

# Monitorización de Redes

Zabbix vs Pandora FMS



Juan María Cobo Jódar

2º ASIR

# Índice

<b>1. Introducción</b> .....	<b>4</b>
1.2 Objetivos .....	4
<b>2. Escenario</b> .....	<b>5</b>
<b>3. Introducción Zabbix</b> .....	<b>6</b>
3.1 ¿Qué es Zabbix? .....	6
3.2 Características principales Zabbix .....	8
3.3 Funcionamiento de Zabbix.....	8
<b>4. Instalación de Zabbix</b> .....	<b>10</b>
4.1 Instalación de paquetes.....	10
4.2 Creación y configuración de la base de datos.....	11
4.3 Inicio de servicios.....	12
4.4 Instalación de agente en el servidor Zabbix.....	12
4.5 Configuración interfaz de Zabbix.....	13
<b>5. Configuración Zabbix</b> .....	<b>17</b>
5.1 Configuración agentes .....	17
5.1.1 Configuración agente Servidor Zabbix .....	17
5.1.2 Configuración agente Máquina Debian .....	17
5.1.3 Configuración agente Máquina Windows .....	18
5.2 Configuración principal Zabbix .....	20
5.2.1 Configuración de host .....	20
5.2.2 Configuración de Item .....	21
5.2.3 Configuración de Triggers .....	22
5.2.4 Configuración de notificaciones .....	24
5.2.5 Configuración de plantillas .....	26
5.2.6 Configuración Auto-registro .....	28
<b>6. Introducción Pandora FMS</b> .....	<b>31</b>
6.1 ¿Qué es Pandora FMS? .....	31
6.2 Funcionalidades de Pandora FMS .....	31
6.3 Funcionamiento de Pandora FMS .....	33
<b>7. Instalación de Pandora FMS</b> .....	<b>34</b>
7.1 Requisitos Mínimos .....	34
7.2 Creación base de datos .....	34
7.3 Instalación Pandora FMS en Centos7 .....	34
7.4 Instalación de paquetes .....	36
7.5 Configuración inicial .....	36
7.5.1 Pasos iniciales .....	36

7.5.2 Configuración inicial de la Consola .....	37
7.5.3 Configuración inicial básica del Servidor .....	39
<b>8. Configuración Pandora FMS .....</b>	<b>40</b>
8.1 Configuración Agentes .....	40
8.1.1 Configuración agente en CentOS .....	40
8.1.2 Configuración agente Debian .....	40
8.1.3 Configuración agente Windows .....	41
8.2 Configuración principal Pandora FMS .....	41
8.2.1 Configuración de equipos .....	41
8.2.2 Configuración de tarea de reconocimiento .....	43
8.2.3 Configuración de módulos .....	44
8.2.4 Configuración de alertas .....	46
8.2.5 Configuración de notificaciones .....	47
8.2.6 Configuración de plantillas .....	49
<b>9. Comparativa de herramientas .....</b>	<b>51</b>
<b>10. Configuración adicional Zabbix .....</b>	<b>54</b>
10.1 Configuración aplicación Java .....	54
10.2 Monitorización de Logs .....	57
<b>11. Conclusión .....</b>	<b>59</b>
<b>12. Referencias y bibliografía .....</b>	<b>60</b>

# 1. Introducción

Tener una herramienta de monitorización es prácticamente imprescindible para cualquier empresa o particular que quiera tener el control de sus equipos, servicios de red, servidores o hardware de red.

Por eso en este proyecto se hablará sobre algunas de las herramientas de monitorización más presentes en la actualidad, como son Zabbix y Pandora FMS.

Zabbix comenzó en 2001 como un proyecto nuevo, que parte desde cero y que dispone de un panel web que permite gestionarlo de forma centralizada, sin ficheros de configuración. Zabbix está enfocada tanto a la monitorización de estados como al rendimiento y la usabilidad.

Pandora surge en 2004 también como un proyecto nuevo. Al igual que Zabbix cuenta con un panel web que gestiona la información de manera centralizada. Pero a diferencia de Zabbix, Pandora cuenta con versiones de pago, que proporcionan la funcionalidad completa. Esta herramienta está orientada a grandes entornos y cubre aspectos como la monitorización de infraestructuras, negocios o aplicaciones.

## 1.2 Objetivos

El objetivo principal de este proyecto será el de implementar ambas herramientas, exponiendo cuales son las características y funcionalidades más importantes que presentan, y realizando una configuración básica del funcionamiento de cada una.

A continuación se mostraría una comparativa sobre las diferencias y similitudes encontradas al realizar las respectivas configuraciones, así como las características presentes y ausentes en cada una de ellas.

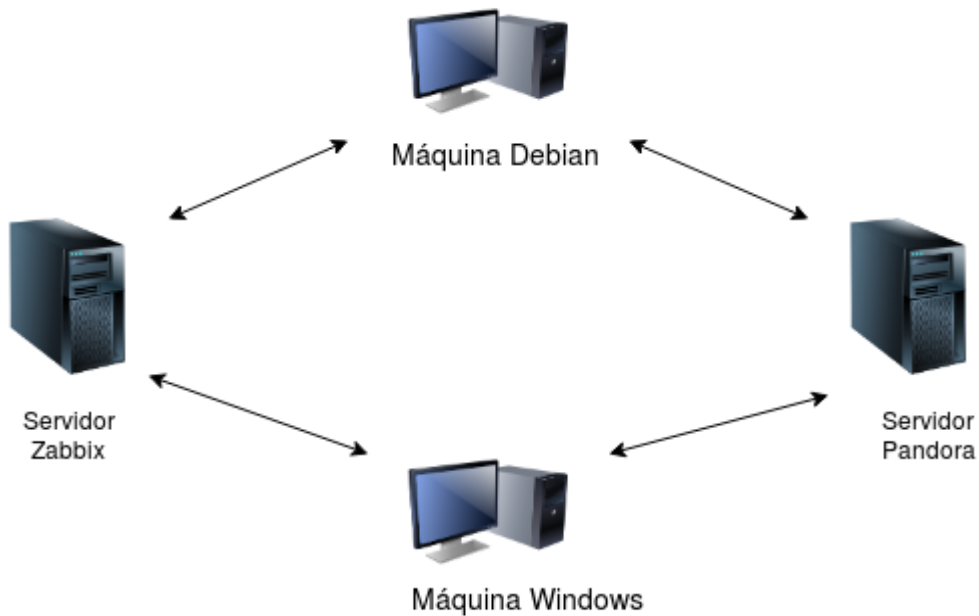
Por último se realizaría una configuración un poco más avanzada de aquella herramienta que se adaptara mejor a mis necesidades o me pareciera más completa.

