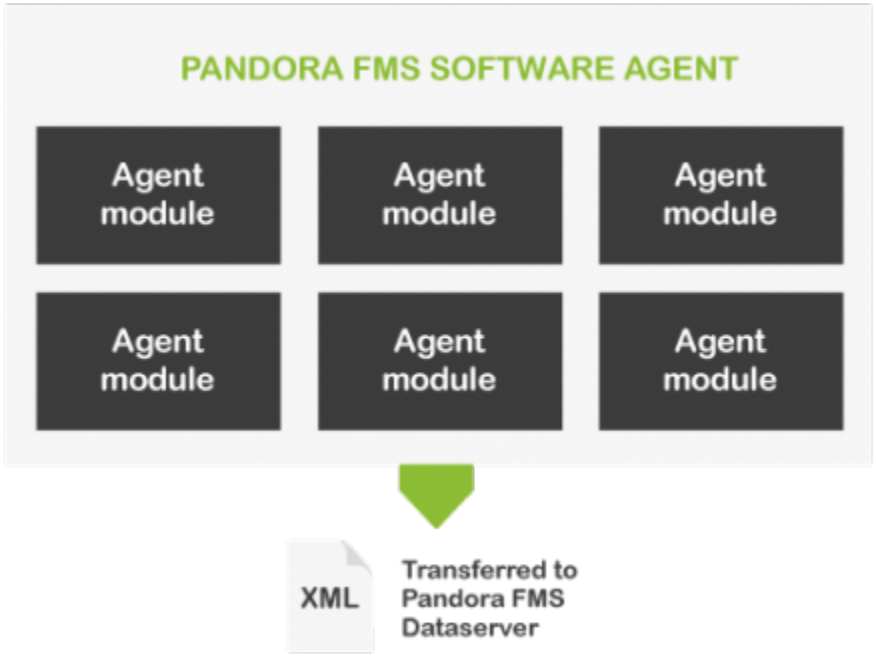
Los agentes de Pandora FMS están pensados para su ejecución en el sistema desde el cual recolectan datos, aunque los agentes pueden recolectar información de maquinas accesibles desde el anfitrión donde están instaladas mediante la ejecución de comandos de red contra los sistemas accesibles.

Fichero de datos XML

Este fichero de datos contiene una estructura XML y su nombre se forma mediante la combinación del nombre del anfitrión o host donde esta el agente, un numero de serie diferente para cada paquete de datos y la extensión .data que indica que es un paquete de datos.

```
<nombredehost>.<nº de serie>.data
```

Ilustración: Estructura lógica de los modulos de un agente software



El fichero de datos es el fichero con extensión .data. El fichero de verificación, con extensión .checksum contiene un hash MD5 del fichero de datos. Esto permite hacer una última verificación para asegurarse de que los datos no han sido alterados de ninguna manera antes de ser procesados.

```
<nombredehost>.<nº de serie>.checksum
```

El fichero de datos XML contiene toda la información recogida por el Agente durante su ejecución. Este paquete de datos tiene un diseño compacto, flexible y ligero que permite que cualquier usuario pueda utilizar los agentes de Pandora FMS o sus propios desarrollos para generar información y que esta sea procesada en Pandora FMS. El fichero de datos es un XML similar al siguiente:

```
<agent data os_name=”SunOS” os_version=”5.8” timestamp=”300” agent_name=”pdges01” version=”1.0”>
<module>
<name>FTP Daemon</name>
<type>generic_proc</type>
<data>0</data>
</module>
<module>
<name>DiskFree</name>
<type>generic_data</type>
<data>5200000</data>
</module>
<module>
<name>UsersConnected</name>
<type>generic_data_inc</type>
<data>119</data>
</module>
<module>
<name>LastLogin</name>
<type>generic_data_string</type>
<data>slerena</data>
</module>
</agent_data>
```

Topologías, esquemas y modelos de monitorización

Existen diferentes modelos a la hora de abordar la monitorización, tanto remota como local. Enumeramos los siguientes casos habituales de diferentes topologías con el fin de familiarizar al lector con las posibles problemáticas y las soluciones ofrecidas por Pandora FMS. En sucesivos capítulos se describe el funcionamiento de cada solución.

