Manual de instalación y configuración Pandora FMS

Equipo:
Humanlinks

Modulo:
Administración

Tutor:
Germán Leal

Centro de servicios y gestión empresarial

SENA
2010

Introducción

La siguiente documentación fue realizada en conjunto por un grupo de estudiantes del área de telecomunicaciones del SENA, hacemos referencia a la herramienta Pandora FMS (Sistema de monitoreo flexible) la cual nos proporciona una excelente interfaz para el monitoreo de aplicaciones, hardware, y software en diferentes plataformas.

Queremos llegar al lector de una manera clara y concisa tratando de explicar lo mas detalladamente posible cada proceso, en esta guía monitoreamos diferentes procesos, desde el funcionamiento de una memoria ram, hasta el funcionamiento de toda una red estructurada.

Esperamos que al finalizar la lectura de este documento, pueda aclarar muchas dudas, he inquietarse por otras mas.

Justificación

La implementación de este proyecto nos acerco bastante, a lo que significa monitoreo y gestión de elementos simulados y reales, además queremos que sirva de referencia para todas las personas que necesiten herramientas libres, y con una robustez excelente como la que posee Pandora FMS.

Objetivo General

Afianzar en la búsqueda de nuevas herramientas que nos brinden una solución competente, y proporcionar documentación que sirva a otras personas interesadas en el tema, cumplir con nuestras expectativas académicas, y por sobretodo adquirir y compartir conocimiento.

Objetivos específicos

- Comprender las diferentes formas en las que podemos monitorear una red de datos
- Estudiar protocolos de diferentes plataformas que nos arrojan datos estadísticos, tales como: WMI, SNMP, Tentacle, WQL, etc... Introduciéndonos en conocimientos que nos sirven para nuestra experiencia académica
- Afianzar nuestra formación autónoma demostrando, que de una u de otra forma, somos totalmente autodidactas

Que es Pandora FMS:

Pandora FMS (FMS viene de Flexible Monitoring System) es una aplicación de monitorización para vigilar todo tipo de sistemas y aplicaciones. Pandora FMS permite conocer el estado de cualquier elemento de sus sistemas de negocio. Pandora FMS vigila su hardware, su software, sus aplicaciones y por supuesto, su Sistema Operativo. Pandora FMS es capaz de detectar una interfaz de red que se ha caído así como el movimiento de cualquier valor del NASDAQ. Si es necesario, Pandora FMS puede enviar un mensaje SMS cuando falle cualquier sistema o aplicación... o cuando el valor de Google caiga por debajo de los 330 US $.

Pandora FMS se ajusta como un pulpo a sus sistemas y necesidades ya que ha sido diseñado para ser abierto, modular, multiplataforma y fácil de personalizar sin necesidad de ser un experto desarrollador.
Pandora FMS está hecho para administradores de sistemas, aunque se puede adaptar a todo tipo de entornos software o incluso hardware.

Pandora FMS es una herramienta de monitorización que no sólo mide si una parámetro está bien o mal. Pandora FMS puede cuantificar el estado (bien, mal y valores intermedios) o almacenar un valor (numérico o alfanumérico) durante meses si es necesario.
Pandora FMS permite medir rendimientos, comparar valores entre diferentes sistemas y establecer alertas sobre umbrales.
Pandora FMS trabaja sobre una base de datos de forma que puede generar informes, estadísticas, niveles de adecuación de servicio (SLA) y medir cualquier cosa que proporcione o devuelva un dato. Es decir, Pandora FMS puede medir cualquier cosa: sistemas operativos, servidores, aplicaciones y sistemas hardware— tal como cortafuegos, proxies, bases de datos, servidores web, VPN, routers,
switches, procesos, servicios, acceso remoto a servidores, etc. todo integrado en una arquitectura abierta y distribuida.
Pandora FMS se puede implementar sobre cualquier sistema operativo, con agentes específicos para cada plataforma. Ya existen agentes para Windows (2000, XP, 2003, 2008, Vista, 7), Linux, Mac, Solaris, HP-UX, BSD, AIX, IPSO, y OpenWRT.

Requisitos mínimo de hardware:

Agente:

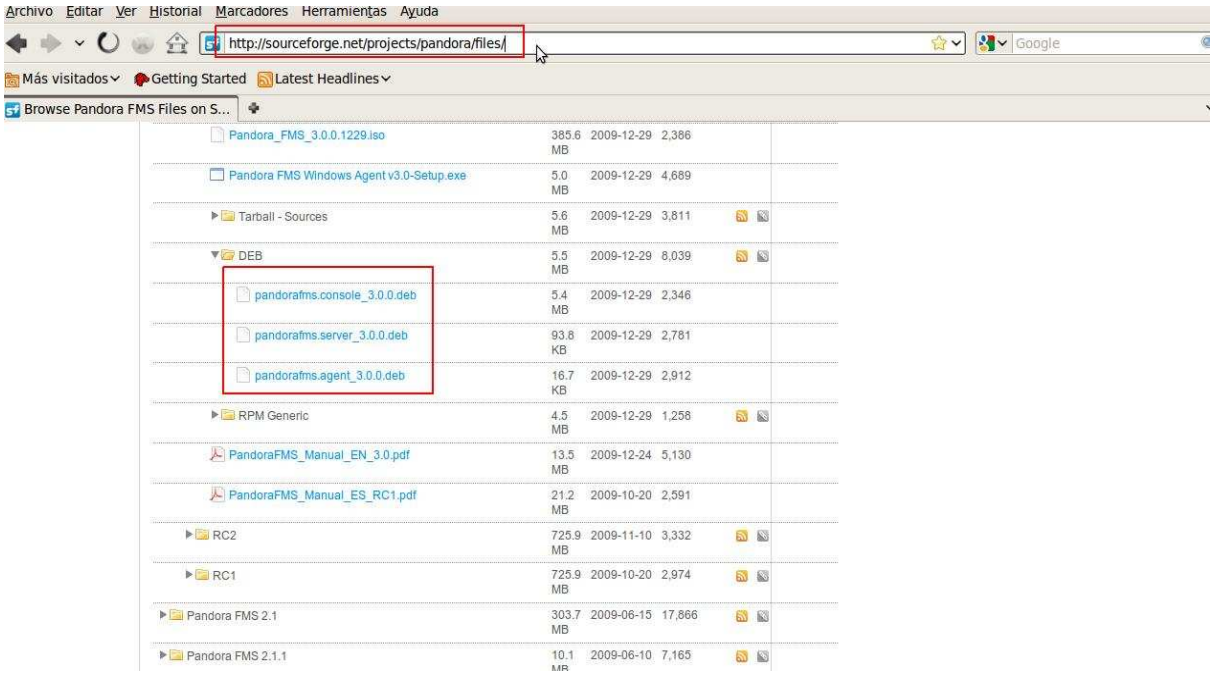
• Hasta 500 agentes o 5.000 módulos: 2GB de RAM y una CPU de un sólo núcleo a 2GHz de reloj. Disco duro rápido, 7200rpm o equivalente.
• Hasta 2.000 agentes o 10.000 módulos: 4GB de RAM y una CPU de doble núcleo a 2.5GHz de reloj y disco duro rápido (7.200 rpm o más)
• Para más de 4.000 agentes: 12GB de RAM, una CPU con cuatro núcleos a 3GHZ y disco duro muy rápido (15.000 rpm o más).

Requisitos mínimos de software:

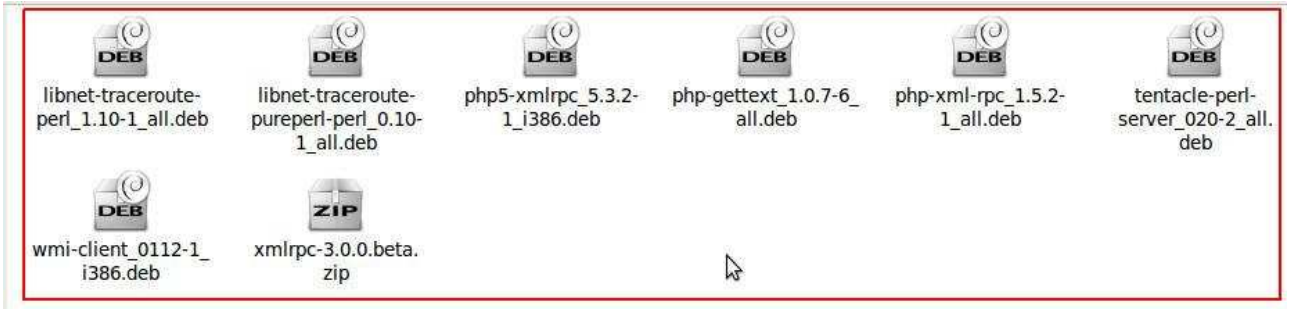
El agente puede ejecutarse en cualquier hardware que pueda ejecutar el sistema operativo mínimo requerido, siendo: Windows 2000 SP3 , Windows 2003 , Windows XP, Windows Vista , Windows 7 , Windows 2008 , SUSE Linux 10 , Ubuntu Linux 8.04 , Debian Linux , AIX 4.3.3 , HP-UX 11.x , Solaris 2.6 .

Instalación

Primero que todo nos bajamos los paquetes necesarios desde los repositorios de Pandora FMS, en la siguiente URL: http://sourceforge.net/projects/pandora/files/



Nota: En la anterior imagen mostramos subrayado algunos de los paquetes necesarios, tales como. El servidor, la consola y un agente, a continuación mostramos, otros paquetes que son necesarios los cuales se encuentran en este mismo repositorio.



- Lo siguiente que haremos sera agregar un repositorio en esta ruta /etc/apt/sources.list para no tener inconvenientes con algunos paquetes:

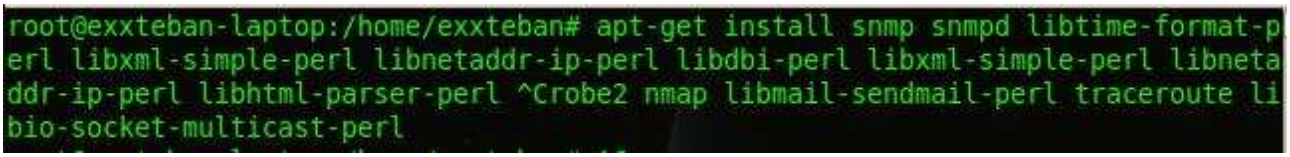
deb http://ftp.us.debian.org/debian sid main

- Actualizamos:

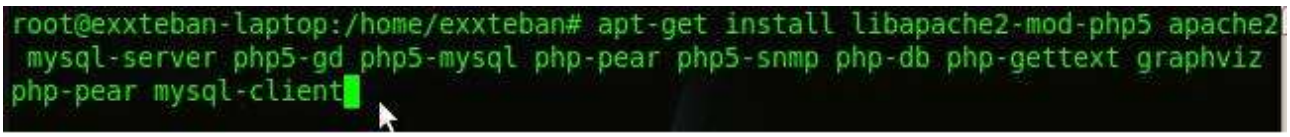
apt-get update

- A continuación instalaremos algunos paquetes que son necesarios para instalar Pandora FMS:

Del lado del servidor:



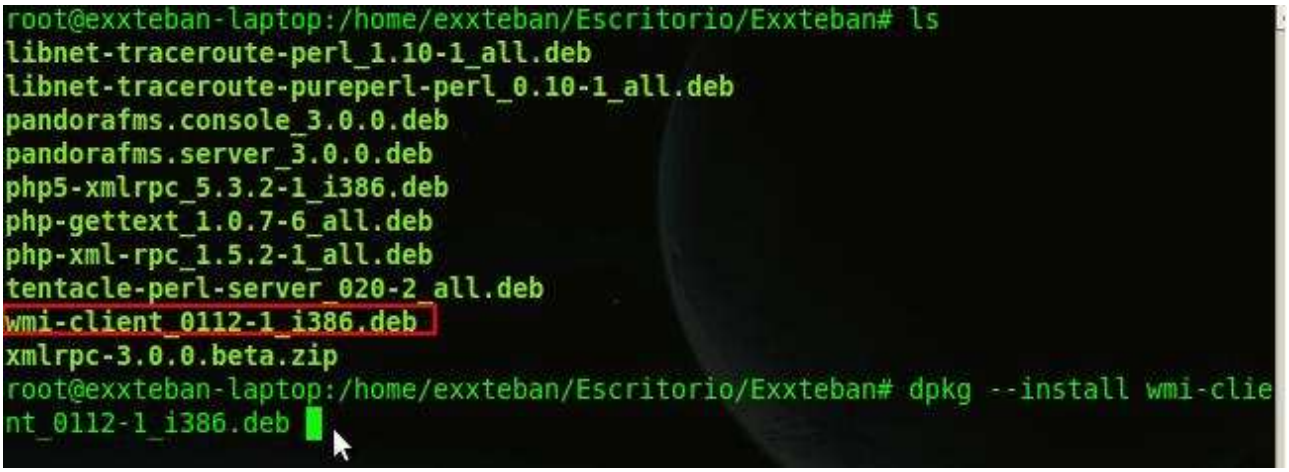
Del lado de consola:



Vamos a instalar algunas dependencias que nos faltan, nos ubicamos en la ruta donde nos hemos descargado los paquetes:

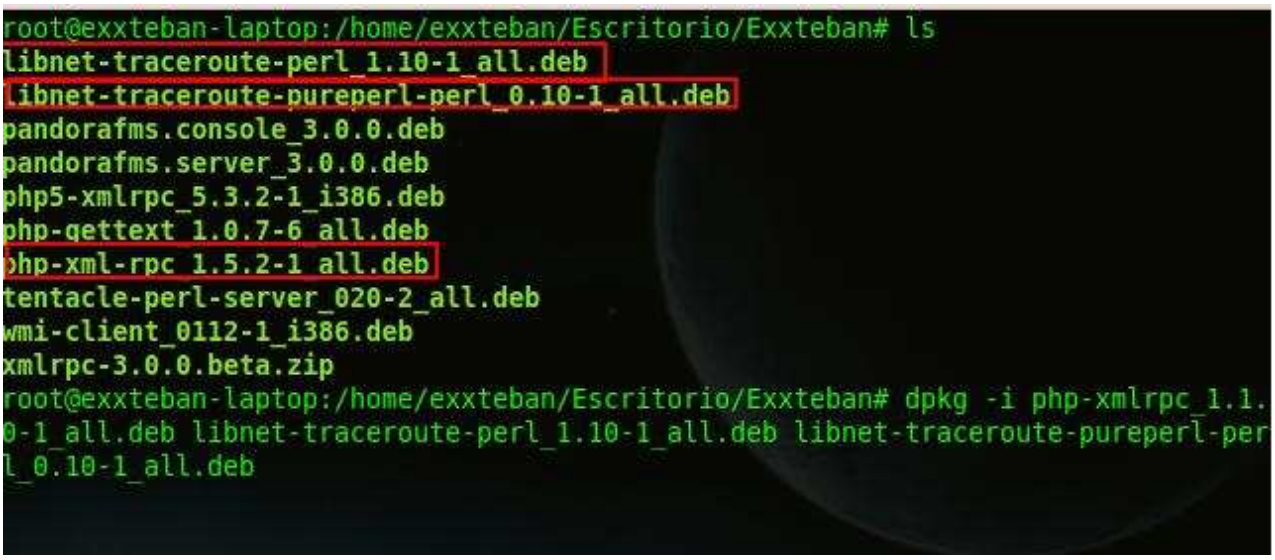
- **wmi-client**
- **php5-xmlrpc**

Instalamos Wmi-client

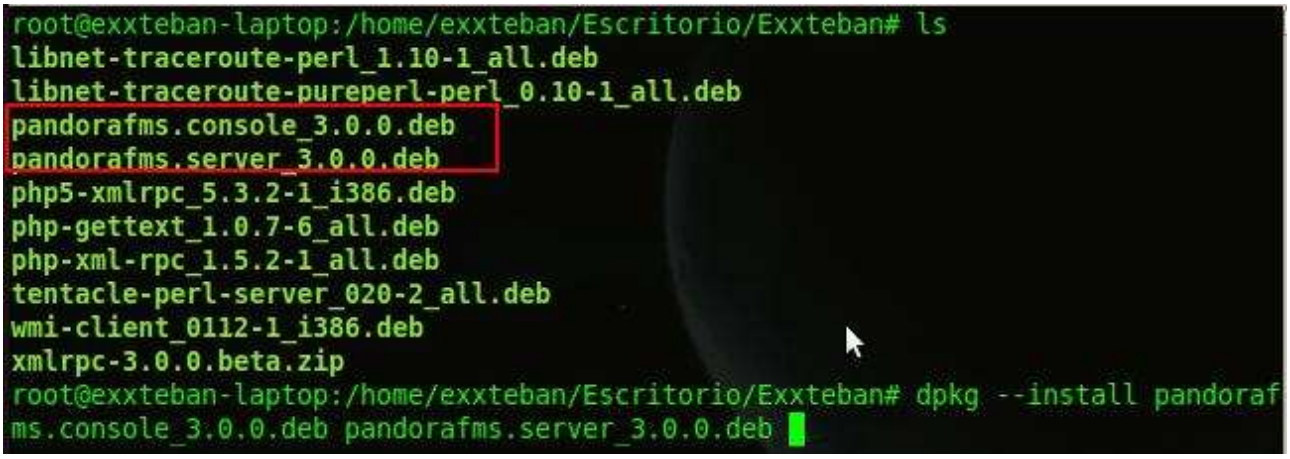


Instalamos php5-xmlrpc

Procedemos a instalar las siguientes dependencias, que debimos bajarlas previamente desde los repositorios de Pandora FMS:



- **Procedemos a instalar el servidor y la consola de Pandora FMS:**



Nota: Si nos saca un error por falta de dependencias podemos utilizar el comando **apt-get -f install**

- **Arrancamos los siguientes servicios**

Arrancamos Mysql:

/etc/init.d/mysql start

Si queremos tener una contraseña diferente en Mysql difenete a la que configuramos en el momento de la instalación lo podemos hacer con el siguiente comando:

mysqladmin password <la contraseña que queramos>

Arrancamos apache:

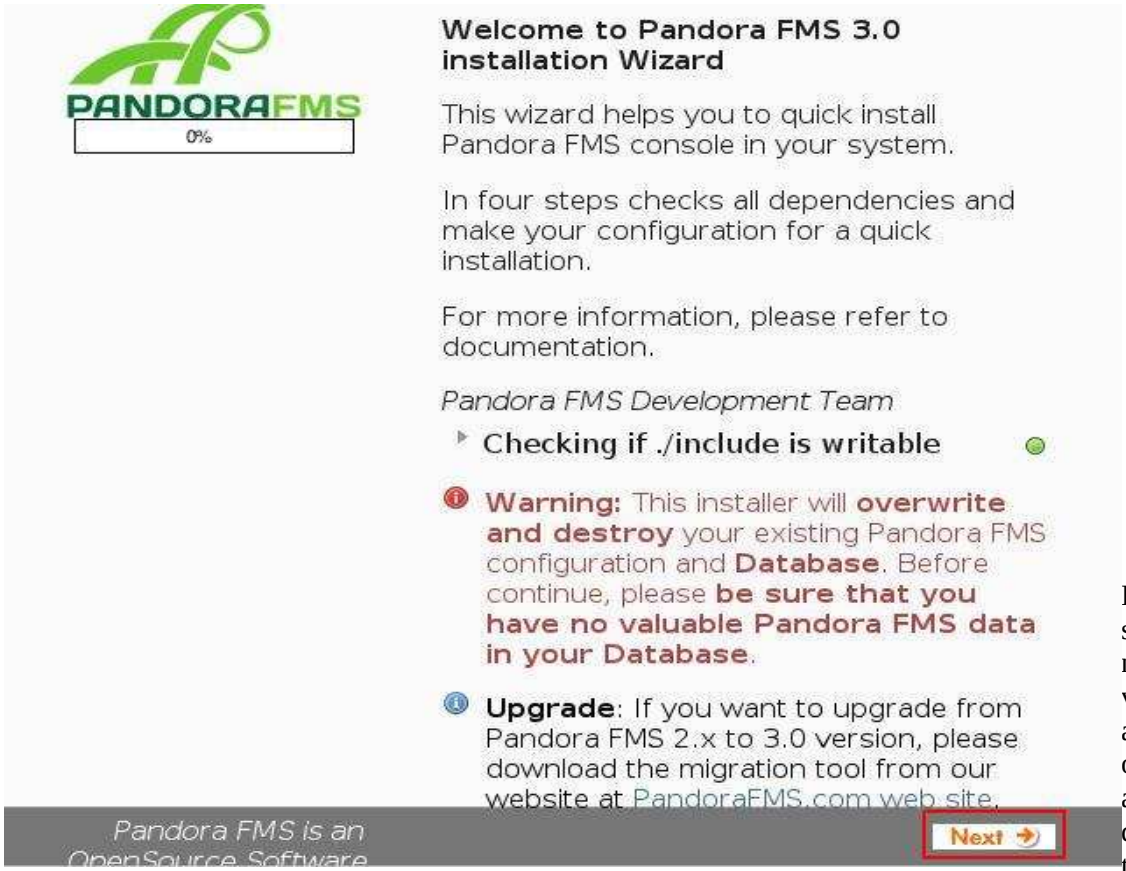
/etc/init.d/apache2 start

- **Instalando nuestra consola:**

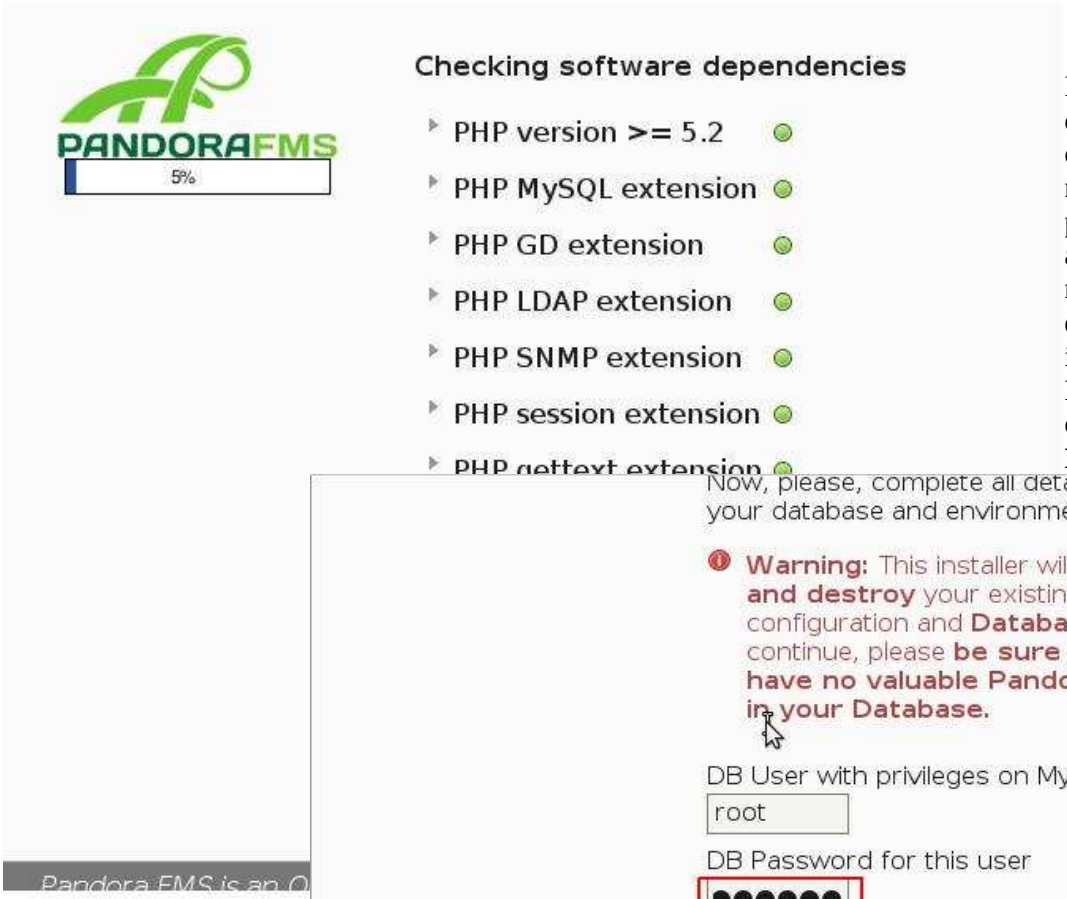
Ingresamos a nuestro navegador, y digitamos los siguiente:

http://localhost/pandora_console/install.php

Ingresamos en la siguiente ventana y damos clic en **Next:**

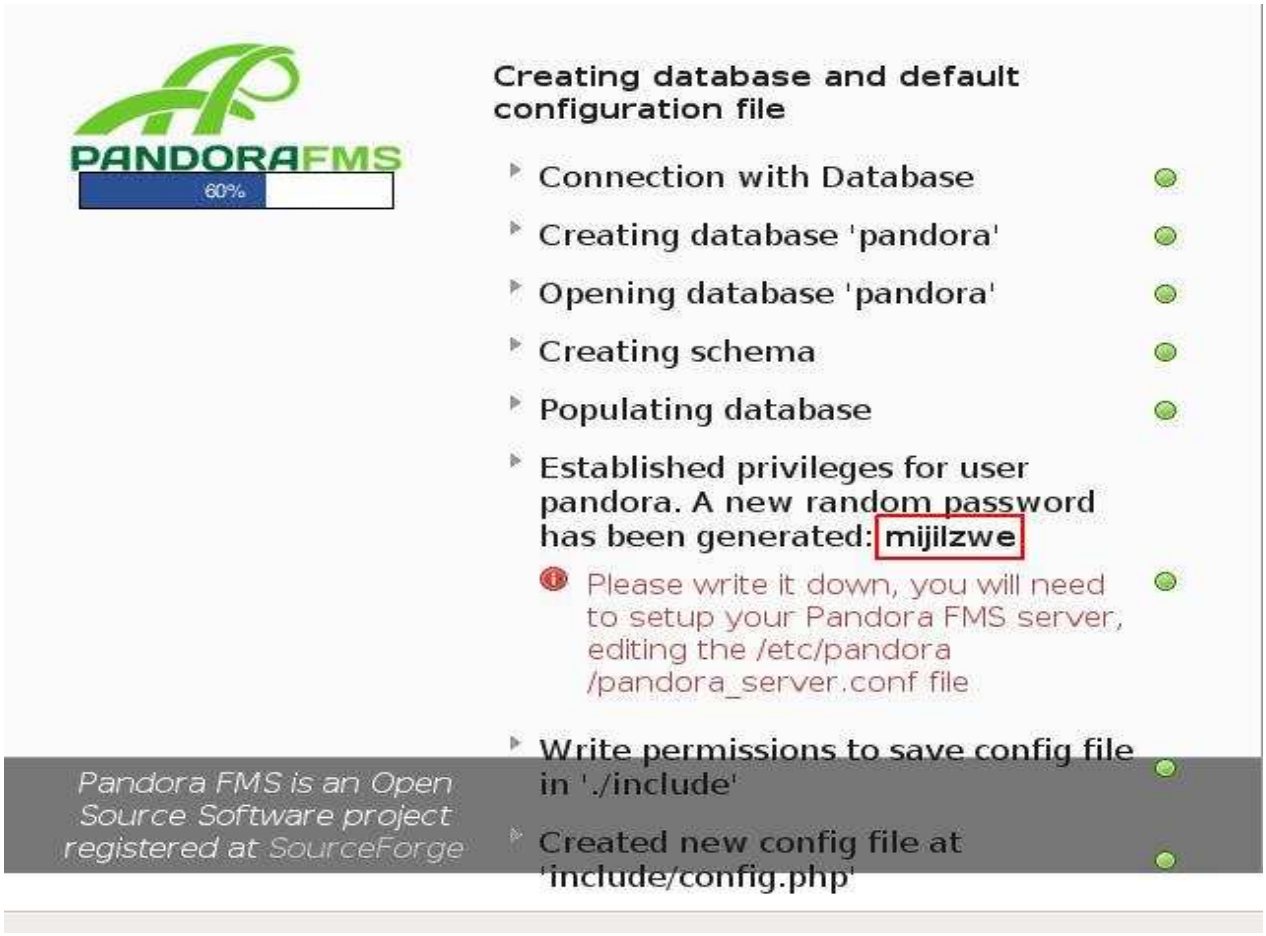


En la siguiente ventana observamos que todos los puntos estén en verde, ya que estos paquetes son necesarios, clic en **Next**:



Ingresamos la contraseña que pusimos al momento de instalar Mysql, clic en **Next:**