## 2. Escenario

El escenario de este proyecto estará compuesto por cuatro máquinas virtuales utilizando la herramienta VMware:

- Una actuará de servidor principal para la herramienta Zabbix.
- Una actuará de servidor principal para la herramienta Pandora FMS.
- Las otras dos serán las máquinas de las que recopilaremos información a través de agentes instalados de cada una de las herramientas.

	<b>IP Interna</b>	<b>Sistema Operativo</b>
<b>Servidor Zabbix</b>	10.0.0.4	Centos 7
<b>Servidor Pandora FMS</b>	10.0.0.5	Centos 7
<b>Máquina Agente Debian</b>	10.0.0.6	Debian 9
<b>Máquina Agente Windows</b>	10.0.0.7	Windows 7



## 3. Introducción Zabbix

### 3.1 ¿Qué es Zabbix ?

Zabbix es un software de código abierto que monitoriza numerosos parámetros de una red y el rendimiento, disponibilidad e integridad de los servidores y equipos.

Esta herramienta ofrece funciones de informes y visualización de datos basadas en la información almacenada.

La forma de acceder a todos los informes y estadísticas de Zabbix, así como los parámetros de configuración, es a través de una interfaz web.

Zabbix utiliza un mecanismo de notificación flexible que permite a los usuarios configurar alertas basadas en correo electrónico para prácticamente cualquier evento.

Con una configuración adecuada, Zabbix puede desempeñar un papel importante en la monitorización de la infraestructura de TI, ya sean organizaciones pequeñas con algún servidor como grandes empresas con multitud de servidores.



### 3.2 Características principales Zabbix

Zabbix ofrece múltiples opciones a la hora de la monitorización, como por ejemplo:

#### **Recopilación de datos:**

- A través de Agentes recolectores disponibles en todas las plataformas
- Muestra la disponibilidad y hace comprobaciones de rendimiento
- Ofrece soporte para SNMP, IPMI, JMX, monitorización de VMware
- Se realiza en el servidor y en los agentes

#### **Monitorización personalizada:**

- Permite ejecutar scripts personalizados
- Carga de módulos nuevos para aumentar la funcionalidad y el rendimiento

### **Configuración de alertas:**

- Personalización del servicio de alertas, como por ejemplo cambio de mensaje según destinatario
- Escalado de respuesta a los problemas
- Envío de mensajes por diferentes métodos

### **Detección de problemas:**

- Funciones de predicción
- Diversos niveles de seguridad
- Análisis de datos históricos

### **Diferentes opciones de visualización:**

- Múltiples personalizaciones de gráficos, pudiendo combinar varios elementos en una sola vista
- Mapas de red
- Distintas configuraciones a la hora de monitorizar o visualizar los datos recopilados
- Informes detallados

### **Uso de plantillas:**

- Múltiples plantillas para un solo host
- Plantillas anidadas, por lo que el host hereda todos los elementos de una plantilla

### **Seguridad y autenticación:**

- Diferentes métodos de autenticación
- Cifrado en las comunicaciones entre los componentes de Zabbix
- Administración de los permisos de los usuarios

### **Automatización de entornos:**

- Detección de redes y dispositivos de red
- Registro automático de agentes
- Detección automática de sistemas de archivos, elementos o gráficos

## API Zabbix:

- Posibilidad de acceder a las funciones de Zabbix desde aplicaciones externas a través de la API de Zabbix.

### 3.3 Funcionamiento de Zabbix

Zabbix se instala en un servidor y se dedica a recolectar información. Cuenta con agentes para Linux, Mac y Windows que se instalan en los servidores o máquinas que interese monitorizar.

Zabbix almacena la información que recibe de los agentes y de los dispositivos de red que han sido configurados para su monitorización. Se puede acceder a esta información a través de la interfaz gráfica instalada en el Servidor Zabbix.

El agente espera las ordenes del servidor recolector Zabbix y enviará únicamente la información que le pida.

El funcionamiento de Zabbix es el siguiente:

1. El agente debe de estar configurado para informar al “Servidor Zabbix” en nuestra red, salvo en el caso del Hardware, que no se utiliza el agente.
2. A través del panel web del servidor se registran los equipos y dispositivos que deseamos monitorizar.
3. El equipo registrado se convierte en un elemento a ser monitorizado y recibe el nombre de “Host”.
4. Cada Host esta compuesto por elementos llamados “Items”, que son los módulos que recogen datos del Host, y en el caso de Hardware qué obtiene información del dispositivo.
5. Los Items usan “Keys”, que son parámetros de Zabbix que nos permiten indicar específicamente que tipo de información vamos a solicitarle al agente Zabbix o al Hardware.
6. Los “Trigger” en Zabbix son módulos que creamos a uno o múltiples Items para evaluar o comparar los valores recolectados por los Items con las condiciones que nosotros definamos. Por ejemplo, podemos crear un Trigger al Item con la Key llamada ‘Memoria’ e indicar que emita una alerta si este llega al 95% de ocupación.



7. Los Trigger generan eventos que se reflejan en el panel web, permitiendo mostrar gráficamente la situación del entorno.
8. Zabbix captura los eventos, pudiendo enviar alertas a través de correo electrónico. Esto se define en el Trigger.

## 4. Instalación de Zabbix

### 4.1 Instalación de paquetes

Realizaremos la instalación utilizando los paquetes oficiales de Zabbix para Centos7.

Lo primero que haremos será instalar los paquetes requeridos por Zabbix para el despliegue, teniendo en cuenta que las versiones de cada uno tienen que ser las siguientes:

Software	Versión
Apache	1.3.12 or later
PHP	5.4.0 or later
MySQL	5.0.3 or later

Instalamos los paquetes:

```
[root@zabbix usuario]# yum install httpd mariadb mariadb-server php
```

Instalamos el paquete de configuración del repositorio:

```
[root@zabbix usuario]# rpm -ivh
http://repo.zabbix.com/zabbix/3.4/rhel/7/x86\_64/zabbix-release-3.4-2.el7.noarch.rpm
Recuperando http://repo.zabbix.com/zabbix/3.4/rhel/7/x86\_64/zabbix-release-3.4-2.el7.noarch.rpm
advertencia:/var/tmp/rpm-tmp.pRAMj5: EncabezadoV4 RSA/SHA512 Signature, ID de clave a14fe591: NOKEY
Preparando... #####
[100%]
Actualizando / instalando...
  1:zabbix-release-3.4-2.el7 #####
[100%]
```

Habilitamos el repositorio de rpms para instalar paquetes adicionales que no están disponibles en la instalación básica.

