

PANDORAFMS



Topologías distribuidas: Satellite Server

30-12-2021





Topologías distribuidas: Satellite Server

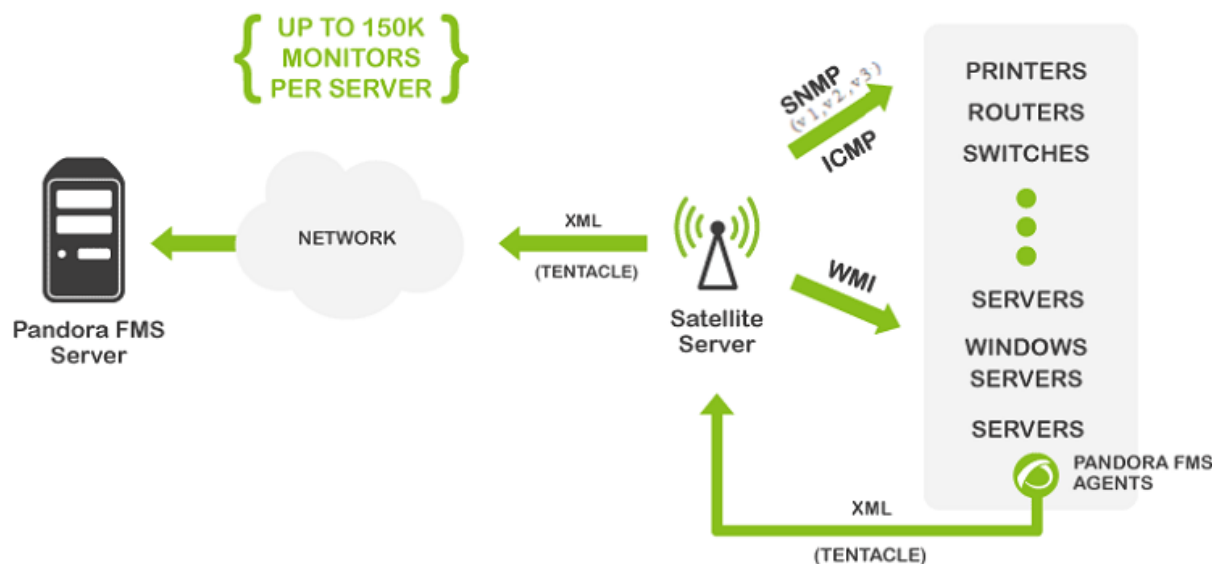
[Volver al Índice de Documentación Pandora FMS](#)

Satellite Server

Introducción

E

El **Satellite Server** se emplea para **descubrir y monitorizar redes y equipos remotos**, bien elementos de red (*routers, switches, etc.*) vía SNMP o ICMP, o bien servidores MS Windows® (vía WMI) o Linux® (vía SNMP). Este no es un servidor “ordinario”, sino que más bien se podría considerar como un Agente Software en **modo broker** pero con funcionalidades extendidas. Es especialmente útil para monitorizar redes remotas inaccesibles desde el servidor de Pandora FMS, y donde tampoco podemos instalar Agentes Software.



El Satellite Server funciona tanto en Windows® como en GNU/Linux® (sistema operativo recomendado) y tiene algunas características que lo hacen especial, más que recomendable en determinados entornos.

- Puede ejecutar pruebas de red (ICMP, Latencia y SNMP v1 y v2) a una tasa extremadamente alta (500 chequeos por segundo). Para SNMP v3 debe **configurar las credenciales de acceso** y debido al cifrado de datos hará un chequeo menos



rápido.

- Solo envía datos al servidor cada X segundos (por defecto 300), pero puede ejecutar las pruebas de latencia, ICMP y SNMP con un intervalo menor (por ejemplo 30 segundos) de forma que, cuando detecta cambios de estado, notifica inmediatamente al servidor. Estos cambios de estado se han de definir previamente si el tipo de Módulo no es un *_proc (por ejemplo interfaces de red o conectividad general de red).
- **Es un servidor autónomo**, no requiere conexión a la base de datos de Pandora FMS. Envía todos los datos como XML de forma que funciona como un servidor independiente, similar a como lo hace un Agente Software en modo *broker* o a un Export Server.
- Tiene un mecanismo de autodiscovery para SNMP y WMI, de forma que crea los Agentes detectados (por dirección IP), detecta los elementos dinámicos (interfaces de red, almacenamiento) y los monitoriza de forma automática.
- En sistemas Windows® detecta discos, CPU y memoria.
- En sistemas de red con SNMP detecta estado de las interfaces, tráfico de entrada y salida por cada interfaz, y el nombre del sistema.
- Los Módulos autogenerados se pueden modificar, como otro módulo más, gestionando el Agente desde la consola, como si fuera un Agente ordinario (en la sección de **Operaciones masivas** → **Satélite**).
- **Puede crear Agentes manualmente** generando un fichero de configuración de Agente en el directorio de configuraciones del Satellite Server (explicado más adelante).



Versión NG 759 o posterior.

- Desde la versión 759 NG, tanto el Satellite server como el Enterprise Network Server soportan IPv6 en todas sus funcionalidades avanzadas. Ahora el código de alto rendimiento que antes solo se soportaba en IPv4 aplica también a IPv6 mejorando las capacidades de *polling* existentes.

Capacidad

La capacidad máxima del **Satellite Server** depende totalmente del hardware del servidor donde se ejecuta, y el tipo de chequeos que se necesitan realizar. En entorno de pruebas se ha logrado realizar 500 chequeos ICMP y SNMP por segundo, pero eso depende mucho de los tiempos de respuesta del dispositivo remoto (no es lo mismo uno que responde en 10 milisegundos que uno que tarda 2 segundos en responder). En condiciones ideales



teóricas se puede hablar de que se pueden monitorizar unos 150 000 monitores con un solo **Satellite Server**. En condiciones reales se ha probado en entornos más o menos controlados (redes locales) unos 50 000 Módulos con un Satellite Server en un ordenador de hardware muy discreto (procesador Intel i5®, 2 GHz, 4 GB RAM).



Si existen muchos Módulos críticos, el rendimiento puede verse muy afectado. También hay que tener en cuenta el **timeout** configurado, ya que solo se realiza una comprobación crítica por **timeout**. Si tiene 1000 Módulos críticos y el **timeout** configurado en 4 segundos, se tardará 4000 segundos en ejecutar todos estos chequeos con un único hilo.

Instalación

El Satellite Server se distribuye en forma de **tarball** (GNU/Linux®) o **.exe** (Windows®), de forma que no hace falta instalar Perl ni ninguna librería adicional. El funcionamiento en las versiones Windows® o Linux® es idéntico. En caso de Windows® se instala como servicio, y en el caso de Linux® se instala como demonio del sistema. El fichero de configuración y las especificaciones de ambos son idénticas.

La versión de Linux® del **Satellite Server** depende de paquetes externos que se especifican en la sección correspondiente de esta documentación.

Instalación de Satellite Server en Linux

El sistema operativo GNU/Linux recomendado es CentOS. Una vez descargado el paquete que contiene el Satellite Server es necesario ir a la carpeta de descarga con privilegios de **root** y descomprimir el binario:

```
tar -xvzf pandorafms_satellite_server_X.XNG.XXX_x86_64.tar.gz
```



```
[root@localhost ~]# ls
pandorafms_satellite_server_7.ONG.726_180831_x86_64.tar.gz  README
[root@localhost ~]# tar -xvzf pandorafms_satellite_server_7.ONG.726_180831_x86_64.tar.gz
satellite_server/satellite_server
satellite_server/satellite_server.conf
satellite_server/satellite_serverd
satellite_server/satellite_server_installer
satellite_server/pandora_satellite_logrotate
satellite_server/README
satellite_server/bin/braa
satellite_server/bin/wmic
satellite_server/bin/tentacle_client
satellite_server/bin/pandorafsnmp
[root@localhost ~]#
```

A continuación se generará una carpeta denominada `satellite_server`. Vaya a dicha carpeta tecleando:

```
cd satellite_server/
```

Antes de proceder con la instalación es necesario dejar claro cuáles son las dependencias fundamentales del Satellite Server: **Perl**, **Braa**, **Wmic**, **Fping** y **Nmap**.

