Topologías distribuidas: Satellite Server

Topologías distribuidas: Satellite Server

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). Es especialmente útil para monitorizar redes remotas inaccesibles desde el servidor de Pandora FMS, y donde tampoco se pueden instalar Agentes Software.

El Satellite Server tiene algunas características que lo hacen especial:

- 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).
- Tanto el Satellite server como el Enterprise Network Server soportan IPv6 en todas sus funcionalidades avanzadas.

Instalación

Herramienta de instalación en línea

Esta es una característica especial de Pandora FMS. Una licencia Enterprise es requerida para su uso. En todo caso el parámetro de instalación obligatorio es la dirección IP o FQDN de un servidor Pandora FMS Enterprise. Por favor contacte con el equipo de ventas, pida presupuesto o resuelva sus dudas sobre licencias en este enlace.

Esta herramienta es compatible con Rocky Linux 8.x, AlmaLinux 8.x y RHEL 8.x.

Requisitos para el uso de la herramienta de instalación en línea (*online*):

- Tener acceso a internet.
- Tener instalado curl (viene por defecto en la mayoría de las distribuciones).
- Cumplir con los requisitos mínimos de hardware.
- Ser usuario administrador root.
- Contar con un SO compatible.
- En el caso de usar RHEL 8 será necesario que previamente esté activado con una licencia y subscrito a los repositorios estándar.

Para usar la herramienta de instalación *online* simplemente acceda a la línea de comandos dispuesta por su proveedor en la Nube, con usuario administrador root, y ejecute:

```
export PANDORA_SERVER_IP='<PandoraServer IP or FQDN>' && curl -Ls
https://pfms.me/satellite-ent-deploy| bash
```

Instalación personalizada utilizando la herramienta de instalación *online :*

- `PANDORA_SERVER_IP`: Dirección IP o FQDN del servidor Pandora FMS Enterprise al que apuntará el Satellite server. Parámetro obligatorio.
- `TZ`: Huso horario del Satellite server. Parámetro opcional.
- `SATELLITE_SERVER_PACKAGE`: URL personalizado de paquete tarball de instalación del Satellite server. Parámetro opcional.
- `SATELLITE_KEY`: Licencia Satellite server para activar automáticamente. Parámetro opcional.
- `REMOTE_CONFIG`: Configuración remota. Parámetro opcional, habilitado por defecto (valor 1).
- `INSTALL_AGENT`: Parámetro opcional, habilitado por defecto (valor 1), permite instalar el Agente software (se pueden usar todas las variables de configuración del instalador en línea del agente).
- `VMWARE_DEPENDENCIES`: Opcional, permite instalar dependencias del *plugin* de VMware®, deshabilitado por defecto (`0`).
- `ORACLE_DEPENDENCIES`: Opcional, permite instalar dependencias del *plugin* de Oracle®, deshabilitado por defecto (`0`).
- `MSSQL_DEPENDENCIES`: Opcional, permite instalar dependencias del *plugin* de MS SQL Server®, deshabilitado por defecto (`0`).
- `SKIP_KERNEL_OPTIMIZATIONS`: Deshabilitar la optimización del *kernel* recomendada, avanzado, deshabilitado por defecto (`0`).

Ejemplo:

```
env TZ='Europe/Madrid' \
SATELLITE_KEY='SOPORTEDEV00RS0REB3M2T7ZHISO51IIQH52JISJ47VGHIRM...'\
  PANDORA_SERVER_IP='192.168.10.10' \
  REMOTE_CONFIG=1 \
  INSTALL_AGENT=1 \
  VMWARE_DEPENDENCIES=1 \
  ORACLE_DEPENDENCIES=1 \
  MSSQL_DEPENDENCIES=1 \
  SKIP_KERNEL_OPTIMIZATIONS=0 \
```

```
sh -c "$(curl -fsSL https://pfms.me/satellite-ent-deploy)"
```

Instalación de Satellite Server en Linux

El sistema operativo GNU/Linux recomendado es RedHat Enterprise (RHEL) 8 / Rocky Linux 8.

Es necesario instalar Fping, Nmap y libnsl de forma independiente y primero se debe configurar el repositorio EPEL, visite el siguiente enlace:

```
https://docs.fedoraproject.org/en-US/epel/#_quickstart
```

y seleccione el sistema operativo. Si se utiliza Rocky Linux 8:

```
dnf config-manager --set-enabled powertools
dnf install epel-release
```

Instale Perl con el siguiente comando:

```
dnf install perl
```

Dependencias fundamentales del Satellite Server: PandoraWMIC (versión 762 y posteriores), Fping, Nmap y libnsl. En el instalador se adjuntan las dependencias de Braa y PandoraWMIC.

```
dnf install fping nmap libnsl
```

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
```

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