Antes tendríamos que instalar el paquete yum-utils:

```
[root@zabbix usuario]# yum install yum-utils

[root@zabbix usuario]# yum-config-manager --enable rhel-7-server-optional-
rpms
Complementos cargados:fastestmirror
```

Instalamos los paquetes de zabbix necesarios para el servidor y el frontend:

```
[root@zabbix usuario]# yum install zabbix-server-mysql zabbix-web-mysql
```

## 4.2 Creación y configuración de la base de datos

Reiniciamos el servicio de mariadb y nos creamos una base de datos para el servidor:

```
[root@zabbix usuario]# systemctl restart mariadb

[root@zabbix usuario]# mysql -u root -p
MariaDB [(none)]> create database zabbix character set utf8 collate
utf8_bin;
MariaDB [(none)]> grant all privileges on zabbix.* to zabbix@localhost
identified by 'zabbix';
MariaDB [(none)]> quit;
```

Ahora importamos el esquema inicial y los datos para el servidor con MySQL.  
Se nos pedirá el ingreso de la contraseña de la base de datos recién creada:

```
[root@zabbix usuario]# zcat /usr/share/doc/zabbix-server-
mysql*/create.sql.gz | mysql -u zabbix -p
```

Realizamos la configuración de la base de datos del servidor. Para ello editamos el fichero **zabbix\_server.conf** para utilizar la base de datos creada:

```
[root@zabbix usuario]# nano /etc/zabbix/zabbix_server.conf  
  
DBHost=localhost  
DBName=zabbix  
DBUser=zabbix  
DBPassword=zabbix
```

### 4.3 Inicio de servicios

Iniciamos los servicios necesarios para el funcionamiento de zabbix:

```
[root@zabbix usuario]# systemctl restart zabbix-server httpd
```

Los habilitamos para que inicien automáticamente al iniciar el sistema:

```
[root@zabbix usuario]# systemctl enable zabbix-server httpd mariadb
```

### 4.4 Instalación de agente en el servidor Zabbix

Instalamos en el servidor el agente zabbix para poder recopilar información del servidor y poder mostrarla gráficamente mas adelante:

```
[root@zabbix usuario]# yum install zabbix-agent
```

Iniciamos y habilitamos el servicio para que inicie automáticamente con el sistema:

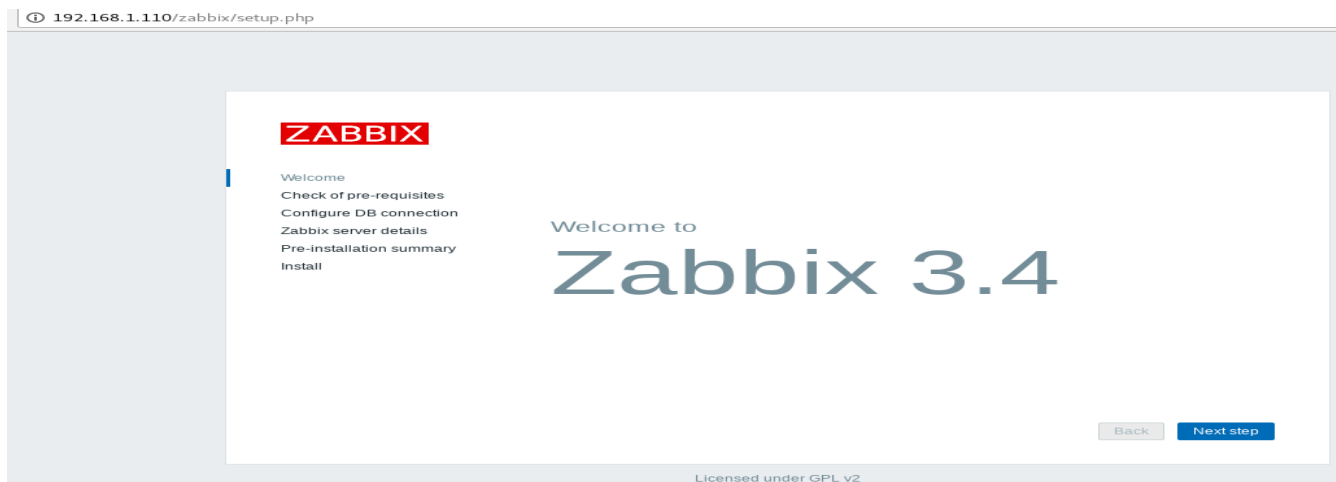
```
[root@zabbix usuario]# systemctl start zabbix-agent  
  
[root@zabbix usuario]# systemctl enable zabbix-agent
```

## 4.5 Configuración interfaz de Zabbix

Lo primero que haremos será irnos al fichero `/etc/httpd/conf.d/zabbix.conf` y descomentamos la línea `"date.timezone"` para establecer nuestra zona horaria:

```
[root@zabbix usuario]# nano /etc/httpd/conf.d/zabbix.conf  
  
php_value date.timezone Europe/Madrid
```

A continuación nos vamos a nuestro navegador e introducimos la URL: <http://serverIP/zabbix> para acceder al frontend:



Le damos a siguiente y nos aseguramos de que se cumplen todos los requisitos previos del software:

The screenshot shows the Zabbix installation pre-requisites check page. The browser address bar displays "192.168.1.110/zabbix/setup.php". On the left, a sidebar contains a navigation menu with the following items: Welcome, Check of pre-requisites, Configure DB connection, Zabbix server details, Pre-installation summary, and Install. The main content area is titled "Check of pre-requisites" and features a table comparing current values to required values for various PHP configurations. All items are marked as "OK".

	Current value	Required	
PHP version	5.4.16	5.4.0	OK
PHP option "memory_limit"	128M	128M	OK
PHP option "post_max_size"	16M	16M	OK
PHP option "upload_max_filesize"	2M	2M	OK
PHP option "max_execution_time"	300	300	OK
PHP option "max_input_time"	300	300	OK
PHP option "date.timezone"	Europe/Madrid		OK
PHP databases support	MySQL		OK
PHP bcmath	on		OK
PHP mbstring	on		OK
PHP option "mbstring.func_overload"	off	off	OK

At the bottom right of the table, there are two buttons: "Back" and "Next step".