El siguiente paso es importante ya que debemos copiar la contraseña aleatoria que nos da, en la imagen aparece subrayada en rojo, clic en **Next:**



Finalmente nos muestra esta imagen que nos dice que para poder acceder a la consola debemos borrar el fichero **install.php:**

Ingresamos en la siguiente ruta **/etc/pandora/pandora_server.conf** y buscamos las siguiente linea:

dbpass pandora

y la editamos con la contraseña que se nos arrojo en el momento de la instalación, en nuestro caso quedaría algo como:

dbpass mijilzwe

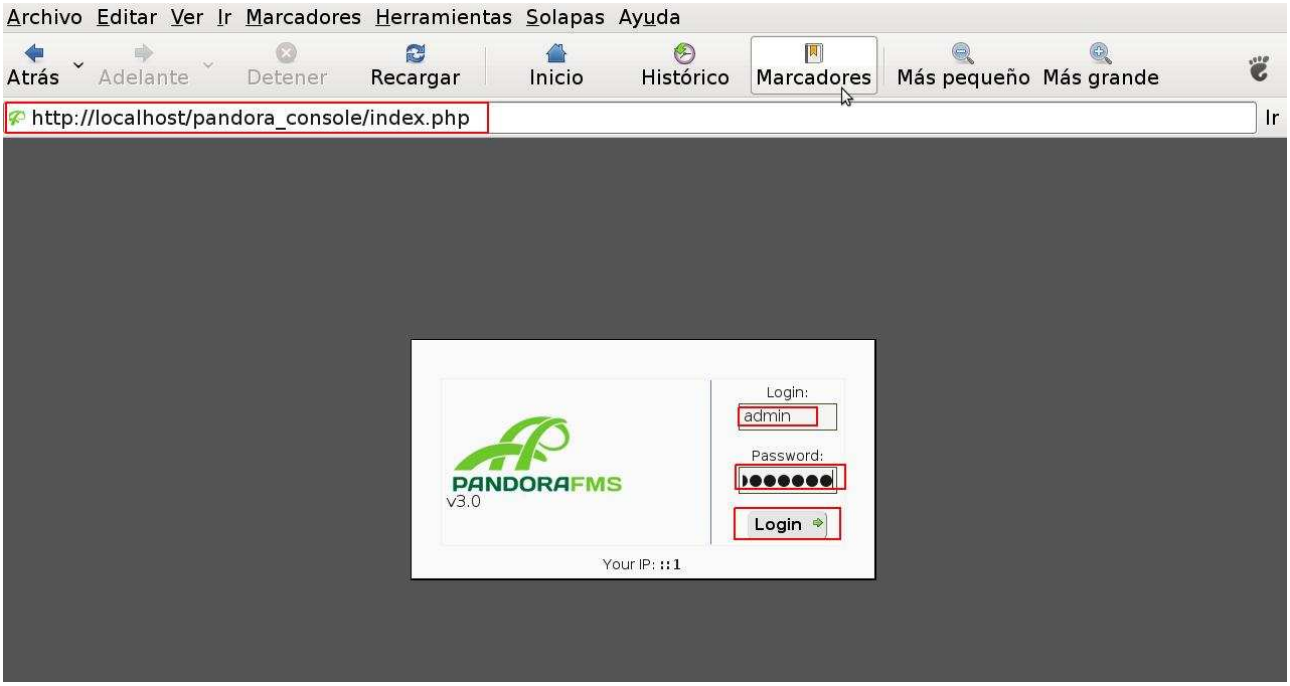
```
  GNU nano 2.0.7     Fichero: /etc/pandora/pandora_server.conf

# dbuser:  Database user name (pandora by default)

dbuser pandora

# daemon: Runs in daemon mode (background) if 1, if 0 runs in foreground
# this could be setup on command line with -D option

# daemon 1

# dbpass: Database password

dbpass mijilzwe

# dbhost: Database hostname or IP address

dbhost localhost

# verbosity: level of detail on errors/messages (0 default, 1 verbose, 2 debug.$
# -v in command line (verbose) or -d (debug)
```

Borramos el archivo **install.php** que comentábamos mas arriba, para esto ingresamos en la siguiente ruta **/var/www/pandora_console,** y borramos el **install.php** tal como esta en la imagen:

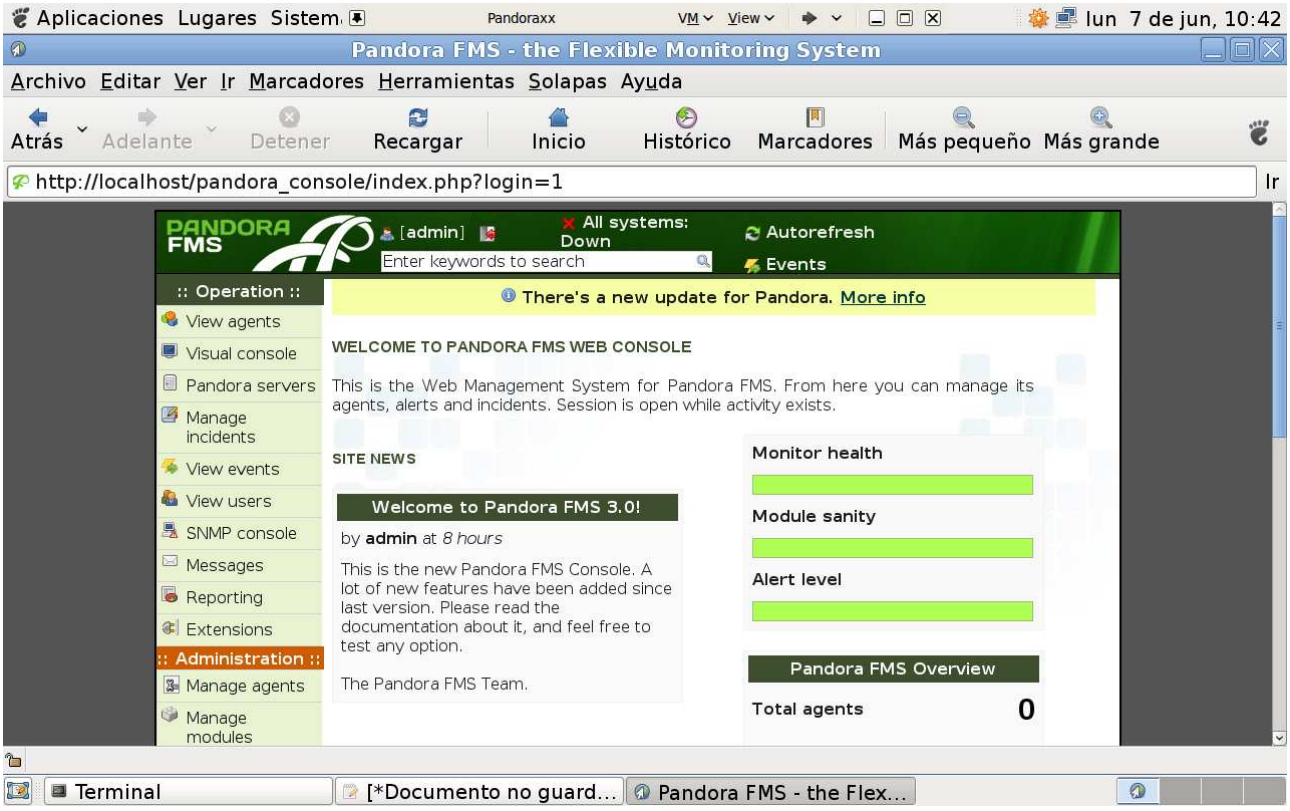
```
pandora:~# cd /var/www/pandora_console/
pandora:/var/www/pandora_console# ls
ajax.php    COPYING     godmode    install.php              pandoradb_data
attachment  extensions  images     operation                pandoradb.sql
AUTHORS     extras      include    pandora_console_install
ChangeLog   general     index.php  pandora_console_upgrade
pandora:/var/www/pandora_console# rm -R install.php
pandora:/var/www/pandora_console#
```

- Finalmente ingresamos en la consola de administración, para esto digitamos en el navegador:

http://localhost/pandora_console



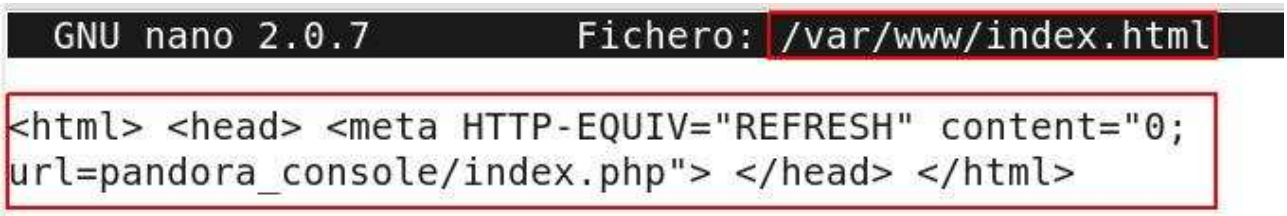
- Después de ingresar nos aparecerá esta ventana donde tenemos una serie de opciones para configurar nuestro server:



- **Bonus track**

Podemos hacer que cada vez que vayamos a ingresar a configurar Pandora FMS lo podamos hacer simplemente digitando la dirección ip en nuestro navegador, para esto ingresamos el index de apache he

ingresamos las lineas que aparecen en la imagen a continuación:



Después de guardarlo y reiniciar apache, digitamos en nuestro navegador:

http://<nuestra dirección ip>

Configuración de los agentes:

Que es un agente

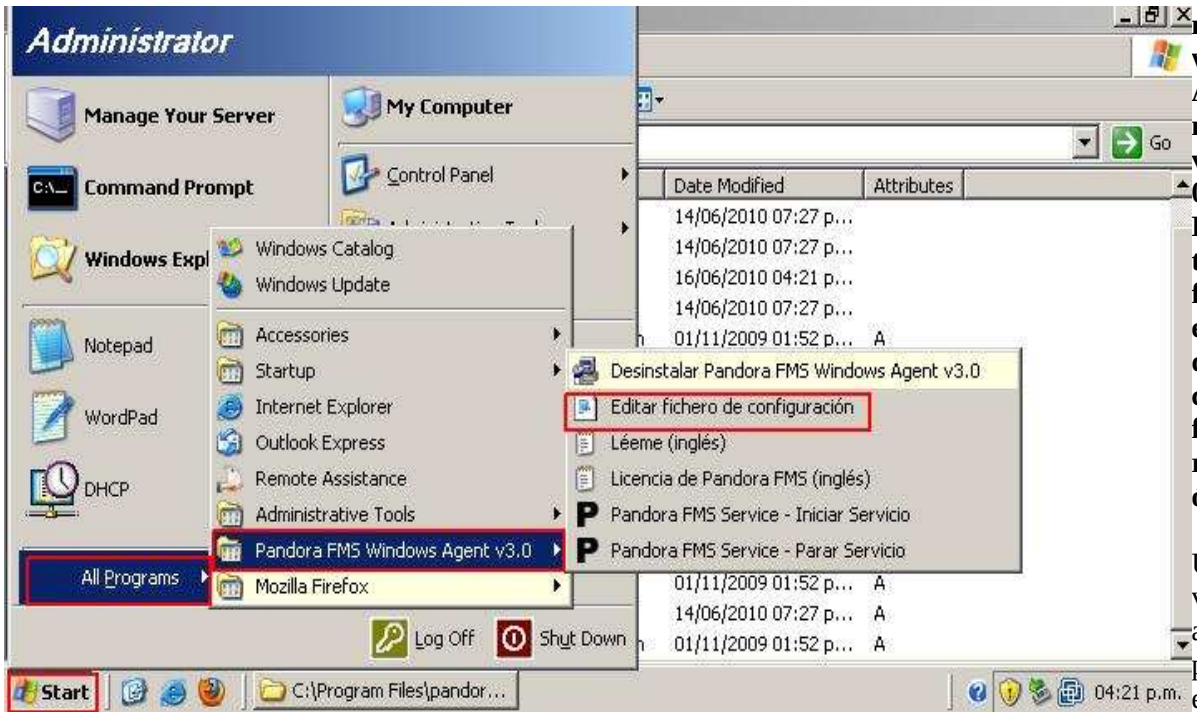
Son los que recogen informes estadísticas y demás desde una maquina hacia un servidor que es el encargado de gestionar dicha información, esta información la recibe en formato de ficheros con extensión XML, además esta contenida en el servidor en unos contenedores llamados módulos. Están desarrollados para trabajar en una plataforma fija, generalmente Windows o Unix.

Configuración del fichero pandora_agent.conf

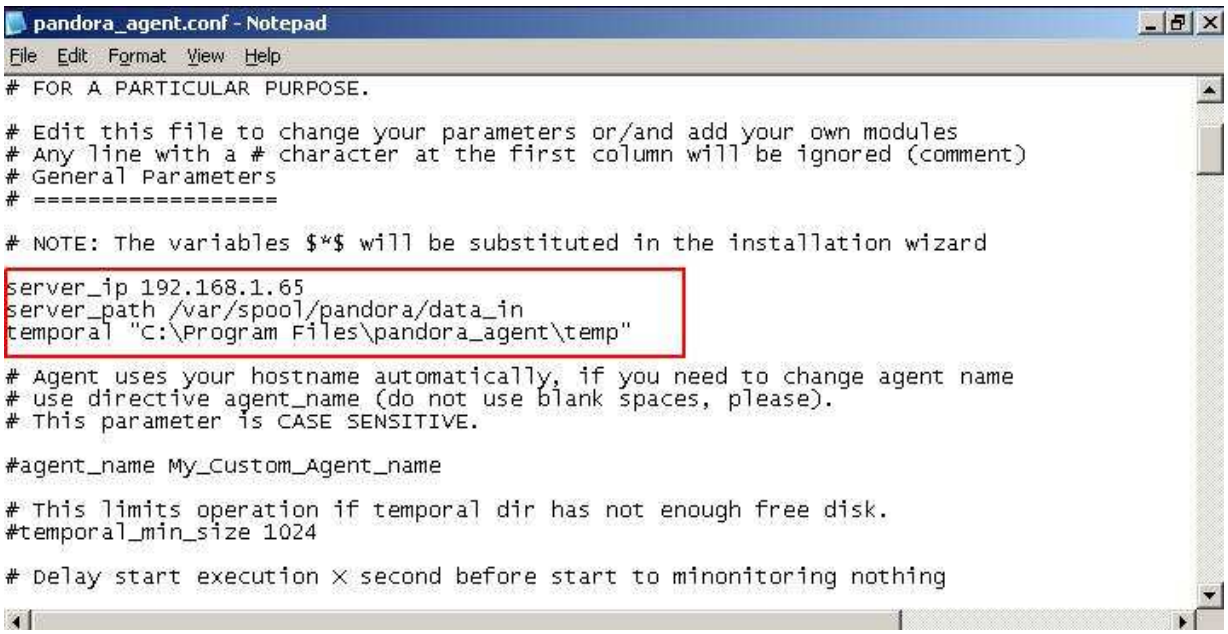
Prácticamente la configuración de este fichero es igual tanto para sistemas Windows como para sistemas Unix, en sistemas Unix lo ubicamos en la siguiente ruta: **/etc/pandora/pandora_agent.conf**, por lo tanto en sistemas Windows lo ubicamos en la siguiente ruta: **C:\Program Files\pandora_agent.**

Configuración en un agente Windows:

Podemos proceder a editar este archivo en la siguiente ruta: **Inicio>todos los programas>Pandora FMS Windows Agent v3.0> Editar fichero de configuración**



Una vez allí podemos ver algunas lineas por defecto que seria importante aclararlas:

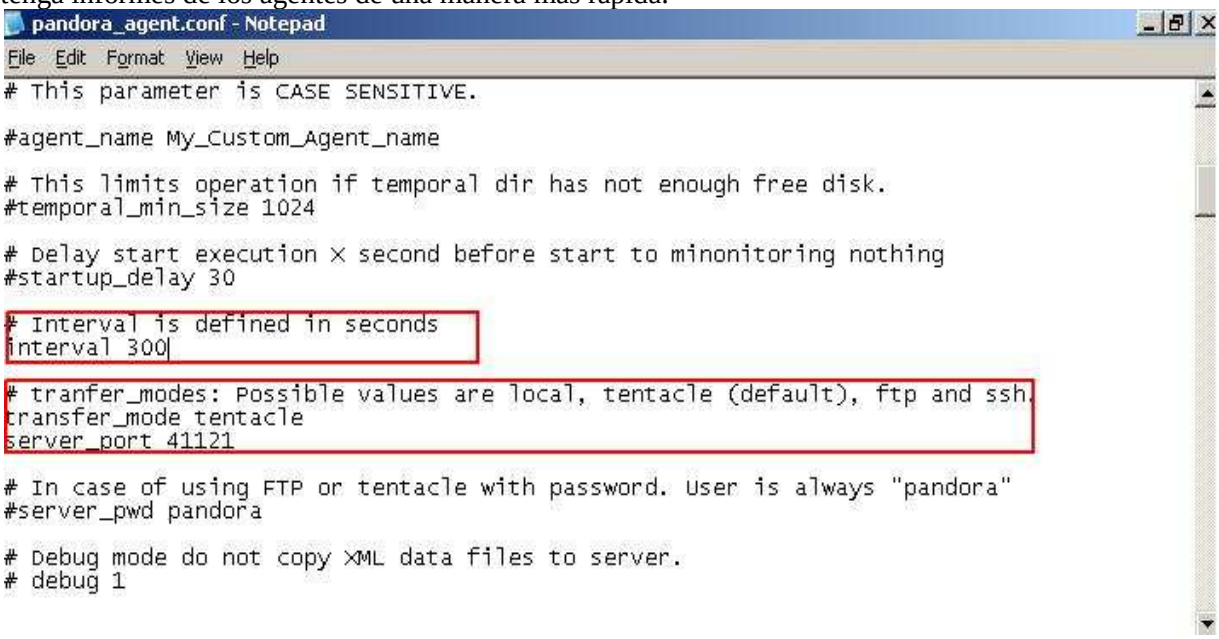


Server_ip: Allí debe ir la dirección de nuestro servidor.

Server_path: esta es la ruta donde el servidor almacena los datos enviados por el agente.

Temporal: es la ruta donde esta la carpeta donde se almacenan los datos, antes de ser enviados a el servidor.

A continuación mostraremos una linea que es importante cambiarle, si queremos que nuestro servidor obtenga informes de los agentes de una manera mas rápida:



- La linea que dice **interval 300 s**ignifica que cada 300 segundos= 5 minutos, el agente actualizara los sucesos que ocurran en la maquina local, y luego enviara el informe al servidor, yo recomendaría que cambiásemos la cantidad de segundos a una cantidad menor, aunque dependerá de las necesidades de cada quien.
- La linea que dice **server_port 41121 c**orresponde al puerto por defecto que utiliza Tentacle server, Tentacle lo que hace al igual que WMI es recoger información de la maquina local, podría decirse que es el protocolo con el cual trabaja el agente, aunque Tentacle esta mas orientado a trabajar en maquinas Linux, ya que el protocolo de Windows normalmente es WMI.

Para mirar los logs del agente: Ingresamos en la siguiente ruta

- **C:\archivos de programa\pandora_agent\pandora_agent.log**

Agregando módulos:

Modulo de un servicio

Bueno, como primera practica vamos a mirar como se agrega un modulo desde el archivo de configuración en el agente Pandora. Para este ejemplo agregaremos un servidor DHCP, y veremos como automáticamente aparece en la consola del server Pandora FMS, a continuación explicaremos linea por linea.

module_begin ------> Tal y como en un algoritmo, es obligatorio definir un **inicio** y un final.

module_name Service_DHCPServer ------> Es el nombre del proceso que vamos a monitorear. No podemos tener dos nombres iguales en un mismo agente.

module_type generic_proc -------> Hay varios tipos de módulos, pero en este ejemplo nos hablan de el tipo: **generic_proc.** Este lo que hace es medir el estado de un proceso o servicio, se asigna un valor "0" a un estado erroneo, y a cualquier estado en "1" o por encima de "1" es correcto.

module_service DHCPServer ------->Comprueba si un determinado servicio se está ejecutando en la máquina, si el nombre del servicio contiene espacios, debemos encerrarlo entre ""

module_description Service DHCP Server ------> Se utiliza para añadir un comentario al modulo.

module_end ------> Tal y como en un algoritmo, es obligatorio definir un inicio y un **final**.

Ahora miremos como se ve en nuestra consola:

Nota: Antes debemos aplicar los cambios y para esto debemos reiniciar el agente los hacemos en los siguientes dos pasos:

Inicio>todos los programas>Pandora FMS Windows Agent v3.0> Pandora FMS Service - Parar Servicio

Inicio>todos los programas>Pandora FMS Windows Agent v3.0> Pandora FMS Service - Iniciar

Servicio
Ahora si veamos nuestra consola, y miremos los pasos para acceder a mirar los módulos que tiene nuestro agente:

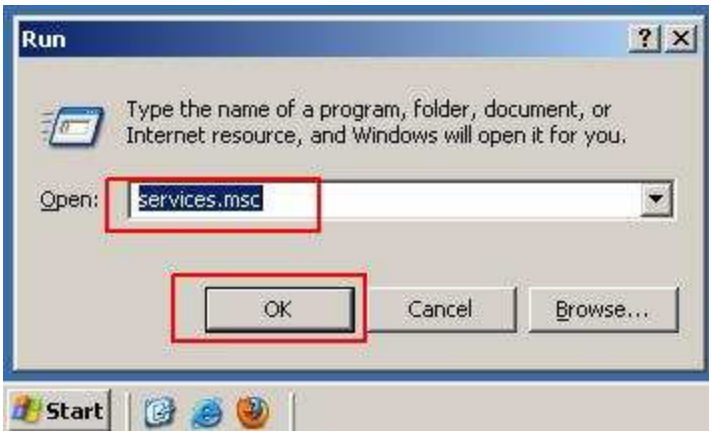
- Una vez logiados en la consola de nuestro servidor, vamos a dar clic al lado izquierdo en el botón que dice: **Manage Agents,** y luego al ubicarnos en el nombre del agente nos aparece una opción que dice **View**, damos clic allí.

- Luego podemos observar nuestros módulos, y allí ubicamos el modulo de DHCP que acabamos de agregar.

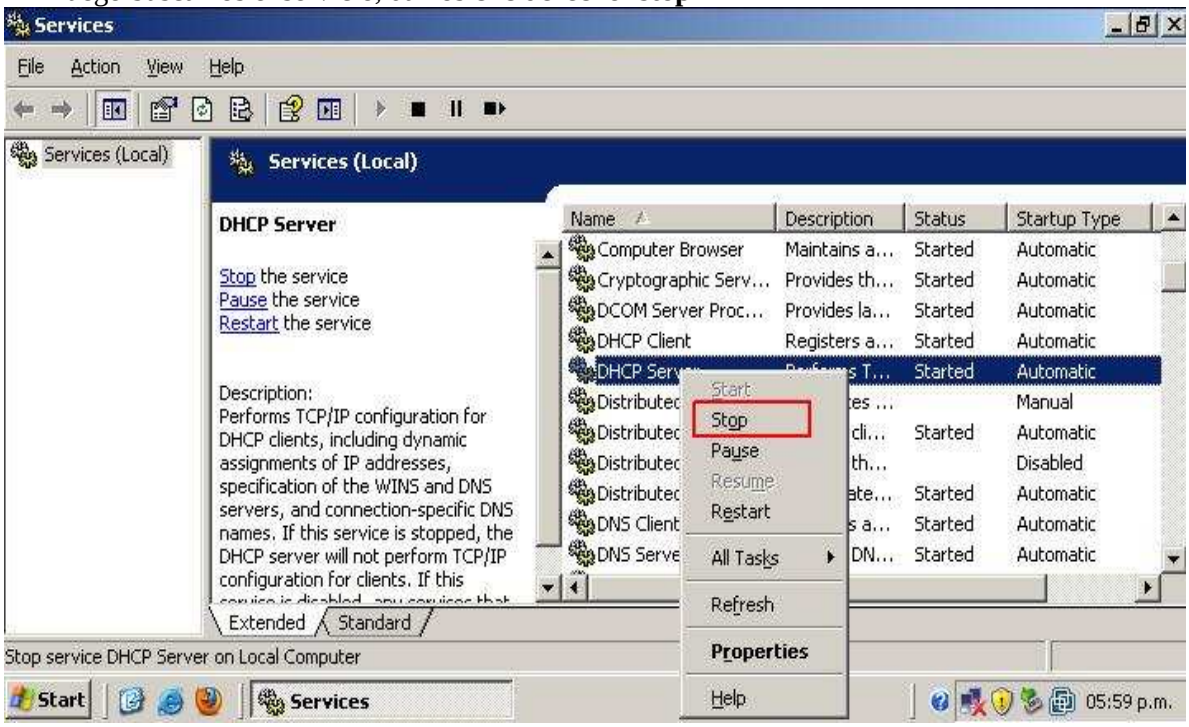
Nota: El cuadro que vemos en verde significa que el servicio esta en un estado correcto. Mas adelante veremos mas detalladamente el significado de cada color.

Ahora haremos una prueba:

- Vamos a tumbar el servicio DHCP, y veremos el comportamiento en nuestra consola, a continuación ingresamos en nuestro Windows server y procedemos a para el servicio DHCP de la siguiente forma:
-
- Vamos a **inicio>ejecutar>services.msc**



- Luego buscamos el servicio, damos **clic derecho>stop**

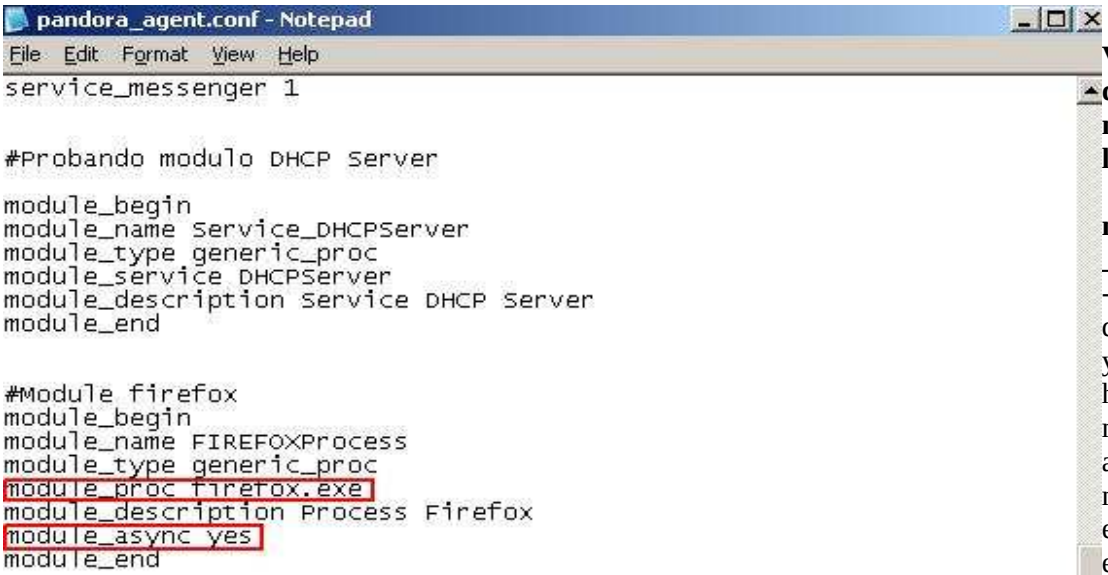


- Observamos en la consola de nuestro servidor, como el modulo cambia a color rojo:

Nota: El color rojo indica que el servicio o proceso esta en un estado critico, Además debemos recordar que hay que actualizar para poder ver los efectos.