```
cd satellite_server/
```

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

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

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

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

Busque el *token* server_ip e indique ahí la dirección IP o dominio del servidor Pandora FMS

Enterprise al cual se conectará el servidor Satélite.

Tras ello puede guardar el archivo e iniciar 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

Con derechos de administrador ejecute el instalador firmado digitalmente (versión 762 y posterior). Será necesario instalar tambien WinPCap. La ventana de instalación aparecerá en el siguiente paso de la instalación.

Lugo 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 MS Windows®.

Dependiendo del año de su versión de MS Windows® necesitará instalar alguna(s) de estas librerías:

Microsoft Visual C++ Redistributable (últimas descargas con soporte técnico):

- Visual Studio 2015, 2017, 2019, and 2022.
- Visual Studio 2013 (VC++ 12.0).
- Visual Studio 2012 (VC++ 11.0) Update 4.
- Visual Studio 2010 (VC++ 10.0) SP1 (sin soporte técnico).
- Visual Studio 2008 (VC++ 9.0) SP1 (sin soporte técnico).

Están disponibles tanto para procesadores de 32 bits (X86), 64 bits (X64) y ARM64 en el siguiente enlace:

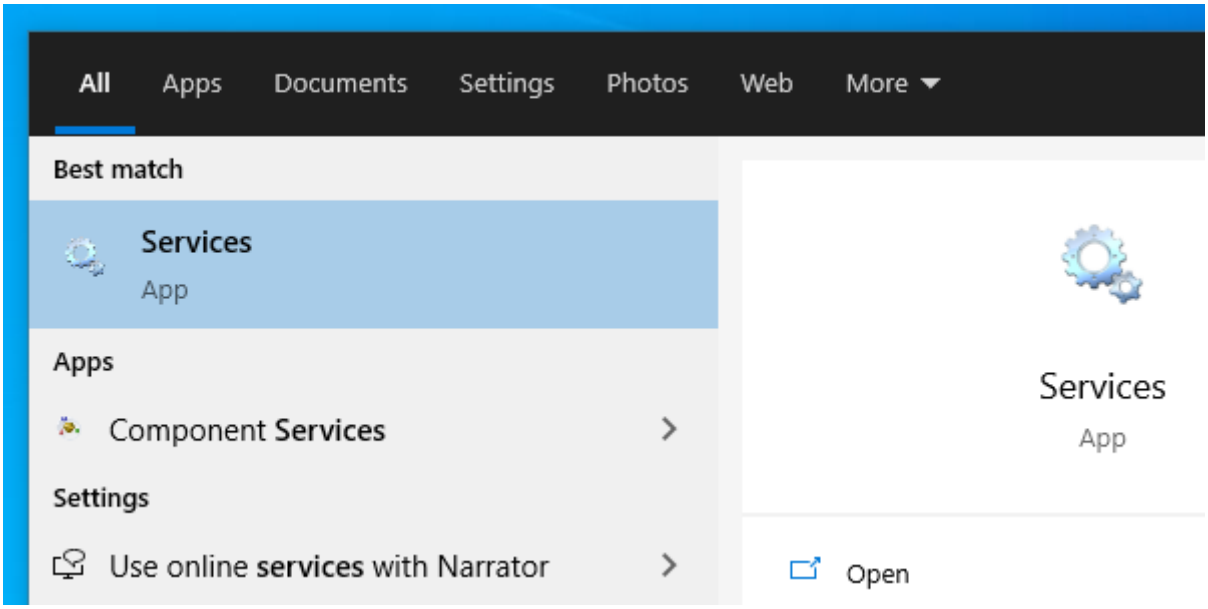
https://docs.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170&viewFallbackFrom=msvc-170

Funcionamiento de Módulos WMI en algunas versiones de Windows

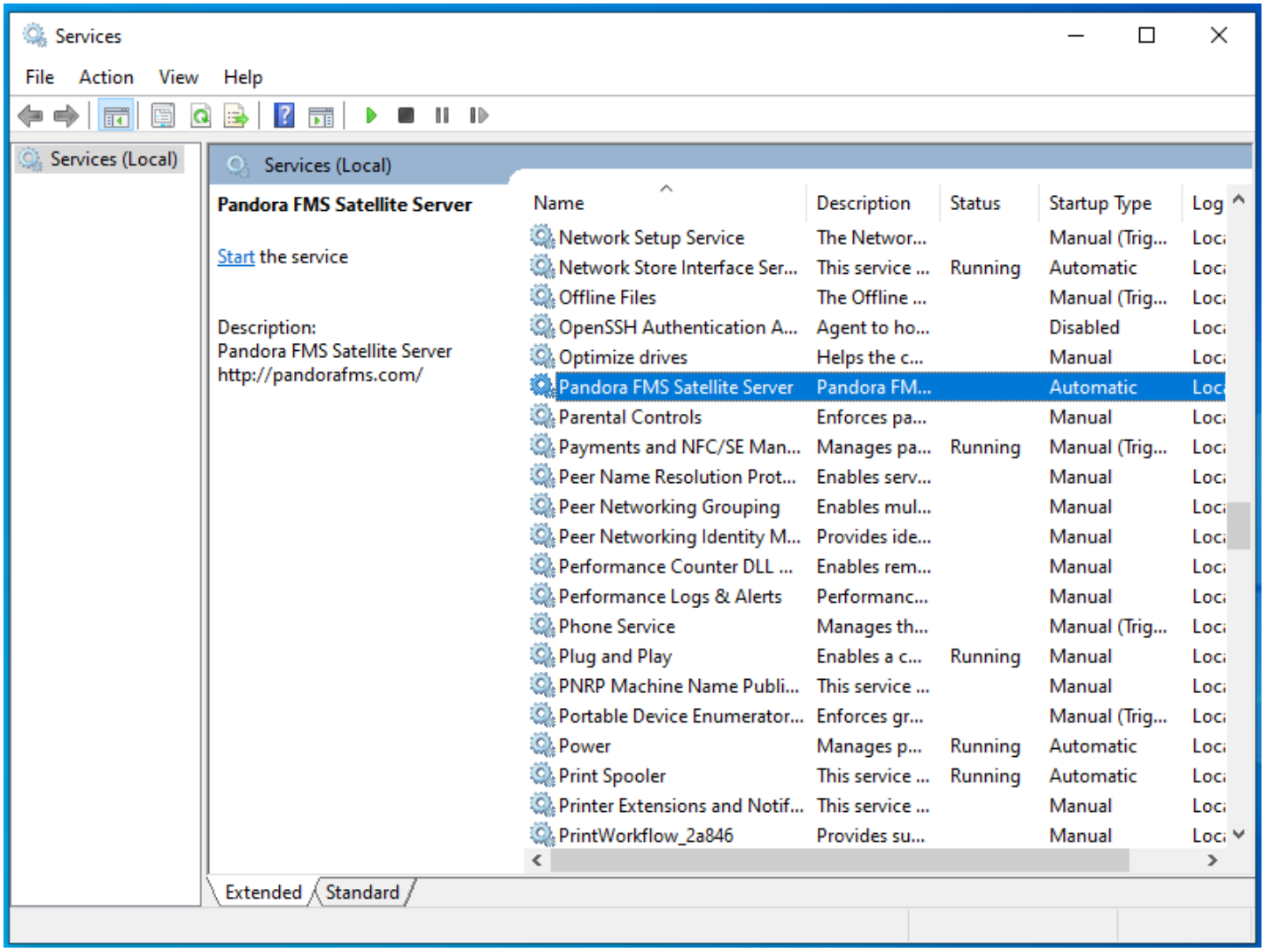
Por motivos de seguridad de Windows®, algunas versiones tienen limitados los usuarios con los que realizar consultas WMI remotas. En el caso de que estas consultas no se lleven a cabo, la solución es ejecutar el servicio del Satellite Server como usuario Administrador.

El proceso a seguir es el siguiente:

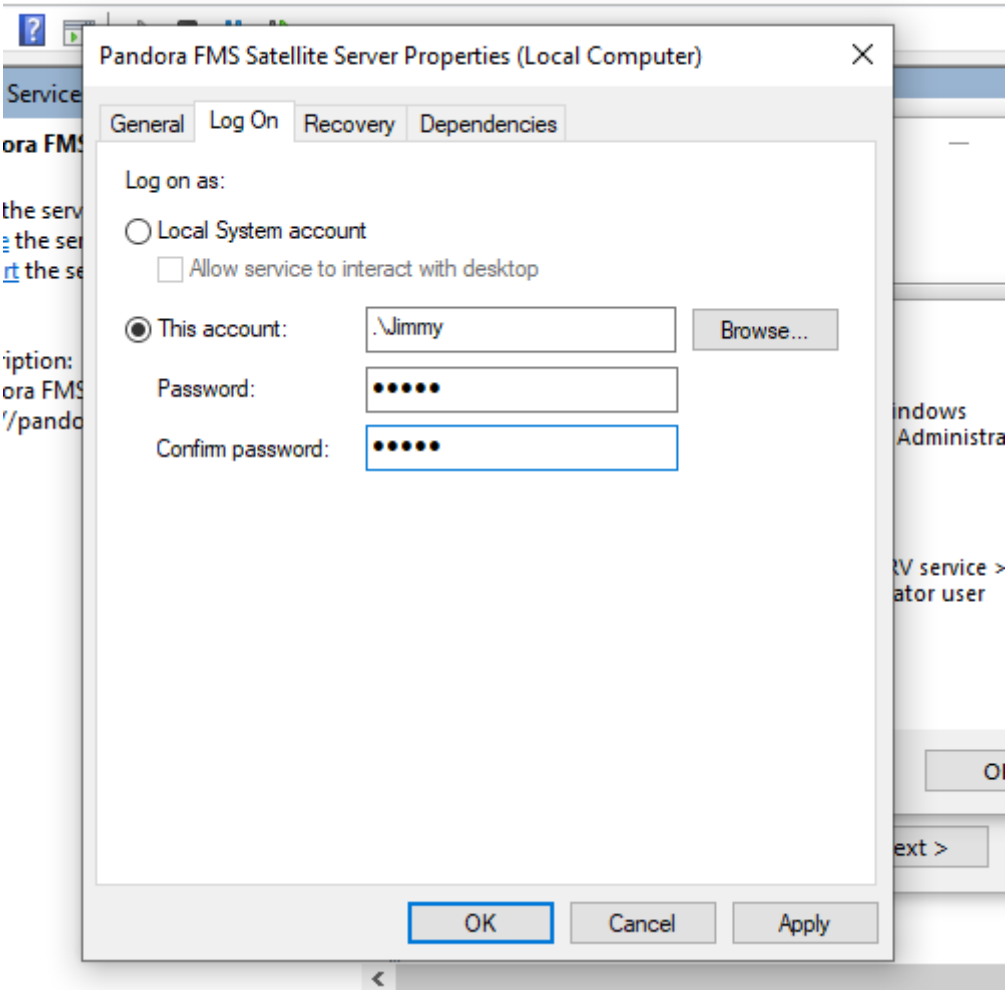
Abra los servicios:



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.

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.

agent_threads