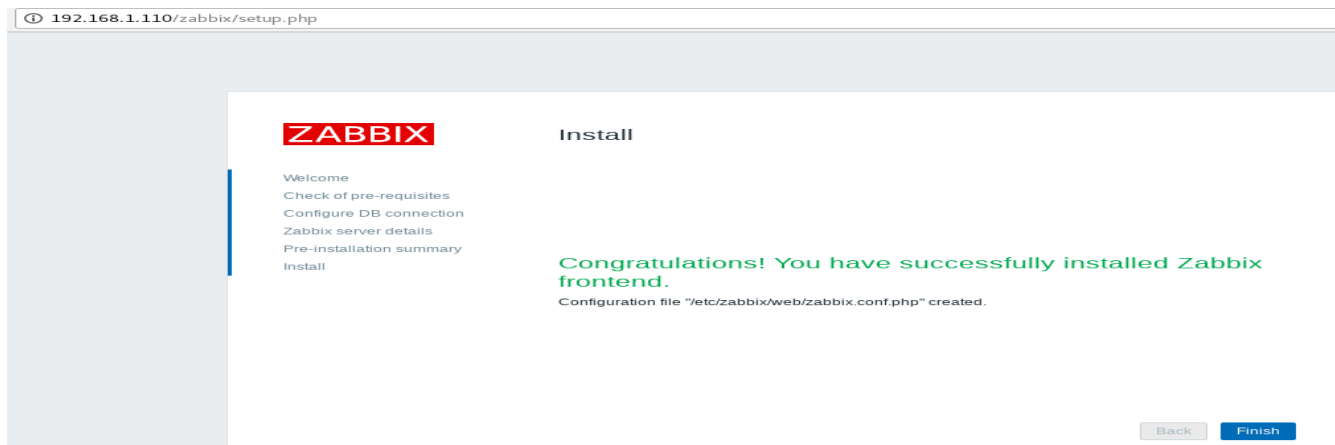
Ingresamos las credenciales de la base de datos MySQL antes creada para conectarse a ella:

The screenshot shows the Zabbix installation database configuration page. The browser address bar displays "No es seguro | 192.168.1.110/zabbix/setup.php". The sidebar navigation menu is the same as in the previous screenshot. The main content area is titled "Configure DB connection" and includes the instruction: "Please create database manually, and set the configuration parameters for connection to this database. Press 'Next step' button when done." Below this, there are several input fields: "Database type" (a dropdown menu set to "MySQL"), "Database host" (text input with "localhost"), "Database port" (text input with "0" and a note "0 - use default port"), "Database name" (text input with "zabbix"), "User" (text input with "zabbix"), and "Password" (password input field with masked characters). At the bottom right, there are "Back" and "Next step" buttons.

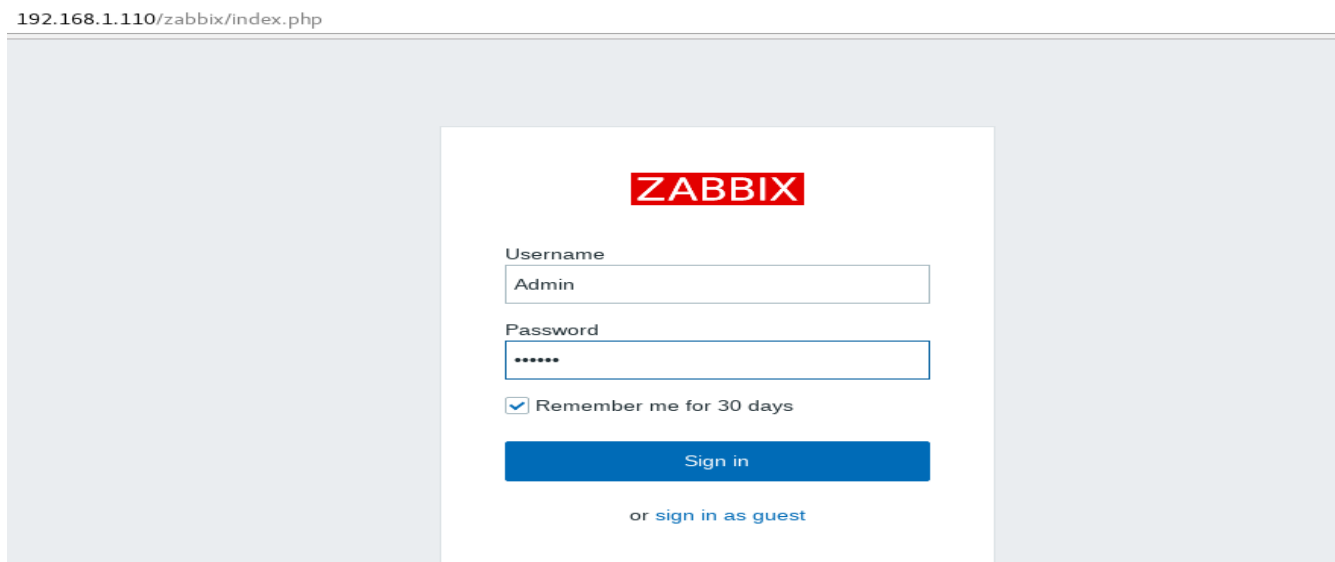
Añadimos los detalles del servidor:

The screenshot shows the Zabbix installation server details page. The browser address bar displays "No es seguro | 192.168.1.110/zabbix/setup.php". The sidebar navigation menu is the same as in the previous screenshots. The main content area is titled "Zabbix server details" and includes the instruction: "Please enter the host name or host IP address and port number of the Zabbix server, as well as the name of the installation (optional)." Below this, there are three input fields: "Host" (text input with "localhost"), "Port" (text input with "10051"), and "Name" (text input with "servidor"). At the bottom right, there are "Back" and "Next step" buttons.

Le damos a continuar y ya tendríamos instalado correctamente Zabbix:



El siguiente paso sería acceder al panel web con el usuario “**Admin**” y contraseña:”**zabbix**”:



Ya podríamos ver el panel web de Zabbix:

The screenshot shows the Zabbix web interface. The browser address bar displays `192.168.1.110/zabbix/zabbix.php?action=dashboard.view`. The Zabbix logo is in the top left, followed by navigation tabs: Monitoring, Inventory, Reports, Configuration, and Administration. A search bar and user profile icon are in the top right. Below the navigation is a secondary menu with links: Dashboard, Problems, Overview, Web, Latest data, Triggers, Graphs, Screens, Maps, Discovery, and Services. The main content area is titled "Dashboard" and includes an "Edit dashboard" button. It features several widgets:

- Favourite graphs**: "No graphs added." Updated: 20:51:27
- Favourite screens**: "No screens added." Updated: 20:51:28
- Favourite maps**: "No maps added." Updated: 20:51:27
- Host status**: A table with columns: Host group ▲, Without problems, With problems, Total. Content: "No data found." Updated: 21:02:34
- Problems**: A table with columns: Time ▼, Recovery time, Status, Info, Host, Problem • Severity, Duration, Ack, Actions. Content: "No data found." Updated: 21:02:34
- System status**: A table with columns: Host group ▲, Disaster, High, Average, Warning, Information, Not classified. Content: "No data found." Updated: 21:02:34