Redes accesibles

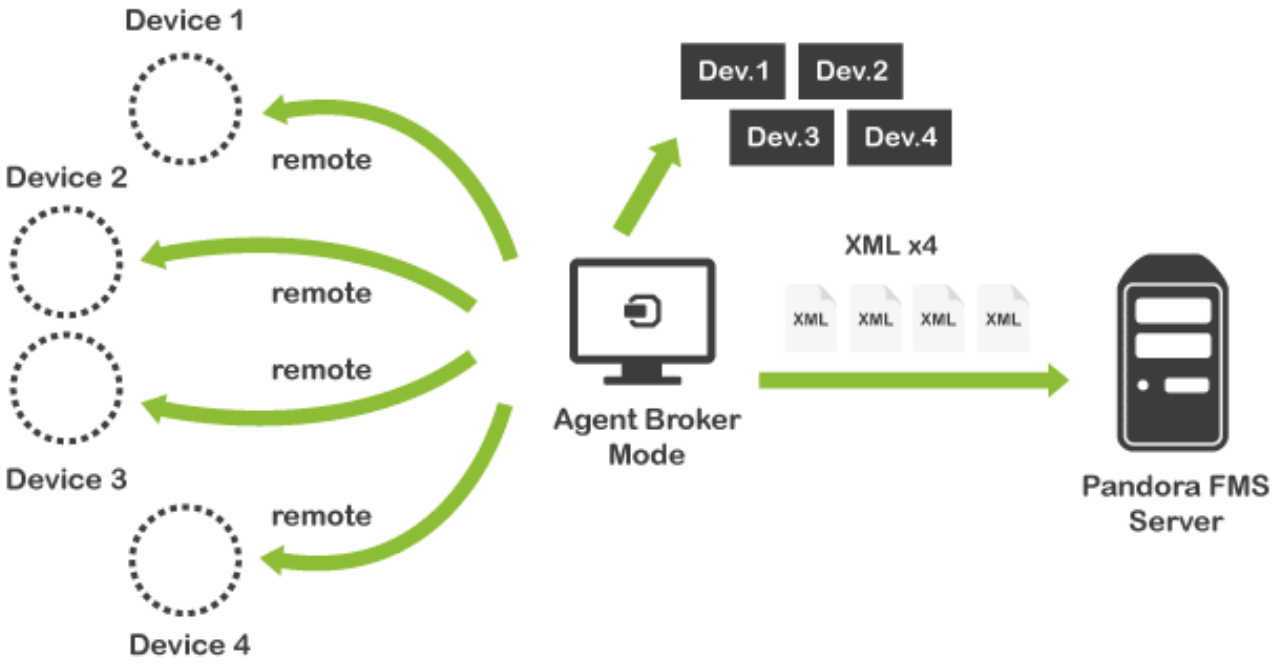
Esto sólo es lo habitual en redes sencillas y de pequeño tamaño o muy centralizadas y organizadas. Es el modelo más fácil de implantación.

Red accesible para *monitorización remota centralizada. Donde desde el servidor de Pandora FMS podemos acceder a todas las máquinas 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.