```
agent_threads xxx
```

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

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 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).

host_file

```
host_file <path_filename>
```

Es un método alternativo o complementario al de explorar una red para encontrar *hosts*.

En este fichero (< path_filename >), en cada línea hay una dirección. Alternativamente, se le puede pasar en la misma línea el *hostname* seguido de la dirección IP, de esa forma el Agente será creado con ese nombre y que 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_key

Versión 765 o posterior.

```
# Encryption key for the Pandora FMS license.
# pandora_license_key
```

Para la transmisión segura de la licencia al servidor Satélite, deberá configurar en la Consola Web o en la Metaconsola la misma clave de cifrado que colocará en este *token.*

Véase también el *token* server_ip .

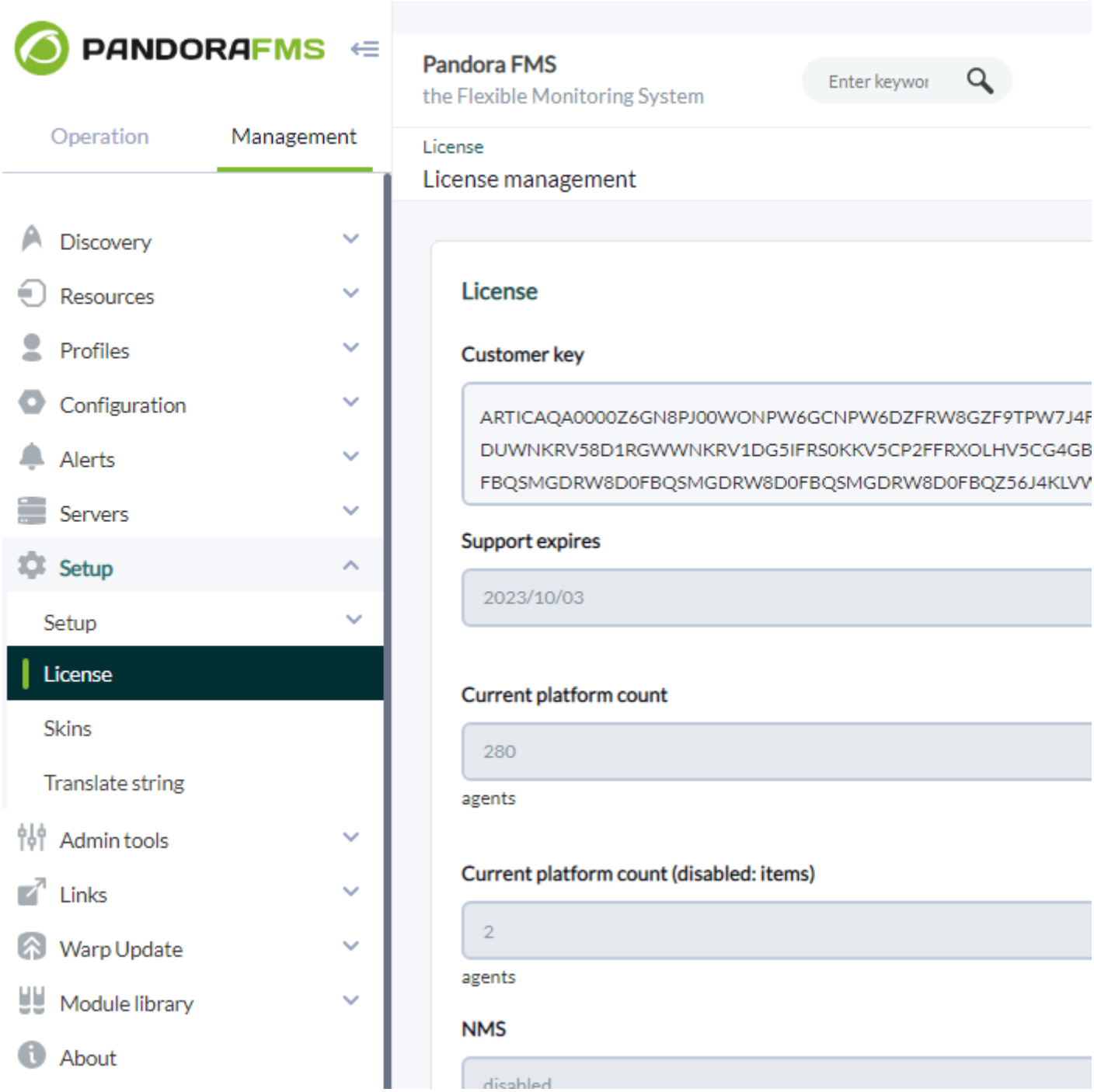
pandora_license

Desde la versión 761 y posteriores el licenciamiento del servidor Satélite se hace automáticamente y este *token*

queda obsoleto.

```
pandora_license xxxxxxx
```

Escribe y almacena la licencia del servidor Pandora FMS Enterprise, tal como se muestra en la sección Management → Setup → License de la Consola web de 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 (SNMPv3). 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 x 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
```

Número de 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`).

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.

Para utilizar SNMP v3 consulte en este enlace cómo configurar las credenciales de acceso conocidas.

snmp3_seclevel

Nivel de seguridad utilizado para los mensajes SNMPv3 (`noauth`, `authnopriv` o `authpriv`).

Para utilizar SNMP v3 consulte en este enlace cómo configurar las credenciales de acceso conocidas.

snmp3_secname

Nombre de seguridad utilizado para los mensajes SNMPv3.