Instale Perl con el siguiente comando:

```
yum install perl
```

En el instalador se adjuntan las dependencias de Braa y Wmic. Es necesario instalar Fping y Nmap de forma independiente:

```
yum install fping nmap
```

Para instalar el Satellite Server en sí, debe ejecutar el comando de instalación:

```
./satellite_server_installer --install
```

```
[root@localhost satellite_server]# ./satellite_server_installer --install
Pandora FMS Satellite Server installer for GENERIC. (c) 2014-2015 Artica ST.

>Installing the Pandora FMS Satellite Server binary to /usr/bin...
>Installing the tentacle_client binary to /usr/bin...
>Installing the braa binary to /usr/bin...
>Installing the pandorafsnmp binary to /usr/bin...
>Installing the wmic binary to /usr/bin...
>Copying configuration file to /etc/pandora...
>Creating agent configuration directory /etc/pandora/conf...
>Copying startup script to /etc/init.d...
>Linking startup script to /etc/rc.d/rc2.d
Creating logrotate.d entry for Pandora FMS log management

Edit the file /etc/pandora/satellite_server.conf and manually configure the Satellite Server.

[root@localhost satellite_server]#
```



Una vez terminado el proceso, será necesario editar el fichero de configuración del satélite localizado en:

```
/etc/pandora/satellite_server.conf
```

El **editor de texto por defecto** en CentOS es **VIM**. Busque el *token* `pandora_license`, proceda a descomentarlo e **introduzca la licencia** del servidor Pandora FMS Enterprise. Tras ello puede guardar el archivo y levantar el servicio, ejecutando lo siguiente:

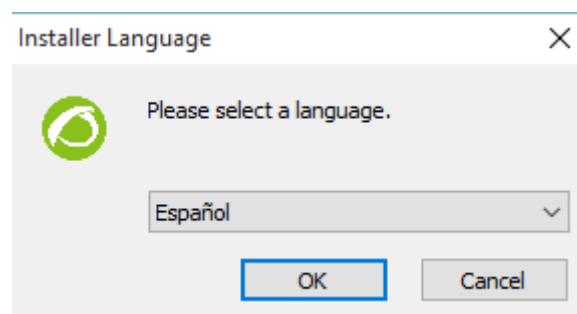
```
sudo /etc/init.d/satellite_serverd start
```

En caso de algún error o mal funcionamiento, puede revisar el fichero de registro en:

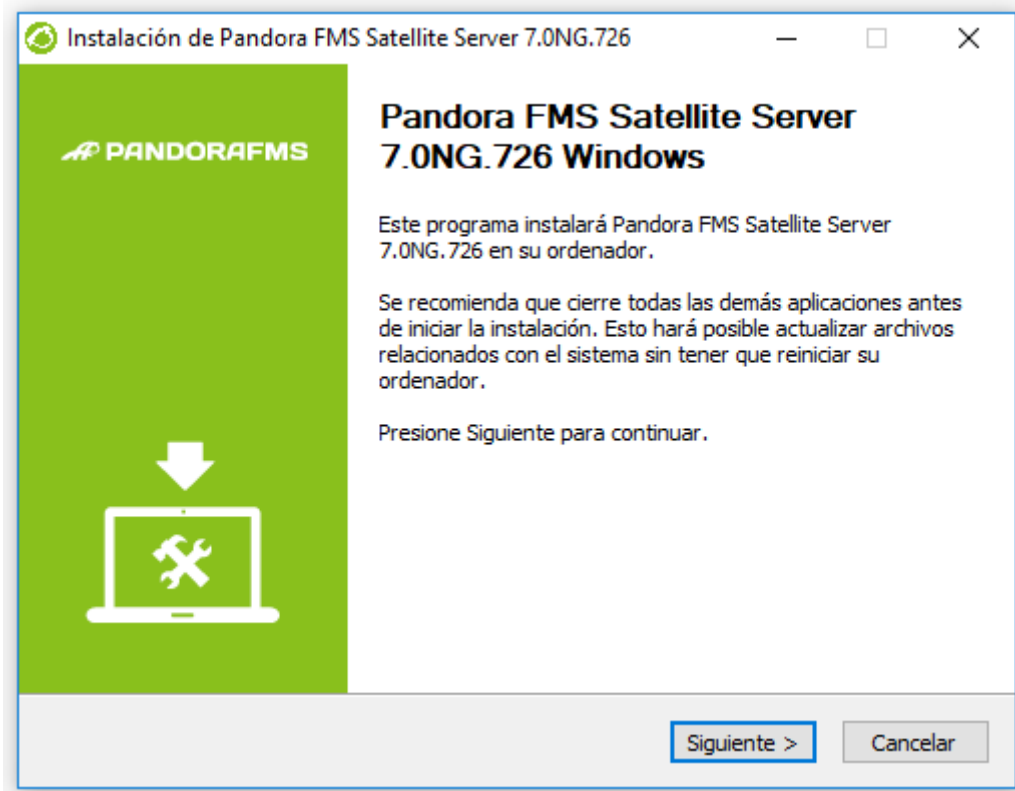
```
/var/log/satellite_server.log
```

Instalación en Windows

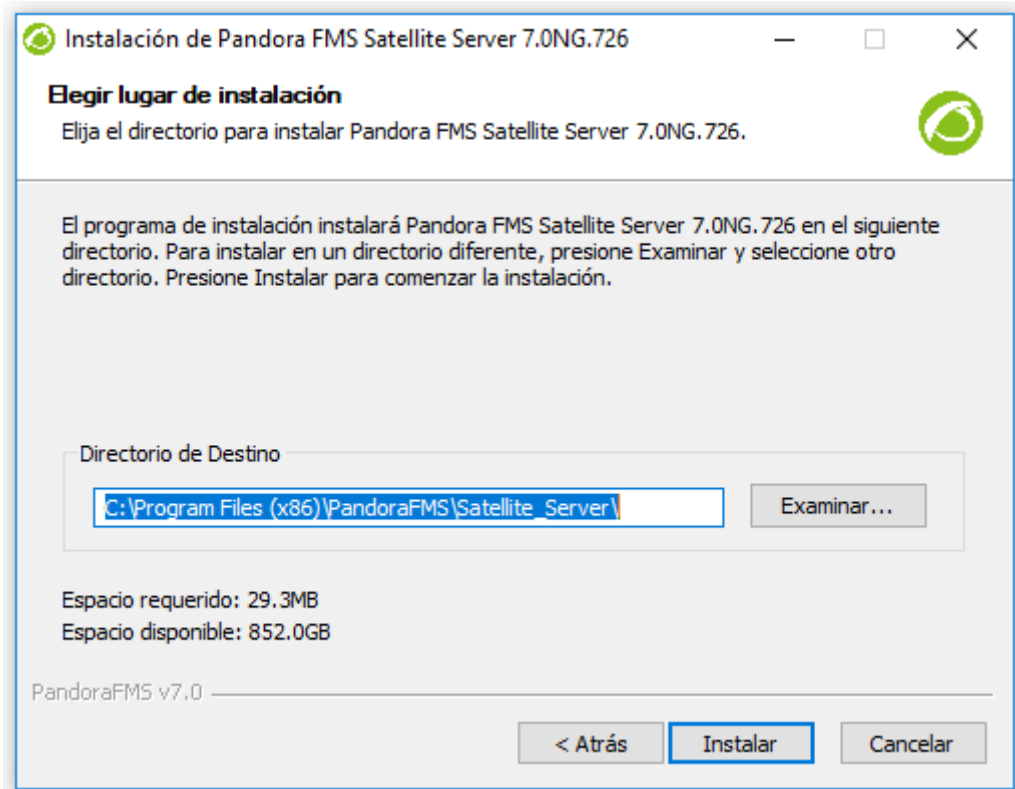
Elija el idioma de instalación:



Haga clic en Siguiente:



Elija el lugar para instalar el programa:





Será necesario instalar también **WinPCap**. La ventana de instalación aparecerá en este paso de la instalación.