Modulo de un proceso:

Comprueba si un proceso esta corriendo o no en a maquina local. Debemos tener en cuenta que si el nombre del proceso tiene espacios, **no debemos poner “”,** el nombre del proceso debe ir tal cual se ve en el administrador de procesos de windows, y diferencia entre mayúsculas y minúsculas. Para este ejemplo vamos a monitorear a firefox mozilla:

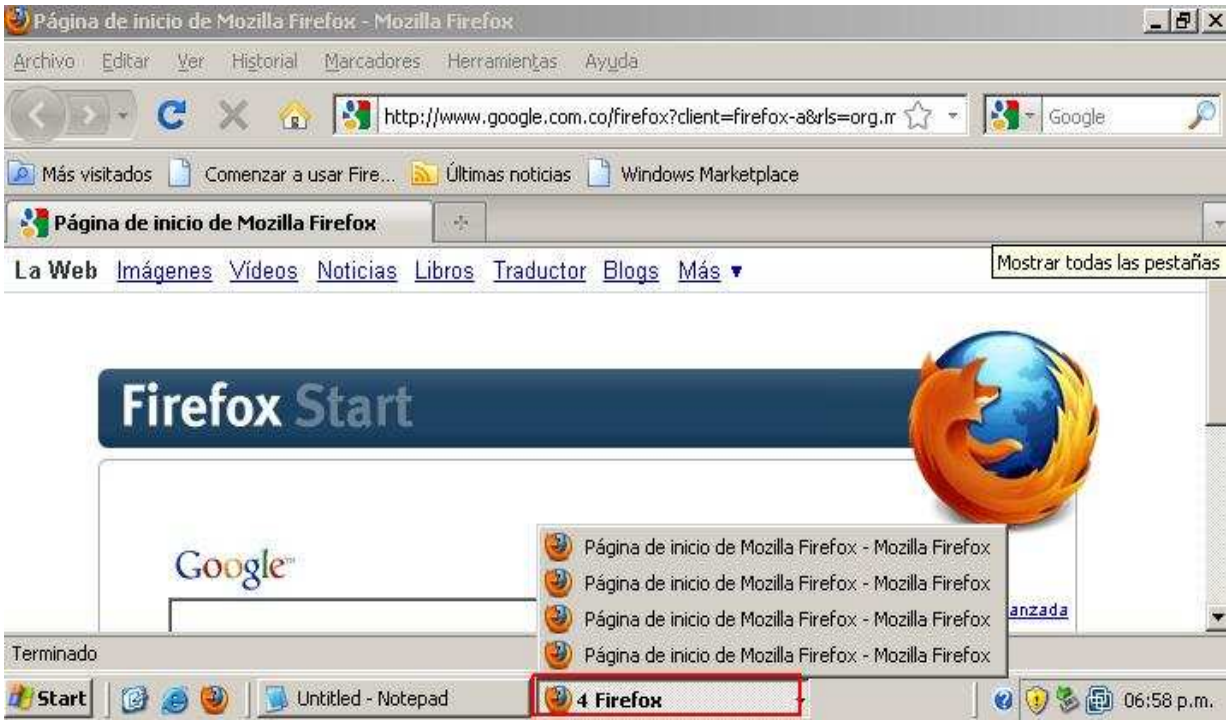


Vemos dos nuevas linea:

module_proc -----> de esta ya hablábamos anteriormente y es la encargada de ver si un proceso esta corriendo o no en a maquina local

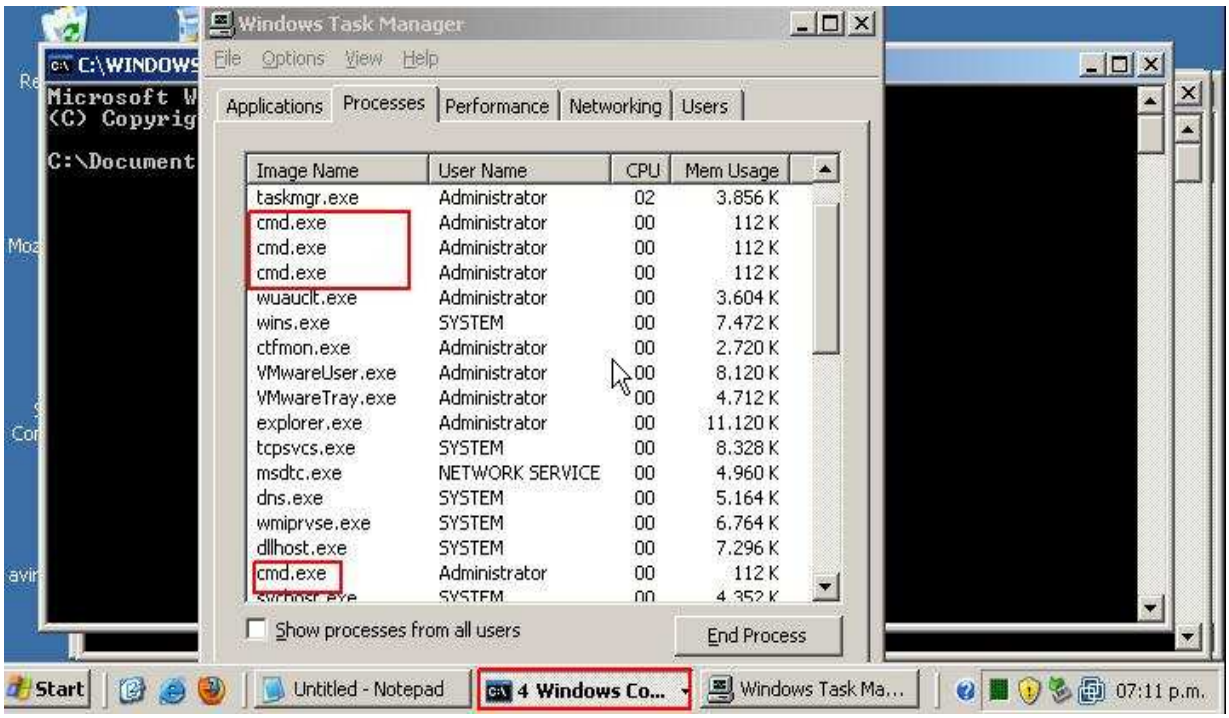
module_async yes -------> Sirve para notificar inmediatamente cuando un proceso cambia de estado.

- Antes de ingresar en nuestra consola y verificar si el modulo se ha agregado, vamos a abrir 4 ventanas de firefox:



- Vamos a nuestra consola y verificamos el modulo

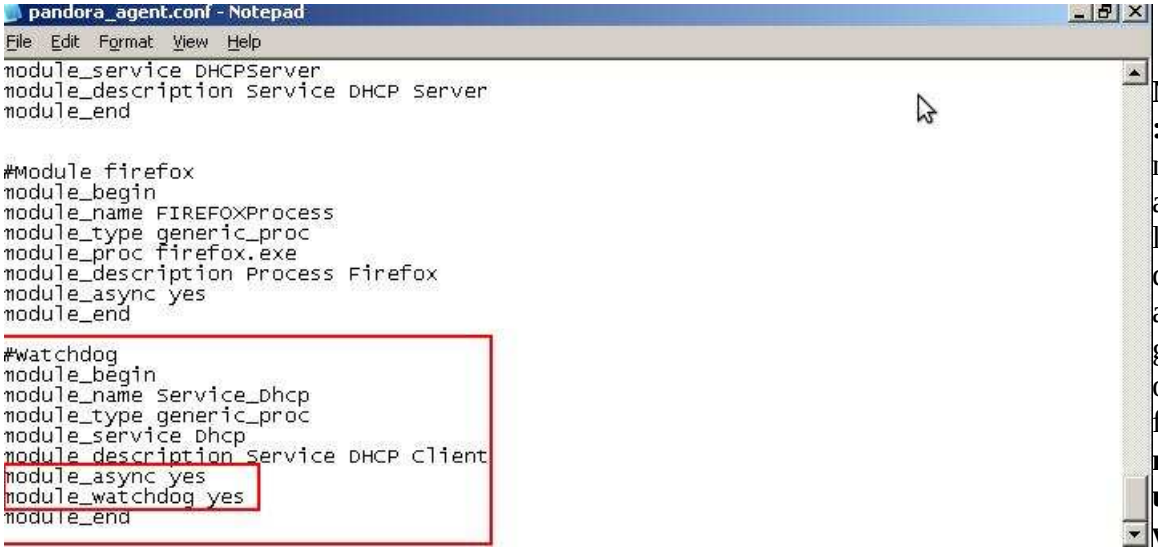
Nota: Vemos que efectivamente nos reconoce el modulo, pero en la cantidad de procesos, nos aparece solo uno, investigue un poco mas, y me doy cuenta de que firefox como otras aplicaciones, manejan un solo proceso, así tenga abierta varias ventanas, todo dependerá como se vea en el administrador de procesos. Veamos como a diferencia de firefox, la consola de Windows al momento de abrir varias ventanas, se manejan diferentes procesos:



Nota: Vemos como tengo abiertas cuatro consolas, y en el administrador de procesos aparecen en diferentes procesos, cosa que no pasa con firefox, queda de tarea ensayar con el proceso de cmd y luego mirar en la consola cual es el comportamiento.

Modulos Watchdog:

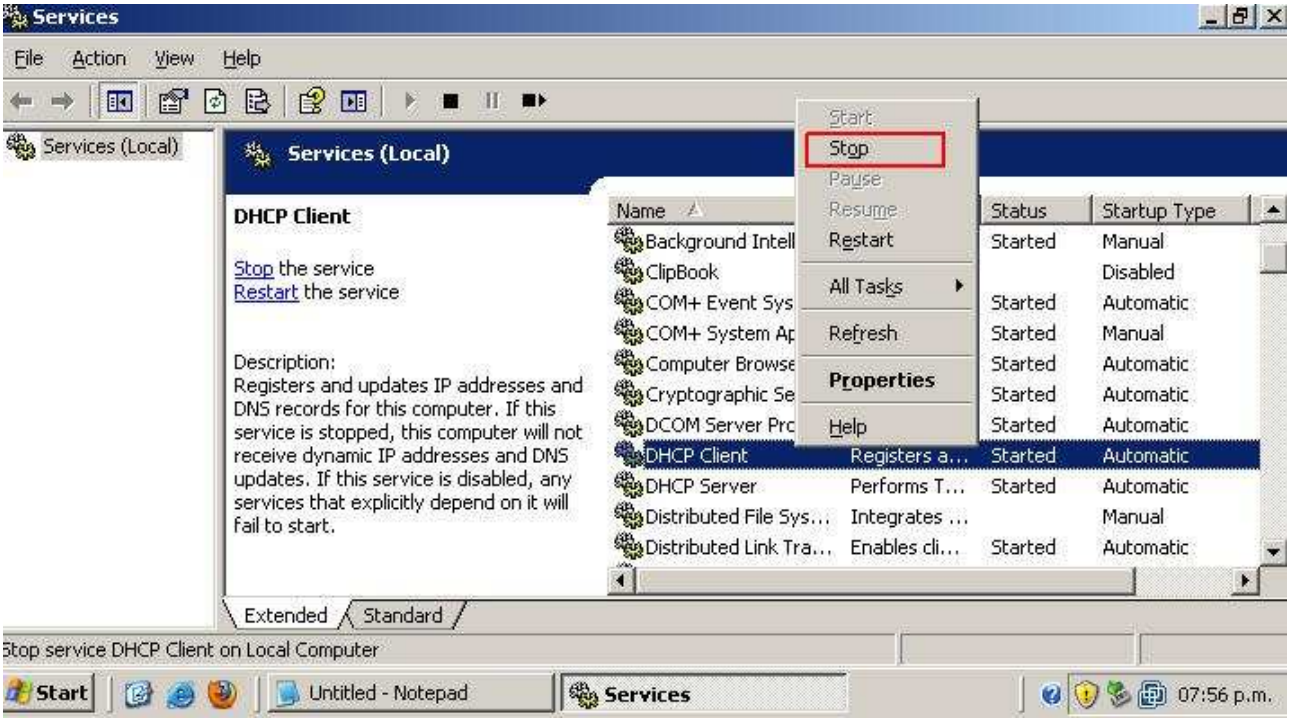
Primeramente vamos a implementar uno sencillo. Antes que nada, los módulos watchdog lo que hacen es: Al caerse un servicio ellos vuelven y lo inician, de forma que este es un excelente modulo que nos ayudara mucho, otro aspecto a tener es que solo funciona cuando el modulo esta en modo asíncrono, osea con la linea **module_async yes,** veamos entonces su implementación, y esta vez probaremos con el servicio cliente de DHCP.



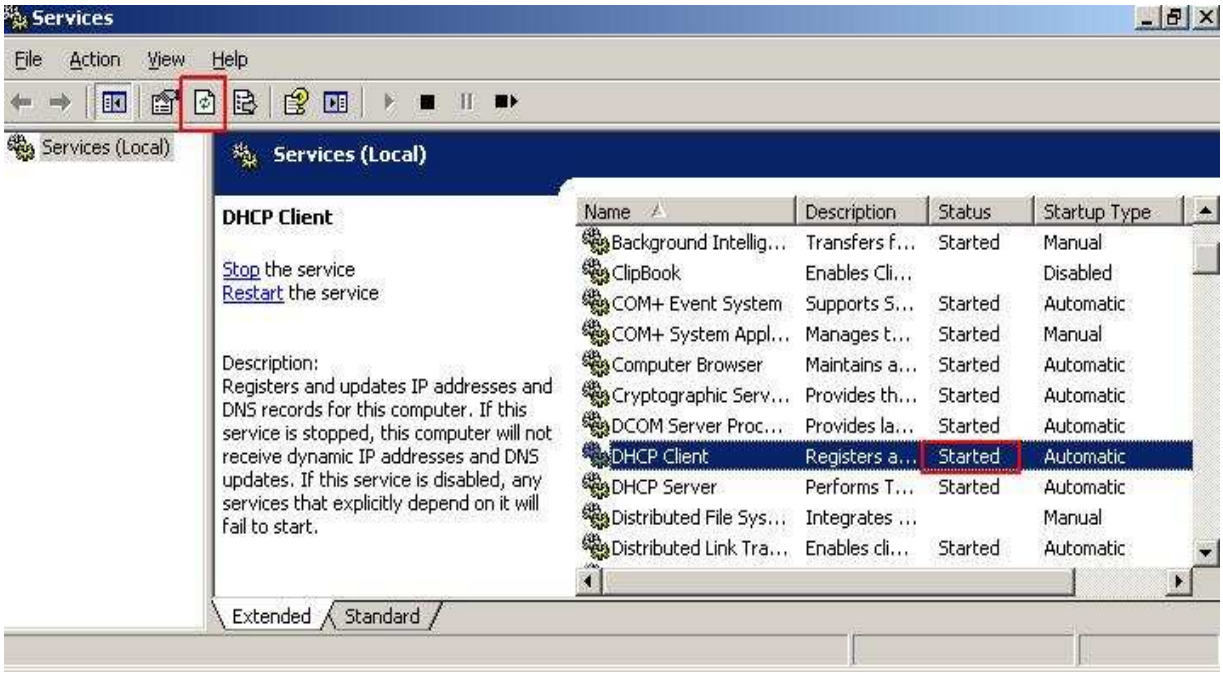
Nota: La nueva linea que agregamos fue: **module_watchdog yes.**

Ahora veamos el efecto:

- Damos **Stop** a nuestro servicio



- Una vez el servicio pare, procedemos a actualizar tal y como vemos en la pantalla, y



podemos ver que nuevamente esta iniciado:

Configurando un agente Linux:

Explicaremos a continuación las rutas mas importantes con las cuales trabaja nuestro agente Pandora:

/etc/pandora/pandora_agent.conf -----------> Esta es la ruta donde esta el fichero de configuración de nuestro agente, acá definimos los datos a recoger y algunas otras políticas que veremos mas adelante.

usr/bin/tentacle_client -----> El agente tentacle en plataformas Linux es el encargado de enviar los datos recogidos al servidor Pandora.

/etc/init.d/pandora_agent_daemon <stop/start/restart> -------> Con este mandato lanzamos, detenemos o reiniciamos nuestro demonio.

/var/log/pandora/pandora_agent.conf----> como su nombre lo indica, nos sirve para mirar los log del agente de Pandora.

Configurando nuestro primer modulo:

A continuación vamos a configurar un modulo, que nos mostrara cuantas visitas se han hecho a la pagina principal de un servidor apache. Recordemos entonces que previamente debemos instalar un servidor apache y además una vez hecha nuestras modificaciones en el archivo de configuración del agente, debemos reiniciar, lo veremos a continuación.

Ingresamos en:

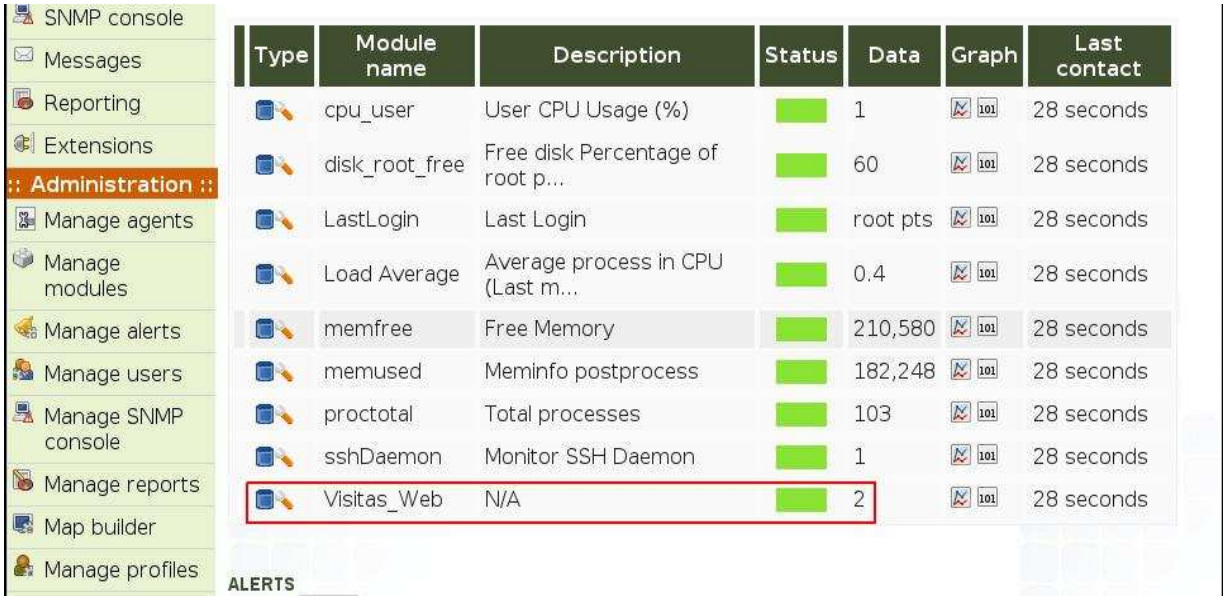
/etc/pandora/pandora_agent.conf

Ingresamos los datos que aparecen subrayados en verde, y luego guardamos:

Vamos a probarlo:

Lo primero que haremos sera mirar los log de apache, y veremos cuantas visitas hemos tenido, debo aclarar que hemos puesto a que busque la "/ " en vez del "**index**" ya que no nos registraba al ingresar en la pagina un log **index** a menos que pusiéramos algo como: www.humanlinks.com/index.html, entonces nos ha tocado poner la raíz como patrón de contabilización. Ahora vamos a ver que nos arroja los log de apache en nuestro agente Pandora:

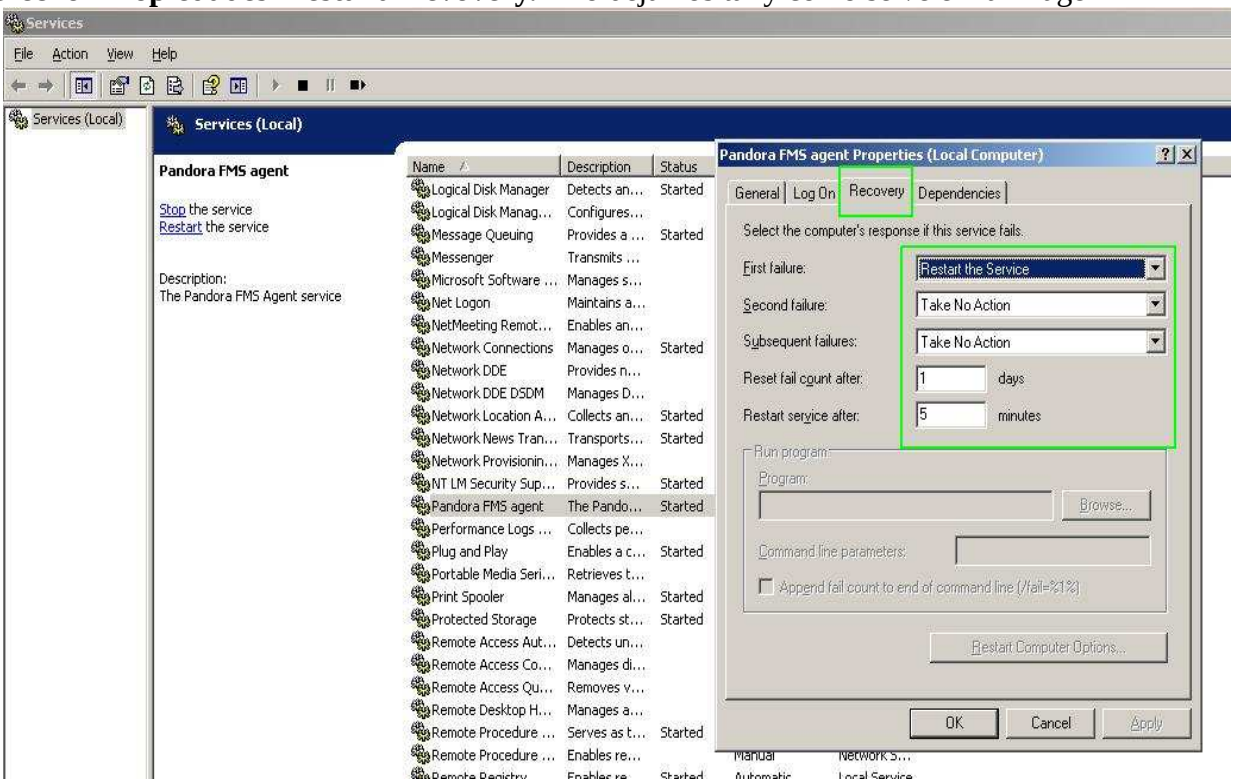
Vemos que el nos ha registrado **2** visitas, ahora vamos a nuestro server Pandora y verificamos el modulo.



También podemos ver como en la parte subrayada en rojo, nos muestra en la columna Data, que hemos tenido 2 visitas.

Modo de recuperación:

Debemos tener en cuenta a futuro, que se podría ocasionar una caída del servicio de Pandora en uno de nuestros agentes, aunque no debería ocurrir, siempre es mejor estar prevenido, y deberíamos fijarnos en el servicio de Pandora que corre en los host clientes, que tengamos el servicio configurado para que se vuelva a reiniciar solo, en caso de una caída, para esto vamos a **Inicio>Ejecutar>Services.msc>Pandora FMS Agent**. Luego damos **click derecho>Propiedades>Pestaña Revovery.** Y lo dejamos tal y como se ve en la imagen



Vemos en la imagen que hemos definido que el primer fallo del sistema, se reinicie el servicio una vez por día, pero si falla mas de una vez por día, no debe hacer nada. Esto se da porque podemos saturar mucho la memoria RAM, o porque a lo mejor la caída se deba a problemas internos de la maquina, ya que Pandora no debería caerse mas de una vez por día.

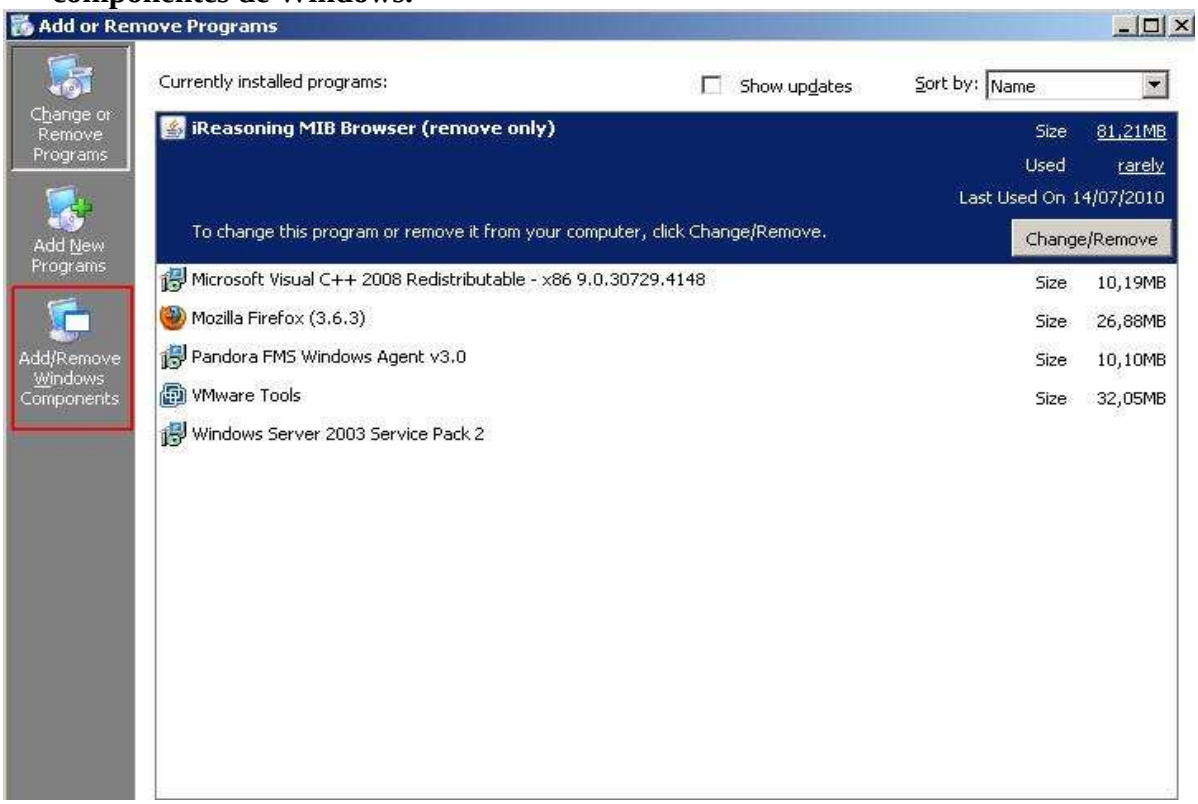
Otra forma de reiniciarlo seria con la opción de tareas programadas de Windows, o también con el comando **at**.

SNMP

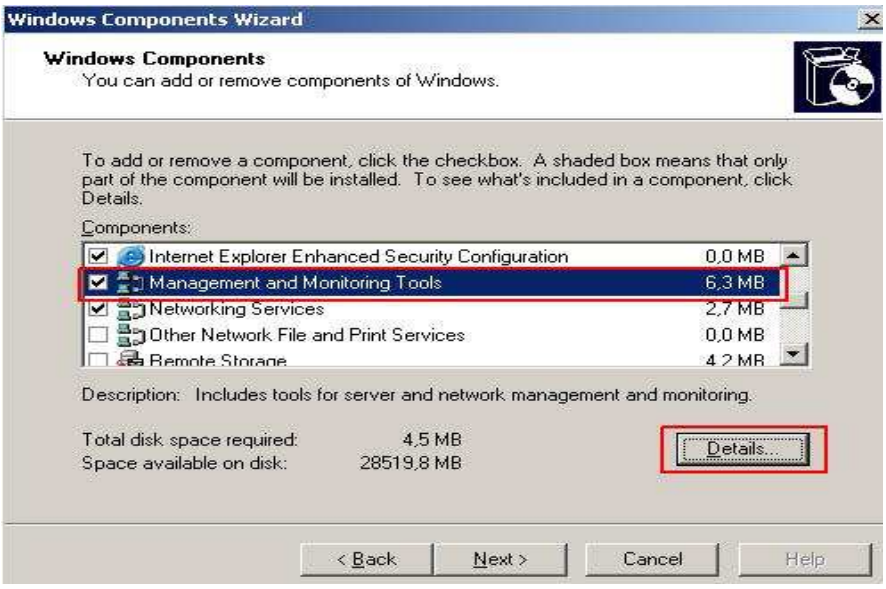
Instalar SNMP en Windows 2003 server

Nota: recordemos que antes de instalar cualquier servicio adicional en nuestro server Windows 2003 server, debemos tener a la mano el CD de instalación.