## 5. Configuración Zabbix

### 5.1 Configuración agentes

#### 5.1.1 Configuración agente Servidor Zabbix

Primero modificamos el fichero de configuración del agente en el servidor para que nos muestre los datos de la máquina. Para ello tenemos que añadirle la IP del servidor Zabbix en las siguientes líneas:

```
[root@zabbix usuario]# nano /etc/zabbix/zabbix_agentd.conf  
  
Server=10.0.0.4           <----- IP del Servidor Zabbix  
ListenIP=10.0.0.4       <----- IP de la máquina del Agente de Zabbix  
ServerActive=10.0.0.4   <----- IP del Servidor Zabbix  
Hostname=Zabbix server  <----- Nombre de la máquina del Agente de Zabbix
```

Reiniciamos el agente para acabar:

```
[root@zabbix usuario]# systemctl restart zabbix-agent
```

#### 5.1.2 Configuración agente Máquina Debian

Lo primero será instalar el agente mediante el comando:

```
root@debian:/home/usuario# apt install zabbix-agent
```

A continuación iniciamos el agente:

```
root@debian:/home/usuario# systemctl start zabbix-agent
```

Modificamos el fichero de configuración del agente para añadirle los siguientes datos:

```
root@debian:/home/usuario# nano /etc/zabbix/zabbix_agentd.conf

Server=10.0.0.4          <----- IP del Servidor Zabbix
ListenIP=10.0.0.6       <----- IP de la máquina del Agente de Zabbix
ServerActive=10.0.0.4   <----- IP del Servidor Zabbix
Hostname=debian         <----- Nombre de la máquina del Agente de Zabbix
```

Por último reiniciamos el servicio:

```
root@debian:/home/usuario# systemctl restart zabbix-agent
```

### 5.1.3 Configuración agente Máquina Windows

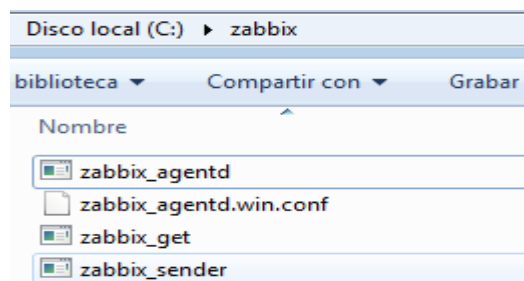
Lo primero que haremos será crearnos un directorio para almacenar los archivos de configuración del agente. En nuestro caso será:

```
C:\zabbix
```

A continuación nos descargamos y guardamos en la carpeta creada el paquete de zabbix\_agent para Windows a través del siguiente enlace:

```
https://www.zabbix.com/downloads/3.4.6/zabbix\_agents\_3.4.6.win.zip
```

Copiamos los ficheros ejecutables de la carpeta **bin** y el fichero de configuración de la carpeta **conf**, y los pegamos en la carpeta antes creada, quedando de la siguiente manera:



Configuramos el fichero **zabbix\_agentd.win.conf**, modificándole las siguientes líneas:

```
LogFile=c:\zabbix\zabbix_agentd.log
Server=10.0.0.4          <----- IP del Servidor Zabbix
ListenIP=10.0.0.7       <----- IP de la máquina del Agente Zabbix
ServerActive=10.0.0.4   <----- IP del Servidor Zabbix
Hostname=WINDOWS7       <----- Nombre de la máquina del Agente Zabbix
```

Ejecutamos el siguiente comando en la **cmd**(como administrador) para instalar el agente Zabbix como servicio de Windows:

```
C:\Windows\system32>C:\zabbix\zabbix_agentd.exe -c
"c:\zabbix\zabbix_agentd.win.conf" -i

zabbix_agentd.exe [3748]: service [Zabbix Agent] installed successfully
zabbix_agentd.exe [3748]: event source [Zabbix Agent] installed
successfully
```

Por último arrancamos el servicio y ya estaría configurado el agente de Zabbix en Windows:

```
C:\Windows\system32>C:\zabbix\zabbix_agentd.exe -c
"c:\zabbix\zabbix_agentd.win.conf" -s

zabbix_agentd.exe [1728]: service [Zabbix Agent] started successfully
```