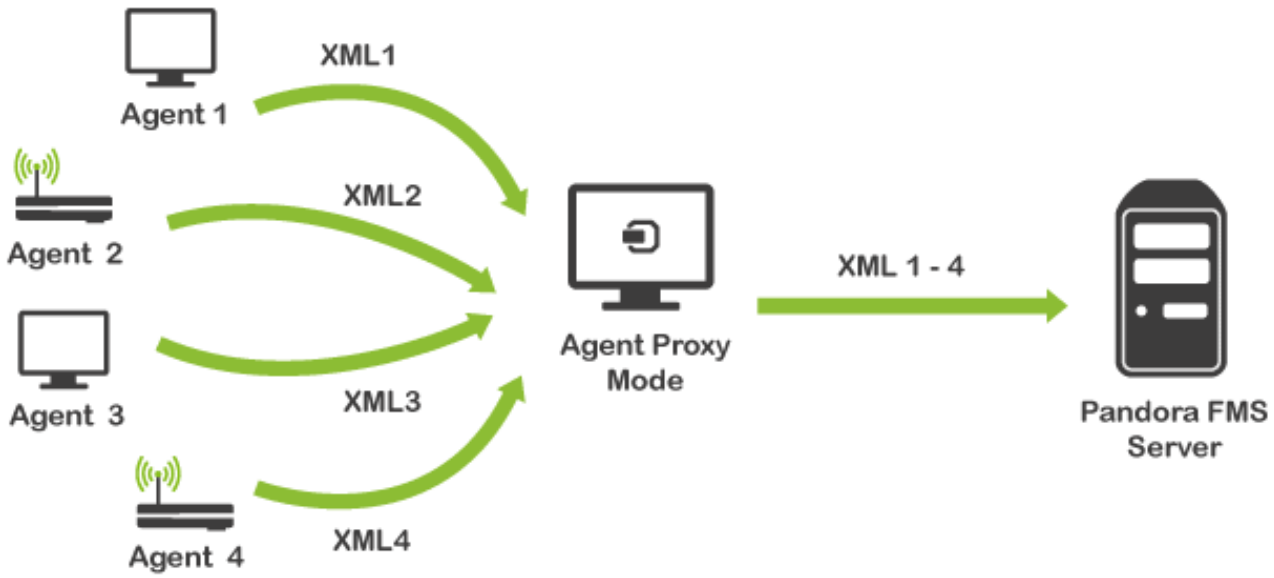
Redes con dificultad de acceso

***Red remota no alcanzable por los chequeos remotos de Pandora**. En este escenario tenemos varias opciones, bien el uso de un agente software que ejecute chequeos remotos hacia otros sistemas (utilizando la modalidad *agente broker*), o bien mediante el uso del *Satellite Server*, que es capaz de ejecutar chequeos remotos y tiene una serie de funcionalidades avanzadas.



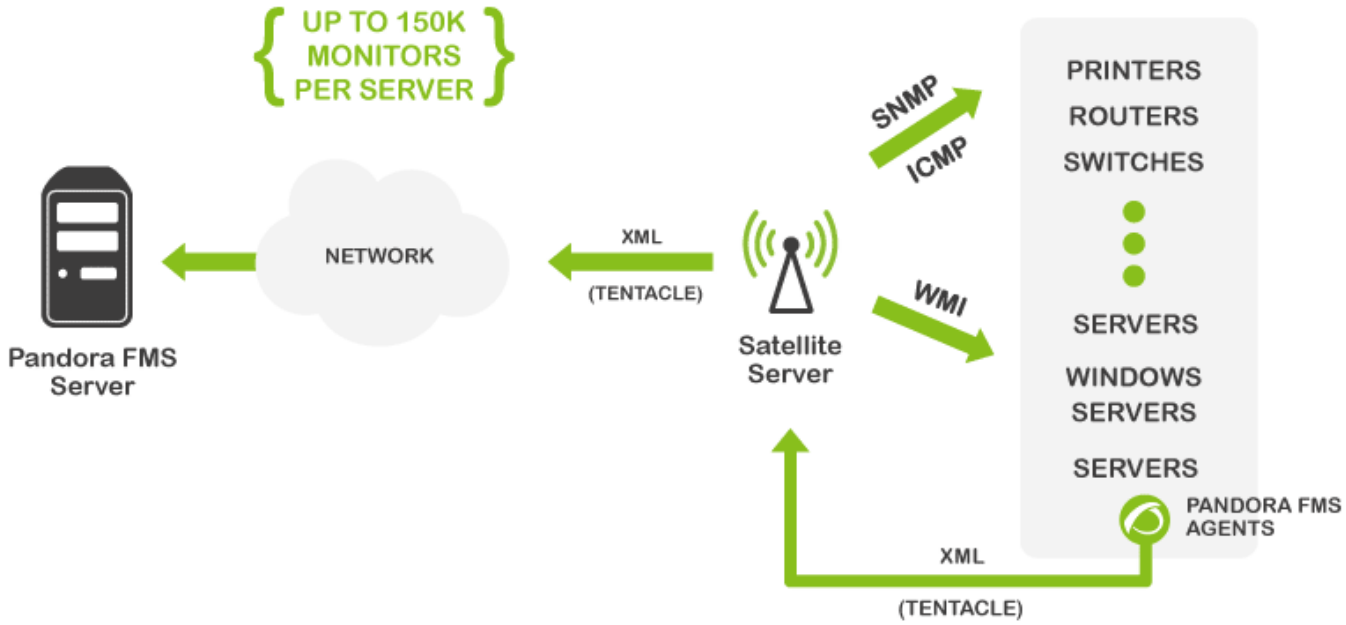
Modelo de despliegue en redes remotas no accesibles en modo broker

*__Agentes software que no tienen acceso al servidor de Pandora__. En este caso, utilizaremos la característica de "proxy" de los agentes software, que permite que un agente que no tiene acceso, utilice un agente que si tiene acceso al servidor, para conectarse a través de él, reenviando los ficheros XML de todos los agentes demás del suyo propio. El *Satellite Server* también puede actuar como proxy de agentes.