Para utilizar SNMP v3 consulte en este enlace cómo configurar las credenciales de acceso conocidas.

snmp3_authproto

Protocolo de autenticación (`md5` o `sha`) para peticiones SNMPv3 autenticadas.

Para utilizar SNMP v3 consulte en este enlace cómo configurar las credenciales de acceso conocidas.

snmp3_authpass

Contraseña de autentificación para la solicitud SNMPv3 autentificada.

Para utilizar SNMP v3 consulte en este enlace cómo configurar las credenciales de acceso conocidas.

snmp3_privproto

Protocolo de privacidad (`des` o `aes`) para peticiones SNMPv3 cifradas.

Para utilizar SNMP v3 consulte en este enlace cómo configurar las credenciales de acceso conocidas.

snmp3_privpass

Contraseña de privacidad para mensajes SNMPv3 cifrados.

Para utilizar SNMP v3 consulte en este enlace cómo configurar las credenciales de acceso conocidas.

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 <IP_addr> [agent_name]
```

Añade el *host* dado (`[agent_name]`) a la lista de agentes monitorizados. Se puede especificar el nombre del Agente después de la dirección IP (<IP_addr>). 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
```

delete_host

```
delete_host <agent_name>
```

Elimina el *host* dado de la lista de Agentes monitorizados de forma permanente, borrando su fichero de configuración. El *host* debe identificarse por el nombre del Agente. Se pueden borrar múltiples *hosts*, uno por cada línea. Por ejemplo:

```
delete_host 192.168.0.1
delete_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

```
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

```
agents_blacklist_snmp 10.0.0.0/24[,8.8.8.8/30] (Version> 7.0OUM713)
```

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

```
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

```
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 y reflejar en pantalla las coordenadas con el formato <longitud>,<latitud>,[<altitud>] El tercer parámetro, la altitud, es opcional.

forced_add

```
force_add [0|1]
```

Si se configura a `1`, los *hosts* añadidos de forma manual (a través de host_fileo add_host) se crearán siempre, aunque no respondan a ping, con un fichero de configuración sin módulos.

agent_block

```
agent_block XX
```

Número de ficheros de datos XML enviados en una sola llamada al cliente Tentacle, por defecto `50`.

conf_interval

```
conf_interval XXX
```

Intervalo de comprobación de la configuración remota, por defecto `300` segundos.

exec_interval

```
exec_interval XXX
```

Tiempo entre comprobaciones de ejecución, por defecto `300` segundos.

exec_threads

```
exec_threads X
```

Número de hilos utilizados para los módulos de ejecución, 5 por defecto. 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.

latency_block

```
latency_block XXX
```

Número de *hosts* procesados en una sola llamada a nmap (latencia), por defecto `400`.

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.

latency_interval

```
latency_interval XXX
```

Tiempo entre comprobaciones de latencia, por defecto `180` segundos.

latency_retries

```
latency_retries X
```

Número de reintentos para los módulos de latencia, por defecto 2 intentos.

latency_threads

```
latency_threads X
```

Número de hilos utilizados para la comprobación de la latencia, por defecto 4 hilos.

latency_timeout

```
latency_timeout X
```

Tiempo de espera para las comprobaciones de latencia en segundos, por defecto 1.

ping_block

```
ping_block XXX
```

Número de *hosts* procesados en una sola llamada a nmap (ping), por defecto `400`.

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.

ping_interval

```
ping_interval XXX
```

Tiempo entre comprobaciones de ping, `120` segundos por defecto.

ping_retries

```
ping_retries X
```

Número de reintentos para los módulos de latencia, 2 por defecto.

ping_threads

```
ping_threads X
```

Número de hilos utilizados para las comprobaciones de ping, 4 por defecto.

ping_timeout

```
ping_timeout X
```

Tiempo de espera para las comprobaciones de ping en segundos, por defecto 1.

plugin_interval

```
plugin_interval XXX
```

Tiempo entre comprobaciones del *plugin*, por defecto `300` segundos.

plugin_threads

```
plugin_threads X
```

Número de hilos utilizados para la comprobación de los *plugins*, por defecto 2 hilos.

plugin_timeout

```
plugin_timeout XX
```

Tiempo de espera para las comprobaciones de los *plugins* en segundos, por defecto `10` segundos.

recon_interval

```
recon_interval XXXXXX
```

Tiempo entre escaneos de red en segundos, por defecto `604800` segundos.

snmp2_block

```
snmp2_block XX
```

Número de hosts procesados en una sola llamada a Braa (SNMPv2c), `50` por defecto.

snmp2_interval

```
snmp2_interval XXX
```

Tiempo entre comprobaciones SNMP (SNMPv2c), por defecto `180` segundos.

snmp2_retries

```
snmp2_retries X
```

Número de reintentos para los módulos SNMP (SNMPv2c), por defecto 2 reintentos.

snmp2_threads

```
snmp2_threads X
```

Número de hilos utilizados para las comprobaciones de SNMP (SNMPv2c), por defecto 8 hilos.

snmp2_timeout

```
snmp2_timeout X
```

Tiempo de espera para las comprobaciones SNMP(SNMPv2c) en segundos, por defecto 5.

snmp3_block

```
snmp3_block XX
```

Número de *hosts* procesados en una sola llamada a Braa (SNMPv3), 50 por defecto.

snmp3_interval

```
snmp3_interval XXX
```

Tiempo entre comprobaciones SNMP (SNMPv3), por defecto 180 segundos.

snmp3_retries

```
snmp3_retries X
```

Número de reintentos para los módulos SNMP (SNMPv3), por defecto 2 reintentos.

snmp3_threads

```
snmp3_threads X
```

Número de hilos utilizados para las comprobaciones de SNMP (SNMPv3), por defecto 4 hilos.

snmp3_timeout

```
snmp3_timeout X
```

Tiempo de espera para las comprobaciones de SNMP (SNMPv3) en segundos, por defecto 5 segundos.

snmp_block

```
snmp_block XX
```

Número de *hosts* procesados en una sola llamada a Braa (SNMPv1), por defecto 50.

snmp_interval

```
snmp_interval XXX
```

Tiempo entre comprobaciones SNMP (SNMPv1), por defecto 180 segundos.

snmp_retries

```
snmp_retries X
```

Número de reintentos para los módulos SNMP (SNMPv1), 2 por defecto.

ssh_interval

```
ssh_interval XXX
```

Tiempo entre comprobaciones SSH, por defecto 300 segundos.

ssh_threads

```
ssh_threads XXX
```

Número de hilos utilizados para los módulos SSH, por defecto 5 hilos.

ssh_timeout

```
ssh_timeout X
```

Tiempo de espera para las comprobaciones SSH en segundos, por defecto 2 segundos.

tcp_interval

```
tcp_interval XXX
```

Tiempo entre comprobaciones TCP, por defecto 300 segundos.

tcp_threads

```
tcp_threads X
```

Hilos dedicados a las comprobaciones TCP, por defecto 5 hilos.

tcp_timeout

```
tcp_timeout X
```

Tiempo de espera para las comprobaciones TCP, por defecto 1 segundo.

snmp_threads

```
snmp_threads X
```

Número de hilos utilizados para las comprobaciones SNMP (SNMPv1), por defecto 8 hilos.

snmp_timeout

```
snmp_timeout X
```

Tiempo de espera para las comprobaciones SNMP en segundos (SNMPv1), por defecto 5 segundos.

wmi_interval

```
wmi_interval XXX
```

Tiempo entre comprobaciones de WMI, por defecto 300 segundos.

wmi_threads

```
wmi_threads X
```

Hilos dedicados al sondeo de WMI, por defecto 5 hilos.

ipam_task

```
ipam_task <id IPAM TASK> , <CIDR>
```

Lista de redes separadas por comas (en notación SLASH) a explorar por IPAM. Debe estar precedido por el identificador de tarea IPAM asignado en PFMS al ser creado (se debe dejar sin asignar el campo Discovery server para luego ser asignado dicha labor a un Satellite server). Por ejemplo: `1,192.168.0.0/24` .

ipam_interval

```
ipam_interval XXXXXX
```

Tiempo entre las tareas de exploraciones en segundos.