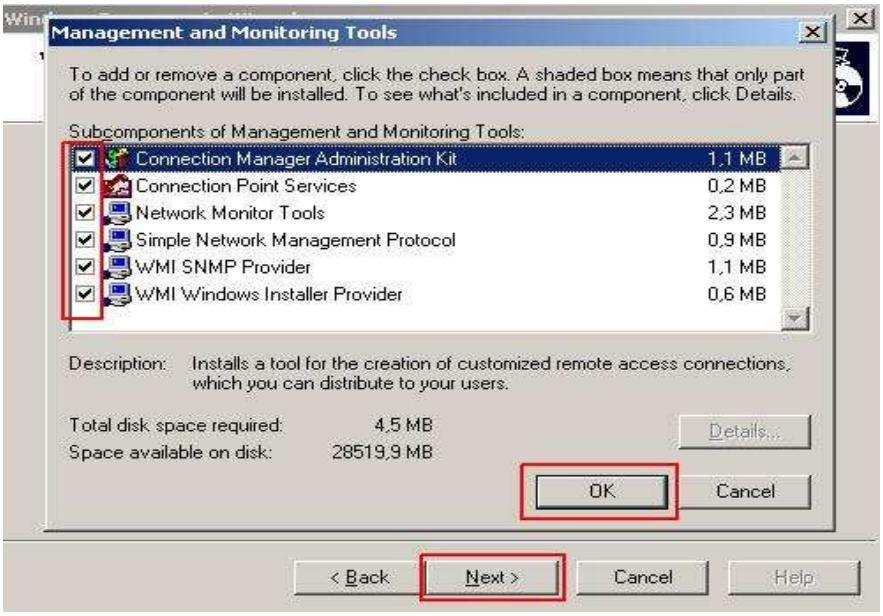
- Vamos a **Inicio>Panel de control> Agregar o quitar programas>Agregar o quitar componentes de Windows.**



- Luego seleccionamos la casilla donde dice: **Herramientas de administración y monitoreo>Clic en Detalles:**

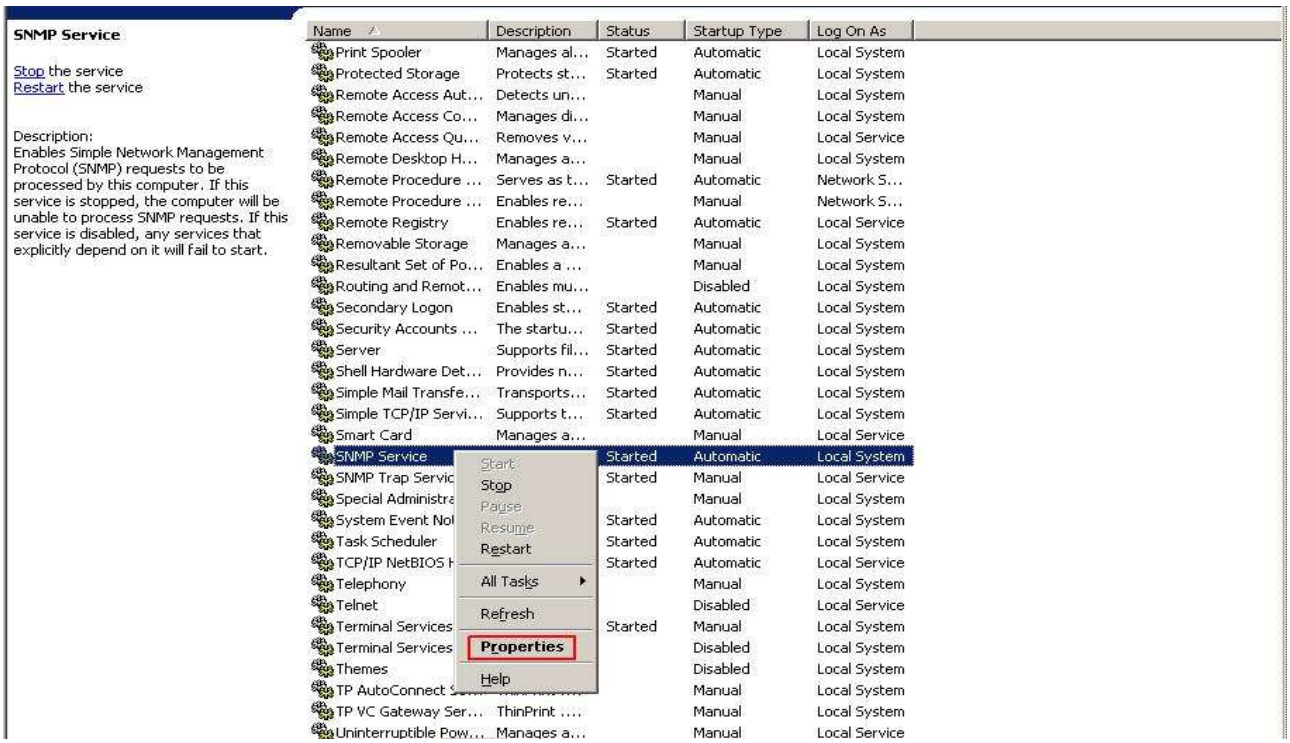


- Luego verificamos que todas las casillas esten seleccionadas tal y como vemos en la imagen, luego damos clic en “Ok” y luego clic en “Next”

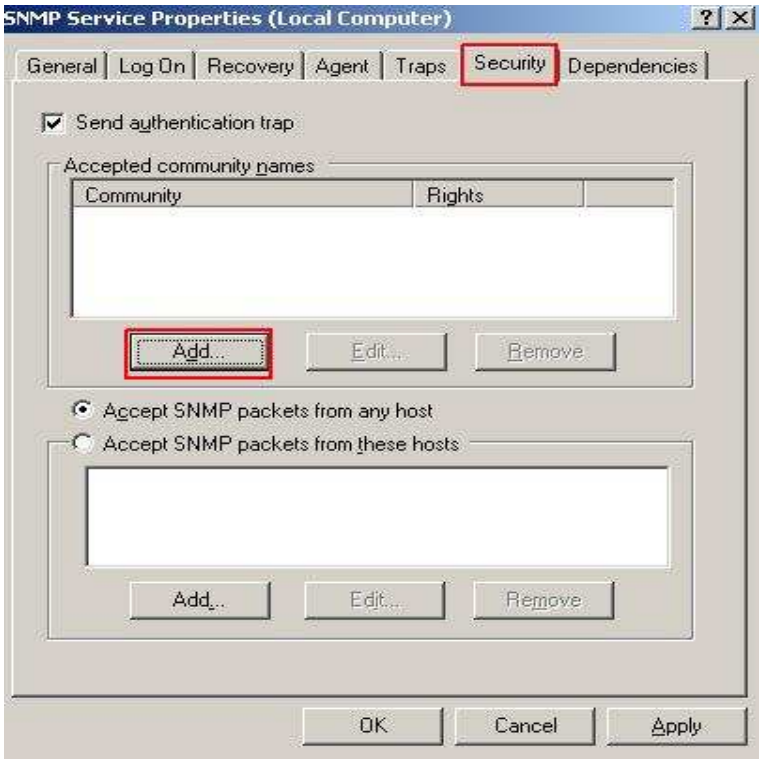


- Una vez instalado el servicio vamos a proceder a crear la comunidad y a indicarle que equipos pueden recibir los traps de SNMP, primero que todo vamos a: **Inicio>Ejecutar>services.msc**

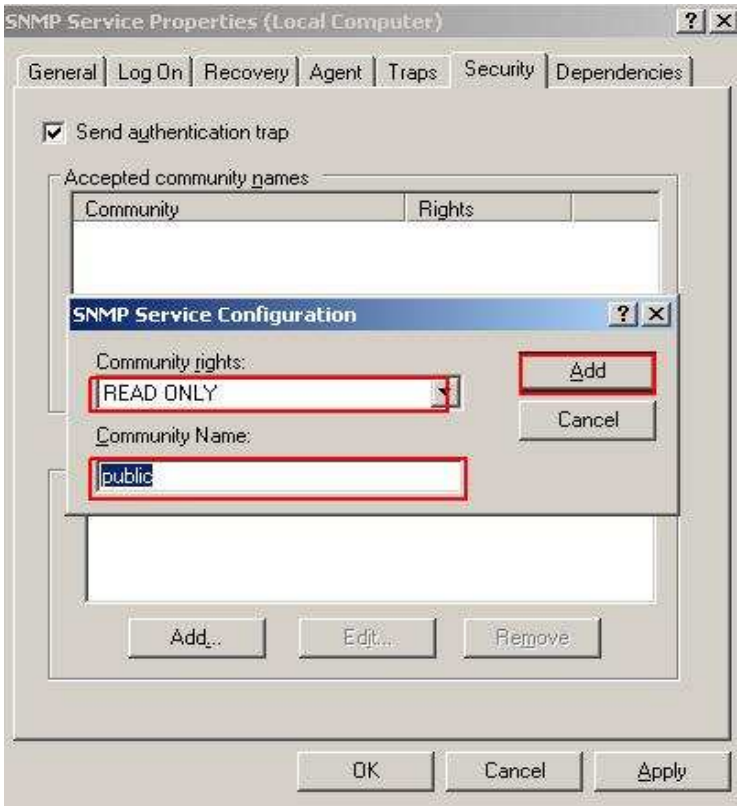
- Luego vamos y buscamos el servicio SNMP y damos **clic derecho>Propiedades**



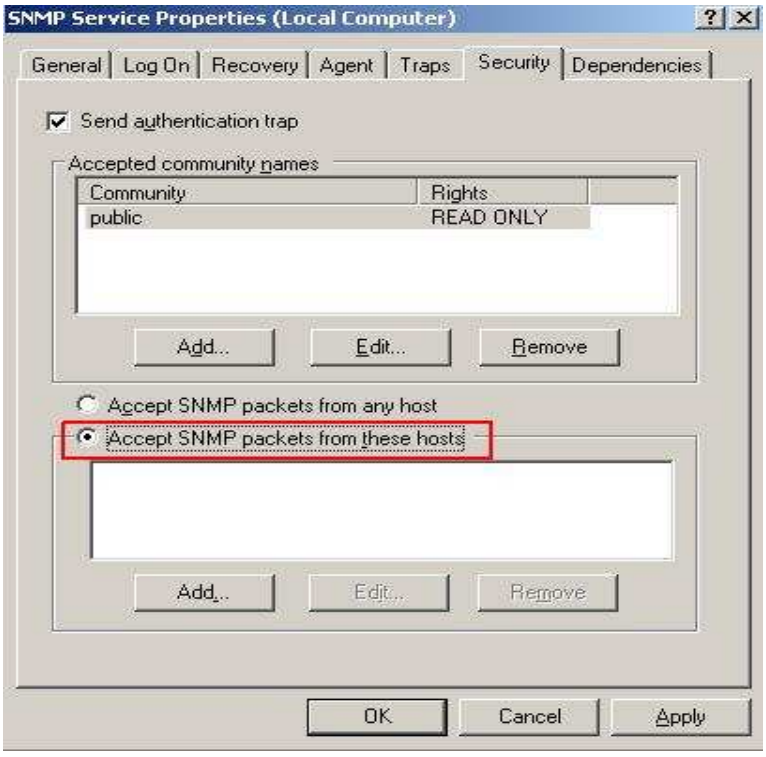
- Vamos a la pestaña **“Security”** Y luego damos clic en **“Add”**



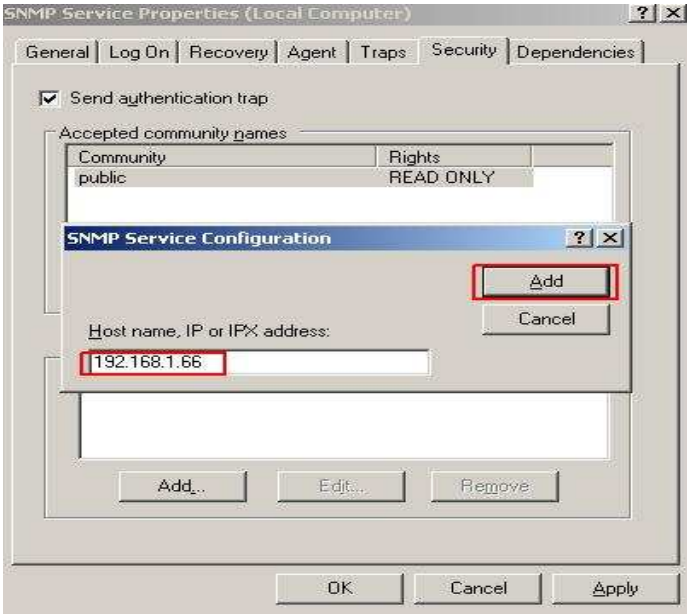
- Le damos los derechos, en este caso de “solo lectura”, y le ponemos un nombre a nuestra comunidad en este caso “Public”

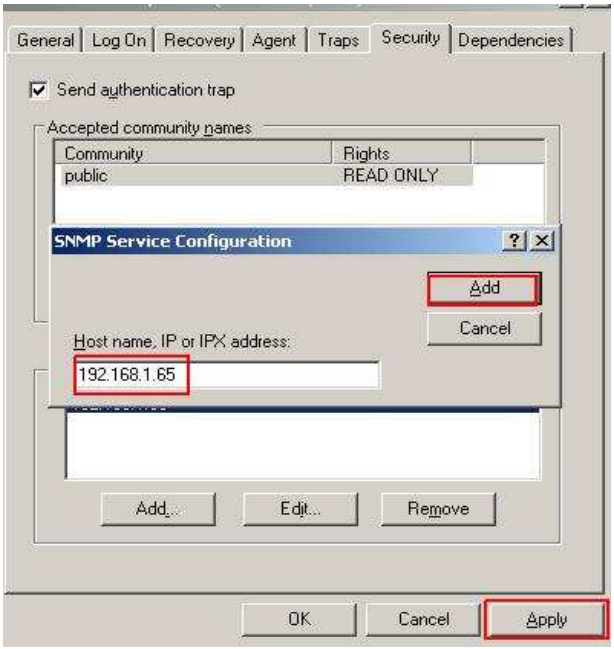


- Ahora para darle mas seguridad le vamos a indicar que equipos pueden recibir los traps de SNMP, en este caso le especificaremos la dirección IP del mismo equipo y de nuestro servidor Pandora. Escogemos la opción que dice "**Accept SNMP Packets from these hosts**" y luego le damos clic en "**Add**":

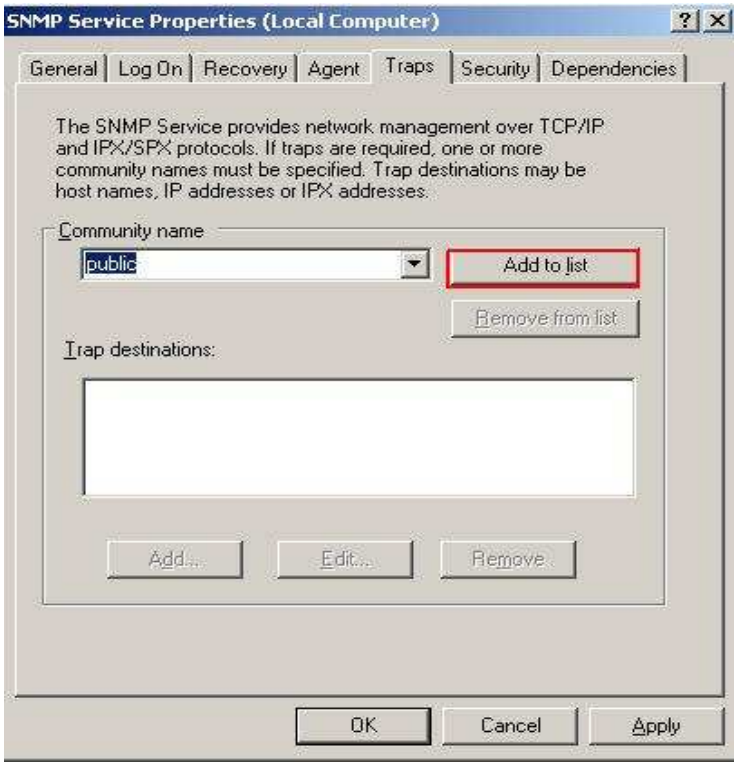


- Le indicamos las direcciones IP:





- Ahora vamos a la pestaña “**Traps**” y prácticamente hacemos lo mismo: en el campo Community name ponemos **public** y damos clic en el botón que dice **Add to list:**



- Agregamos las direcciones ip tal y como hicimos mas arriba, tanto la dir ip 192.168.1.65 (Servidor) como la 192.168.1.66 (Cliente)

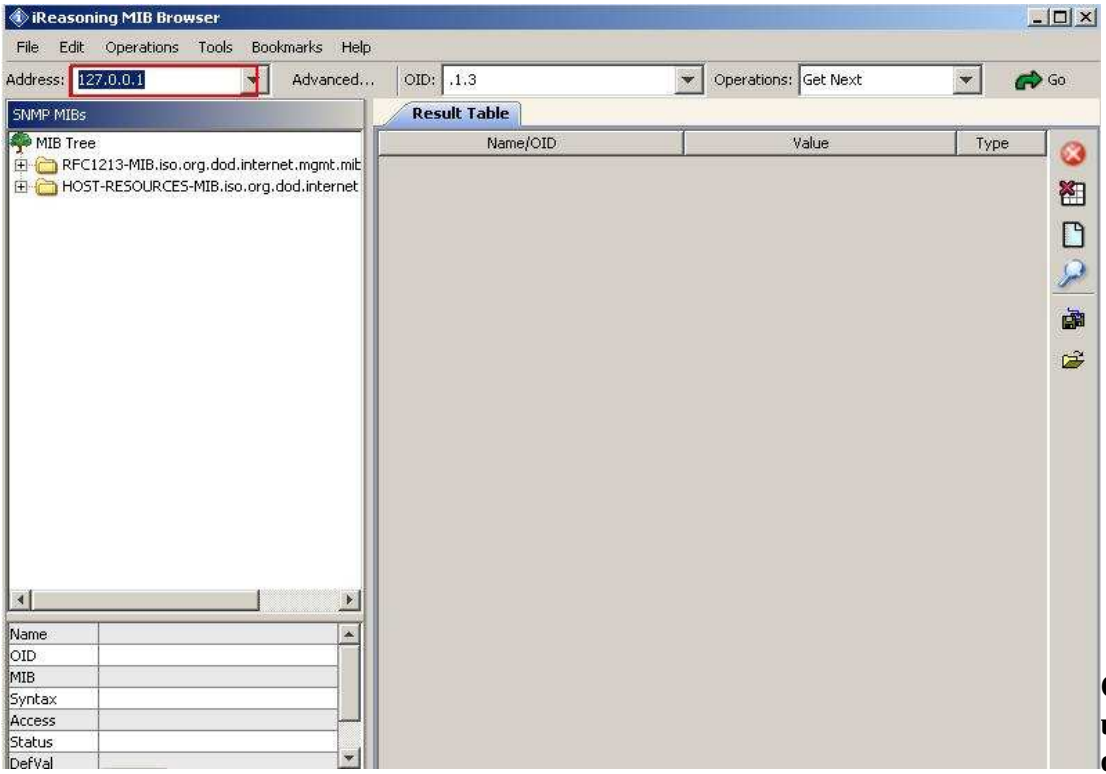
Ahora vamos a aprender a identificar los OID que son códigos para los traps, para esto vamos a descargarnos la siguiente herramienta:

Ireasoning MiB Browser: http://www.ireasoning.com/downloadmibbrowserlicense.shtml

Nota: en la parte de abajo de la pagina nos da la opción de aceptar el contrato, damos clic en aceptar y luego iniciamos la descarga, la instalación de esta herramienta es demasiado intuitiva, por eso no explicaremos como instalarla.

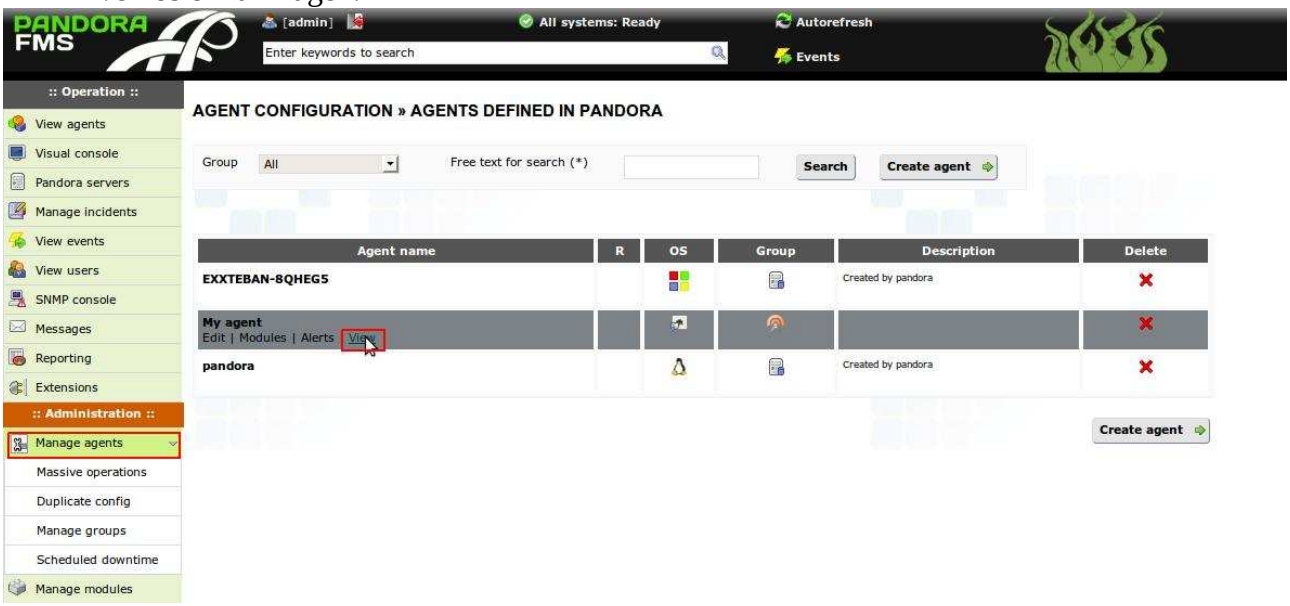
- Una vez instalada la herramienta vemos la siguiente área de trabajo donde la parte subrayada en rojo, nos indica cual va a ser la maquina que vamos a monitorear para saber que OID

contiene:

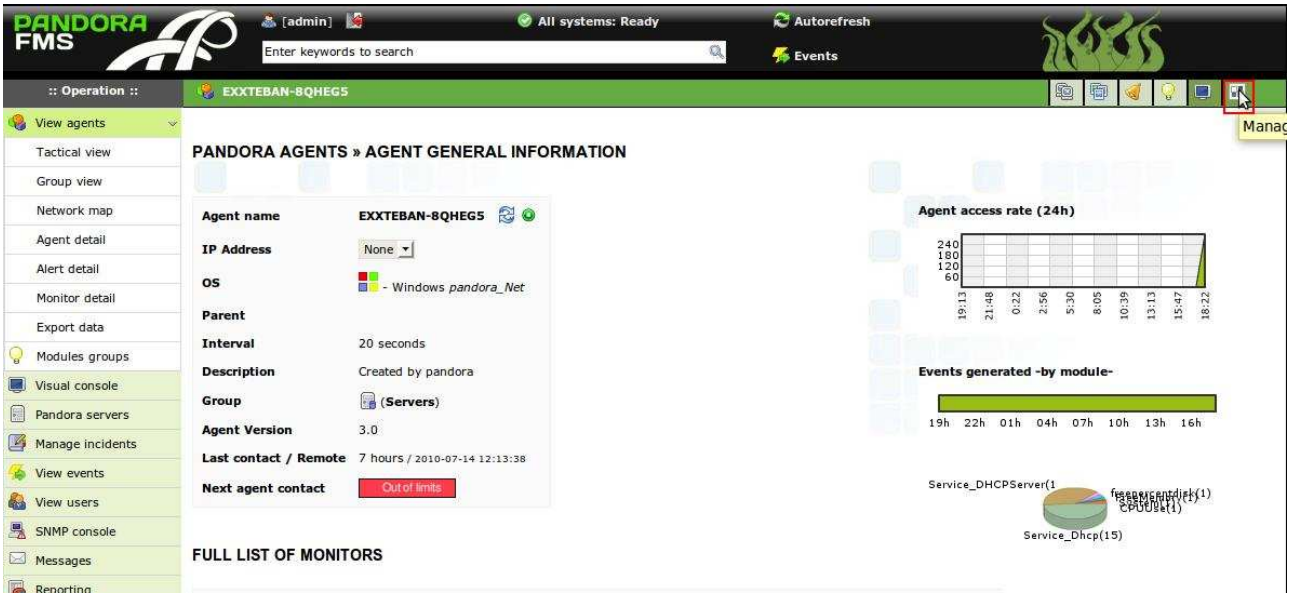


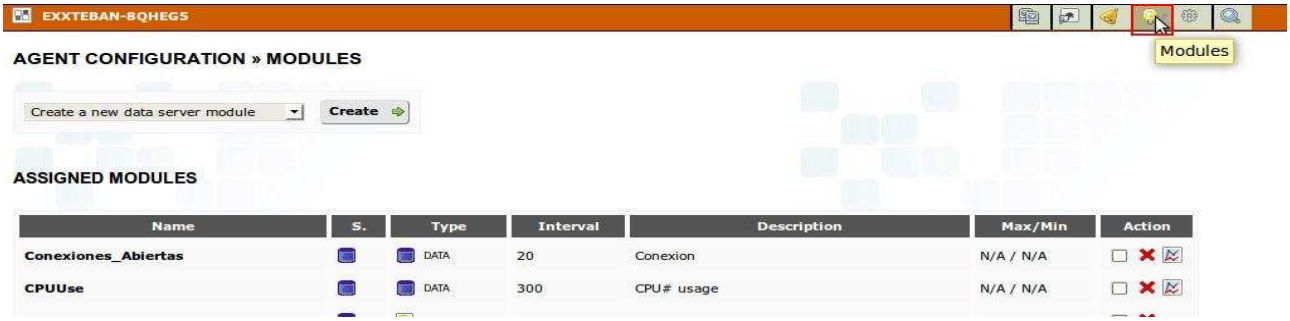
Configurando un modulo SNMP en Pandora FMS

- Ingresamos a nuestro servidor Pandora FMS luego vamos a “manage agents”, una vez allí escogemos el agente que vamos a monitorear y le damos en la opcion “View” tal y como vemos en la imagen.