Modelo de despliegue en redes remotas usando el modo proxy del agente

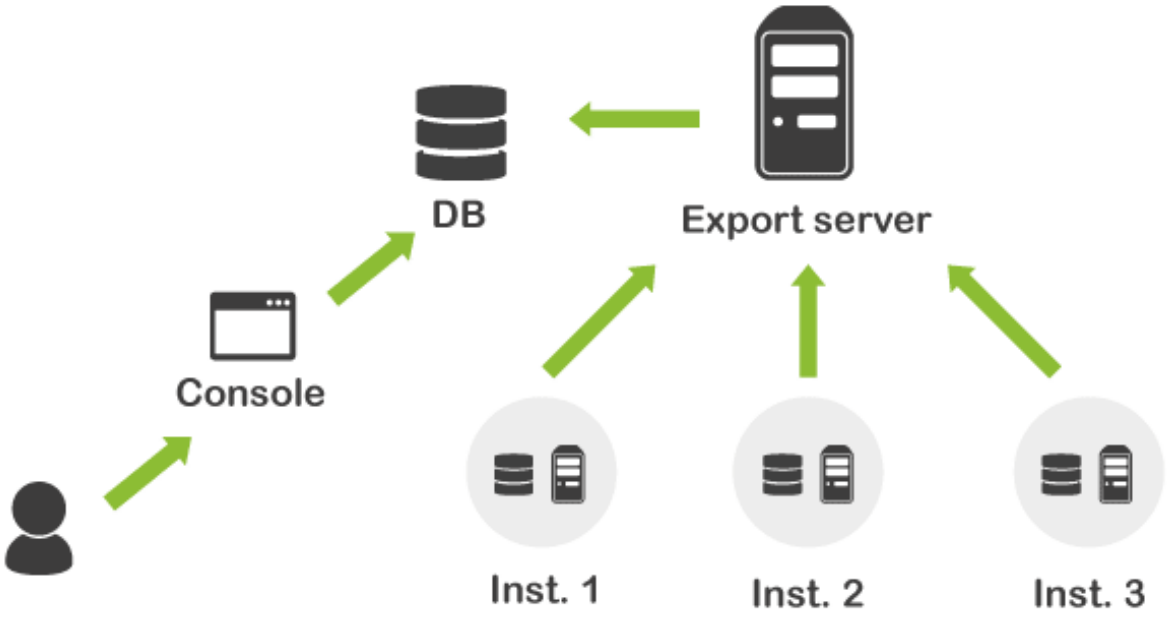
Necesidad de monitorizar *redes diferentes para monitorización remota con el servidor. En este caso podremos también hacer uso del *Satellite Server*, o bien montar varios servidores diferentes de Pandora FMS conectados a la misma base de datos, un servidor ejecutará un conjunto de chequeos, y otro servidor otro conjunto diferente. La forma de realizar el despliegue será distinta pero en ambos casos cada componente se encargará completamente de la monitorización de su red y la gestión será centralizada desde la Consola.



Modelo de despliegue en redes remotas usando el Satellite Server

Características especiales organizativas

Necesidad de tener *varias sedes monitorizadas, con equipos de monitorizacion y configuraciones diferentes. En este caso utilizaremos un servidor de exportación (Export Server), para duplicar parte de la monitorización en un entorno segregado de Pandora FMS, independiente.



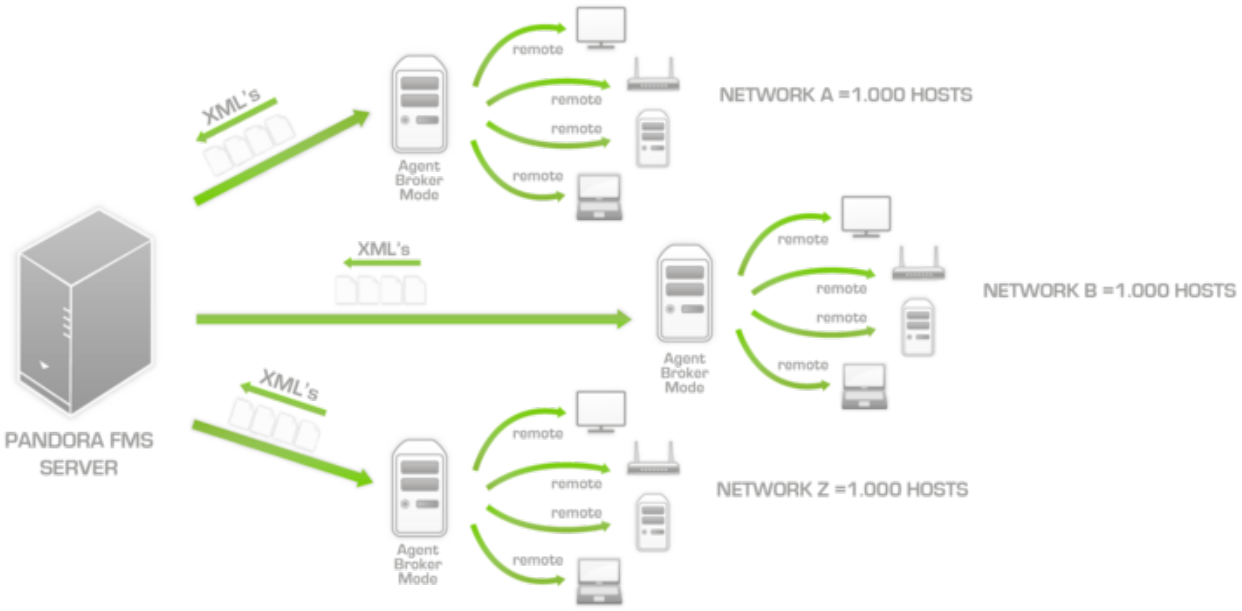
Modelo de exportación jerárquica con Export Server