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:

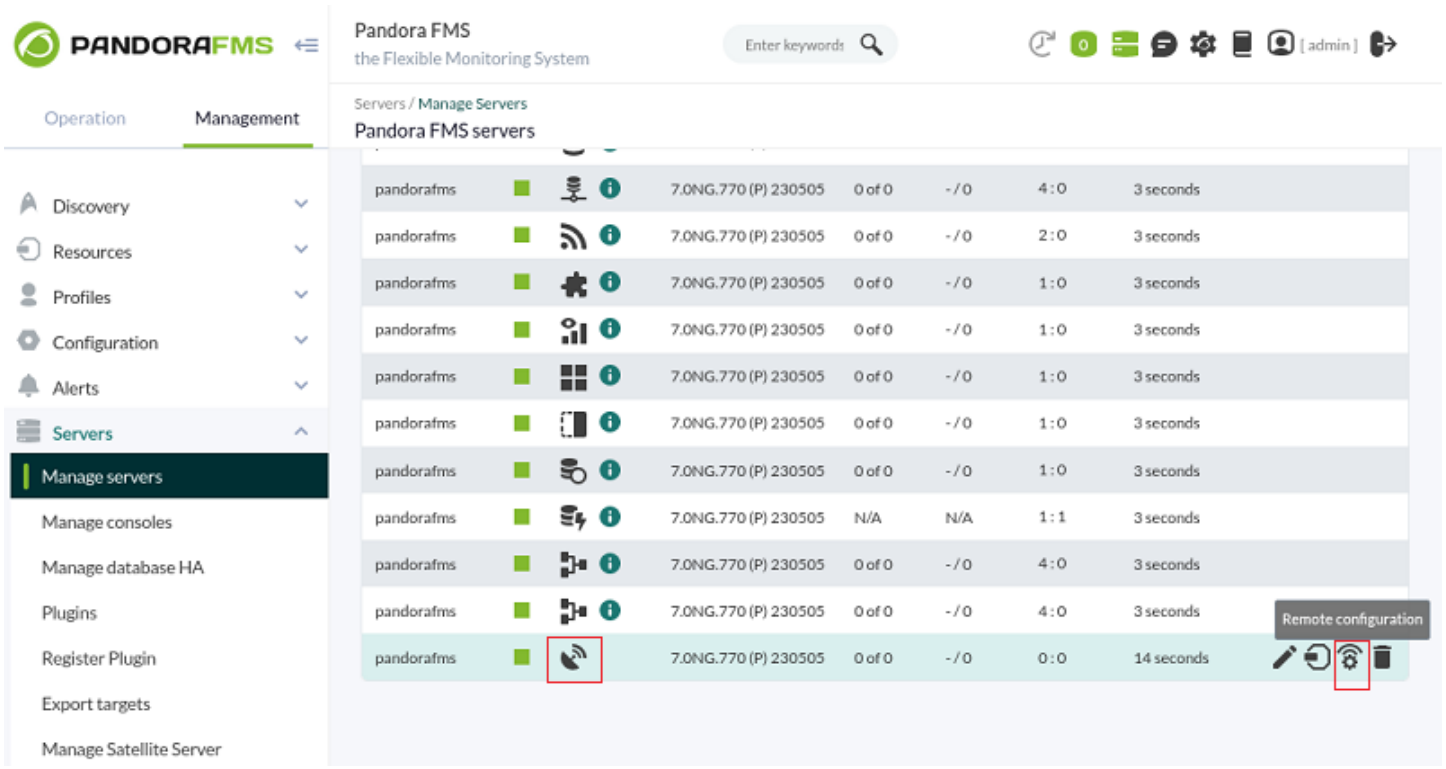
```
secondary_server_ip     192.168.1.123
secondary_server_path   /var/spool/pandora/data_in
secondary_mode          on_error
secondary_transfer_mode tentacle
secondary_server_port   41121
```