## 5.2 Configuración principal Zabbix

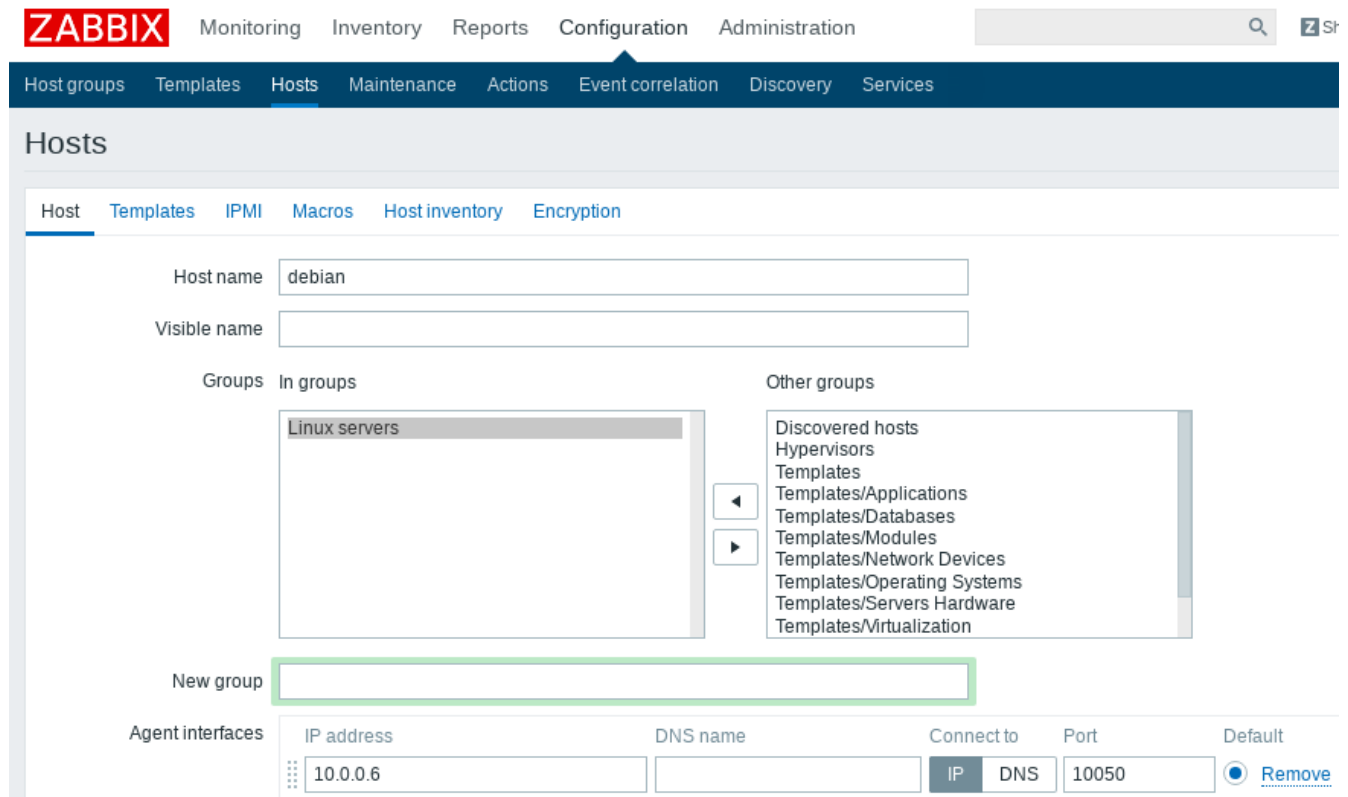
### 5.2.1 Configuración de host

En Zabbix se le denomina "host" a cualquier equipo, dispositivo o aplicación que se quiera monitorizar. Para agregar un nuevo host a Zabbix tendríamos que irnos a **“Configuración → Hosts”**.

Aquí haríamos clic en **“Create Host”** y nos mostraría el formulario de configuración.

Como mínimo tendríamos que introducir:

- Host Name → Nombre de host.
- Groups → Grupo que tiene aplicado los permisos de acceso.
- Dirección IP → Se introduce la IP del "Host". Debe de estar configurado previamente el agente del "Equipo monitorizado" apuntando a la IP del Servidor Zabbix.



The screenshot shows the Zabbix web interface for creating a new host. The navigation bar includes 'Monitoring', 'Inventory', 'Reports', 'Configuration', and 'Administration'. The 'Configuration' menu is expanded to show 'Hosts', 'Maintenance', 'Actions', 'Event correlation', 'Discovery', and 'Services'. The 'Hosts' page has sub-tabs for 'Host', 'Templates', 'IPMI', 'Macros', 'Host inventory', and 'Encryption'. The 'Host' tab is active, showing a form with the following fields:

- Host name:
- Visible name:
- Groups: In groups (Linux servers) and Other groups (Discovered hosts, Hypervisors, Templates, etc.)
- New group:
- Agent interfaces: A table with columns for IP address, DNS name, Connect to, Port, and Default.

IP address	DNS name	Connect to	Port	Default
<input type="text" value="10.0.0.6"/>	<input type="text"/>	<input type="button" value="IP"/> <input type="button" value="DNS"/>	<input type="text" value="10050"/>	<input checked="" type="radio"/> <a href="#">Remove</a>

Por último guardaríamos esta configuración y ya tendríamos el host en la lista de Host.

Para que el agente del servidor le reporte correctamente vamos a configurar el **“Zabbix server”**. Nos vamos a **“Configuration → Hosts → Zabbix Server → Agent Interfaces”** e introducimos la IP interna del servidor, en nuestro caso la 10.0.0.4

Vemos el resultado:

<input type="checkbox"/>	Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Templates	Status	Availability	Agent encryption
<input type="checkbox"/>	debian	Applications	Items	Triggers	Graphs	Discovery	Web	10.0.0.6: 10050		Enabled	ZBX   SNMP   JMX   IPMI	NONE
<input type="checkbox"/>	Zabbix server	Applications 11	Items 68	Triggers 46	Graphs 11	Discovery 2	Web	10.0.0.4: 10050	Template App Zabbix Server, Template OS Linux (Template App Zabbix Agent)	Enabled	ZBX   SNMP   JMX   IPMI	NONE

## 5.2.2 Configuración de Item

Los Items (elementos que recogen datos del host) se agrupan por Host. Para agregar un Item nuevo nos vamos a “**Configuration** → **Hosts**”, y marcamos el Host al que queremos añadirle el Item.

A continuación seleccionamos las pestañas “**Items** → **Create Item**” y configuramos las siguientes opciones:

- Name → Nombre que recibirá el Item.
- Key → Indicamos que tipo de información vamos a solicitarle al Agente Zabbix.
- Type of information → Se indica el formato de los datos que vamos a recibir.

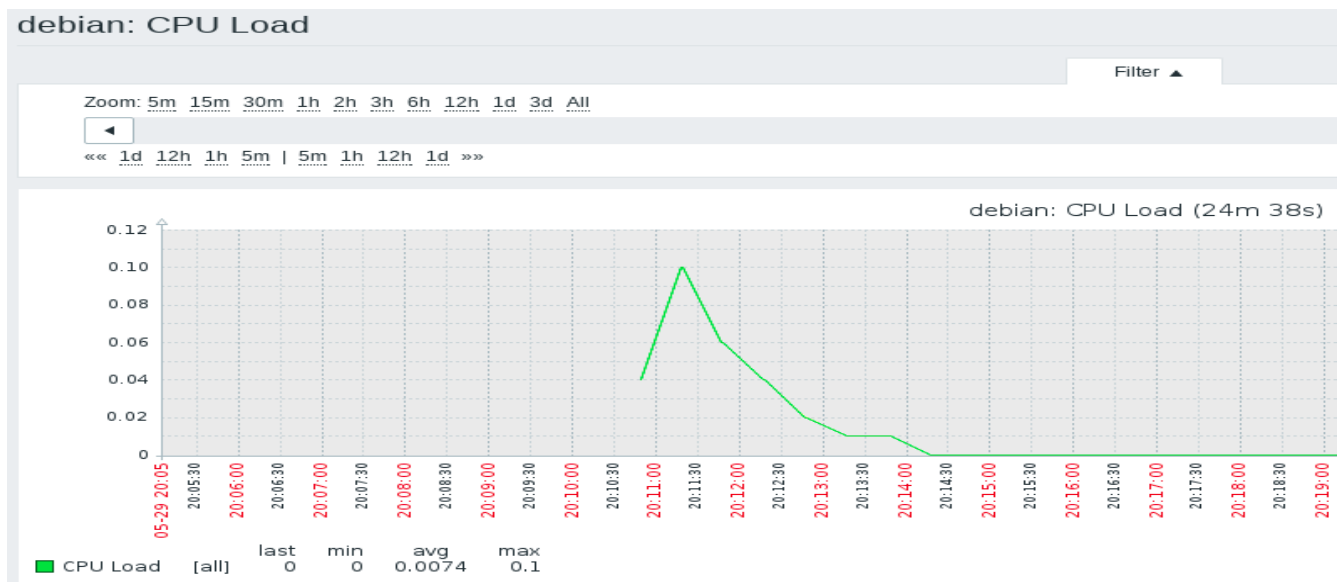
En nuestro caso mostraremos como ejemplo la carga de la CPU:

The screenshot shows the Zabbix web interface. At the top, there is a navigation bar with the ZABBIX logo and menu items: Monitoring, Inventory, Reports, Configuration, and Administration. Below this is a sub-navigation bar with: Host groups, Templates, Hosts, Maintenance, Actions, Event correlation, Discovery, and Services. The main content area is titled 'Items' and has a breadcrumb trail: All hosts / debian. The configuration form is for an 'Item' in the 'Preprocessing' section. The form fields are: Name: CPU Load; Type: Zabbix agent (dropdown); Key: system.cpu.load (with a 'Select' button); Host interface: 10.0.0.6 : 10050 (dropdown); Type of information: Numeric (float) (dropdown).