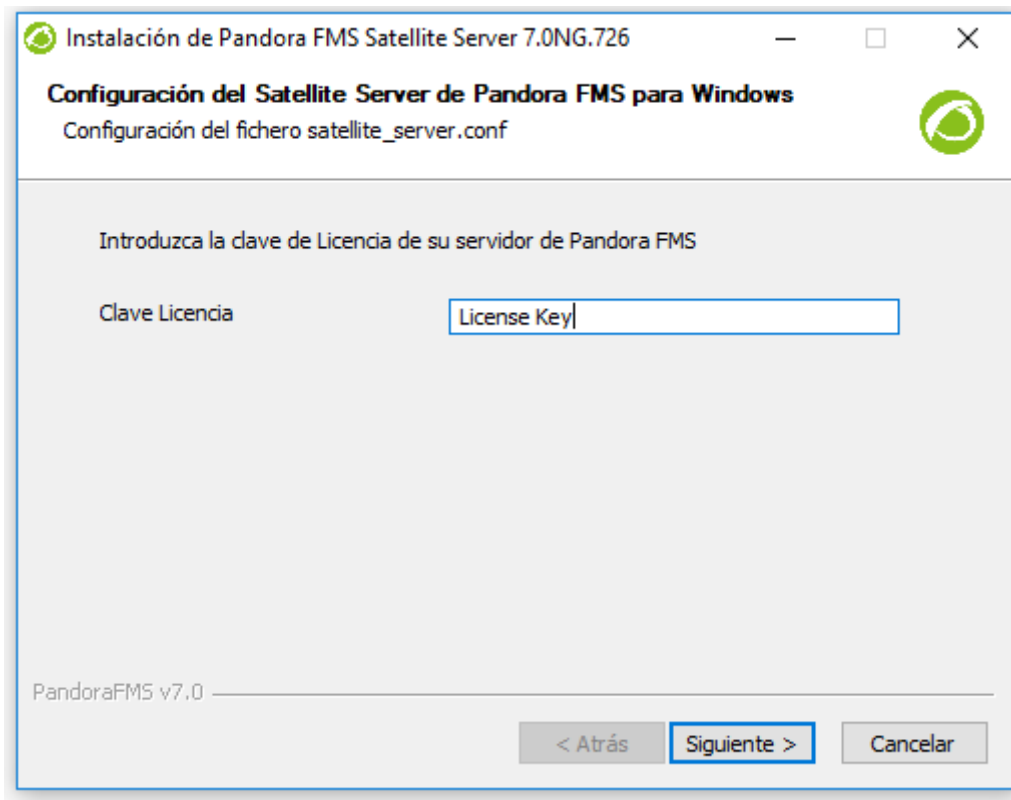
Configure el encendido de WinPCap al iniciar la máquina:



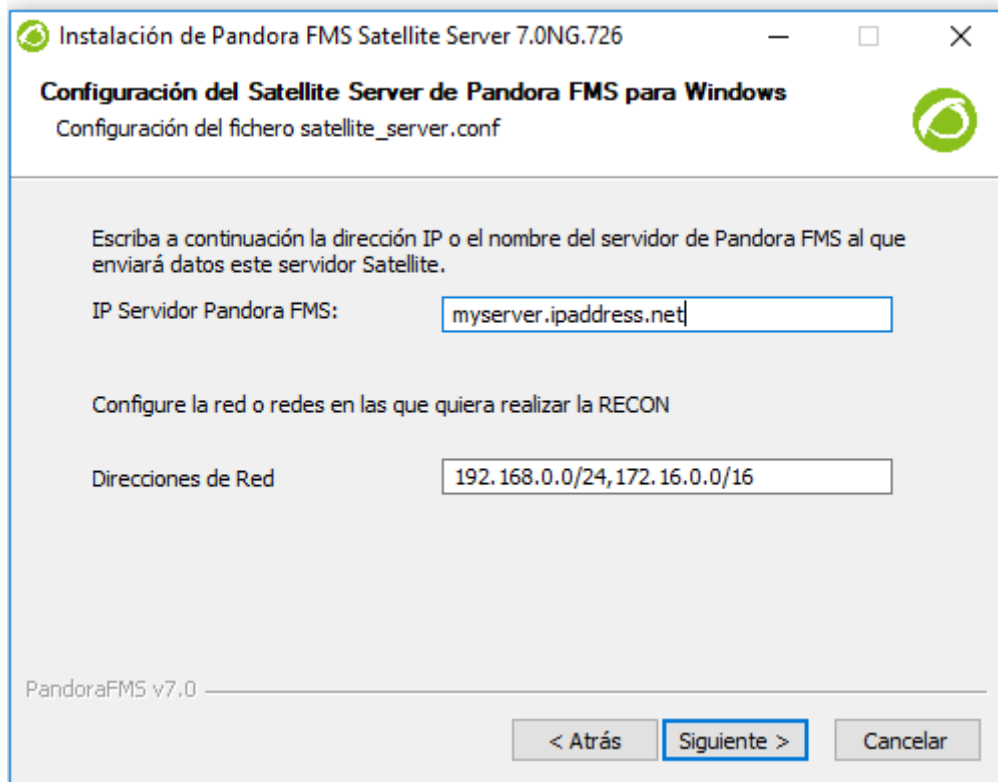
Una vez terminada la instalación de WinCap verá la siguiente pantalla:



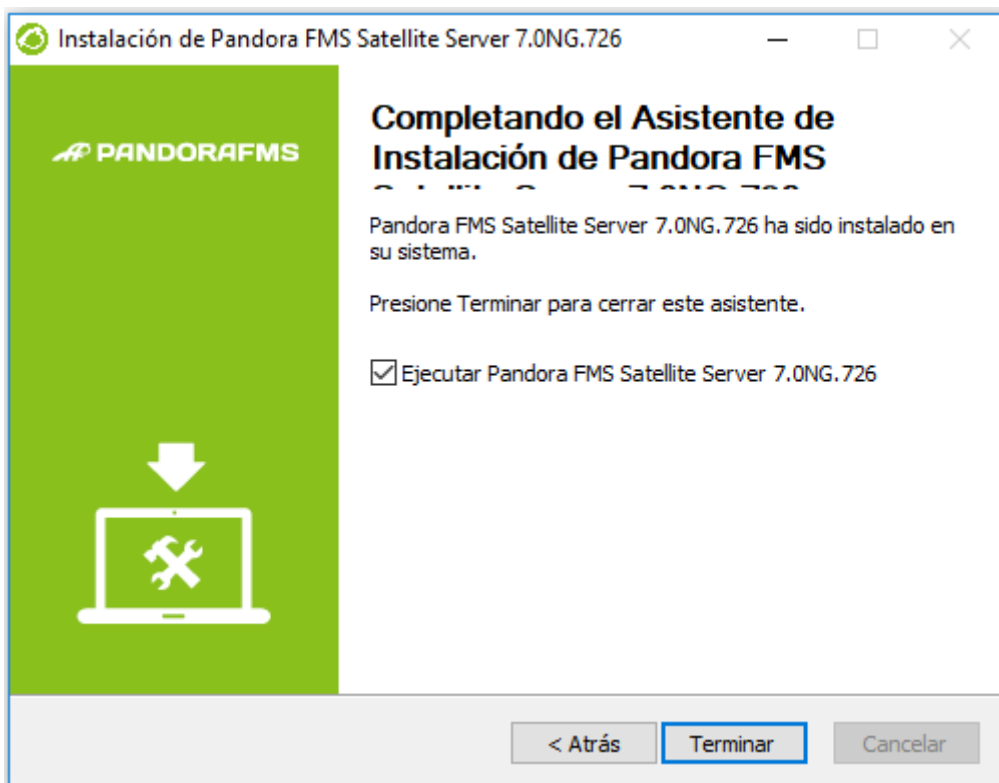
Introduzca la clave de licencia de Pandora FMS Enterprise para continuar con la instalación:



En el siguiente apartado debe configurar la dirección del servidor Pandora FMS para el envío de los datos; puede definir las reglas exploración de red para el Satellite Server.



Será necesario reiniciar la máquina para que se apliquen todos los cambios.



Una vez terminado el proceso, puede arrancar y detener el servicio Satellite Server PFMS



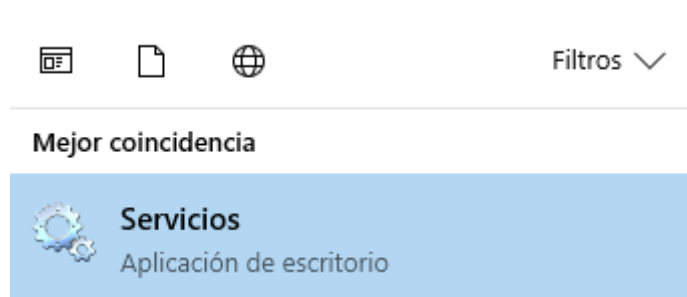
desde el menú Inicio de Windows®.