***Dualidad de reporting**. Adicionalmente, podemos configurar agentes para que reporten a dos servidores de Pandora FMS diferentes, aunque sólo podrán 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

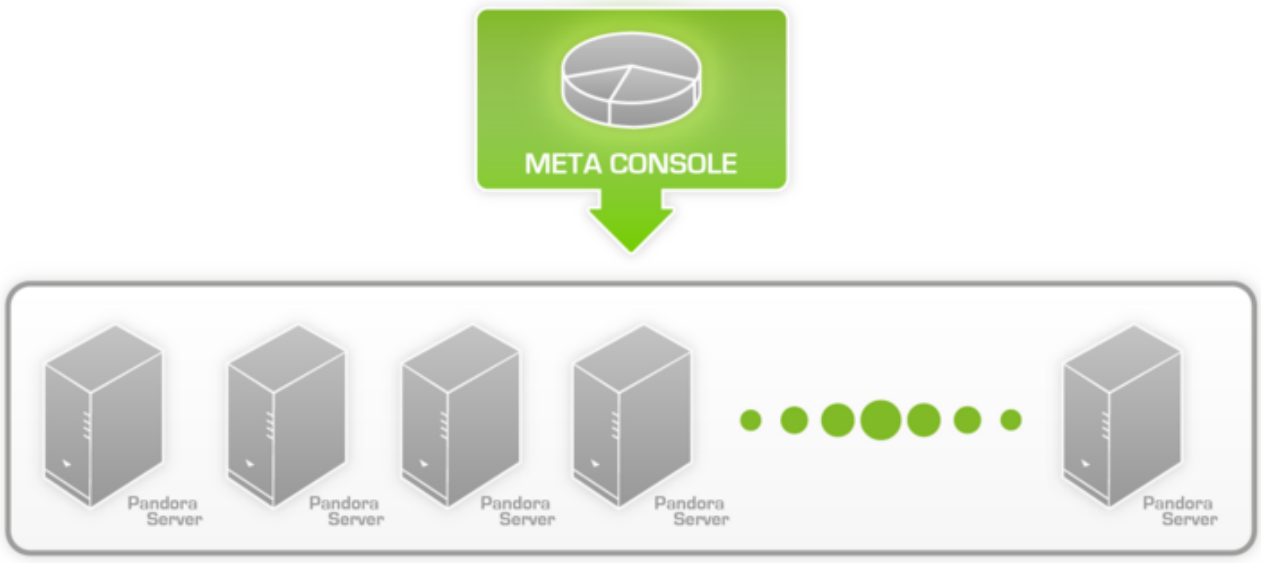
*__Red numerosa__, con miles de chequeos de red que debemos distribuir en diferentes "sondas de monitorizacion remota", ya que por su elevado número (más de 50,000) no podemos centralizarlas todas en un único servidor. Para ello usamos servidores en modo broker, que distribuyen la carga de chequeos remotos.



Modelo de distribución de chequeos remotos con agentes en modo broker

__Necesidad de montar *un servidor en HA__ por seguridad, por si falla el hardware primario. Veremos cómo montar dos servidores, uno "pasivo", esperando a que el activo deje de responder para entrar en funcionamiento. Hay diferentes formas de hacerlo.

__Necesidad de *monitorizar un volumen grande de sistemas y gestionarlas de forma centralizada__ (más de 2500 agentes). Para ello se configuran diferentes servidores de Pandora coordinados por un mismo sistema, llamado metaconsola. De esta forma se puede escalar linealmente



Modelo de metaconsola

Volver al Indice