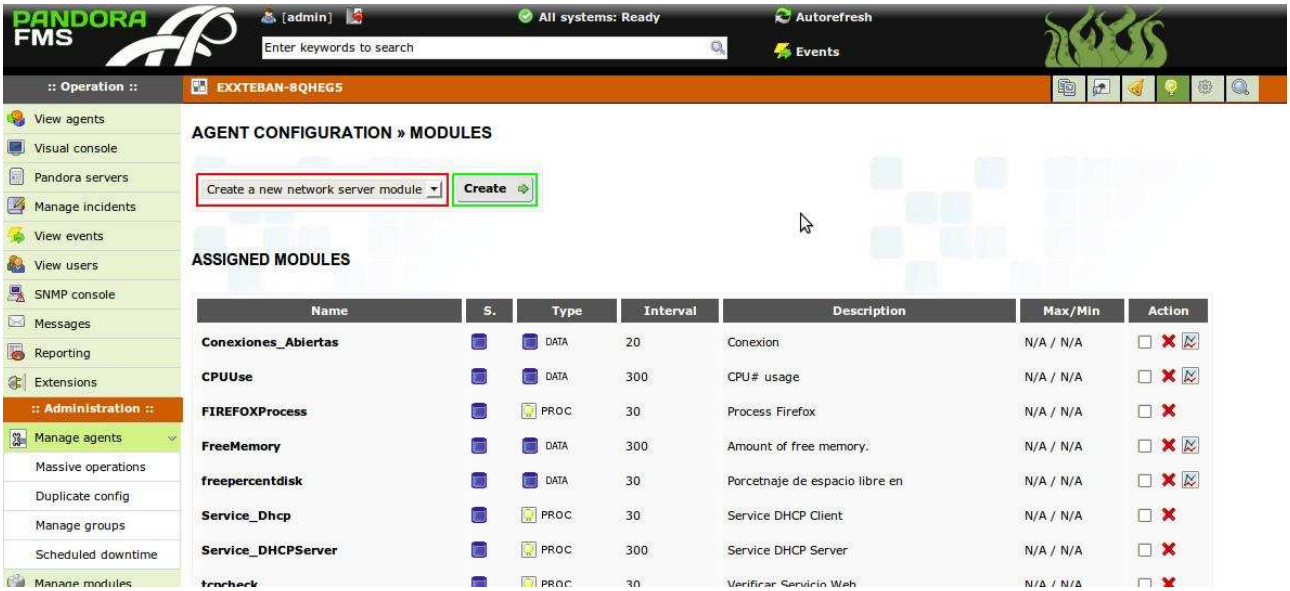
- Damos clic en la opción “Manage” resaltada en rojo





- Luego clic en la opción “Modules” resaltada en rojo

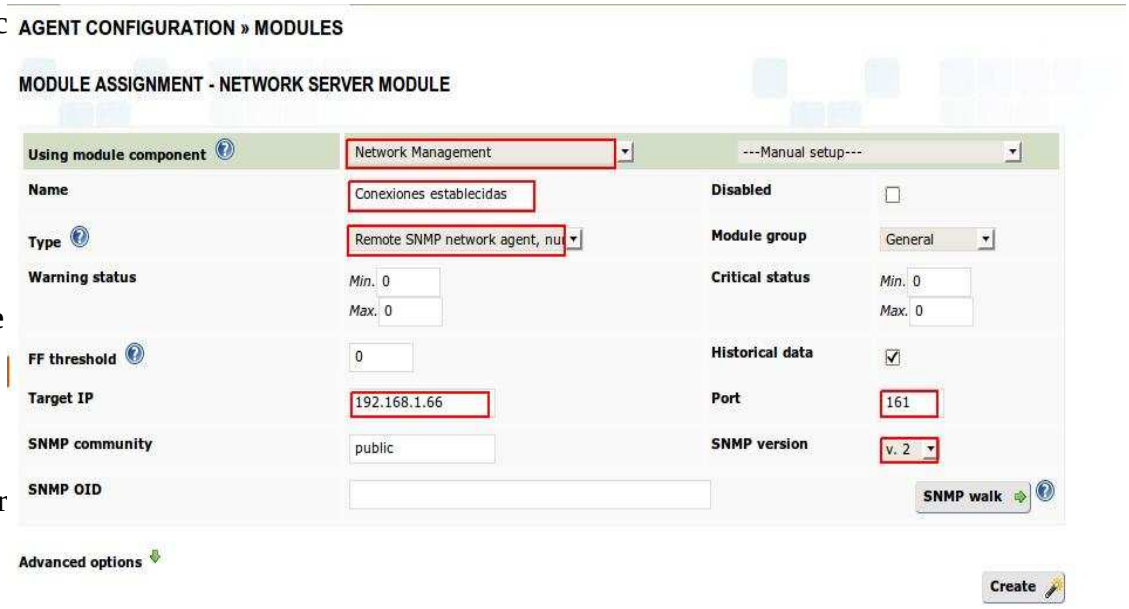
- Vamos entonces a crear un modulo de red, y en la parte subrayada en rojo vamos a darle clic



y seleccionar la opción “**Create a new network server module** ” Luego clic en “**Create**”:

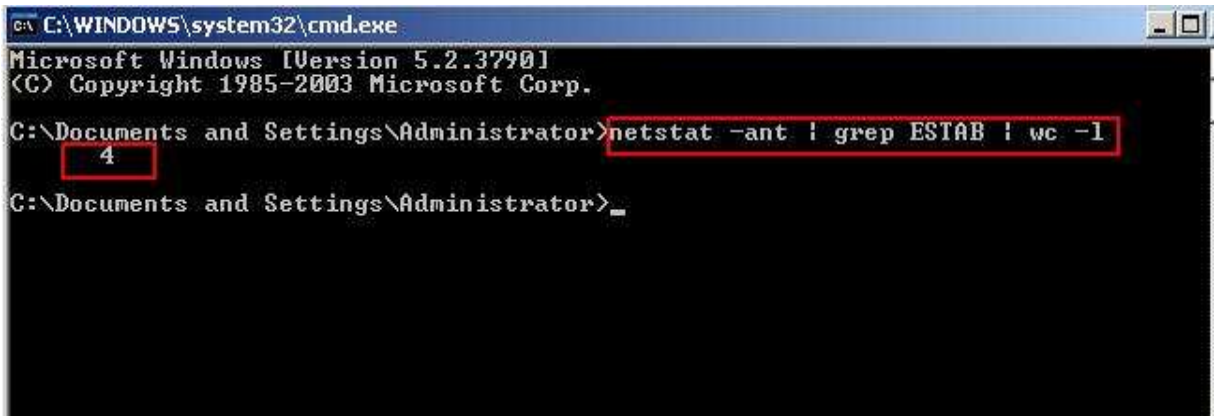
- Llenamos los campos tal y como aparece en la imagen:

Explicamos cada uno de los campos:



Name: Ponemos el nombre que queramos, dependiendo lo que vayamos a monitorear
Type: En este caso pusimos La forma numérica, dependiendo los resultados que cada uno quiere conseguir, podríamos cambiarla por alguna de las diferentes opciones disponibles.
Target IP: Direccion IP del agente a monitorear
SNMP Community: Nombre de la comunidad (Configurada anteriormente)
Port: Numero de puerto con el que trabaja SNMP en este caso el 161
SNMP Version: Para este caso seleccionamos la versión 2 ya que Windows 2003 server trabaja con esta.

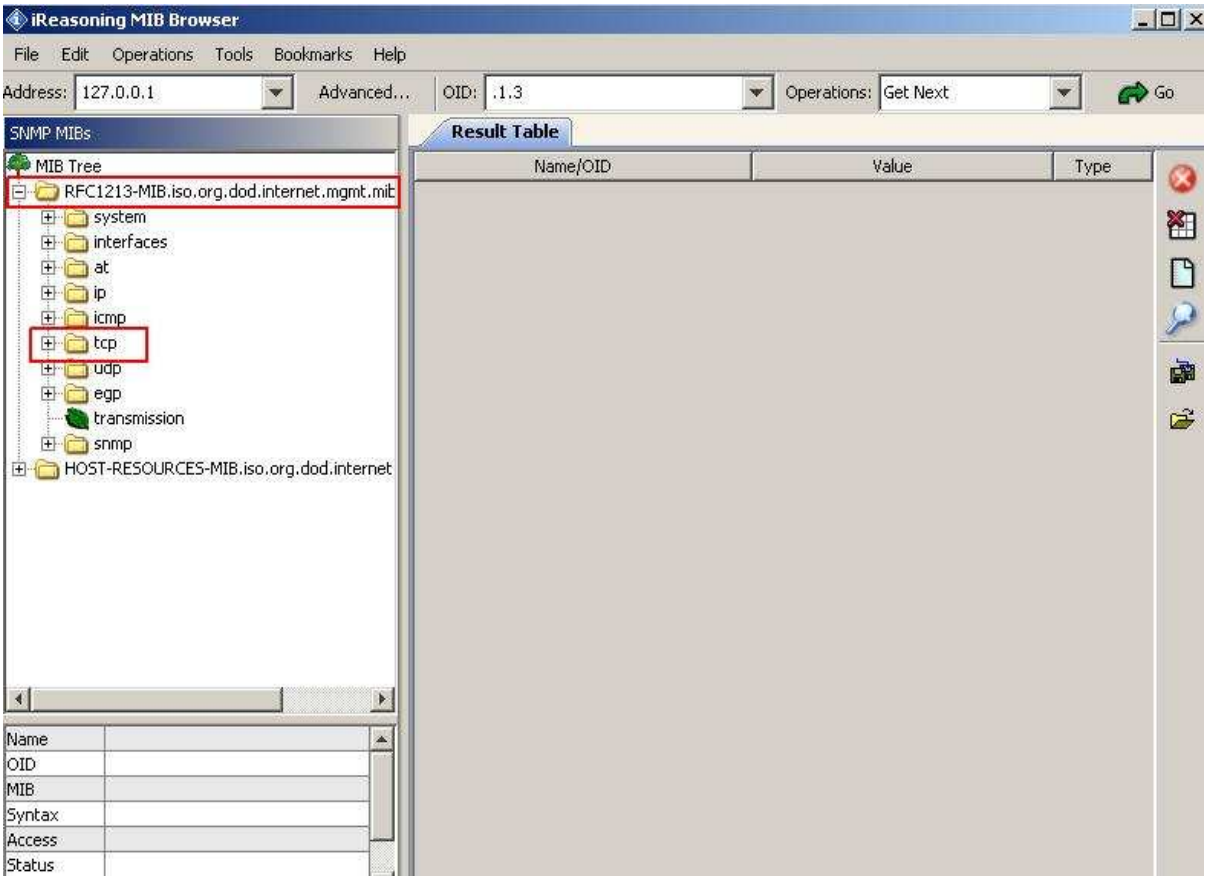
- Por ultimo nos queda pendiente un campo y es el campo **SNMP OID** y este lo vamos a consultar con el programa que nos descargamos para Windows 2003 server. Vamos primero que todo a identificar el OID para el cual estamos configurando el modulo. Antes que nada queremos indicar que este modulo servirá para identificar cuantas puertos tienen sesiones establecidas en el agente, vamos primero que todo a ejecutar en el bash de Windows una



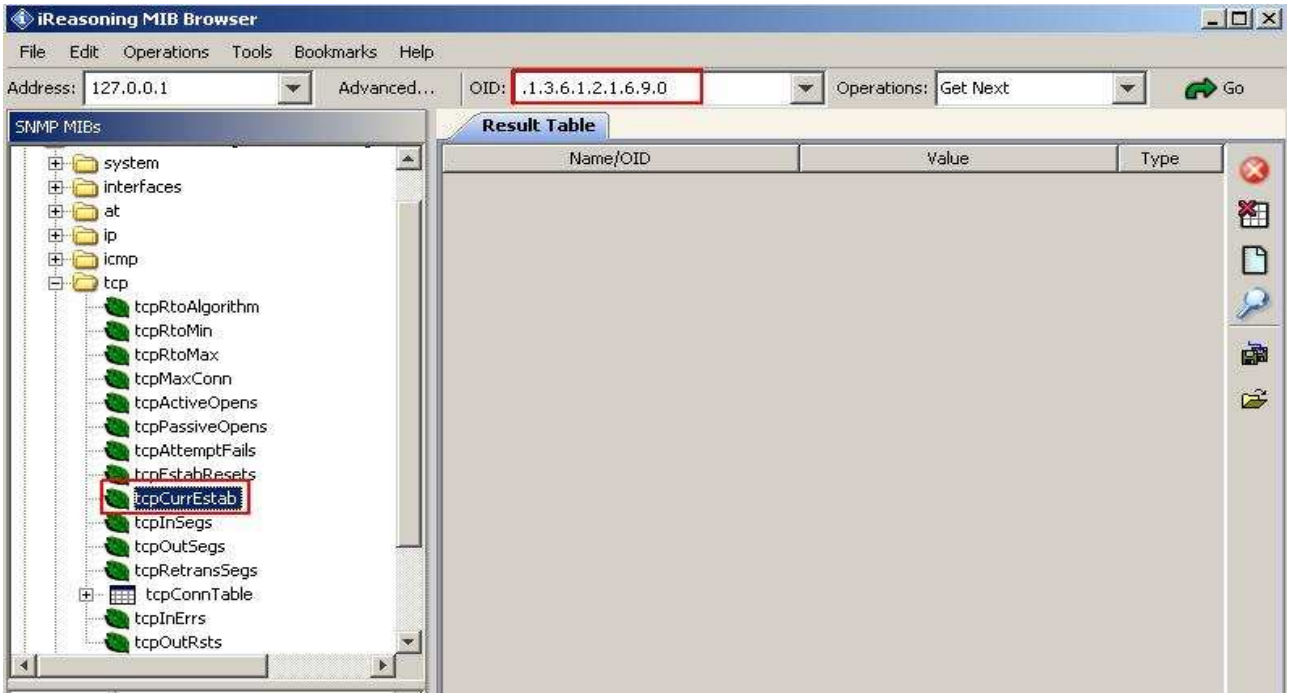
orden que nos indica cuantas conexiones hay establecidas en este momento:

Nos dice en esta ocasión que hay 4 conexiones establecidas.

- Ahora si vamos a mirar nuestro OID para identificar las conexiones establecidas; Primero abrimos el ireasoning MiB Browser, y allí vamos a desplegar la primera carpeta tal y como vemos en la imagen, luego desplegamos la carpeta "**tcp**":

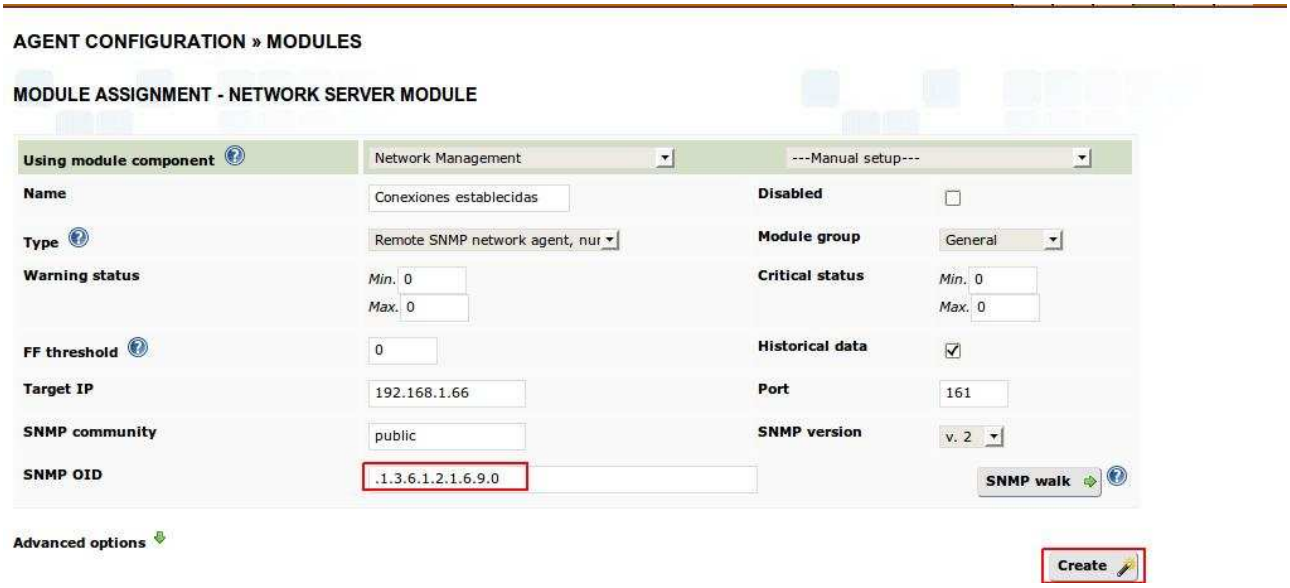


- Nos ubicamos encima de donde dice “tcpCurrEstab” he identificamos el OID que aparece



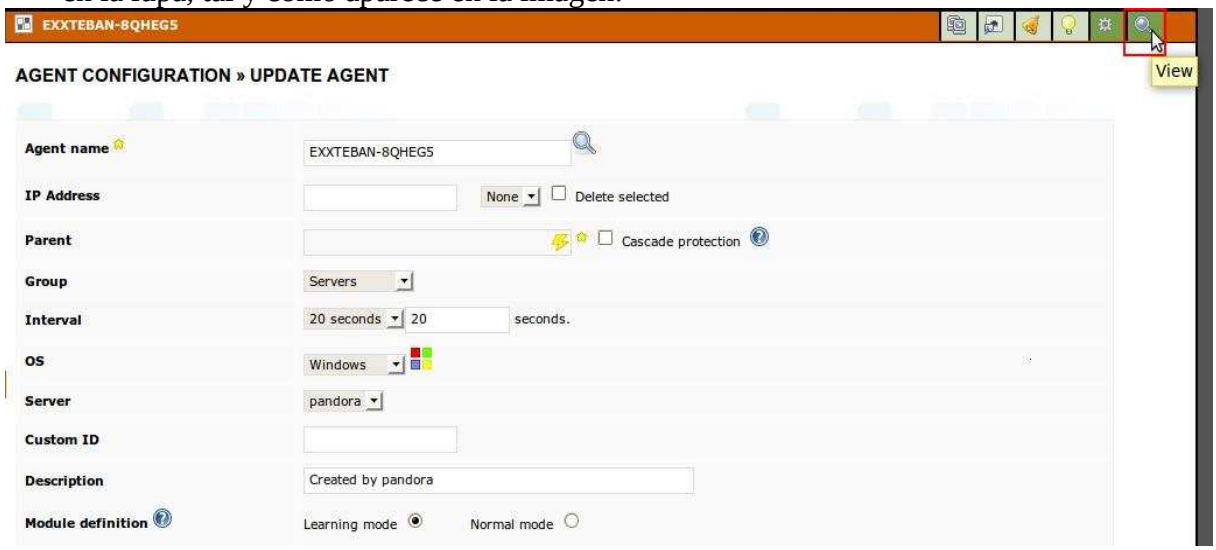
en la parte superior central

- Pegamos este OID en el campo que aparece subrayado en la imagen, en nuestro servidor



Pandora FMS, Y por ultimo le damos clic en “Create”:

- Ahora vamos a verificar cuantas conexiones nos esta arrojando el agente, y vamos a dar clic en la lupa, tal y como aparece en la imagen:



- Finalmente vemos que nos esta mostrando las mismas 4 conexiones que vimos nos arrojaba el bash de Windows:

FULL LIST OF MONITORS

	Type	Module name	Description	Status	Data	Graph	Last contact
		Conexiones_Abiertas	Conexion		4		20 seconds
		CPUUse	CPU# usage		0		20 seconds
		FIREFOXProcess	Process Firefox		1		20 seconds
		FreeMemory	Amount of free memory.		6		20 seconds
		freepercentdisk	Porcetnaje de espacio libre en...		87		20 seconds
		Service_Dhcp	Service DHCP Client		1		20 seconds
		Service_DHCPServer	Service DHCP Server		1		20 seconds
		tcpcheck	Verificar Servicio Web		1		20 seconds
			General				
		Conexiones establecidas			4		16 seconds
		Open Ports			2,442		14 seconds

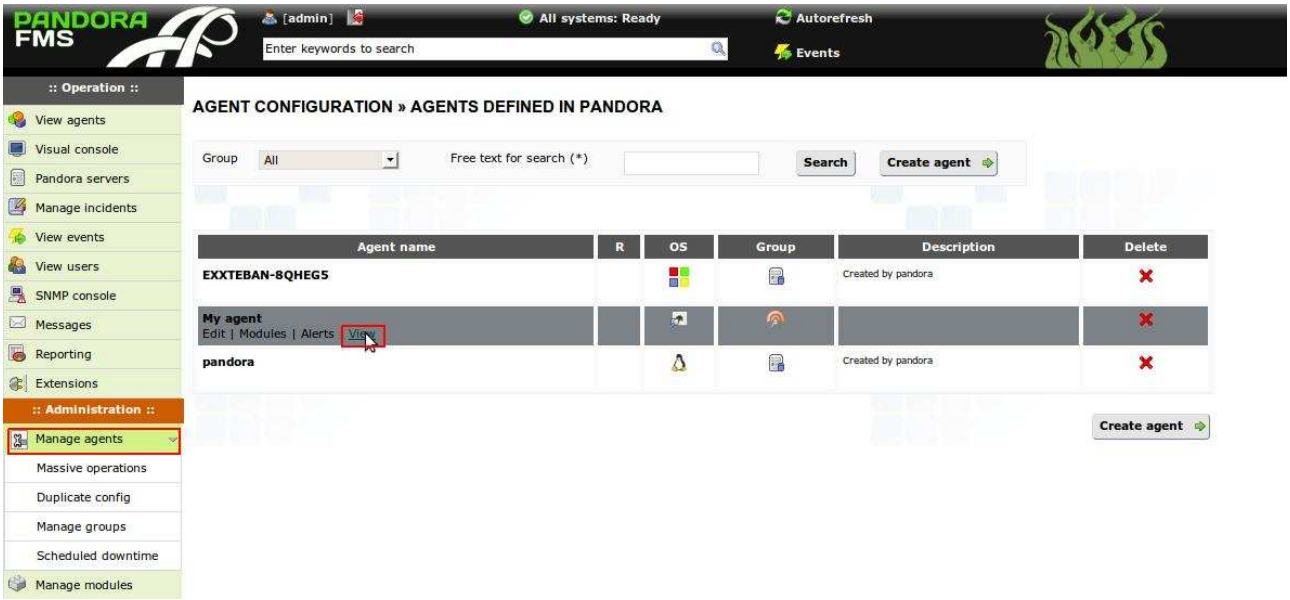
Monitoreo con WMI en windows 2003 server

Con este método las consultas se hacen con WQL que es una base propietaria de Microsoft, muy parecida a SQL. Contiene modulos muy utiles a la hora de monitorear sistemas Windows. En conjunto trabajaremos con una herramienta llamada Wmi Explorer que se encargara de extraer esos módulos para poder definirlos en nuestro servidor Pandora.

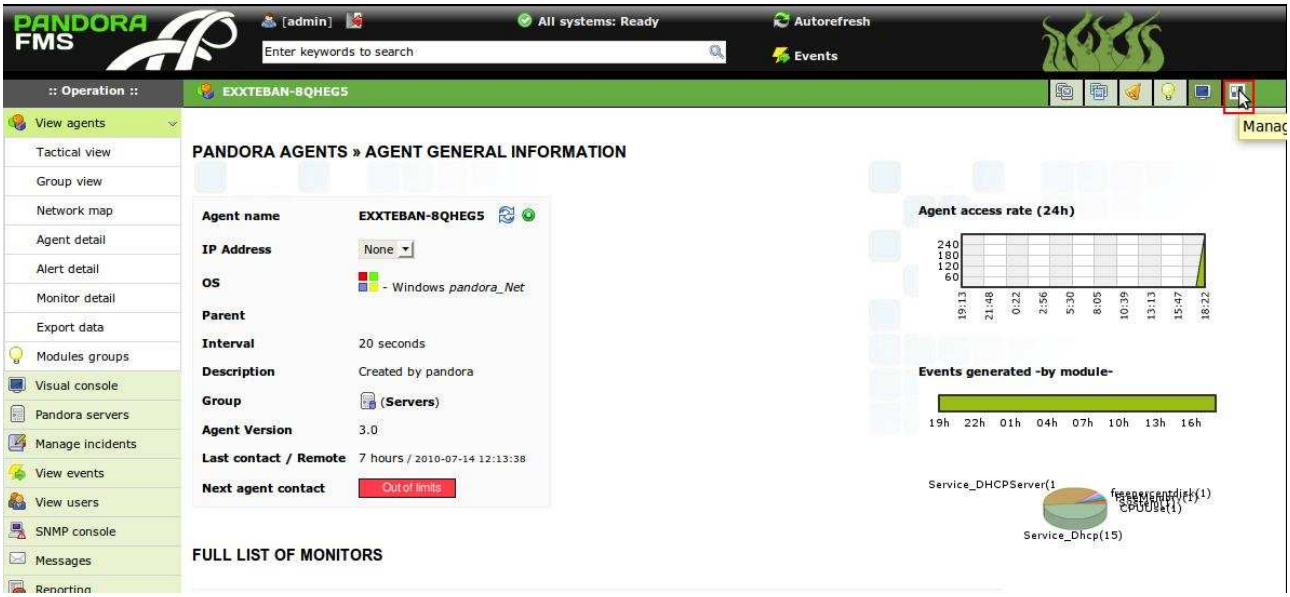
Creación del agente:

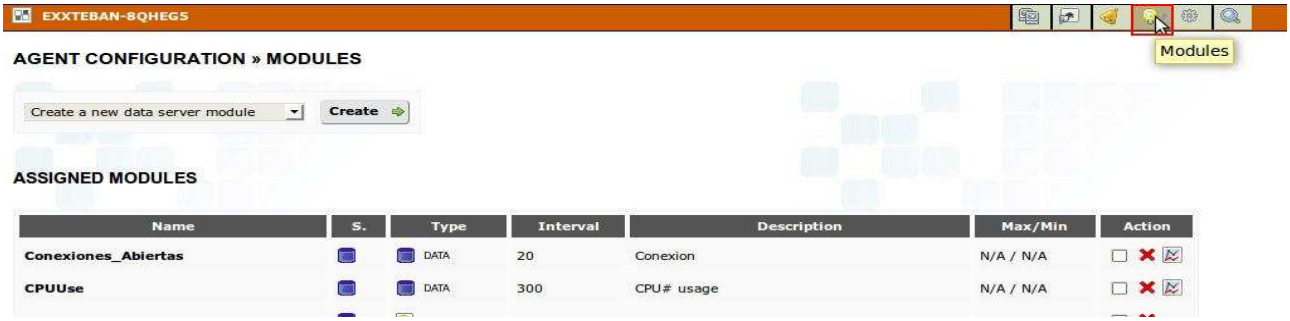
- En la seccion de “Administration”, damos clic en “manage agents”

- Damos clic en “view”



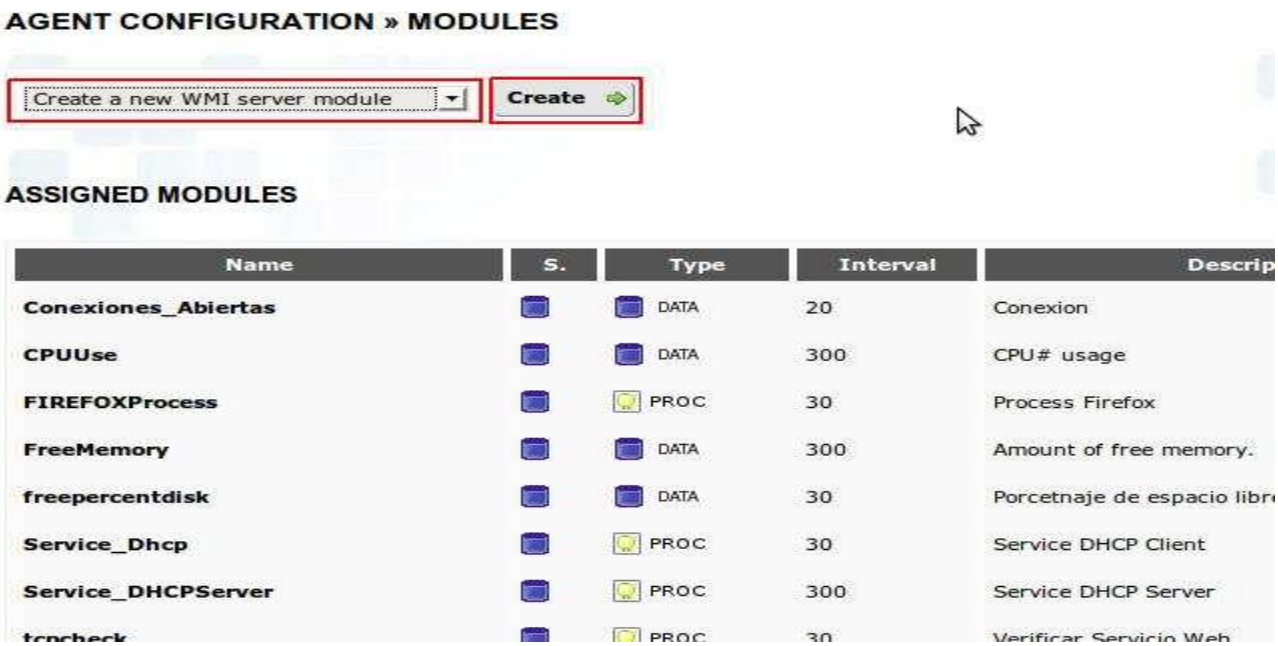
- Clic en “manage” resaltado en rojo





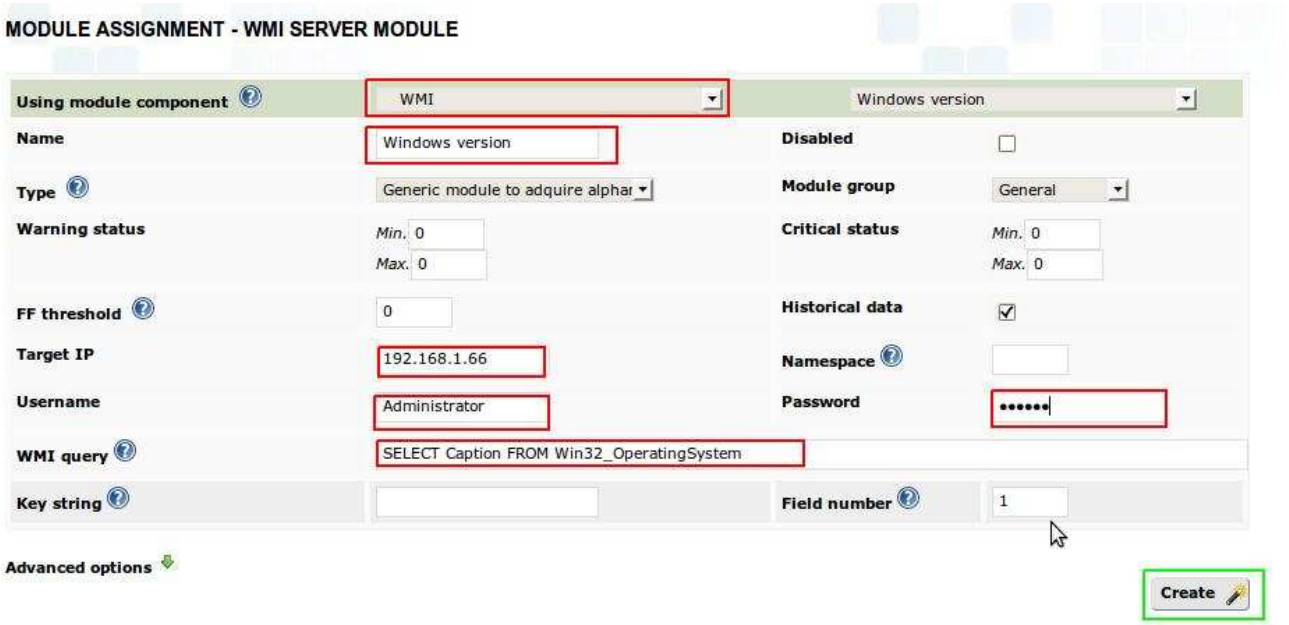
- Luego clic en la opción “Modules” resaltado en rojo

- En la misma ventana vamos a seleccionar la opción “ **create a new WMI server module**”,

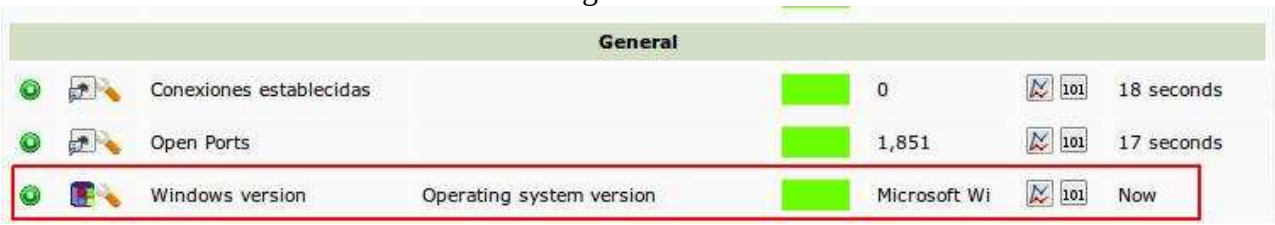


y luego damos clic en “**Create**”.