Funcionamiento de Módulos WMI en algunas versiones de Windows

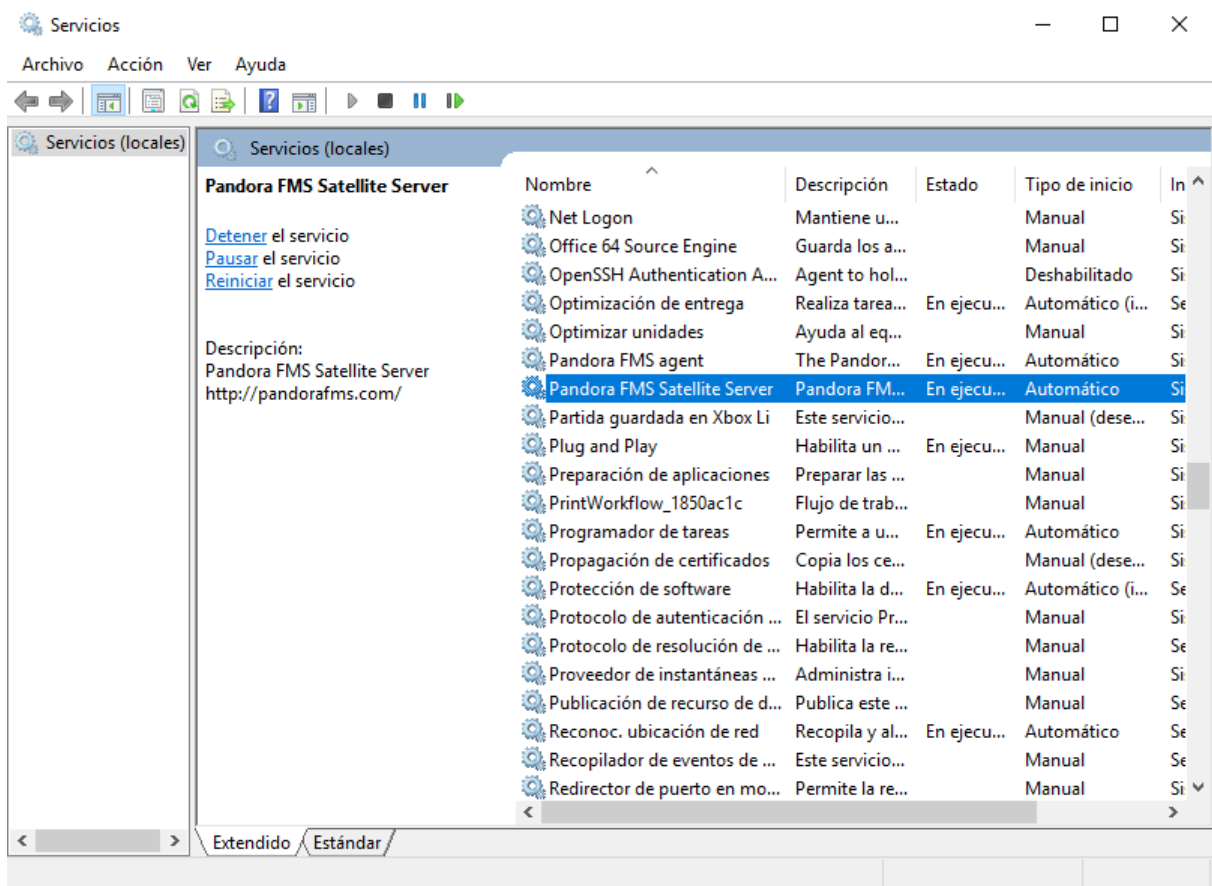
Por motivos de seguridad de Windows®, algunas versiones tienen limitados los usuarios con los que realizar consultas WMI remotas. En el caso de que estas consultas no se lleven a cabo, la solución es ejecutar el servicio del Satellite Server como usuario **Administrador**.

El proceso a seguir es el siguiente:

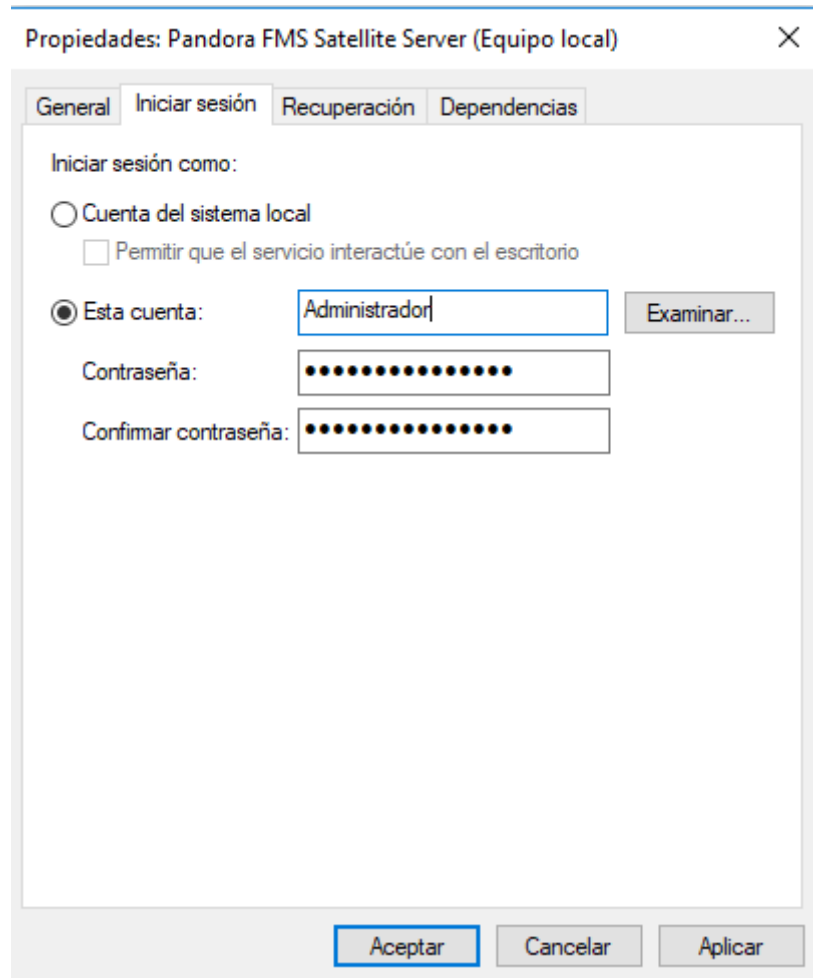
Abra los servicios:



Haga clic sobre el servicio y entre en **Propiedades**:



Sobre la ventana de **Iniciar sesión** seleccione una cuenta con permisos de Administrador y aplique los cambios:



Debe reiniciar el servicio para aplicar los cambios.

Configuración

Todos los parámetros que requieren un *timeout* o tiempo de expiración se deben especificar en segundos (por defecto 300 segundos que es igual a 5 minutos).

Es importante destacar que los intervalos de latency y SNMP son específicos al cambio de estado. En el caso de los chequeos *booleanos* (estado de un puerto, estado de la máquina), el umbral que define el cambio de estado es automático. En el caso de valores numéricos (latencia, tráfico de red en una interfaz, espacio de disco, CPU, etc.), se basa en el umbral. Por defecto no se definen umbrales; esto tiene que hacerse en la definición del Módulo.

agent_interval

```
agent_interval xxx
```



Por defecto, 300 segundos (5 minutos). Será el tiempo tras el que enviará datos al servidor, *independientemente de que los chequeos que haga el Satellite Server sean con un intervalo más corto*. De ser necesario, y por defecto, crea Agentes en el servidor Pandora FMS correspondiente según el tiempo aquí especificado.

agent_threads

```
agent_threads xxx
```

Número de hilos que se utilizan para mandar ficheros XML de datos.

xxxxxx_interval

```
xxxxxx_interval xxx
```

Ejecuta todos los chequeos (latencia, SNMP, etc) cada xxx segundos. Si el dato recopilado cambia respecto al anterior lo envía en ese momento. Si es igual, lo enviará cuando el intervalo de ese Agente así lo ordene. Es útil para realizar pruebas muy intensivas y notificar **solo en el caso de cambio de estado**.

xxxxx_retries

```
xxxxx_retries xxx
```

Número de reintentos xxx en los chequeos (latencia, SNMP, ping, etcétera).

xxxxx_timeout

```
xxxxx_timeout xxx
```

Timeout en segundos para las pruebas de tipo SNMP, latencia y ping.

xxxxx_block

```
xxxxx_block xxx
```

Fuerza al servidor a ejecutar las consultas (latencia, ping y SNMP) en bloques de XXX consultas. Cuanto mayor sea el número (máximo 500) más capacidad de proceso tendrá,



pero a costa de incrementar la latencia. En algunos casos puede ser conveniente disminuir ese número.

xxxxx_threads

```
xxxxx_threads n
```

Número de hilos *n* asignados a cada tipo de chequeo para que trabajen de manera concurrente. Dependerá de la potencia (CPU y RAM) de la máquina. Cuantos más hilos, más se cargará el sistema, pero más capacidad de proceso tendrá. Al superar los 20 hilos, dependiendo del sistema, puede empeorar el rendimiento.