Configuración remota

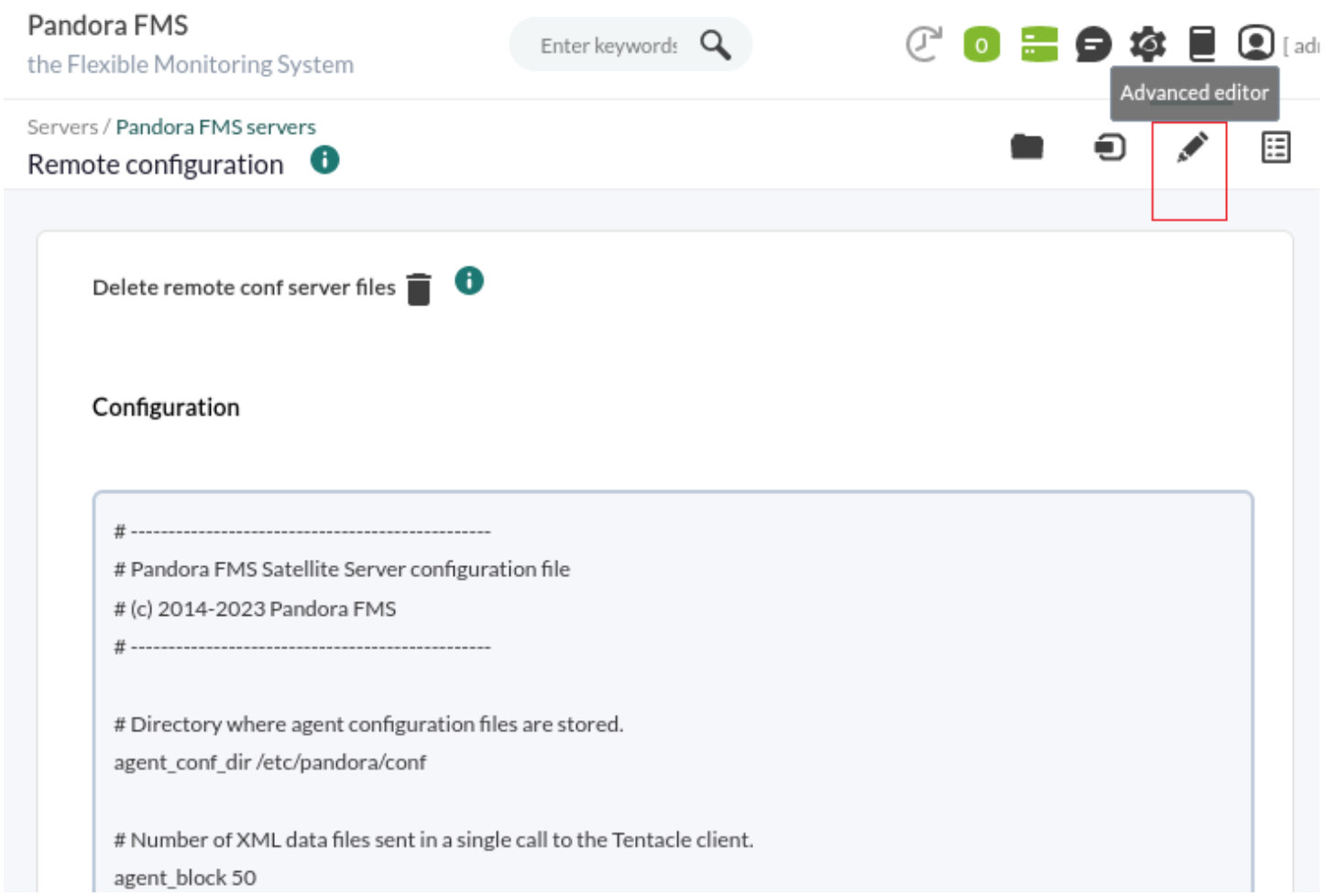
Configuración remota del fichero

Podrá acceder al editor avanzado de configuración remota del servidor Satélite en el servidor PFMS Enterprise al cual pertenezca el servidor Satélite por medio del menú Management →Servers → Manage servers. Una vez haya cargado la página en su navegador web, haga clic en el icono

Remote configuration.



Luego haga clic en el icono Advanced editor (Editor avanzado):



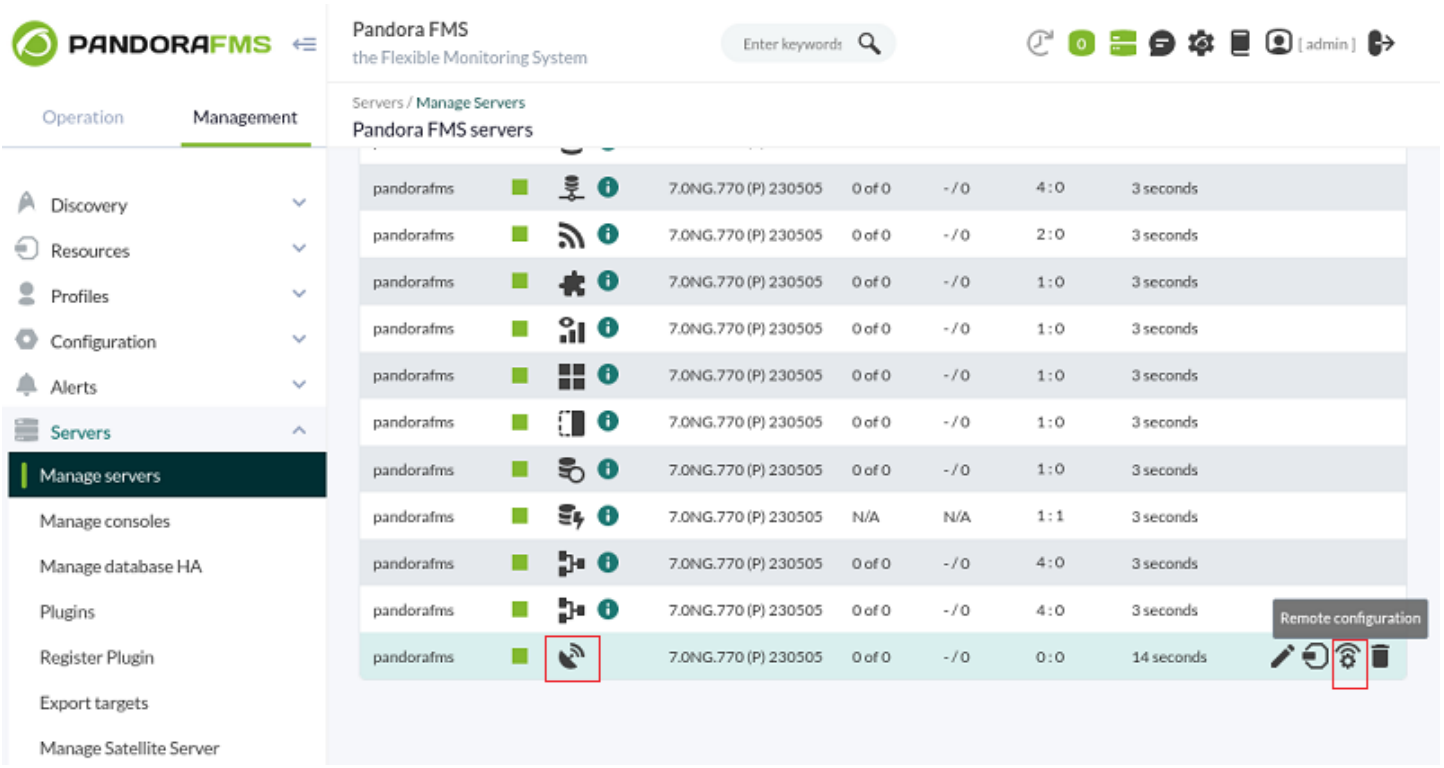
En el cuadro de texto correspondiente a Configuration podrá editar y/o agregar cada uno de los *token* descritos en secciones anteriores. Cuando haya finalizado de editar guarde los cambios pulsando en el botón Update situado al final de la página.

La sincronización y carga de los nuevos *tokens* tomará cierto tiempo. Aguarde unos instantes para que se propaguen los cambios.