- Vamos a insertar un modulo WMI predefinido que nos indicara el S.O del agente monitoreado, vamos a ver la imagen.



Dando clic en la lupa, ubicada al lado superior derecho, observamos como a quedado nuestro modulo indicándonos cual SO tiene nuestro agente.



Using module component: tipo de monitoreo
Target IP: Direccion IP del agente a monitorear.
Username: Un nombre de usuarios con privilegios de administrador.
Password: password del usuario con derechos administrativos, en el agente.
WMI query: camo en el que ingresamos el query a la base de datos WQL dependiendo del modulo a monitorear.

- Por ultimo damos clic en “Create”

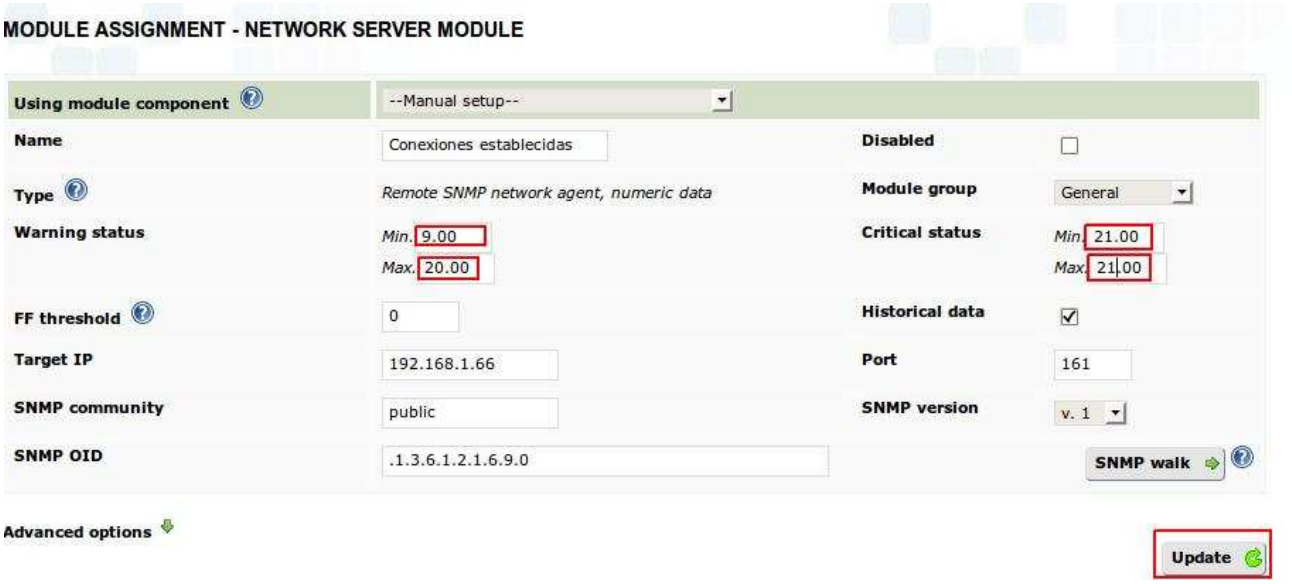
- Si no queremos monitorear con lo query WMI establecidos, podemos bajarnos esta herramienta, y ejecutarla, ella nos dará los query, para poder introducirlos en Pandora.

http://descargar.portalprogramas.com/WMI-Explorer.html

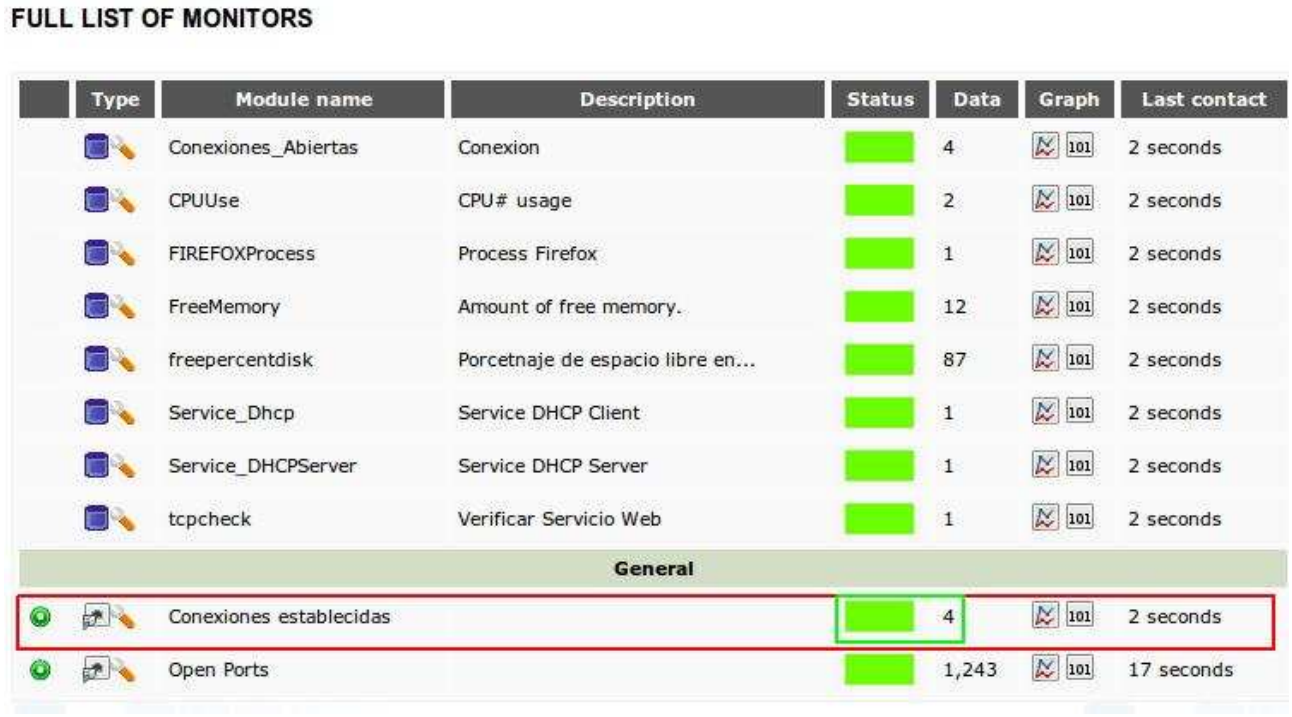
Monitoreo de los estados

Hay tres tipos de estados: Normal,warning, critical. Debemos entonces tener una forma, de establecer cuando un servicio o proceso, nos reporta los diferentes estados, como ejemplo vamos a configurarle esto a un modulo que nos reporta la cantidad de conexiones establecidas. Damos clic en el icono subrayado en verde:

- Ahora vemos que ha dos campos que sirve para nuestro propósito: **Warning status, Critical status**.
- El primero nos mostraría un recuadro de color amarillo, y el segundo un recuadro de color rojo, y cada uno tiene su cantidad mínima y su cantidad máxima. Vamos a ver cual configuración hemos puesto nosotros en este caso.



Hemos puesto una cantidad mínima de 9 conexiones hasta 20, nos mostrara un estado Warning o de advertencia, y una cantidad de 21 conexiones para un estado critico. Sobra decir entonces que por debajo de 9 conexiones, nos mostraría un estado normal. Por ultimo damos clic en el botón **Update**

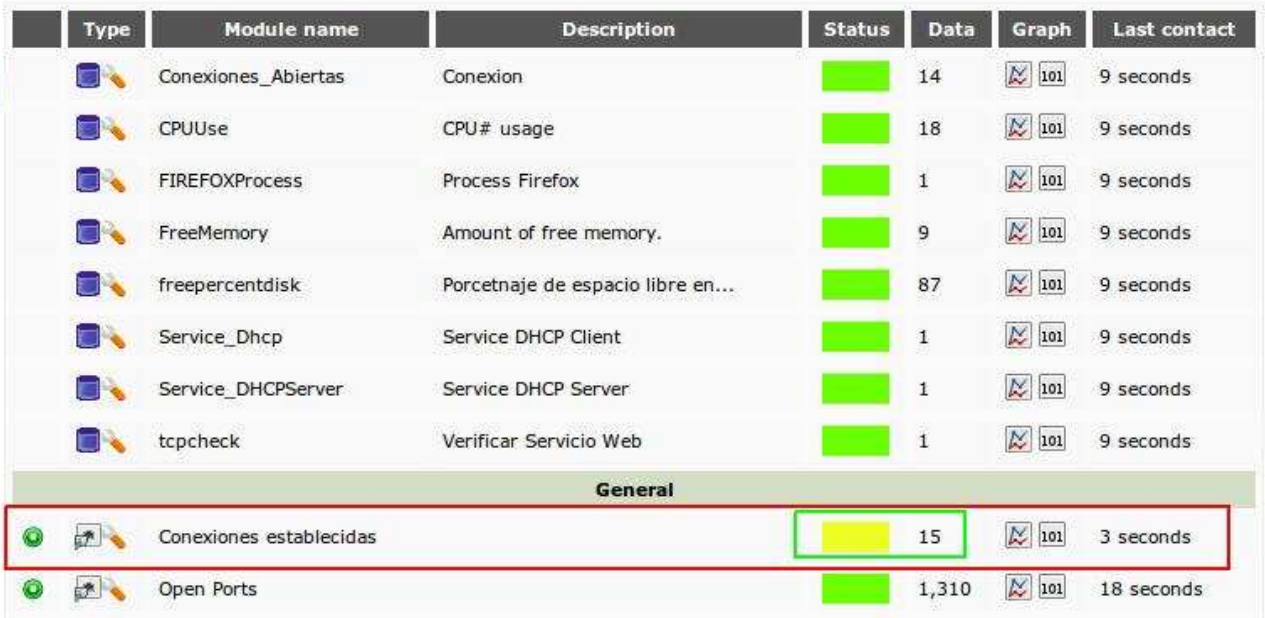


- Miremos el comportamiento:

Nota: Vemos entonces que hay 4 conexiones establecidas, y por esto el recuadro esta de color verde, lo que significa que esta en modo Normal.

- Vamos entonces a abrir mas conexiones para ver el estado Warning.

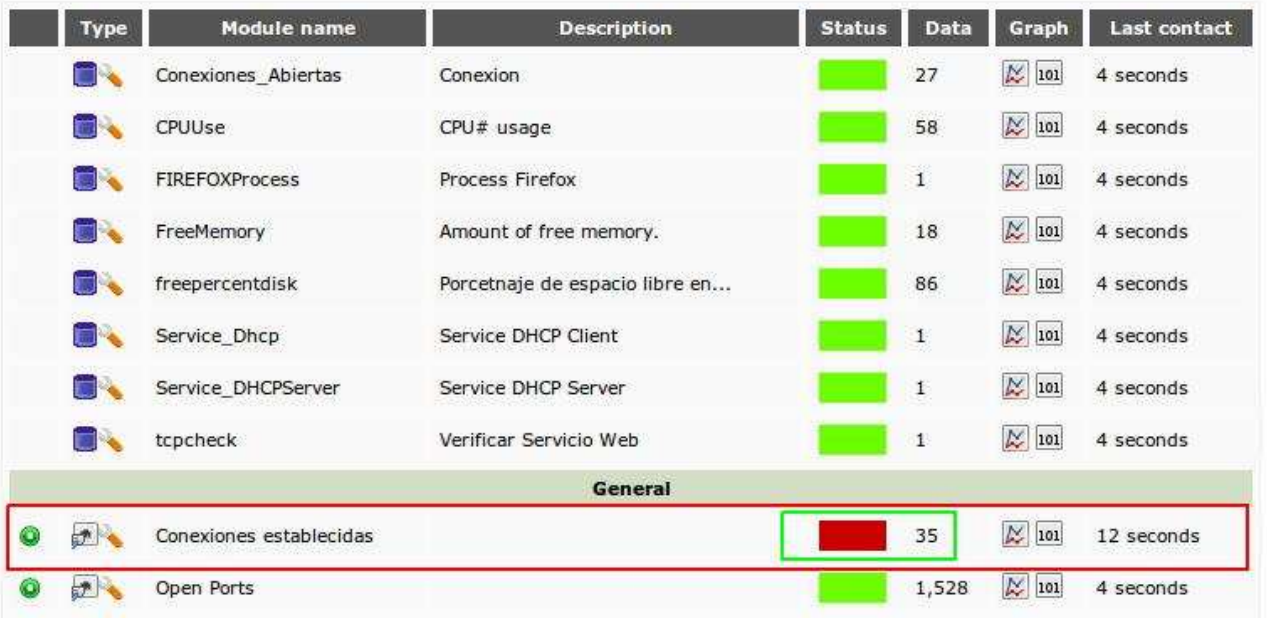
FULL LIST OF MONITORS



Type	Module name	Description	Status	Data	Graph	Last contact
	Conexiones_Abiertas	Conexion		14		9 seconds
	CPUUse	CPU# usage		18		9 seconds
	FIREFOXProcess	Process Firefox		1		9 seconds
	FreeMemory	Amount of free memory.		9		9 seconds
	freepercentdisk	Porcetnaje de espacio libre en...		87		9 seconds
	Service_Dhcp	Service DHCP Client		1		9 seconds
	Service_DHCPServer	Service DHCP Server		1		9 seconds
	tcpcheck	Verificar Servicio Web		1		9 seconds
General						
	Conexiones establecidas			15		3 seconds
	Open Ports			1,310		18 seconds

Nota: Vemos el estado Warning, ya que tenemos 15 conexiones establecidas.

FULL LIST OF MONITORS



Type	Module name	Description	Status	Data	Graph	Last contact
	Conexiones_Abiertas	Conexion		27		4 seconds
	CPUUse	CPU# usage		58		4 seconds
	FIREFOXProcess	Process Firefox		1		4 seconds
	FreeMemory	Amount of free memory.		18		4 seconds
	freepercentdisk	Porcetnaje de espacio libre en...		86		4 seconds
	Service_Dhcp	Service DHCP Client		1		4 seconds
	Service_DHCPServer	Service DHCP Server		1		4 seconds
	tcpcheck	Verificar Servicio Web		1		4 seconds
General						
	Conexiones establecidas			35		12 seconds
	Open Ports			1,528		4 seconds

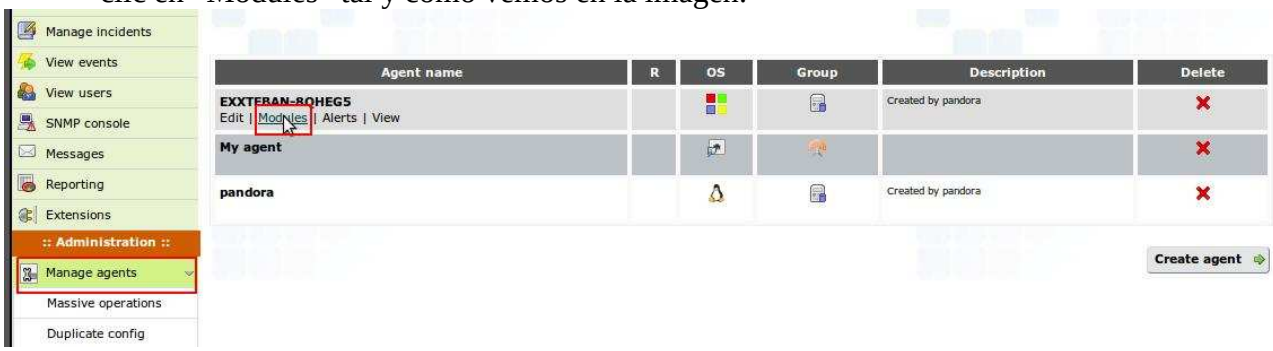
- Por ultimo intentaremos abrir 21 conexiones o mas, para ver el estado critico.

Nota: Si el estado warning y el critical tienen el mismo valor, tiene prioridad el estado critical. Tampoco tiene sentido configurarle estos valores, a estados que solo arrojan estados booleanos como unos y ceros, indicando actividad o inactividad de un servicio o proceso.

Agregando templates preconfigurados

Los templates contienen módulos predefinidos que se pueden aplicar a un agente en especifico, miremos como agregar un template.

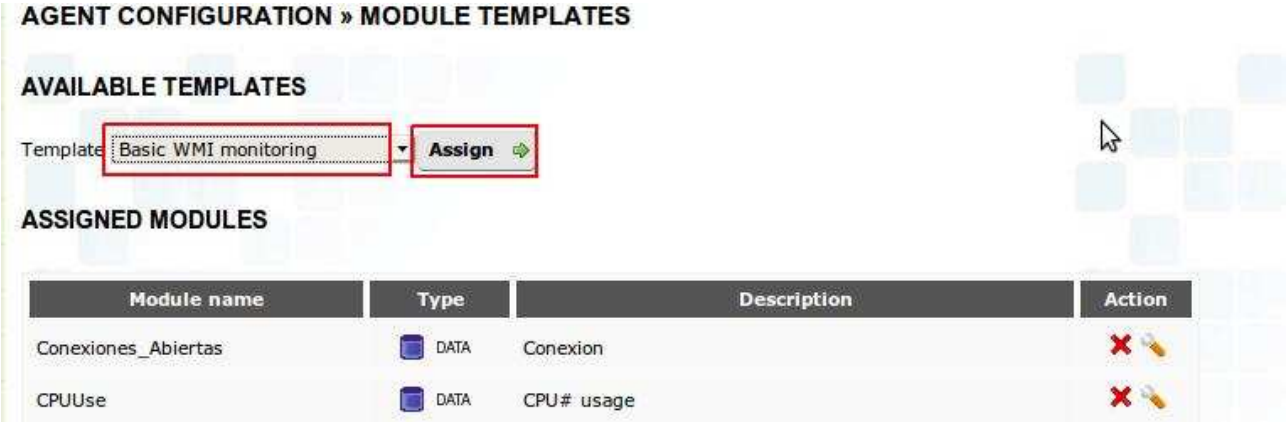
- Vamos a la seccion de “Administration” luego clic en “Manage agents” y una vez allí damos clic en “Modules” tal y como vemos en la imagen.



- Alli vamos a la opcion “Module templates” ubicada en la parte superior.

-

- Alli podemos escoger cualquier plantilla, dependiendo de nuestras necesidades, en nuestro caso escogimos “Basic WMI monitoring”, luego damos clic en “Assing”:

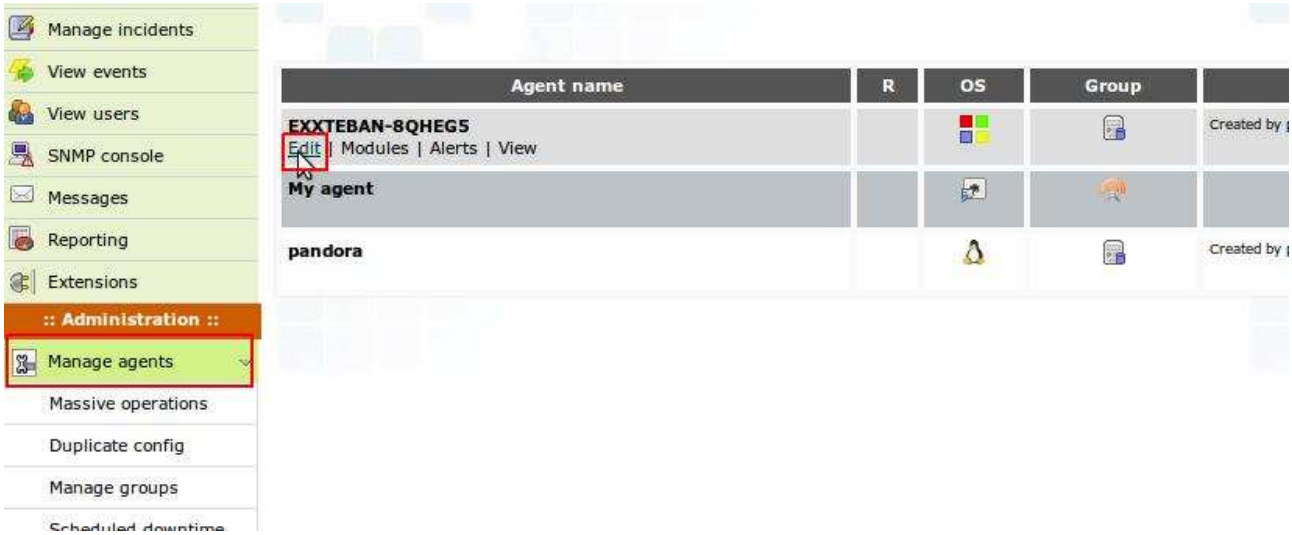


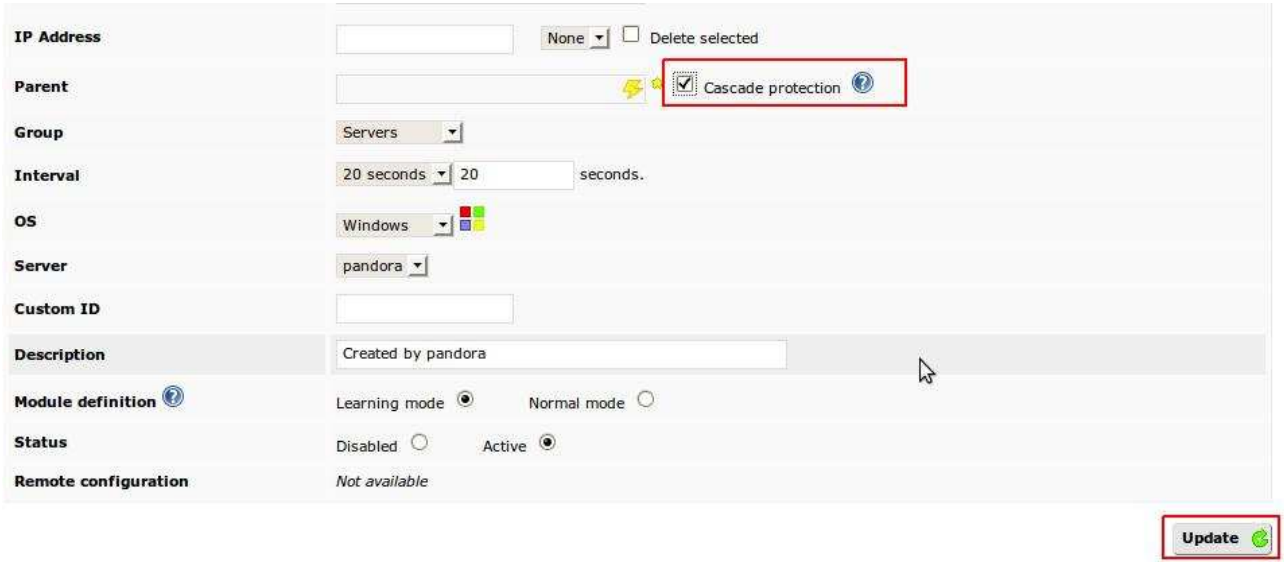
- Nos debe aparecer este mensaje:

Protección en cascada Pandora FMS

La protección en cascada evita que se genere trafico en exceso en nuestra red, y pueda causarse un cuello de botella, en determinados casos, por ejemplo: Tenemos una red de dispositivos activos y estamos monitoreandolos todos, pero el que esta mas cerca a nuestro servidor Pandora se cae, entonces esto traería una reacción en cadena así los demás dispositivos estén funcionando perfectamente, con esta opción evitaríamos cosas como esas.

- En la sección Administration damos clic en “Manage agents” Luego nos ubicamos en el agente y damos clic en “Edit”.