Guardamos y ya podríamos ver el Item en la lista de Items.

Para ver los datos recopilados nos vamos a **“Monitoring → Latest data”** y luego clic en el signo “+” en **“other”**.

Para visualizar la información gráficamente dentro de la pestaña anterior solo tendríamos que marcar **“Graph”**.



### 5.2.3 Configuración de Triggers

Utilizamos los Triggers para comparar los valores recolectados por los Items con unas condiciones antes definidas.

Para crear un Trigger nos vamos a **“Configuration → Hosts”**, le damos a un **“Host”** y luego hacemos clic en **“Trigger”**. Después marcamos **“Create Trigger”**.

La información que tendríamos que indicarle sería:

- Name → Nombre que nos mostrará cuando salte el trigger.
- Expression → Indicamos la condición del trigger.

En nuestro caso crearemos un trigger que nos informe cuando la carga de la CPU de la máquina debian aumente de 0.2 en los próximos 2 minutos:

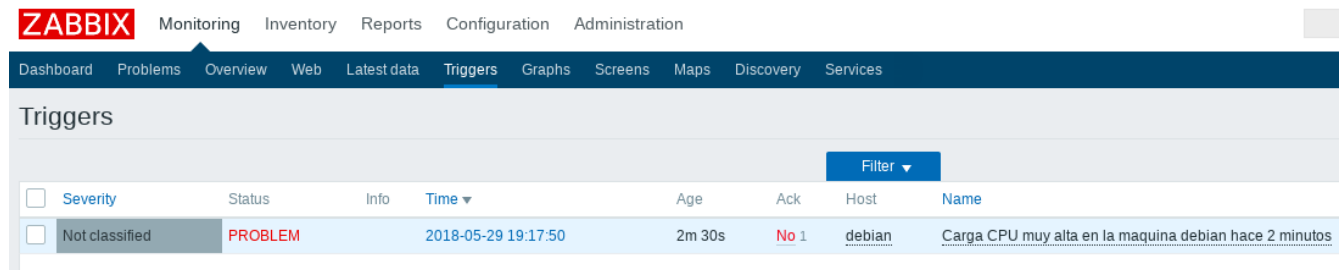


The screenshot shows the Zabbix web interface for configuring a trigger. The top navigation bar includes 'Monitoring', 'Inventory', 'Reports', 'Configuration', and 'Administration'. Below it, a secondary bar shows 'Host groups', 'Templates', 'Hosts', 'Maintenance', 'Actions', 'Event correlation', 'Discovery', and 'Services'. The main heading is 'Triggers'. A breadcrumb trail reads 'All hosts / debian Enabled ZBX SNMP JMX IPMI Applications Items 1 Triggers Graphs Discovery rules Web scenarios'. There are two tabs: 'Trigger' (selected) and 'Dependencies'. The configuration form includes: 'Name' (Carga CPU muy alta en la maquina debian hace 2 minutos), 'Severity' (Not classified, Information, Warning, Average, High, Disaster), and 'Expression' ({debian:system.cpu.load.avg(2m)}>0.2). An 'Add' button is next to the expression field. A link for 'Expression constructor' is at the bottom.

Para ver el estado del Trigger nos vamos a “**Monitoring** → **Triggers**”.

Si se muestra en color verde significa que de momento todo está bien pero si aparece en color rojo significa que ha sobrepasado el valor indicado en la configuración del trigger.

Cargamos la CPU de la máquina debian para que salte el trigger y así comprobar que funciona correctamente:



The screenshot shows the Zabbix web interface for monitoring triggers. The top navigation bar includes 'Monitoring', 'Inventory', 'Reports', 'Configuration', and 'Administration'. Below it, a secondary bar shows 'Dashboard', 'Problems', 'Overview', 'Web', 'Latest data', 'Triggers', 'Graphs', 'Screens', 'Maps', 'Discovery', and 'Services'. The main heading is 'Triggers'. A 'Filter' dropdown is visible. Below is a table with the following data:

<input type="checkbox"/>	Severity	Status	Info	Time	Age	Ack	Host	Name
<input type="checkbox"/>	Not classified	PROBLEM		2018-05-29 19:17:50	2m 30s	No 1	debian	Carga CPU muy alta en la maquina debian hace 2 minutos

## 5.2.4 Configuración de notificaciones

Vamos a mostrar ahora como Zabbix es capaz de notificar a través de correo electrónico aquella información sobre eventos que sea importante.

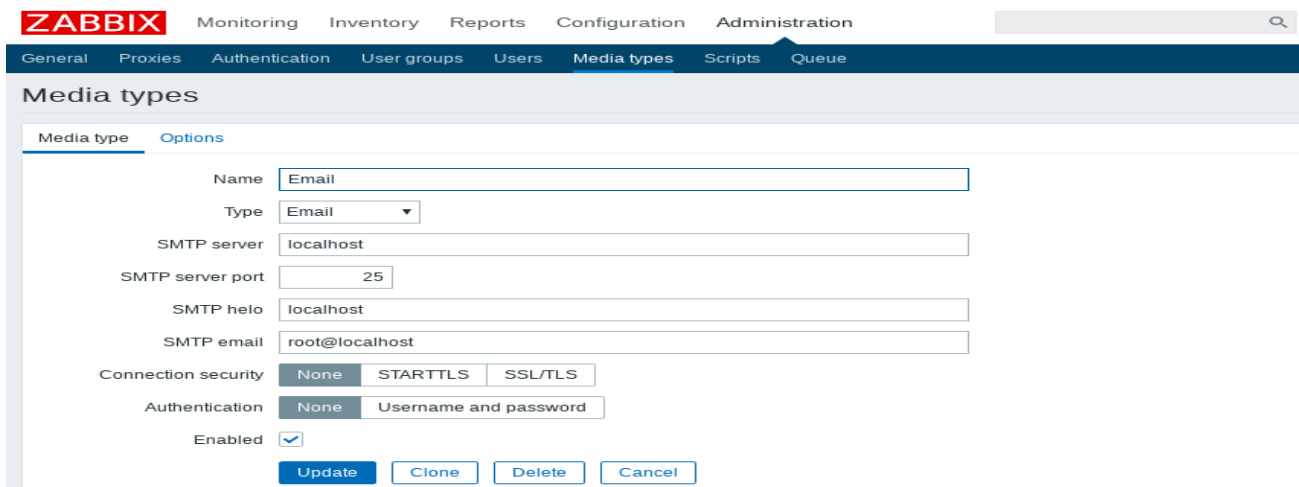
Es necesario tener instalado en el servidor Zabbix un servidor de correo. En nuestro caso utilizaremos postfix, ya que en Centos 7 viene instalado por defecto. De lo contrario lo instalaríamos mediante el comando:

```
[root@zabbix usuario]# yum install postfix
```