log_file

```
log_file <path_file>
```

Indica el fichero en el que se escribe el *log* del Satellite Server, por defecto en `/var/log/satellite_server.log`.

recon_task

```
recon_task xxxxx[,yyyy]
```

Direcciones/Redes IP empleadas para el Autodiscovery, separadas por comas. Ejemplo:

```
192.168.50.0/24,10.0.1.0/22,192.168.70.64/26
```

server_ip

```
server_ip <IP>
```

Dirección IP o nombre DNS del servidor de Pandora FMS al cual enviar la información. Los datos se envían por **Tentacle**, de forma que la comunicación hacia el servidor debe estar permitida y garantizada por el puerto 41121/tcp.

recon_mode

```
recon_mode <mode_discovery>
```



Modo de autodescubrimiento (`<mode_discovery>`) a utilizar. El sistema empleará los siguientes protocolos para descubrir los sistemas:

- `recon_mode icmp` Realiza verificación para determinar si el *host* está en línea (**ping**) y mide el tiempo de latencia.
- `recon_mode snmp` Si es capaz de comunicar por SNMP (v1 y v2 únicamente) buscará todas las interfaces de red y sacará el tráfico de todas ellas, así como su estado operativo, además del nombre del dispositivo y ubicación. Probará con las **diferentes comunidades suministradas en el fichero de configuración** para conectar. *Para utilizar SNMP v3 cuyo reconocimiento es innecesario, consulte en [este enlace](#) cómo configurar las credenciales de acceso conocidas.*
- `recon_mode wmi` Similar al caso anterior, en este caso mostrando Carga de CPU, Memoria y Discos (todos los disponibles).

recon_community

```
recon_community <aaa>,<bbb>,<ccc>...
```

Especifica una lista de comunidades SNMP `<xxx>` para usar en el discovery de SNMP, separadas por comas. Utilizará esta lista en la exploración SNMP: por cada dirección IP encontrada, intentará ver si responde a alguna de estas comunidades.

wmi_auth

```
wmi_auth Administrator%password[,user%pass]
```

Especifica una lista de parejas de credenciales de usuario, cada una de ellas en el formato **<nombre de usuario>%<contraseña>** y separadas por comas.

Por ejemplo: `admin%1234,super%qwerty`. Utilizará esta lista en la exploración WMI. Por cada dirección IP encontrada, intentará ver si responde a alguna de estas combinaciones.

wmi_ntlmv2

```
wmi_ntlmv2 [0|1]
```

Habilita (1) o deshabilita (0) la autenticación con el **W** **protocolo NTLMv2** para WMI.



agent_conf_dir

```
agent_conf_dir <path>
```

Vía (<path>) al directorio que crea y almacena automáticamente los ficheros de configuración de cada Agente creado por el Satellite Server. Por defecto /etc/pandora/conf. Dichos Agentes también pueden ser **creados manualmente**.

group

```
group <group_name>
```

Define el nombre del grupo <group_name> por defecto de los Agentes creados por el Satellite Server. Por ejemplo, "Servers".

daemon

```
daemon [1|0]
```

Si su valor es 1 ejecuta el *demonio* (servicio) en segundo plano (valor por defecto).

hostfile

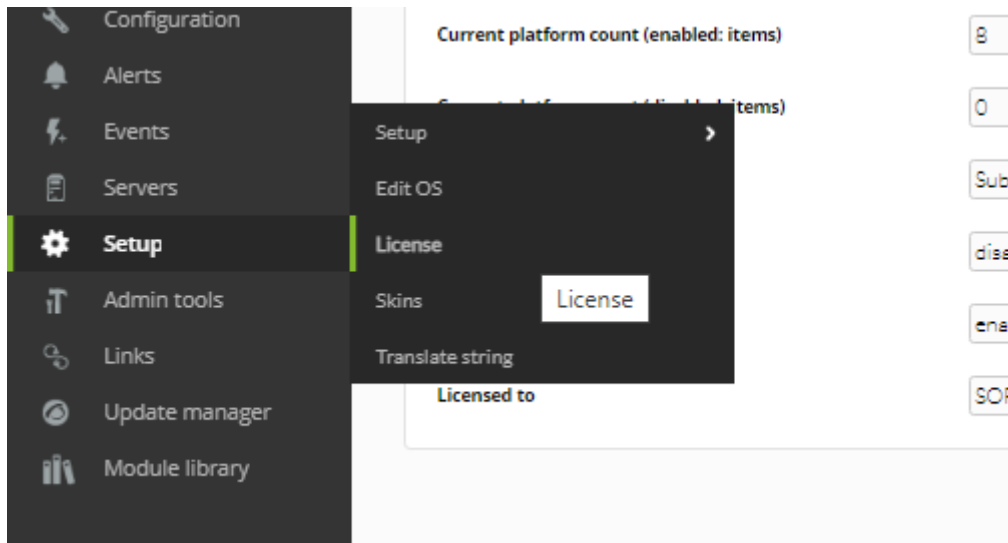
```
hostfile <file>
```

Es un método alternativo o complementario al de explorar una red para encontrar *hosts*. En este fichero <file>, en cada línea hay una dirección. Alternativamente, se le puede pasar en la misma línea el hostname seguido de la IP, de esa forma el Agente será creado con ese nombre y además use esa dirección IP para los Módulos (por ejemplo: 192.168.0.2 <hostname>). Es necesario que al realizar una consulta con Fping a esas direcciones su resultado sea en línea para que dichas direcciones sean válidas.

pandora_license

```
pandora_license xxxxxxxx
```

Escribe y almacena la licencia del servidor Pandora FMS Enterprise, tal como se muestra en la sección **Setup** → **License** de la Consola Pandora FMS.



Puede usar la misma licencia en tantos Satellite Servers como se necesite, ya que el total de Agentes que usan la licencia se verifica en el servidor de Pandora FMS, no en el Satellite Server.

remote_config

```
remote_config [1|0]
```

Activa por defecto la **configuración remota** en los Agentes detectados, necesario si quiere gestionarlos desde la Consola después de detectarlos. También activa la configuración remota del propio Satellite Server.

temporal_min_size

```
temporal_min_size xxx
```

Si el espacio libre (en megabytes) de la partición en la que se encuentra el directorio temporal es menor que este valor, no se siguen generando paquetes de datos. De este modo se evita que se llene el disco si por alguna razón se pierde la conexión con el servidor durante un intervalo de tiempo prolongado.

xml_buffer

```
xml_buffer [0|1]
```

Valor por defecto 0. Estando configurado con valor a 1 el Agente guardará los XML de datos que no haya podido enviar para intentarlo de nuevo más adelante.



En Unix, si está en un entorno seguro considere cambiar el directorio temporal, ya que /tmp tiene permisos de escritura para todos los usuarios.

snmp_version

```
snmp_version xx
```

Versión de SNMP que se utilizará por defecto (1). Para utilizar SNMP v3 consulte en [este enlace](#) cómo configurar las credenciales de acceso conocidas.



Algunos Módulos podrían dejar de funcionar si se cambia este valor.

braa

```
braa <path>
```

Vía <path> al binario de Braa. Valor por defecto /usr/bin/braa.

fping

```
fping <path>
```

Vía <path> al binario de Fping. Valor por defecto /usr/sbin/fping.

fsnmp

```
fsnmp <path>
```

Vía <path> al binario de Fsnmp. Valor por defecto /usr/bin/pandorafsnmp.



latency_packets

```
latency_packets xxx
```

Número de paquetes xxx ICMP que se envían por petición de latencia.

nmap

```
nmap <path>
```

Vía <path> al binario de Nmap. Valor por defecto /usr/bin/nmap.

nmap_timing_template

```
nmap_timing_template x
```

Un valor xxx que especifica nivel de agresividad de Nmap, de 1 a 5. Uno significa más lento pero más fiable, cinco significa más rápido pero menos fiable. Valor por defecto: 2.

ping_packets

```
ping_packets xxx
```

Número de paquetes ICMP que se envían por cada ping.

recon_enabled

```
recon_enabled [0|1]
```

Habilita (1) o deshabilita (0) el autodescubrimiento de equipos.

recon_timing_template

```
recon_timing_template xxx
```

Tal como [nmap_timing_template](#) pero aplicado a los escaneos de red.



server_port

```
server_port xxxxx
```

Puerto del servidor Tentacle.

server_name

```
server_name xxxxx
```

Nombre del servidor Satellite (por defecto toma el *hostname* de la máquina).

server_path

```
server_path <path>
```

Ruta <path> donde los ficheros XML son copiados si el *transfer_mode* está en local (por defecto */var/spool/pandora/data_in*).

server_opts

Parámetros del servidor que son pasados a Tentacle.

transfer_mode

```
transfer_mode [tentacle|local]
```

Modo de transferencia de ficheros. Puede ser únicamente Tentacle o local (por defecto Tentacle).