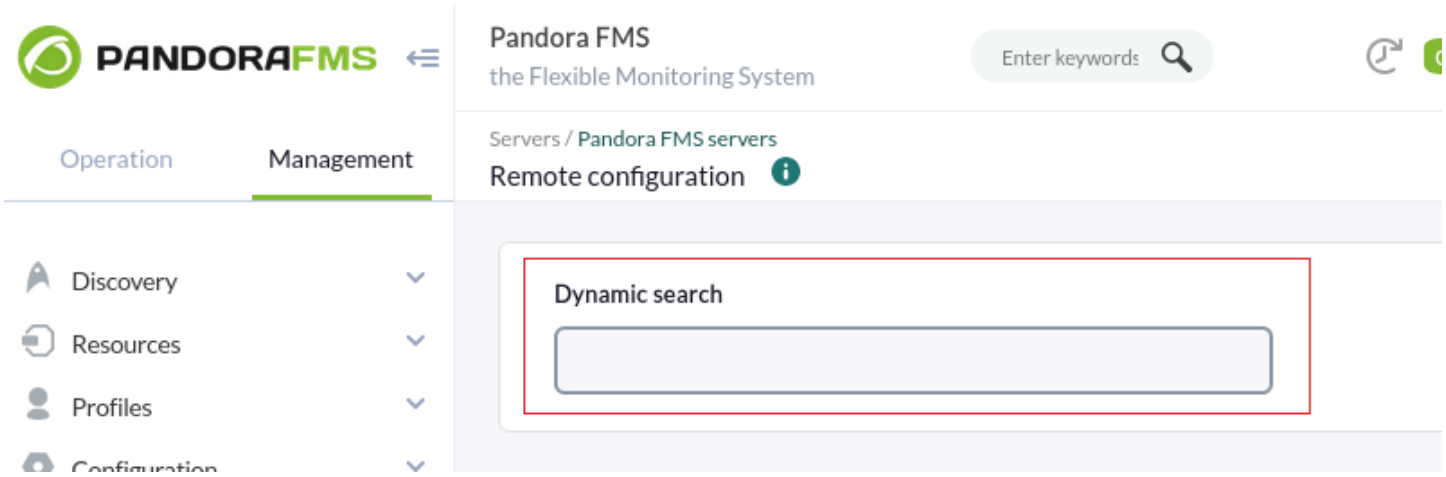
Interfaz gráfica de configuración remota

Versión NG 764 o posterior.

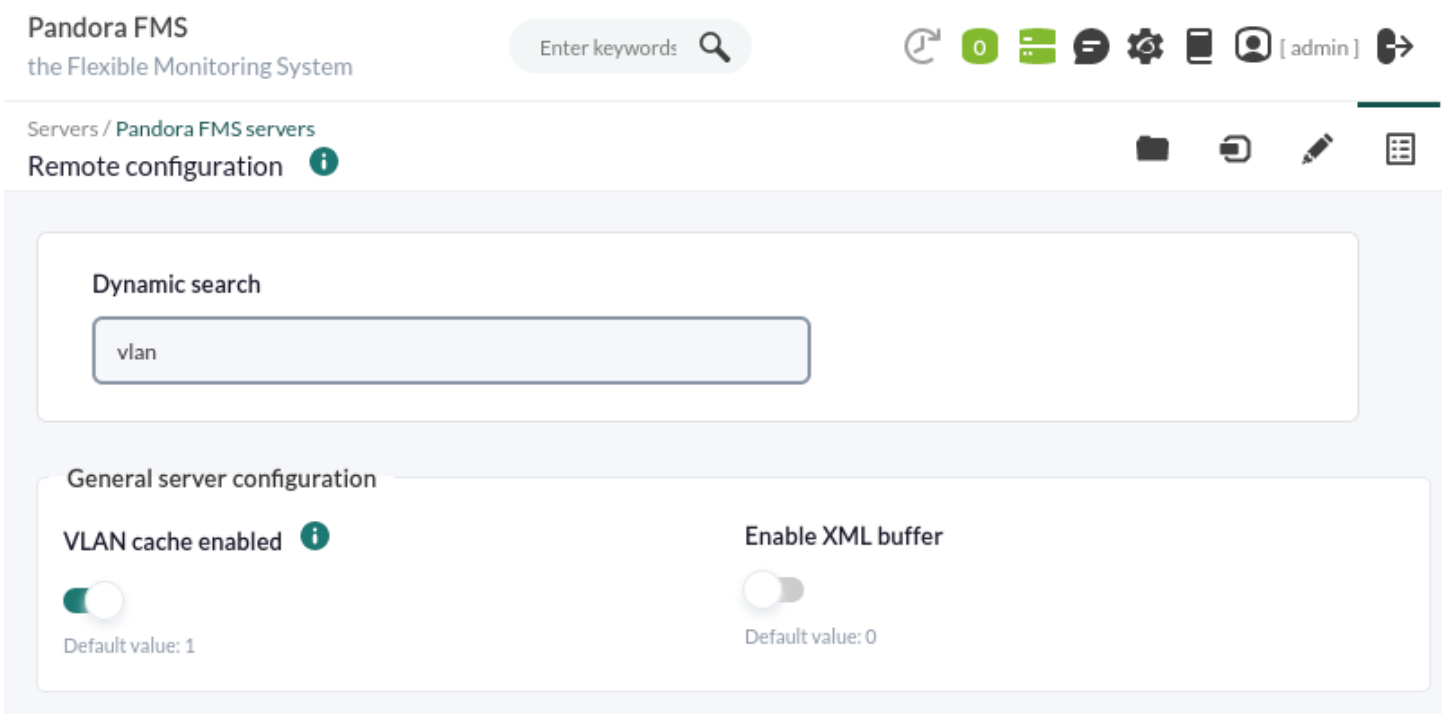
Podrá acceder a la interfaz gráfica en el servidor PFMS Enterprise al cual pertenezca el servidor Satélite, de manera remota, por medio del menú Management → Servers → Manage servers y luego haciendo clic en el icono Remote configuration.



Utilice la búsqueda dinámica (Dynamic search) para introducir texto clave (una letra o más) y buscar un *token* específico.



Algunos *token* únicamente aceptan dos valores (`ON` /`OFF`): utilice el primer botón para cambiar dicho valor. Si con el segundo botón habilita o deshabilita el *token* correspondiente el servidor Satélite tomará el valor por defecto que tenga asignado (`1` ó `0`) *independientemente del valor que marque el primer botón*.



Una vez haya hecho todos los cambios haga clic en el botón Update para guardar sus preferencias.

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 venta 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, sobreescribe 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 la 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.

Consultas ICMP/TCP

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
```

Consultas WMI

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
```

Consultas SNMPv1 y SNMPv2

¡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 añada la línea:

```
module_version 2c
```

Para obligar al módulo a utilizar SNMP versión 1 añada 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
```

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
```

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.

Asegúrese de que los OID empiezan con un punto o los módulos SNMP no funcionarán.

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
```

Para la creación de grupos de componentes (incluyendo SNMPv3) consulte “SNMP wizard”.

Fichero de configuración del Satellite Server *por defecto* para SNMPv3:

Deberá colocar sus propios valores y/o credenciales, así como cambiar los protocolos o métodos de cifrado necesarios. Deberá reiniciar el servidor PFMS para que los nuevos valores de configuración sean leídos y puestos en memoria.