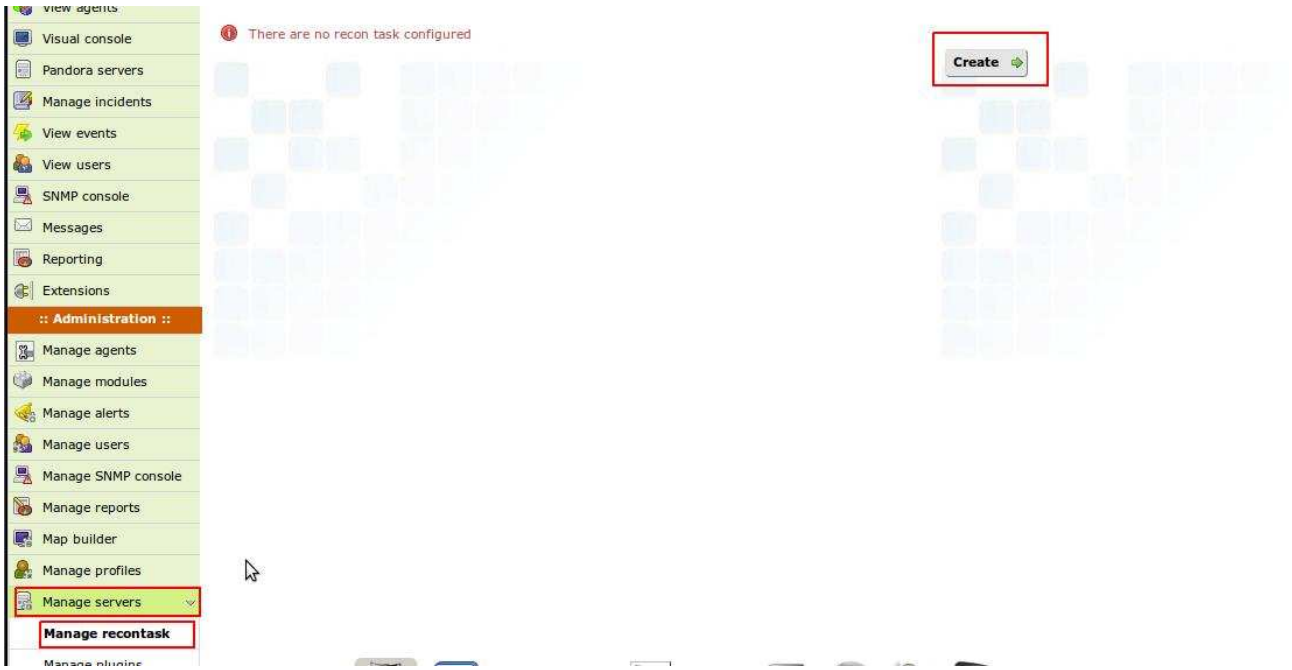


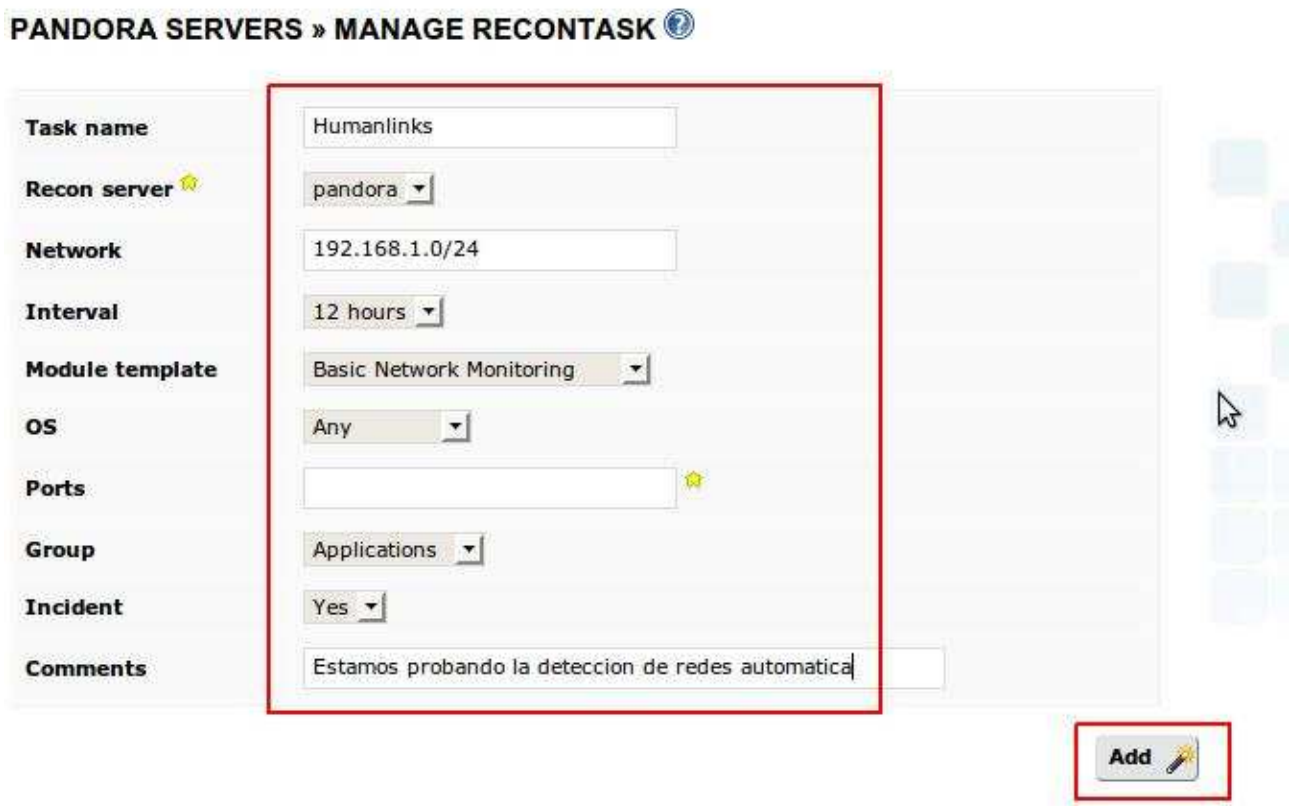
- Luego en la casilla “cascade protection” damos clic y luego clic en “update”.

Descubrimiento automático de la red

Podemos obtener una especie de topología, de la red, haciendo solicitudes ICMP por medio de pings, vamos a mirar como podemos hacer el reconocimiento.

- En la sección “Administration” vamos a la opción “Manage servers” y luego clic en la opción “Manage recontask”, damos clic en el boto “Create”:





- Luego ingresamos en esta ventana y llenamos los campos:

Explicación de los campos:

Task name: Ponemos un valor descriptivo, en este caso como la red es de Humanlinks, pusimos Humanlinks.

Reconserver: Servidor que va a hacer el reconocimiento.

Network: Ponemos el identificador de red o subred, seguido de la mascara separada por un / .

Interval: es cada cuanto se va a hacer la solicitud ICMP por inundación de pings, se recomienda no poner el intervalo muy bajo, para evitar congestión en la red.

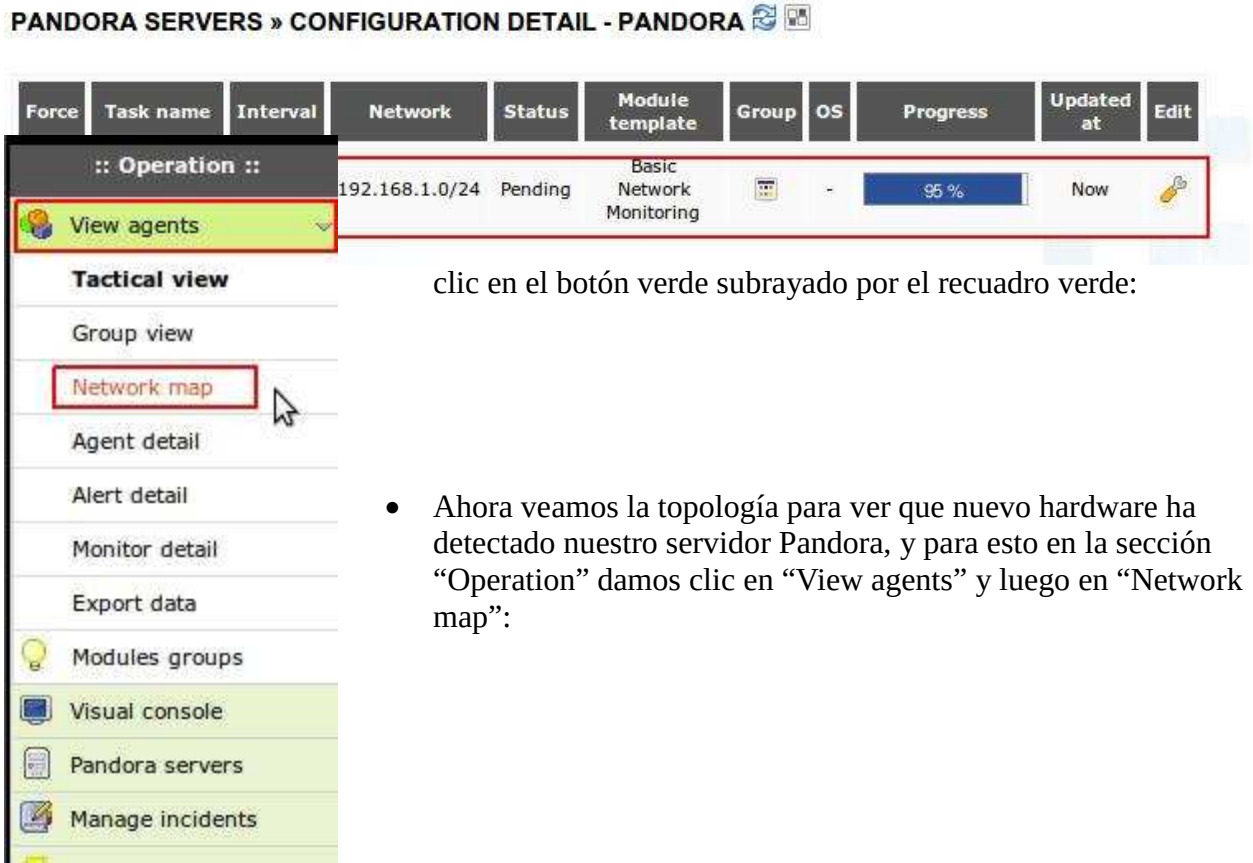
Module template: Plantilla de módulos predefinidos, escogemos uno de acuerdo a nuestras necesidades.

OS: Identifica el sistema operativo de la maquina, dependiendo que puertos tengan abiertos, para realizar la comprobación, debemos tener instalado xprobe2, es recomendable dejarlo en “Any”.

Ports: Detecta las maquinas dependiendo a determinados puertos o intervalos de puertos, que pongamos en este campos, es recomendable no poner nada.

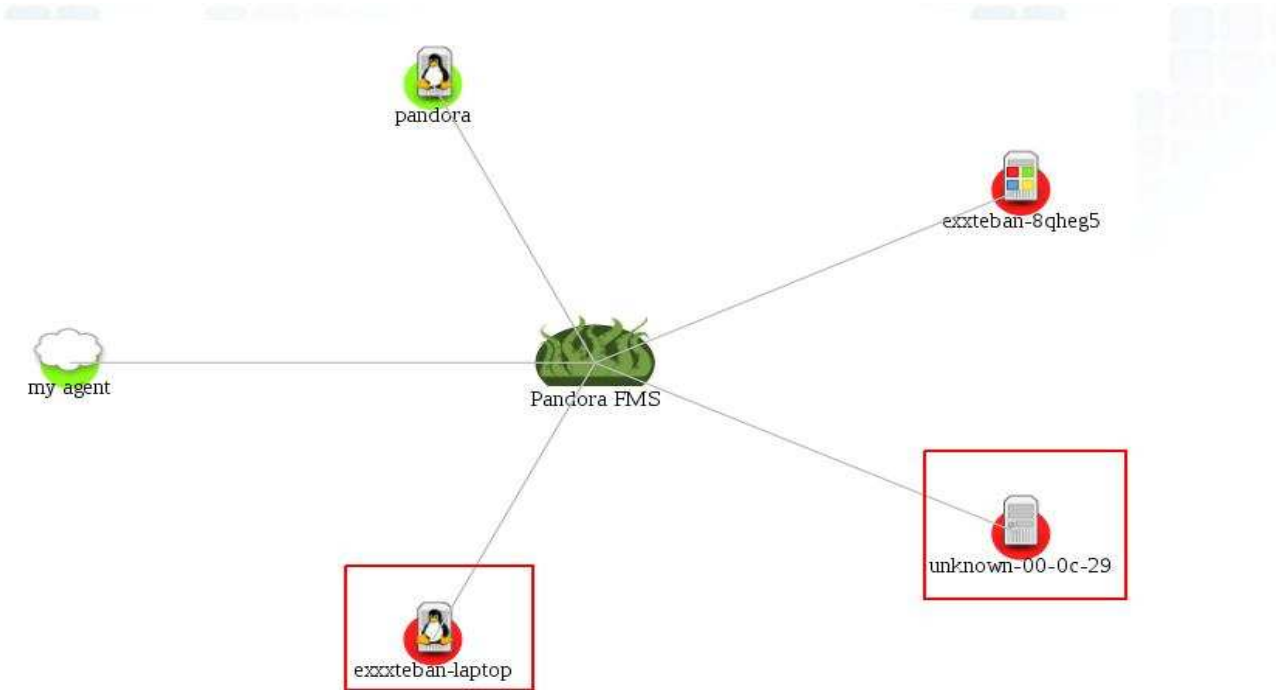
- Si queremos ver el estado de nuestro servidor de reconocimiento damos clic en “All sistems:ready” ubicado en la parte superior, damos clic donde dice pandora, subrayado en rojo:

- Vemos entonces el estado de reconocimiento, si queremos reiniciar el reconocimiento damos clic en el botón verde subrayado por el recuadro verde:



- Ahora veamos la topología para ver que nuevo hardware ha detectado nuestro servidor Pandora, y para esto en la sección “Operation” damos clic en “View agents” y luego en “Network map”:

- Vemos aquí nuestra topología, y subrayados en rojo los dos nuevos host que detecto automáticamente nuestro server Pandora:



Nota: A cada uno de estos nuevos agentes, se le asignan unos módulos, dependiendo del template que hallamos escogido.

Adherir informes personalizados

Adherimos reportes cuando queremos tener un historial del comportamiento de los agentes, o cuando la administración es descentralizada y queremos que otros administradores lean dicha información.

- Para ingresar, vamos a la sección “Administration” luego clic en “Manage reports” y

finalmente clic en “Report builder”

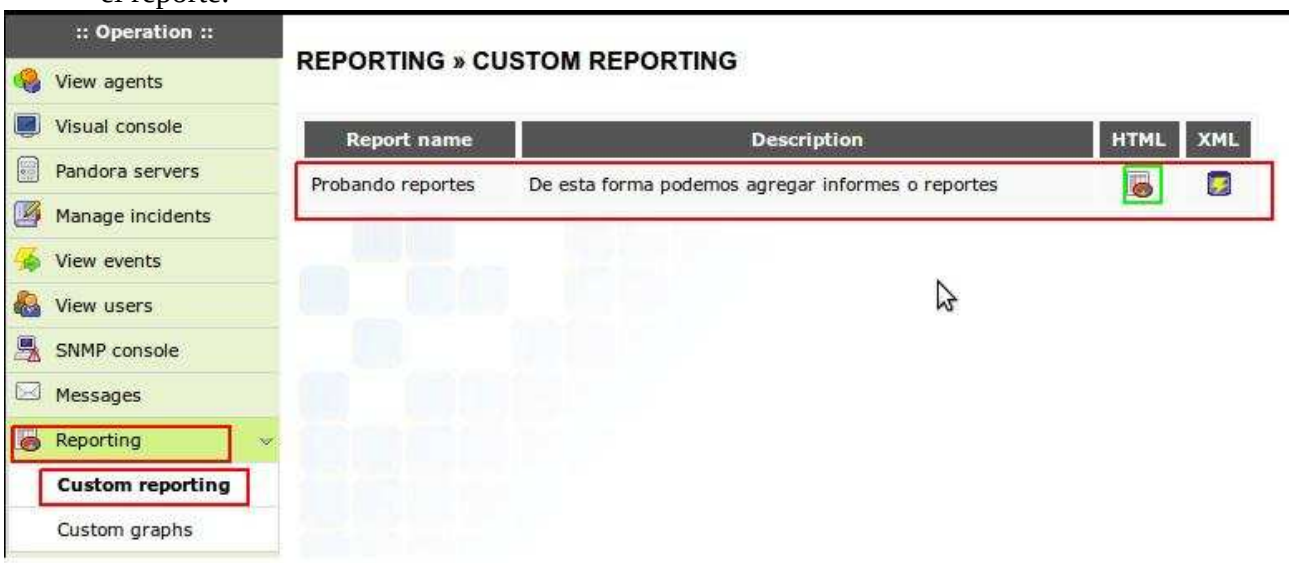
- Damos clic en “create report”:

- Llenamos los campos de acuerdo a nuestras necesidades.

- Una vez le damos en “create” nos aparece una nueva opción para adherir items, que son especies de informes jerarquicos, que se adhieren al reporte raiz. Veamos entonces:

Nota: una vez desplegado el menú, que trae la opción "Reporting type" nos muestra una serie de items que debemos explorar.

- Para observar los reportes, vamos a la sección "Operation" damos clic en "Reporting" y luego en "Custom reporting" damos clic en el icono resaltado en verde, y nos debe mostrar el reporte.



Añadir elementos a un mapa visual

Podemos añadir una especie de un dibujo de topología de nuestra red o de lagunas subredes.

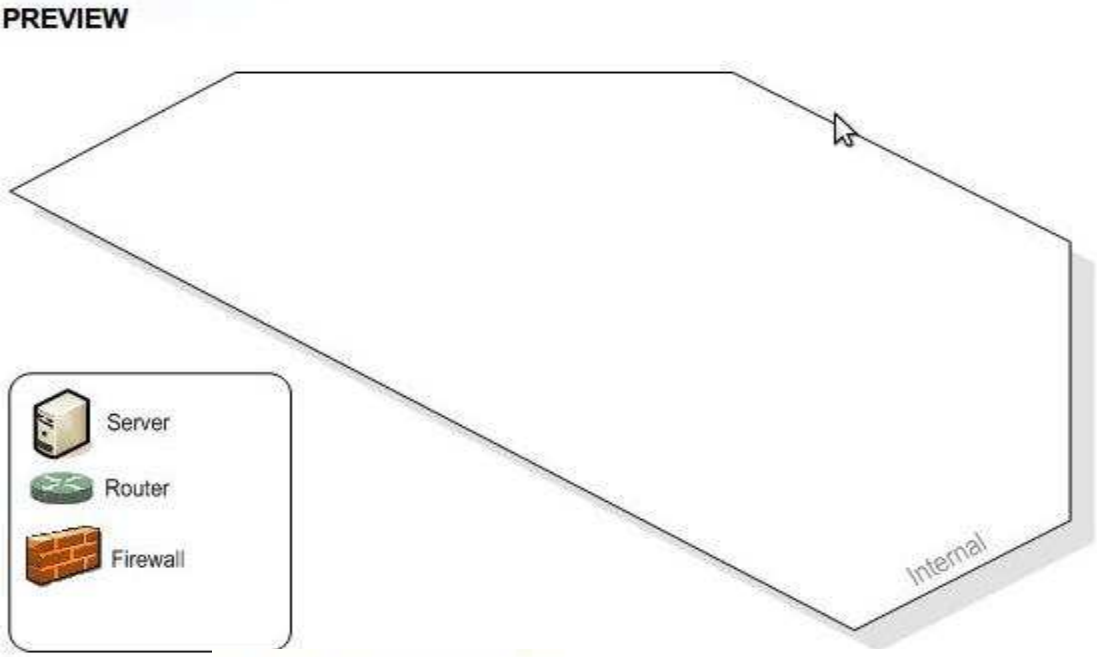
- Para esto vamos a la sección “Administration” y luego en “Map builder”:

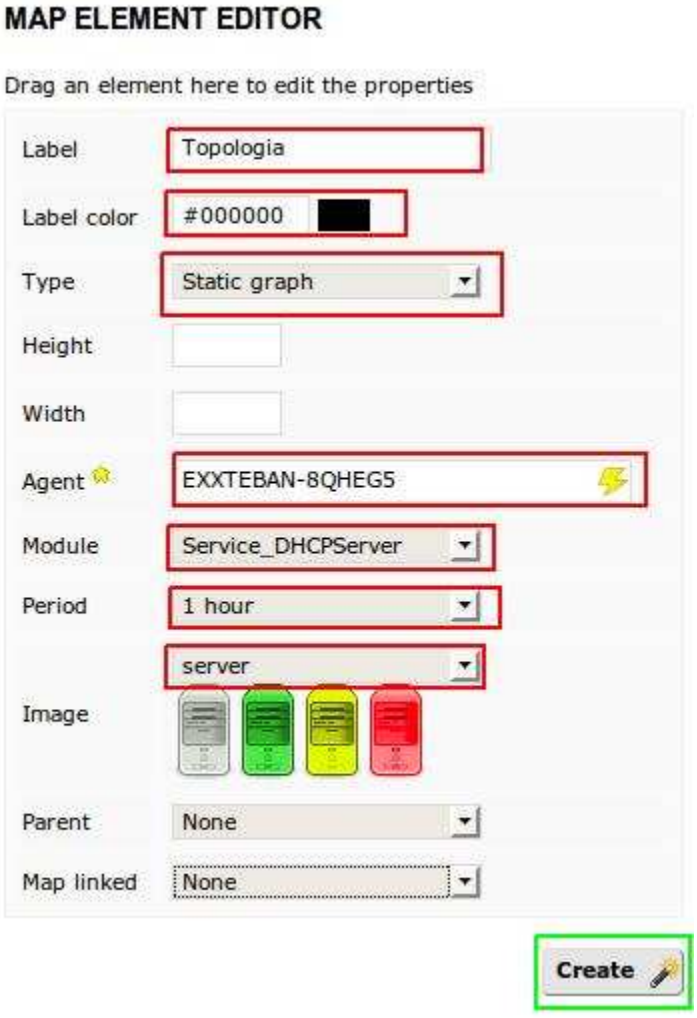
- Damos clic en “Create”:

- Luego llenamos los campos:

Name: Nombre de nuestra topología gráfica.
Group: Grupo al que pertenecen los agentes.
Background: Imagen en la que vamos a representar la topología.

- Nos aparece entonces la imagen que hallamos escogido, para empezar a ubicar los complementos, que hacen parte del mapa o topología física.





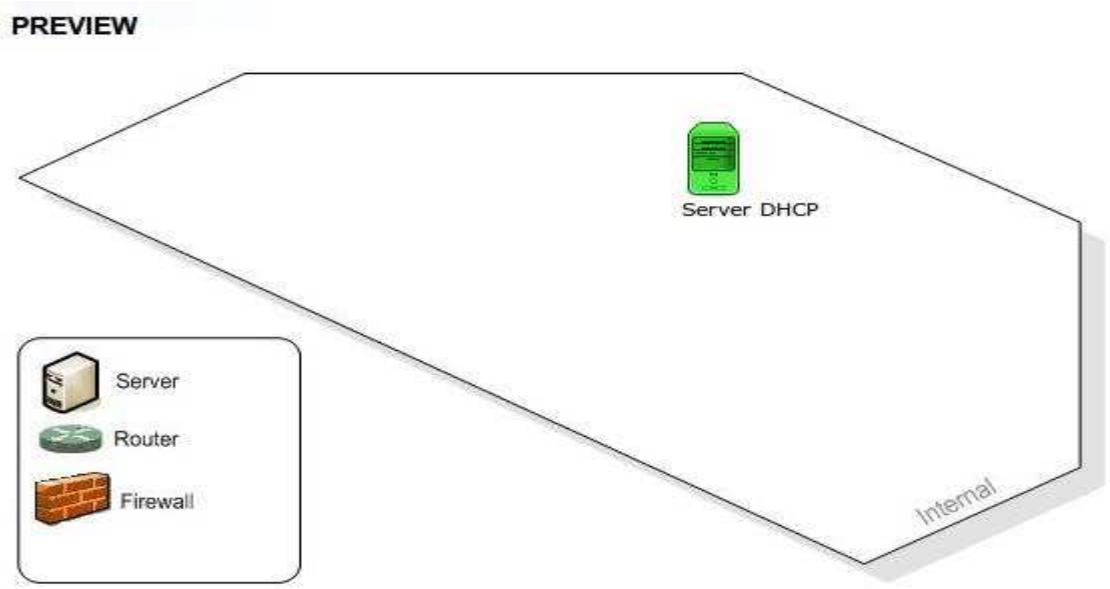
- Ahora vamos a mostrar como insertar complementos, tambien pueden insertarsen modulos..etc...

- Vemos en el lado de abajo las siguientes opciones en algo que se llama “Map element editor”

Label: Descripción del elemento que vamos a agregar.
Type: Hay 4 tipos debemos explorarlos, en nuestro caso escogimos uno de estilo gráfico.
Agent: Nombre del agente
Module: Modulo que vamos a representar
Image: Nos muestra una lista con representaciones de diferentes dispositivos en nuestro caso escogimos un servidor.

- Por ultimo damos clic en “Create”, y en el lado de la imagen, nos aparece el elemento, el cual situaremos donde queramos.

- Nos mostraría algo así:

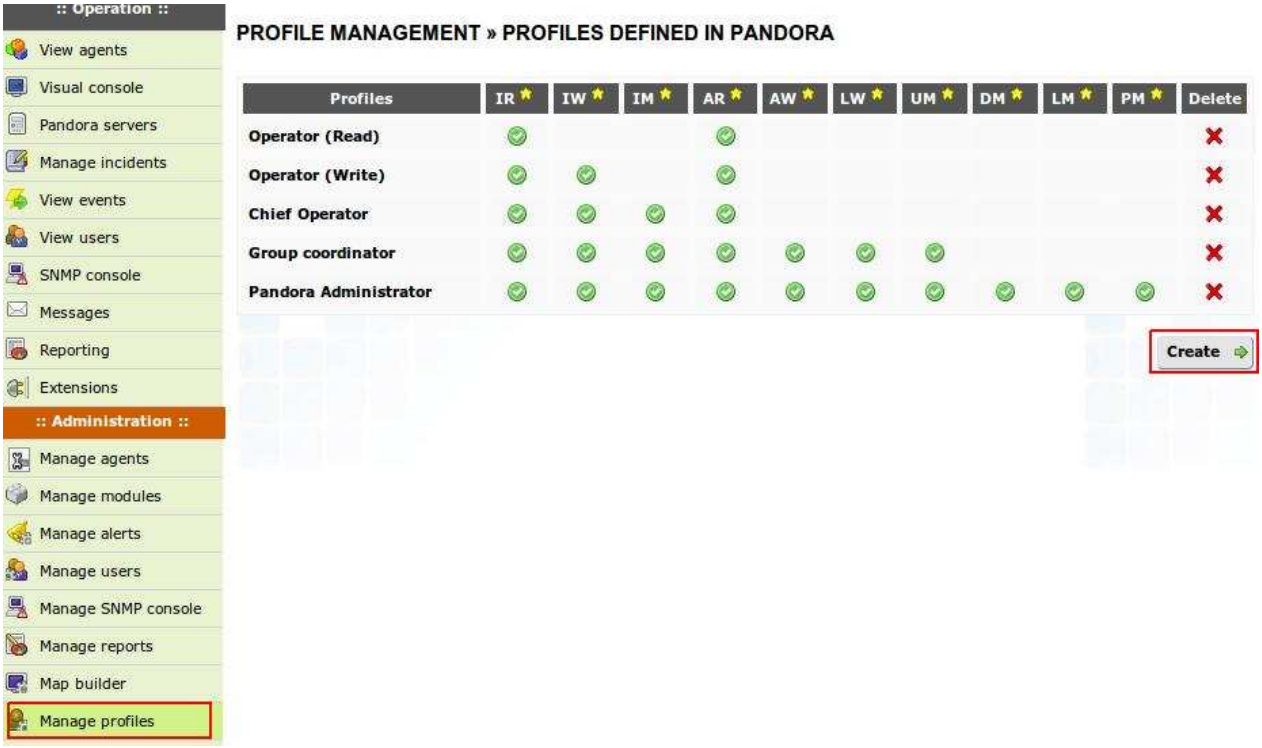


- Si queremos borrar algún complemento, vamos a “Map element trash”, seleccionamos el elemento y luego damos clic en “Delete”

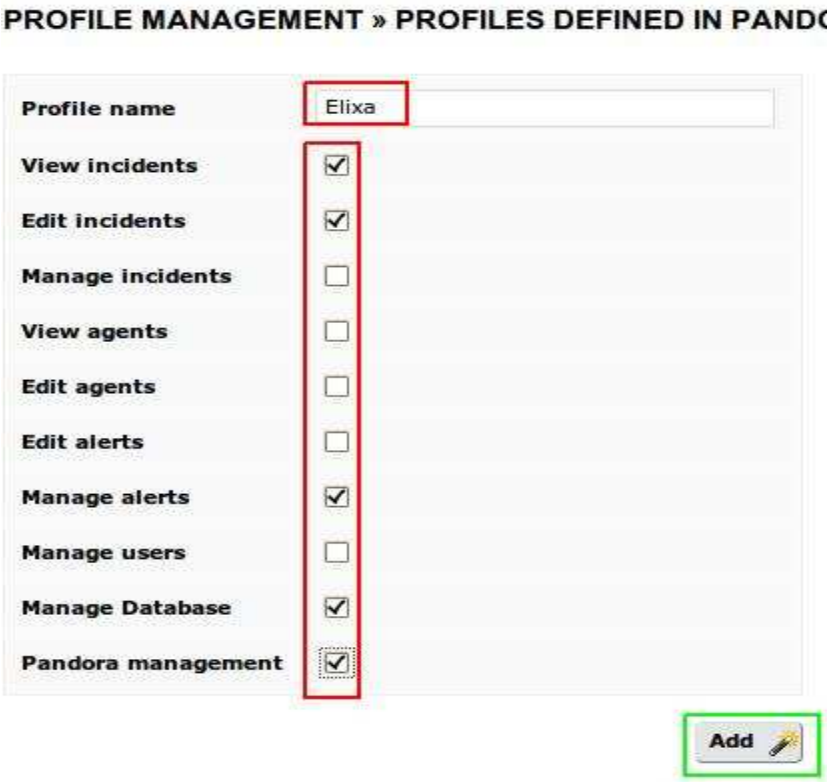
Para observar los mapas nos ubicamos en la sección “Operation” y luego damos clic en “**Visual console**”

Perfiles, grupos y ACL

Cuando tenemos una administración descentralizada, debemos crear perfiles administrativos, con ciertos permisos, esto lo hacemos desde la seccion “Administration” en el boton “Manage profiles”, si queremos crear uno nuevo, damos clic en “Create”



- Allí ingresamos el nombre del usuario, y le damos los permisos correspondientes, por ultimo damos clic en “Add”:



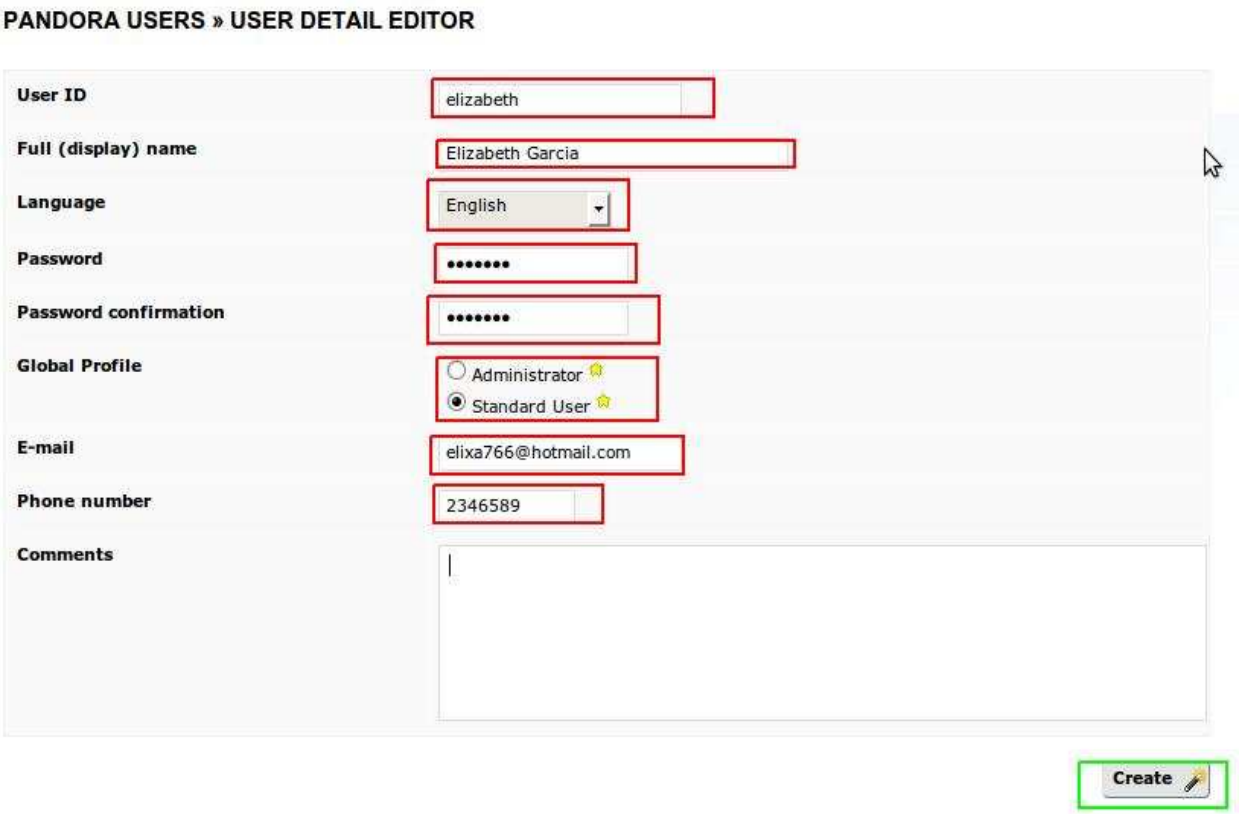
- Nos aparece la siguiente ventana donde nos muestra en nuevo usuario, y nos da la opción de

borrarlo también, desde la X roja:

Nota: Un perfil no es el usuario en si, solo es una serie de características, en las cuales se añaden usuarios.