Servidor Secundario

```
secondary_mode [on_error|always]
```

Un tipo especial de parámetro de configuración general es la definición de un servidor secundario. Esto permite definir un servidor al que se le envían los datos, de forma complementaria al servidor definido de forma estándar. El modo de servidor secundario funciona de dos formas:



- **on_error**: Envía datos al servidor secundario solo si no puede enviarlas al primario.
- **always**: Siempre envía datos al servidor secundario, independientemente de si puede contactar o no con el servidor principal.

Ejemplo de configuración:

```
secondary_server_ip    192.168.1.123
secondary_server_path  /var/spool/pandora/data_in
secondary_mode         on_error
secondary_transfer_mode tentacle
secondary_server_port  41121
```

snmp_verify

```
snmp_verify [0|1]
```

Habilita (1) o deshabilita (0) la comprobación de módulos SNMP v1 que hacen fallar Braa en tiempo real. Estos Módulos serán descartados y dejarán de ejecutarse. Véase también tanto [snmp2_verify](#) como [snmp3_verify](#).

snmp2_verify

```
snmp2_verify [0|1]
```

Habilita (1) o deshabilita (0) la comprobación de módulos SNMP v2 que hacen fallar Braa en tiempo real. Estos módulos serán descartados y dejarán de ejecutarse. Véase también tanto [snmp_verify](#) como [snmp3_verify](#).



¡Comprobar módulos SNMP versión 2 puede ser muy lento!

snmp3_verify

```
snmp3_verify [0|1]
```

Habilita (1) o deshabilita (0) la comprobación de módulos SNMPv3 que hacen fallar Braa en tiempo real. Estos módulos serán descartados y dejarán de ejecutarse. Véase también tanto [snmp_verify](#) como [snmp2_verify](#).



startup_delay

```
startup_delay xxx
```

Espera xxx segundos antes de enviar ficheros de datos por primera vez.

temporal

```
temporal <directory>
```

Directorio temporal donde se crean los ficheros XML, por defecto /tmp.

tentacle_client

```
tentacle_client <path>
```

Vía <path> del cliente de Tentacle. Valor por defecto /usr/bin/tentacle_client.

wmi_client

```
wmi_client <path>
```

Vía <path> al binario de wmi_client. Valor por defecto /usr/bin/wmic.

snmp_blacklist

```
snmp_blacklist <path>
```

Vía <path> a la lista de exclusión de Módulos SNMP. Valor por defecto /etc/pandora/satellite_server.blacklist.

add_host

```
add_host <dir_IP> [agent_name]
```

Añade el *host* dado a la lista de agentes monitorizados. Se puede especificar el nombre del Agente después de la dirección IP. Se pueden añadir múltiples *hosts*, uno en cada línea por separado. Por ejemplo:



```
add host 192.168.0.1
add host 192.168.0.2 localhost.localdomain
```

ignore_host

```
ignore_host <agent_name>
```

Elimina el *host* dado de la lista de Agentes monitorizados, incluso si es encontrado en un escaneo de red por una tarea de reconocimiento (Recon Task). El *host* debe identificarse por el nombre del Agente. Se pueden ignorar múltiples *hosts*, uno por cada línea. Por ejemplo:

```
ignore_host 192.168.0.1
ignore_host localhost.localdomain
```

keepalive

```
keepalive xxx
```

El Satellite Server informa de su estado y comprueba cambios en la configuración remota (de los Agentes y de sí mismo) cada xxx segundos. Valor por defecto: 30 segundos.

credential_pass

```
credential_pass xxx
```

Contraseña utilizada para *cifrar las contraseñas de las cajas de credenciales*. Debe ser la misma que se defina en la Consola de Pandora FMS. Por defecto se utiliza el nombre de *host*.

timeout_bin

```
timeout_bin <path>
```

Si está definido, el programa **timeout** (normalmente `/usr/bin/timeout`) se utilizará al llamar al cliente de Tentacle.



timeout_seconds

```
timeout_seconds xxx
```

Tiempo de expiración, en segundos, para el programa **timeout**. El parámetro **timeout_bin** debe estar configurado.

proxy_traps_to

```
proxy_traps_to <dir_IP[:port]>
```

Redirige los traps SNMP recibidos por el Satellite Server a la dirección (y puerto, opcionalmente) especificados. Por defecto se utiliza el puerto 162.

proxy_tentacle_from

```
proxy_tentacle_from <dir_IP[:port]>
```

Redirige los datos recibidos por Tentacle Server desde la dirección (y puerto, de manera opcional) especificados. Por defecto se utiliza el puerto 41121.

proxy_tentacle_to

```
proxy_tentacle_to <dir_IP[:port]>
```

Redirige las peticiones de clientes de Tentacle recibidas por el Satellite Server a la dirección (y puerto, de manera opcional) especificados. Por defecto se utiliza el puerto 41121.



Esta opción puede entrar en conflicto con la configuración remota de agentes. Esto ocurre si se pretende usar el Satellite Server como *proxy* de algunos Agentes Software y monitorizarlos a su vez desde el mismo Satellite Server de forma remota (ICMP, SNMP, etc.) estando la configuración remota habilitada en ambos casos. En esta situación se deberá, o bien usar Agentes distintos para los chequeos hechos (es decir, con `agent_name` diferente), o bien dejar la configuración remota



habilitada solamente en uno de los dos (Satellite Server o Agentes Software).

dynamic_inc

```
dynamic_inc [0|1]
```

Con valor de 1 mueve los módulos dinámicos descubiertos de forma automática (SNMP, WMI...) a ficheros separados para que no interfieran con la configuración remota de Agentes.

vlan_cache_enabled

```
vlan_cache_enabled [0|1]
```

Habilita (1) o deshabilita (0) la *cache* VLAN de los *hosts* autodescubiertos.

verbosity

```
verbosity <0-10>
```

Nivel de detalle en el registro del *log*, donde 10 es el nivel de información más detallado.

agents_blacklist_icmp



Versión NG 713 o superior.

```
agents_blacklist_icmp 10.0.0.0/24[,8.8.8.8/30]
```

Lista de exclusión de chequeos ICMP. Este campo se puede configurar con una lista de direcciones IP usando la notación CIDR para evitar que se ejecuten módulos de tipo ICMP. Es posible especificar varias subredes separándolas por comas.



agents_blacklist_snmp



Versión NG 713 o superior.

```
agents_blacklist_snmp 10.0.0.0/24[,8.8.8.8/30] (Version> 7.00UM713)
```

Lista de exclusión de chequeos SNMP. Este campo se puede configurar con una lista de direcciones IP usando la notación CIDR para evitar que se ejecuten módulos de tipo SNMP. Es posible especificar varias subredes separándolas por comas.

agents_blacklist_wmi



Versión NG 713 o superior.

```
agents_blacklist_wmi 10.0.0.0/24[,8.8.8.8/30]
```

Lista de exclusión de chequeos WMI. Este campo se puede configurar con una lista de direcciones IP usando la notación CIDR para evitar que se ejecuten módulos de tipo WMI. Es posible especificar varias subredes separándolas por comas.

general_gis_exec



Versión NG 734 o superior.

```
general_gis_exec xxx
```

Activando esta opción, se usará un *script* para proveer posicionamiento GIS a todos los Agentes detectados por el Satellite Server. El *script* debe tener permisos de ejecución e imprimir por pantalla las coordenadas con el formato **<longitud>,<latitud>,[<altitud>]** El tercer parámetro, la altitud, es opcional.

Creación de Agentes en Satellite Server

Existen tres modos de crear los Agentes en el Satellite Server: **Recon Task**, fichero de



satellite_hosts.txt o de manera **manual** creando los .conf de los Agentes a monitorizar.