```
# Security level used for SNMPv3 messages (noauth, authnopriv or authpriv).
#snmp3_seclevel authpriv

# Security name used for SNMPv3 messages.
#snmp3_secname

# Authentication protocol (md5 or sha) for authenticated SNMPv3 requests.
#snmp3_authproto sha

# Authentication password for authenticated SNMPv3 request.
#snmp3_authpass

# Privacy protocol (des or aes) for encrypted SNMPv3 requests.
#snmp3_privproto des

# Privacy password for encrypted SNMPv3 messages.
#snmp3_privpass
```

Consultas SSH

Las consultas SSH en servidores Satélite instalados en MS Windows® todavía está en implementación. El equipo de desarrollo PFMS se encuentra trabajando en ello.

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
```

Consultas con complementos

A partir de la versión 7 de Pandora FMS también pueden añadirse complementos (*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
```

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|]]

Las consultas SSH en servidores Satélite instalados en MS Windows® todavía está en implementación. El equipo de desarrollo PFMS se encuentra trabajando en ello.

Por ejemplo:

```
credential_box 192.168.1.1/32,<user>,<pass1>
```

```
credential_box 192.168.1.0/24,<user>,<pass2>
```

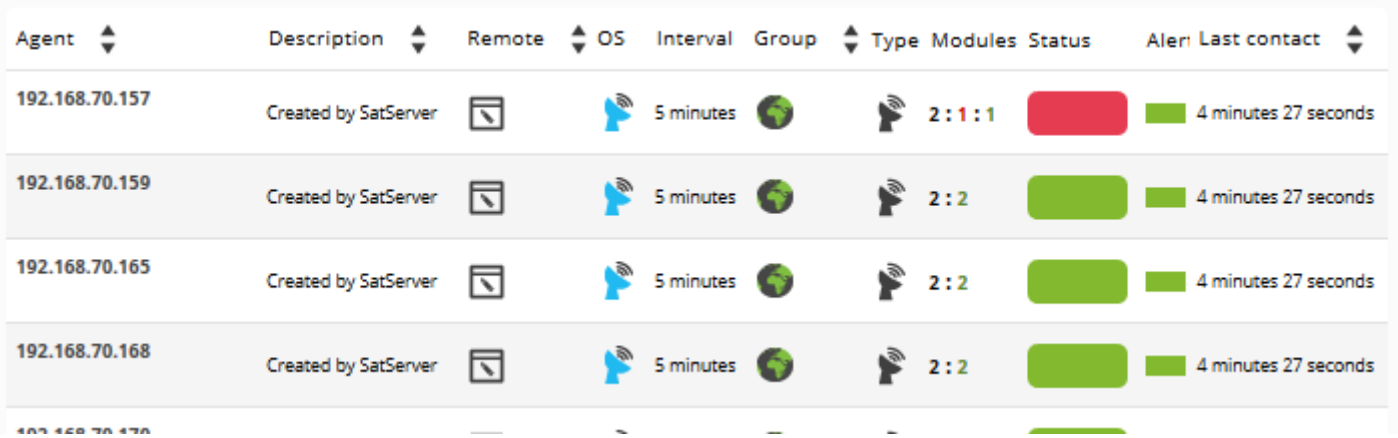
Las búsquedas en las cajas de credenciales se hacen de máscaras más a menos restrictivas.

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:

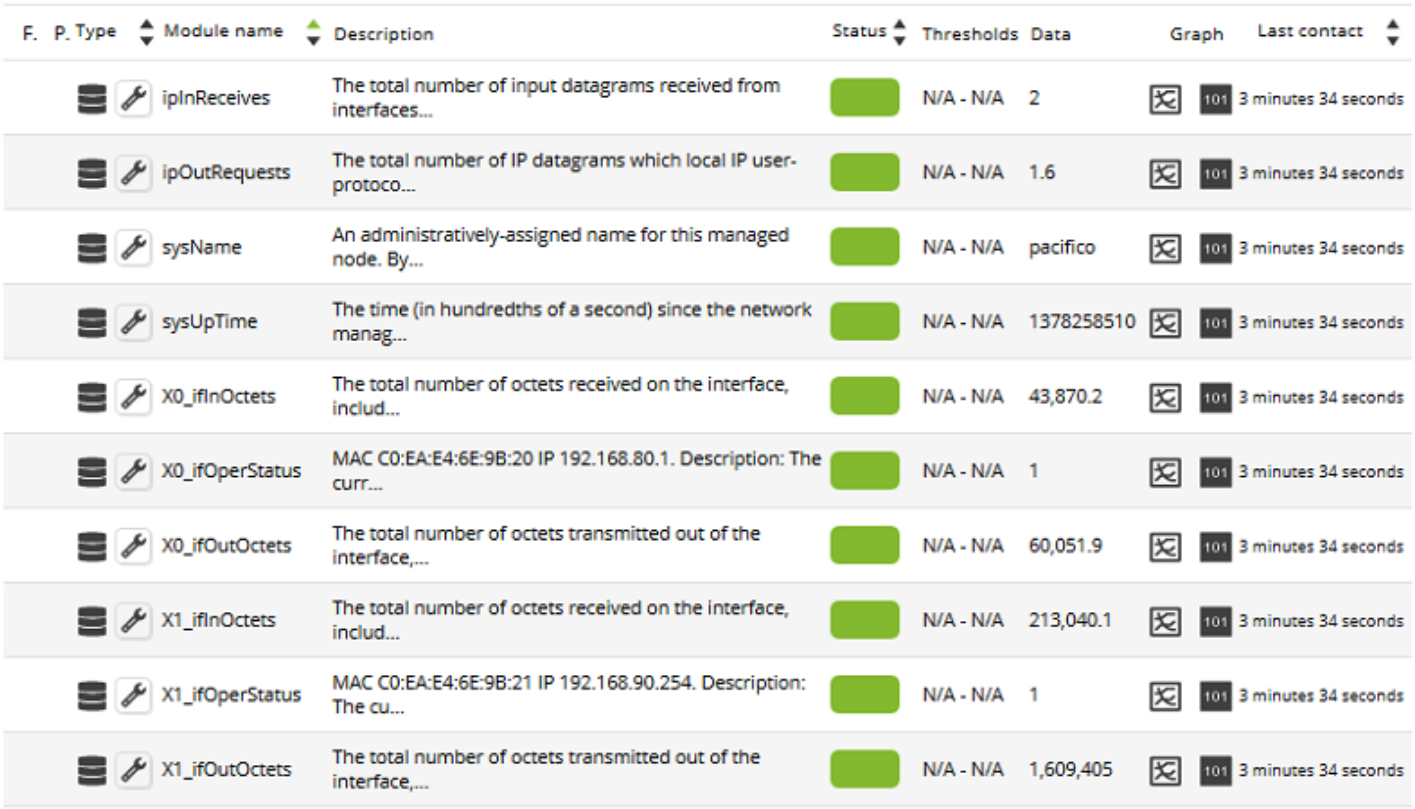
```
credential_box 192.168.1.0/24,<user>,[[80b51b60786b3de2|]]
```

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. 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		3 minutes 34 seconds
			ipOutRequests	The total number of IP datagrams which local IP user-protoco...		N/A - N/A	1.6		3 minutes 34 seconds
			sysName	An administratively-assigned name for this managed node. By...		N/A - N/A	pacifico		3 minutes 34 seconds
			sysUpTime	The time (in hundredths of a second) since the network manag...		N/A - N/A	1378258510		3 minutes 34 seconds
			X0_ifInOctets	The total number of octets received on the interface, includ...		N/A - N/A	43,870.2		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		3 minutes 34 seconds
			X0_ifOutOctets	The total number of octets transmitted out of the interface,...		N/A - N/A	60,051.9		3 minutes 34 seconds
			X1_ifInOctets	The total number of octets received on the interface, includ...		N/A - N/A	213,040.1		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		3 minutes 34 seconds
			X1_ifOutOctets	The total number of octets transmitted out of the interface,...		N/A - N/A	1,609,405		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