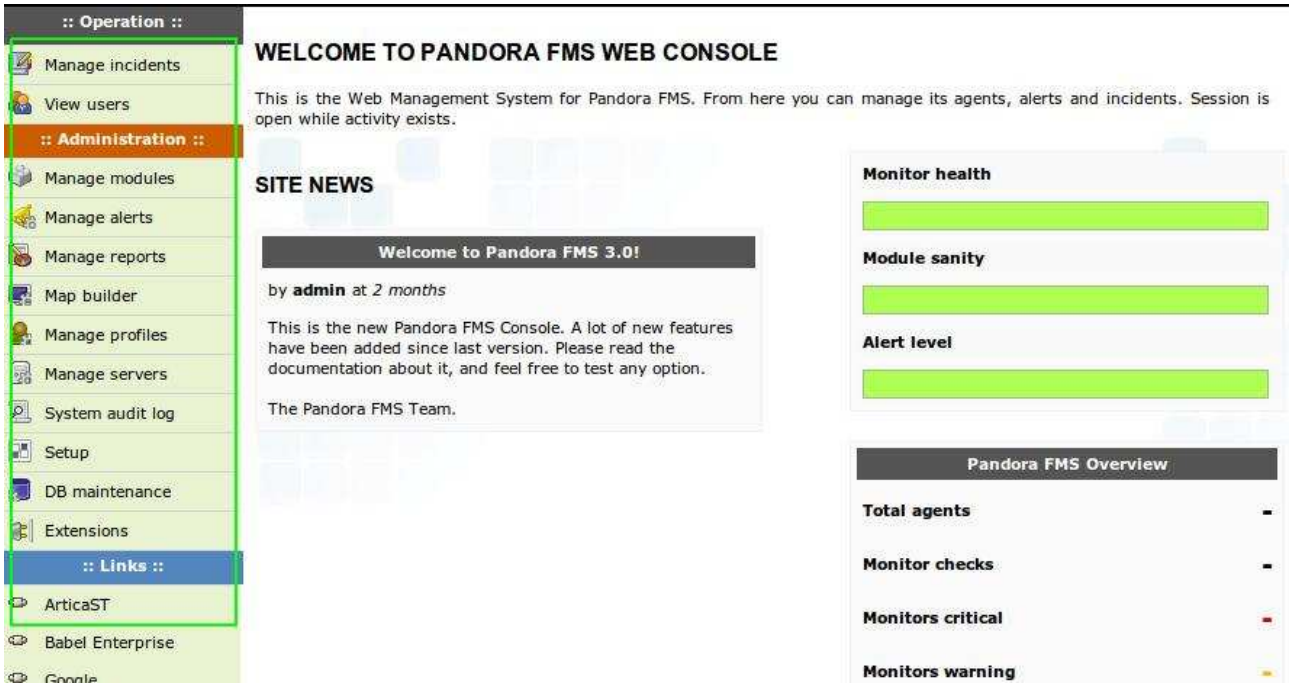
- Vamos entonces a añadir un usuario: Para esto vamos a la sección “Administration” y luego

damos clic en manage users, por ultimo clic en “Create user”

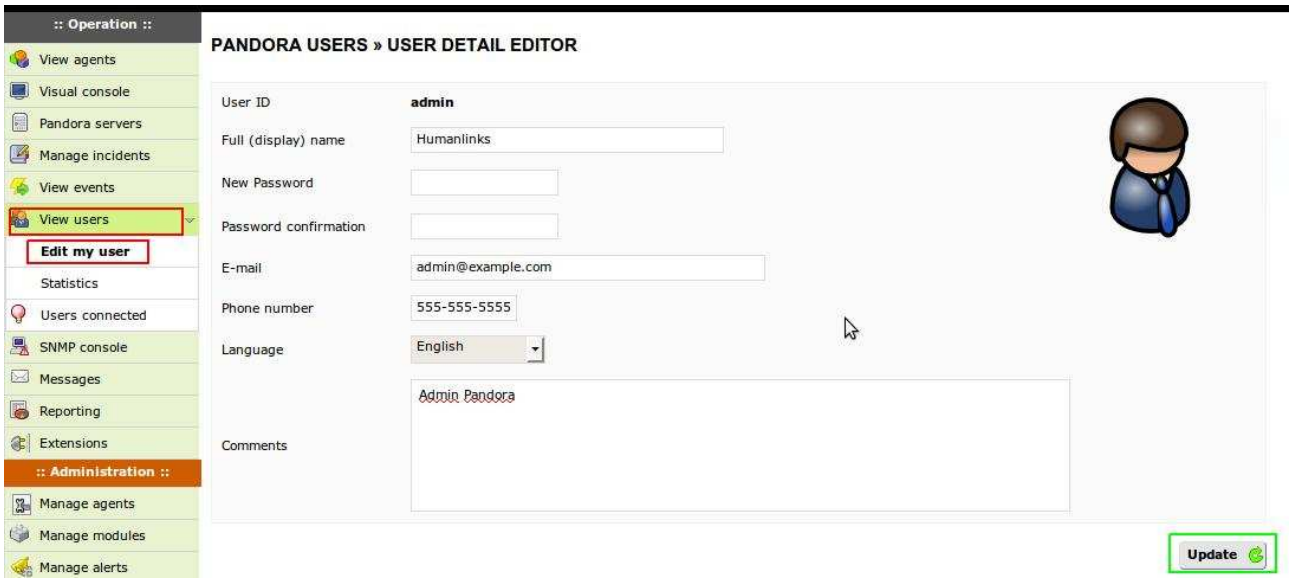


- Rellenamos los campos con sus respectivos datos, y damos clic en “Create”:
- Podemos entonces añadir el usuario a muchos grupos, y a un perfil, en la parte de abajo nos aparece este menú donde escogeremos el grupo y el perfil, luego damos clic en el icono “+”

- Vemos entonces que cuando ingresamos a la cuenta del nuevo usuario, no nos aparecen todas las opciones en el panel de administración que nos aparece con el usuario administrador.



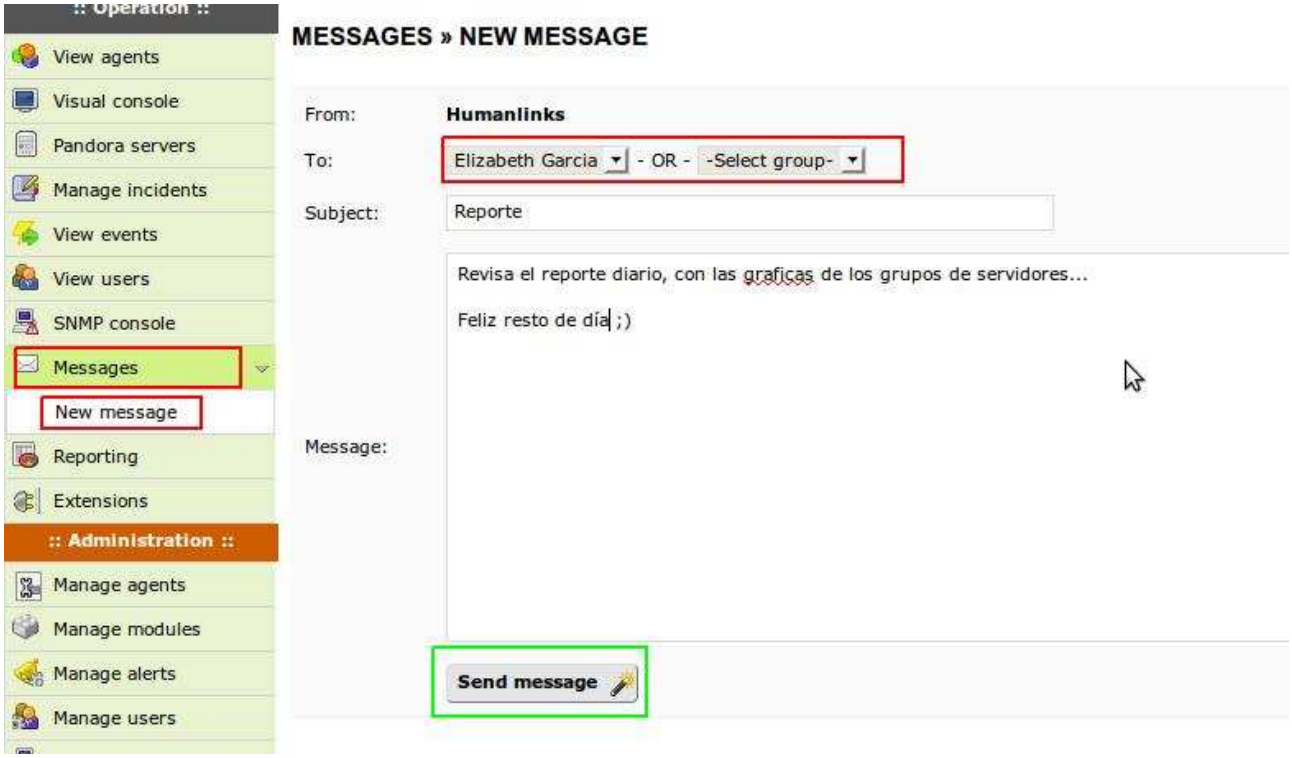
- Para editar nuestro usuario en el que estamos logueados, debemos ubicarnos en la sección “Administration” luego en “View users” y por ultimo clic en “Edit my users”, si queremos



cambiar algo, lo cambiamos y damos clic en “Update”:

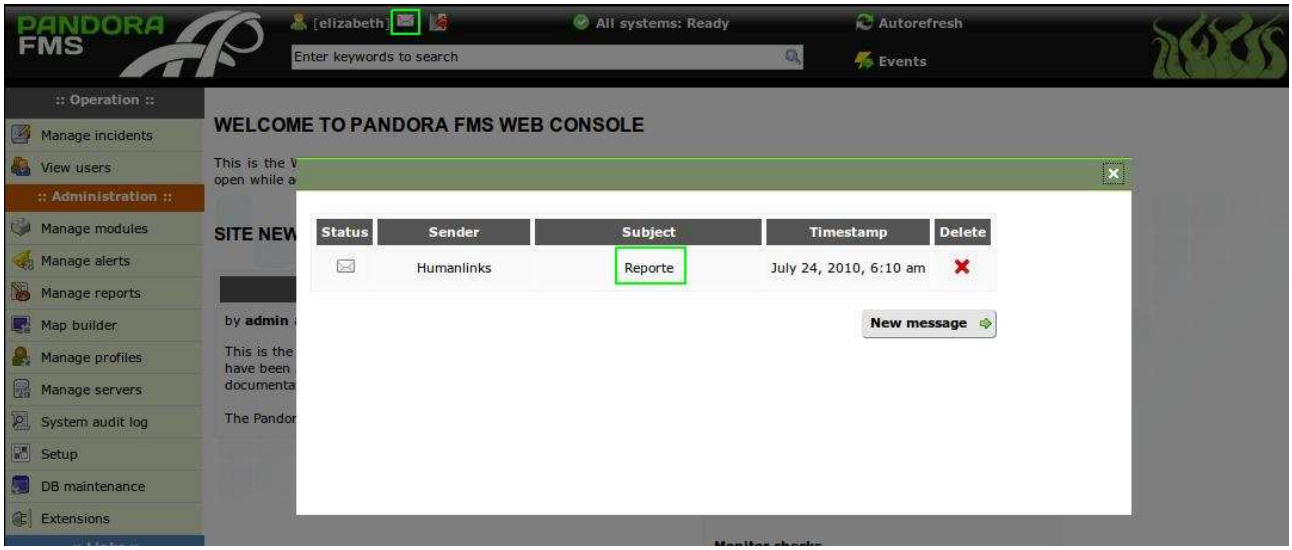
Envío y recepción de mensajes entre usuarios de Pandora

- Para enviar un mensaje, a uno de los usuarios Pandora, podemos hacerlo yendo a la sección “Operation” luego en “Messages” y por ultimo clic en “New message”, Una vez allí llenamos los campos necesarios, y damos clic en “Send message”



Nota: Vemos que en la opcion “**To**” podemos enviar el mensaje ya sea a un usuario o a un grupo completo.

- Ahora nos logueamos con el usuario receptor del mensaje, y verificamos si llego, vemos en la parte superior un icono con un sobre, damos clic allí, y luego en el nombre del tema:



- Vemos entonces el mensaje:

Logs del servidor Pandora FMS

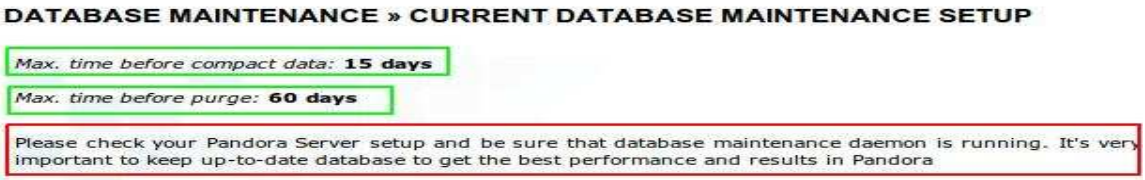
Podemos ver los logs o sucesos de nuestro servidor, ubicándonos en la sección “Administration” y luego clic en “systema audit logs”.

Gestión de la base de datos de Pandora FMS

La base de datos de Pandora, podría decirse que es el kernel de esta gran herramienta de monitoreo y gestión, por tal motivo la buena configuración y mantenimiento, es un punto critico para el buen funcionamiento de esta plataforma.

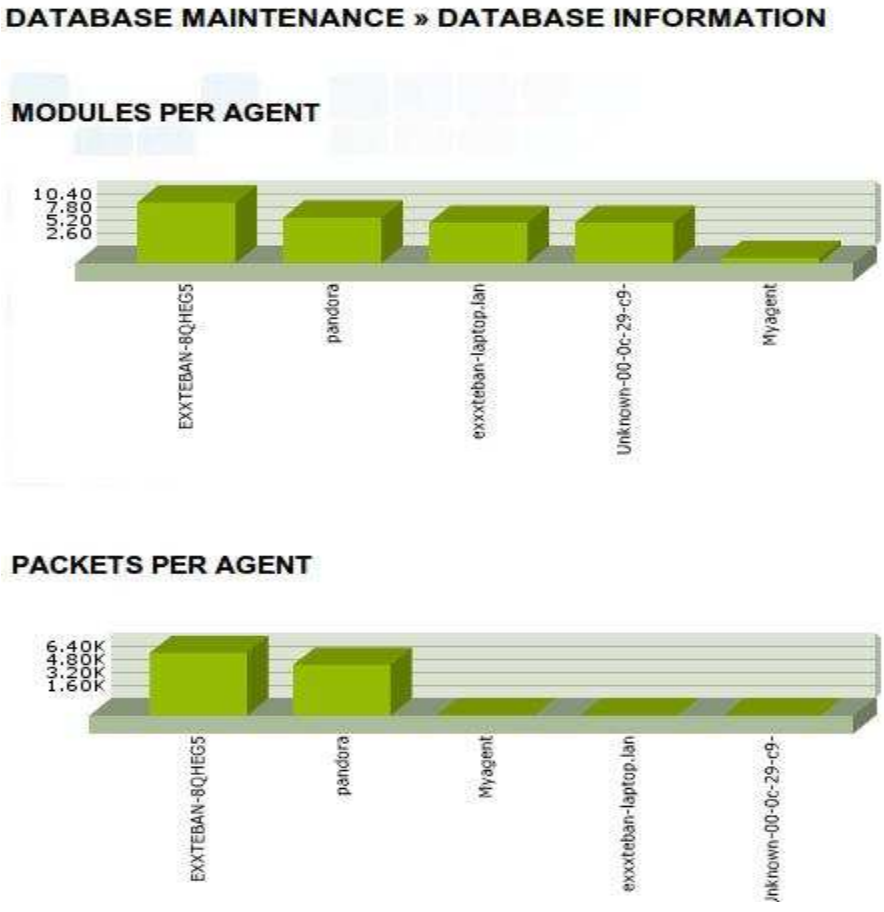
- Para ingresar en la administración de la base de datos de Pandora la cual trabaja con MYSQL, podemos hacerlo desde la consola digitando comandos, o hacerlo por la interfaz gráfica de Pandora, de el siguiente modo:

- Una vez allí nos muestra una gráfica con información general con el tiempo que se tarda en compactar las estadísticas, compactar significa hacer un resumen sin perder datos importantes, lo cual facilita que no llenemos el servidor de datos innecesarios.

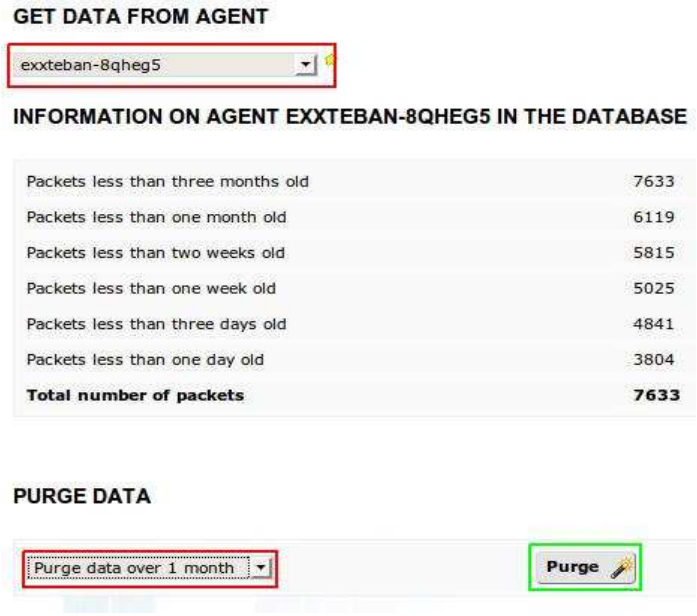


-

r estadísticas gráficas, de modulo por agente y paquetes por agente damos clic en “DB Information”



- Para borrar o purgar datos, que son innecesarios en determinado periodo de tiempo vamos a la opción “Databasepurge” alli seleccionamos el agente y en la opción “PURGE DATA” le decimos cada cuanto vamos a purgar datos: En nuestro caso seleccionamos el agente “Exxteban” y dijimos que purgara la base de datos cada 1 mes.

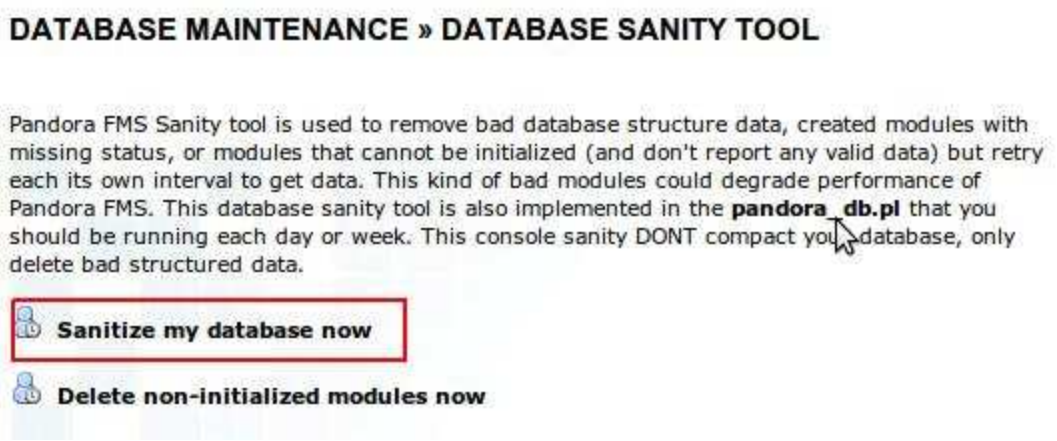


Mantenimiento de la base de datos:

- Cuando hablamos de mantenimiento nos referimos a borrar o configurar elementos que estén afectando la operabilidad del servidor Pandora, veamos entonces donde ingresar, para realizar estas tareas desde la consola:

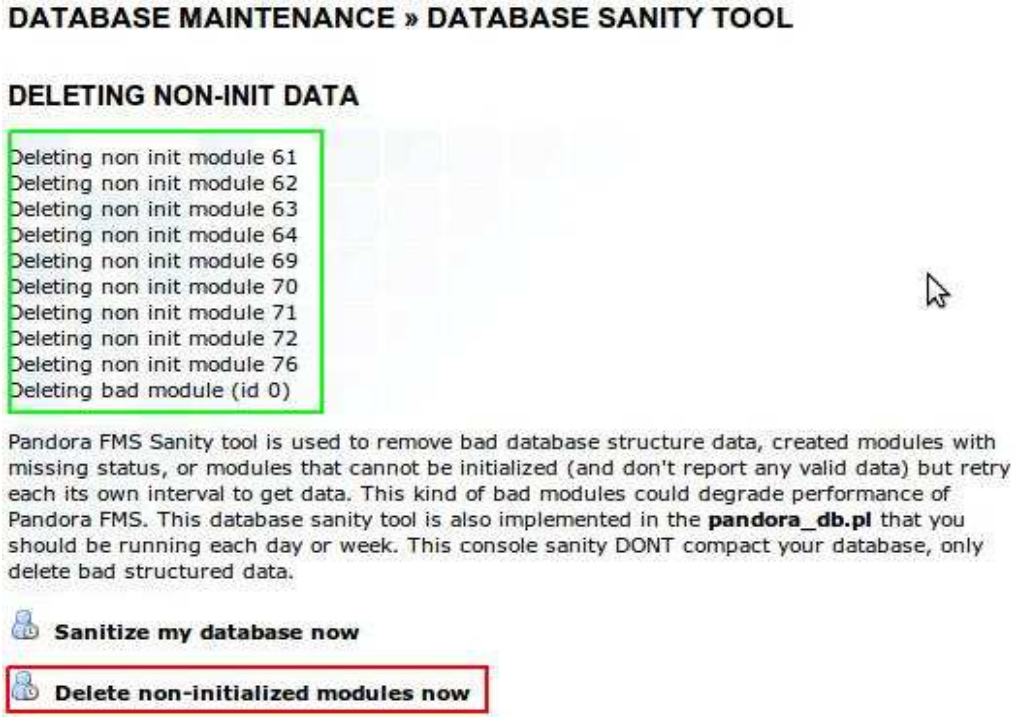
- Una vez allí vemos dos opciones una de ella es la de limpieza que se define como “Satanize my datebase now”.Permite borrar módulos, o estructuras mal configuradas.

- Hay otra opción



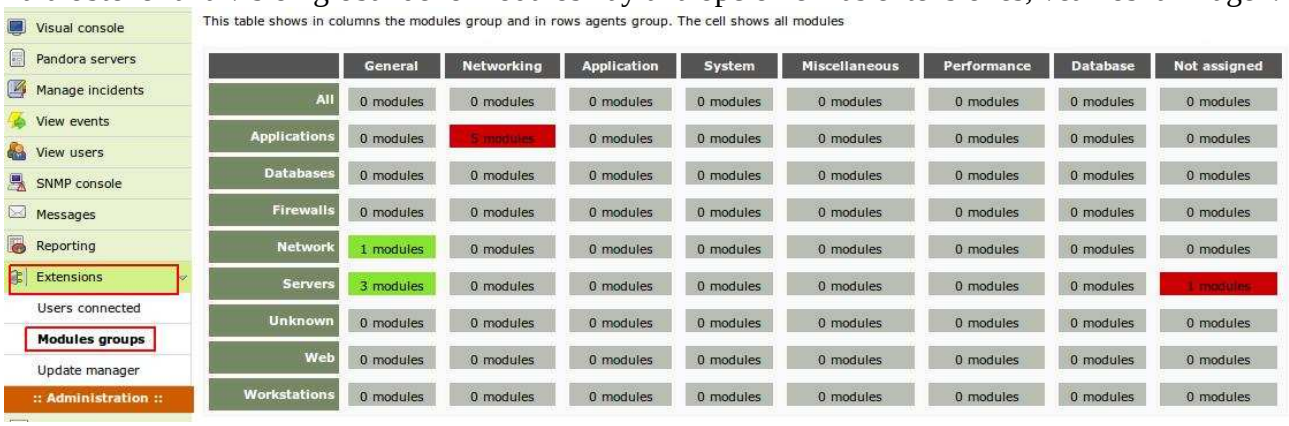
"Delete non-initialized modules now" la cual borra modulos nunca inicializados los cuales nunca se inizializaron por mala configuración o porque nunca se recibieron datos.

- Miramos los datos que nos arroja:



Nota: Estas acciones se realizan automáticamente cada determinado tiempo, pero esta es la forma manual de realizarlas.

Visualización global de los módulos:
Para obtener una visión global de lo módulos hay una opción en las extensiones, veamos la imagen:



Para mas información puede ingresar en esta URL:
http://pandorafms.org/index.php?lang=es&sec=project&sec2=documentation

Conclusiones

- Entendimos lo extenso que puede llegar a ser este tema, y lo importante que es la buena gestión y monitoreo en un ambiente empresarial.
-
- Intentamos profundizar en cada aspecto, en la medida de lo posible, descubriendo nuevos términos, protocolos, estrategias, sistemas, y pasos a seguir, en la elaboración de nuestro proyecto.
-
- Esperamos que este documento sirva a muchas personas que buscan una herramienta de monitoreo, que este al alcance, y además que tenga código abierto, para la mejora y la distribución. Intentamos ser muy claros en cada tema, y creemos que un lector con capacidad básica a media, entenderá la instalación y configuración de este servidor Pandora