Creación de Agentes mediante Recon Task

La creación de Agentes mediante una tarea de reconocimiento (Recon Task) es la más utilizada por los usuarios de Pandora FMS. Para llevarla a cabo, debemos acceder al fichero de configuración del Satellite Server y configurar los siguientes parámetros:

- **recon_community**: Se debe especificar una lista de comunidades SNMP para usar en el discovery de SNMP separadas por comas (en el caso de realizar una Recon Task de tipo SNMP).
- **recon_enabled**: Se debe poner a 1 para habilitar el Recon Task del Satellite Server.
- **recon_interval**: Intervalo de tiempo donde se escanea la red, en segundos (por defecto 604800 segundos, 7 días).
- **recon_mode**: Modo de realizar la Recon Task (SNMP,ICMP,WMI), separados por comas.
- **recon_task**: Lista de redes a las cuales hacer el reconocimiento, separadas por comas.
- **recon_timing_template**: Un valor que especifica cómo de agresivo debe ser **nmap**, de 1 a 5. Uno significa más lento pero más fiable; cinco significa más rápido pero menos fiable (por defecto 3).

Un ejemplo de realización de Recon Task es:

```
recon_community public
recon_enabled 1
recon_interval 604800
recon_mode icmp,snmp,wmi
recon_task 192.168.0.0/24,192.168.1.0/24
recon_timing_template 3
```

Una vez configurados los datos, ejecute el Satellite Server mediante el comando:

```
/etc/init.d/satellite_serverd start
```



Los Agentes cuyos ficheros de configuración no contengan ningún Módulo serán ignorados por el Satellite Server.



Creación de agentes mediante fichero

En primer lugar, para poder crear un Agente mediante el fichero `satellite_hosts.txt`, debe ir al archivo de configuración del Satellite Server y quitar de comentario la línea:

```
host_file /etc/pandora/satellite_hosts.txt
```

En segundo lugar debe crear el fichero en la ruta señalada anteriormente con las direcciones IP de los *hosts* que queremos crear colocando la dirección IP y nombre del Agente a crear:

```
192.168.10.5 Server5  
192.168.10.6 Server6  
192.168.10.7 Server7
```



Para que los Agentes con estas direcciones IP puedan ser creados, es necesario que respondan a la llamada **fping**, pues en caso contrario no se crearán.

Una vez configurados los datos, iniciamos el Satellite Server mediante el comando:

```
/etc/init.d/satellite_serverd start
```

La lectura del fichero indicado se realiza cada `recon_interval` segundos.

Creación de agentes de manera manual

En el directorio `/etc/pandora/conf` (por defecto) van alojados los ficheros de configuración de los nuevos Agentes. Abra una ventana terminal y vaya a esa carpeta:

```
cd /etc/pandora/conf
```

Proceda a crear un fichero con una extensión `.conf`, por ejemplo "archivo.conf". Rellene manualmente los siguientes campos:

- **agent_name**: Nombre que se asignará al Agente.
- **agent_alias**: Alias que se asignará al Agente.
- **address**: Dirección IP del elemento a monitorizar.
- **group**: Grupo al cual asignar el Agente.
- **gis_exec**: *Script* de posicionamiento (opcional). Si se utiliza, sobrescribe la



localización provista por el parámetro `general_gis_exec` del Satellite Server.

- Agregue los Módulos a crear en el Agente.

Un ejemplo sería:

```
agent_name Example
agent_alias This is an example
address 127.0.0.1
group Servers

module_begin
module_name Ping
module_ping
module_end

module_begin
module_name Latency
module_latency
module_end
```

Una vez configurados los datos, inicie el Satellite Server mediante el comando:

```
/etc/init.d/satellite_serverd start
```

Eliminación de agentes en Satellite Server

Puede realizar una eliminación total de Agentes o una eliminación parcial de Agentes.



Haga primero un respaldo de todas las carpetas y sus archivos antes de proceder.

Para la **eliminación total** de Agentes debemos tener en cuenta el método utilizado en la creación de Agentes:

- **Manual:** Habrá que eliminar, en primer lugar, los ficheros `.conf` de los Agentes creados en la carpeta `/etc/pandora/conf` y posteriormente eliminar los Agentes en la consola.
- **Fichero `satellite_hosts.txt`:** Habrá que eliminar el fichero, así como los `.conf` que se hayan creado en la carpeta `/etc/pandora/conf`, y posteriormente eliminar los Agentes en la Consola.
- **Recon_task:** Habrá que desconfigurar la `recon_task` en el fichero `.conf` del



Satellite Server, eliminar los `.conf` que se hayan creado en la carpeta `/etc/pandora/conf` y posteriormente eliminar los Agentes en la Consola.

Para la **eliminación parcial** también debemos de tener en cuenta el método utilizado en la creación de Agentes.

- **Manual:** Habrá que eliminar, en primer lugar, los ficheros `.conf` de los Agentes a borrar en la carpeta `/etc/pandora/conf` y posteriormente eliminar los Agentes en la consola.
- **Fichero `satellite_hosts.txt`:** Habrá que eliminar del fichero las líneas de las direcciones IP a eliminar, así como los `.conf` que se hayan creado en la carpeta `/etc/pandora/conf` con esas direcciones IP, y posteriormente eliminar los Agentes en la consola.
- **Recon_task:** Habrá que configurar la lista de excluidos de la `recon_task` en el fichero `.conf` del Satellite Server, después borrar los `.conf` que se hayan creado en la carpeta `/etc/pandora/conf` con esas direcciones IP y eliminar los Agentes en la consola.

Configuraciones personalizadas por Agente

Adicionalmente a los Módulos “automáticos”, se podrá agregar a la monitorización cualquier chequeo TCP, SNMP, WMI o SSH que esté disponible, usando una sintaxis similar a que se usa para los Módulos locales en los **Agentes Software**. Se exponen algunos ejemplos de Módulos válidos para el Satellite Server, tal como se autogeneran después de detectar el sistema.



¡Asegúrese de que los OID **empiezan con un punto** o los módulos SNMP no funcionarán!

Estado de la interfaz vía SNMP. El Satellite Server detecta automáticamente cada interfaz:

```
module_begin
module_name if eth1 OperStatus
module_description IP address N/A. Description: The current
operational state of the interface. The testing(3) state indicates
that no operational packets can be passed.
module_type generic_data_string
module_snmp 192.168.70.225
module_oid .1.3.6.1.2.1.2.2.1.8.3
module_community artica06
module_end
```



Para obligar al módulo a utilizar SNMP versión 2c añade la línea:

```
module_version 2c
```

Para obligar al módulo a utilizar SNMP versión 1 añade la línea:

```
module_version 1
```

Por ejemplo:

```
module_begin
module_name if eth1 OperStatus
module_description IP address N/A. Description: The current
operational state of the interface. The testing(3) state indicates
that no operational packets can be passed.
module_type generic_data_string
module_snmp 192.168.70.225
module_version 2c
module_oid .1.3.6.1.2.1.2.2.1.8.3
module_community artica06
module_end
```

Conectividad a una máquina (vía PING):

```
module_begin
module_name ping
module_type generic_data
module_ping 192.168.70.225
module_end
```

Comprobación de un puerto (vía TCP):

```
module_begin
module_name Port 80
module_type generic_proc
module_tcp
module_port 80
module_end
```

Consulta genérica SNMP. En este caso el Satellite Server saca automáticamente el tráfico de cada interfaz, con su nombre "real" descriptivo:

```
module_begin
module_name if eth0 OutOctets
module_description The total number of octets transmitted out of
```




```
the interface, including framing characters.  
module_type generic_data_inc  
module_snmp 192.168.70.225  
module_oid .1.3.6.1.2.1.2.2.1.16.2  
module_community public  
module_end
```

Consulta WMI para uso de CPU (porcentaje):

```
module_begin  
module_name CPU  
module_type generic_data  
module_wmicpu 192.168.30.3  
module_wmiauth admin%none  
module_end
```

Consulta WMI para memoria libre (porcentaje):

```
module_begin  
module_name FreeMemory  
module_type generic_data  
module_wmimem 192.168.30.3  
module_wmiauth admin%none  
module_end
```

Consulta genérica WMI:

```
module_begin  
module_name GenericWMI  
module_type generic_data_string  
module_wmi 192.168.30.3  
module_wmiquery SELECT Name FROM Win32_ComputerSystem  
module_wmiauth admin%none  
module_end
```

Comando genérico SSH:

```
module_begin  
module_name GenericSSH  
module_type generic_data  
module_ssh 192.168.30.3  
module_command ls /tmp | wc -l  
module_end
```

Para introducir un umbral hay que hacerlo tanto en la definición de texto del Módulo



(`module_min_warning`, `module_min_critical`) como en la definición de umbrales mediante la interfaz web. Por ejemplo:

```
module_begin
module_name Latency
module_type generic_data
module_latency 192.168.70.225
module_min_warning 80
module_min_critical 120
module_end
```

Manualmente puede crear Módulos de ejecución. Los *scripts* o comandos que ejecute el Satellite Server deben estar previamente desplegados y accesibles por el mismo. En este sentido, funciona igual que un `module_exec` de un Agente. Tenga en cuenta que el uso de `module_exec` puede hacer que el rendimiento del Satellite Server disminuya.

```
module_begin
module_name Sample_Remote_Exec
module_type generic_data
module_exec /usr/share/test/test.sh 192.168.50.20
module_min_warning 90
module_min_critical 95
module_end
```

A partir de la versión 7 de Pandora FMS también pueden añadirse *plugins*. Al igual que estos, hay que tener en cuenta que los *plugins* se ejecutarán en la máquina donde está corriendo el Satellite Server. **Por lo tanto, habrá que implementar en estos *plugins* algún método para conectarse al equipo remoto que se necesita monitorizar.** La ventaja respecto a los anteriores es su gran flexibilidad. De esta forma, se pueden implementar condiciones y otros mecanismos para los que un `module_exec` se queda corto. La sintaxis es la misma que la de los Agentes. Un ejemplo de uso de un *plugin* podría ser el siguiente:

```
module_plugin /usr/share/pandora/remote_advanced_checks.sh
192.168.0.1
```

SNMPv3

Para configurar un módulo SNMPv3, defina `module_version` a 3 y especifique:

- `module_seclevel`: Nivel de seguridad (`noauth`, `authnopriv` o `authpriv`).
- `module_secname`: Nombre de seguridad.
- `module_authproto`: Protocolo de autenticación (`md5` o `sha`).
- `module_authpass`: Clave de autenticación.



- `module_privproto`: Protocolo de privacidad (aes o des).
- `module_privpass`: Clave de privacidad, según sea necesario.

Por ejemplo:

```
module_begin
module_name snmp_noauth
module_type generic_data_string
module_snmp 127.0.0.1
module_version 3
module_oid .1.3.6.1.2.1.1.1.0
module_seclevel noauth
module_secname snmpuser
module_end
```

```
module_begin
module_name snmp_authnopriv
module_type generic_data_string
module_snmp 127.0.0.1
module_version 3
module_oid .1.3.6.1.2.1.1.2.0
module_seclevel authnopriv
module_secname snmpuser
module_authproto md5
module_authpass 12345678
module_end
```

```
module_begin
module_name snmp_authpriv
module_type generic_data_string
module_snmp 127.0.0.1
module_version 3
module_oid .1.3.6.1.2.1.1.2.0
module_seclevel authpriv
module_secname snmpuser
module_authproto sha
module_authpass 12345678
module_privproto aes
module_privpass 12345678
module_end
```

La configuración específica de SNMPv3 se puede compartir entre Módulos sacándola fuera de la declaración del Módulo, en caso de que sea la misma para todos (también se puede compartir entre Agentes moviéndola al fichero de configuración del Satellite Server):



```
agent_name snmp
address 127.0.0.1

seclevel authpriv
secname snmpuser
authproto md5
authpass 12345678
privproto des
privpass 12345678

module_begin
module_name snmp_authpriv_1
module_type generic_data_string
module_snmp
module_version 3
module_oid .1.3.6.1.2.1.1.1.0
module_end

module_begin
module_name snmp_authpriv_2
module_type generic_data_string
module_snmp
module_version 3
module_oid .1.3.6.1.2.1.1.2.0
module_end
```

Cajas de credenciales

Salvo que la autenticación esté configurada con clave privada y clave pública, los Módulos SSH necesitan un nombre de usuario (<user>) y una contraseña (<pass>) para funcionar. Ambos se registran en el fichero de configuración principal, `satellite_server.conf`, utilizando cajas de credenciales (`credential_box`) con los siguientes formatos:

red/máscara,usuario,contraseña

red/máscara,usuario,[[contraseña cifrada]]

Por ejemplo:

```
credential_box 192.168.1.1/32,<user>,<pass1>
credential_box 192.168.1.0/24,<user>,<pass2>
```

Las búsquedas en las cajas de credenciales se hacen de máscaras más a menos



restrictivas.

Las contraseñas se pueden cifrar utilizando Blowfish en modo ECB. Asegúrese de que `credential_pass` está definido, de otro modo el nombre del `host` se utilizará como contraseña de cifrado por defecto. La representación hexadecimal del texto cifrado se debe rodear con corchetes dobles:





















```
credential_box 192.168.1.0/24,<user>,[ [80b51b60786b3de2] ]
```

Vista en la consola de todos los Agentes

Si la configuración del Satellite Server ha sido correcta, debería obtener una vista de Agentes parecida a esta:



Generalmente en todas las máquinas se crearán Módulos de tipo ICMP (Ping y Latencia) pero en algunas también se pueden generar Módulos de tipo SNMP y WMI. En las que tengan WMI habilitado se generarán los siguientes Módulos, de estar disponibles:

F. P. Type	Module name	Description	Status	Thresholds	Data	Graph	Last contact
 	CPU Load	CPU Load (%)		N/A - N/A	21 %	 	39 seconds
 	Free memory	Total free memory in kilobytes		N/A - N/A	7,635,884 KB	 	39 seconds
 	FreeDisk C:	Available disk space in kilobytes		N/A - N/A	214,845,685,284 KB	 	39 seconds
 	FreeDisk D:	Available disk space in kilobytes		N/A - N/A	78,945,619 KB	 	39 seconds

En las máquinas con SNMP habilitado se generarán los siguientes módulos, de estar disponibles:



F.	P.	Type	Module name	Description	Status	Thresholds	Data	Graph	Last contact
			ipInReceives	The total number of input datagrams received from interfaces...	●	N/A - N/A	2		101 3 minutes 34 seconds
			ipOutRequests	The total number of IP datagrams which local IP user-protoco...	●	N/A - N/A	1.6		101 3 minutes 34 seconds
			sysName	An administratively-assigned name for this managed node. By...	●	N/A - N/A	pacifico		101 3 minutes 34 seconds
			sysUpTime	The time (in hundredths of a second) since the network manag...	●	N/A - N/A	1378258510		101 3 minutes 34 seconds
			X0_ifInOctets	The total number of octets received on the interface, includ...	●	N/A - N/A	43,870.2		101 3 minutes 34 seconds
			X0_ifOperStatus	MAC C0:EA:E4:6E:9B:20 IP 192.168.80.1. Description: The curr...	●	N/A - N/A	1		101 3 minutes 34 seconds
			X0_ifOutOctets	The total number of octets transmitted out of the interface,...	●	N/A - N/A	60,051.9		101 3 minutes 34 seconds
			X1_ifInOctets	The total number of octets received on the interface, includ...	●	N/A - N/A	213,040.1		101 3 minutes 34 seconds
			X1_ifOperStatus	MAC C0:EA:E4:6E:9B:21 IP 192.168.90.254. Description: The cu...	●	N/A - N/A	1		101 3 minutes 34 seconds
			X1_ifOutOctets	The total number of octets transmitted out of the interface,...	●	N/A - N/A	1,609,405		101 3 minutes 34 seconds

En el apartado de operaciones masivas de la Consola de Pandora FMS hay una sección especial dedicada al Satellite Server, donde se pueden realizar diversas acciones de edición y borrado de Agentes y Módulos de forma masiva:



Lista de exclusión de SNMP

Al monitorizar redes grandes los Módulos SNMP que devuelven datos inválidos pueden afectar al rendimiento del Satellite Server, y llevar a otros Módulos a estado Desconocido. Para evitar esto, el Satellite Server puede leer una *lista de excluidos* de Módulos SNMP que serán descartados en el arranque antes de la ejecución.

Para crear una lista de excluidos, edite el fichero de configuración `/etc/pandora/satellite_server.conf` y asegúrese de que `snmp_blacklist` está *descomentado* y configurado con la ruta al fichero en el que se guardarán los Módulos de la lista de excluidos. A continuación ejecute:

```
satellite_server -v /etc/pandora/satellite_server.conf
```

Reinicie el Satellite Server. La lista de excluidos se puede regenerar tantas veces como sea necesario.

El formato de la lista de excluidos es:

```
agent:OID
```



```
agent:OID  
...
```

Por ejemplo:

```
192.168.0.1:.1.3.6.1.4.1.9.9.27  
192.168.0.2:.1.3.6.1.4.1.9.9.27
```

[Volver al Índice de Documentación Pandora FMS](#)



From:

<https://pandorafms.com/manual/> - **Pandora FMS Documentation**

Permanent link:

https://pandorafms.com/manual/es/documentation/05_big_environments/05_satellite

Last update: **2021/12/07 13:38**