Para configurar los ajustes de correo electrónico nos vamos a “**Administration** → **Media types**” y hacemos clic sobre “**Email**” en la lista de “**Media Types**”.

Tendremos que definir los siguientes parámetros antes de actualizar:

- Type → Seleccionamos el tipo Email.
- SMTP server → Indicamos el servidor donde se encuentra el servidor de correo.
- SMTP helo → Indicamos un nombre de dominio.
- SMTP email → Dirección de correo que se usará como el “FROM” de los correos enviados.



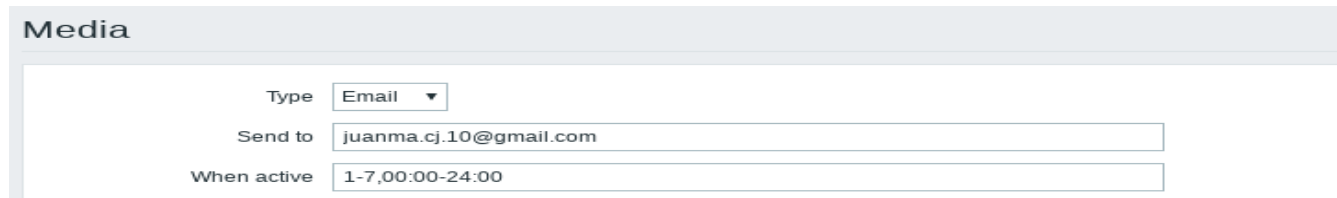
The screenshot shows the Zabbix Administration interface. The top navigation bar includes 'Monitoring', 'Inventory', 'Reports', 'Configuration', and 'Administration'. The 'Administration' menu is expanded, showing 'Media types' as the selected option. The 'Media types' page has two tabs: 'Media type' and 'Options'. The 'Options' tab is active, displaying the configuration for the 'Email' media type. The fields are as follows:

- Name: Email
- Type: Email (dropdown menu)
- SMTP server: localhost
- SMTP server port: 25
- SMTP helo: localhost
- SMTP email: root@localhost
- Connection security: None (selected), STARTTLS, SSL/TLS
- Authentication: None (selected), Username and password
- Enabled:

At the bottom of the form are four buttons: 'Update', 'Clone', 'Delete', and 'Cancel'.



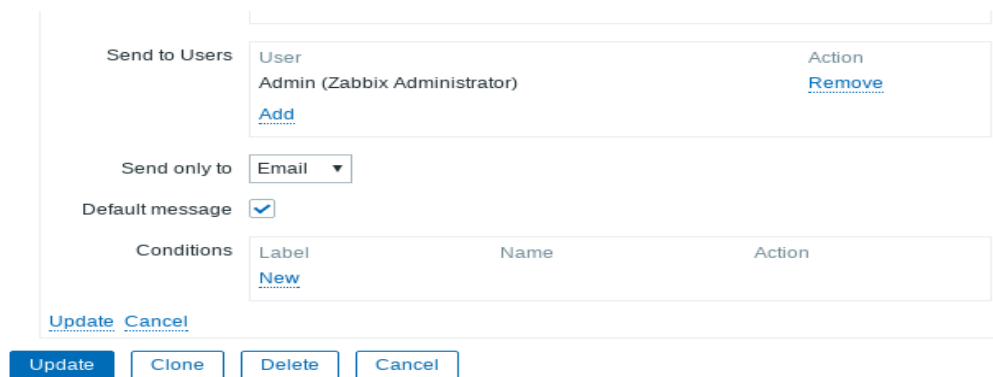
Es necesario agregar un medio a los usuarios para definir las direcciones de entrega. Esto se hace en la pestaña “**Administration** → **Users**” y seleccionamos un usuario. Después vamos a “**Media**” y agregamos el medio:



The screenshot shows the 'Media' configuration interface. It includes a dropdown menu for 'Type' set to 'Email', a text input for 'Send to' containing 'juanma.cj.10@gmail.com', and another text input for 'When active' containing '1-7,00:00-24:00'.

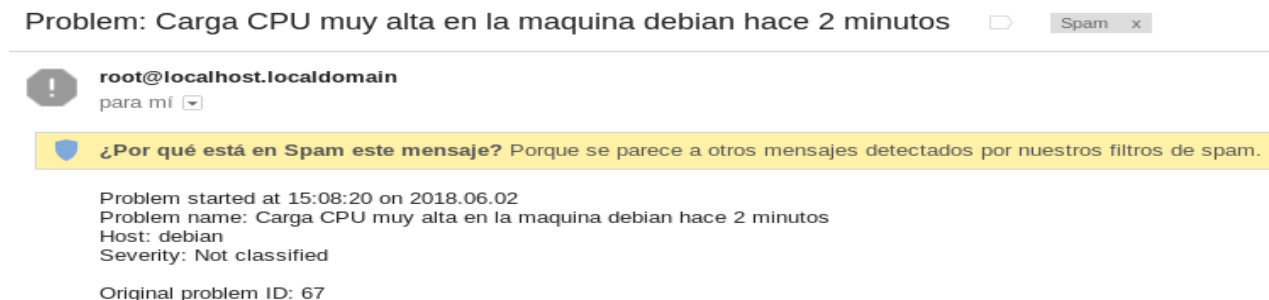
Cuando ya tenemos configurado el correo realizamos una nueva acción. Para ello nos vamos a “**Configuration** → **Actions**” y damos clic en “**Create action**”.

Indicamos un nombre a la acción y nos vamos a la pestaña “**Operations**”. Allí le decimos que esta acción se mande al usuario al que le hemos configurado el correo anteriormente, y que solo se envíe a email:



The screenshot shows the 'Operations' configuration page. It features a 'Send to Users' table with one row: 'Admin (Zabbix Administrator)' with an 'Add' button and a 'Remove' link. Below this, 'Send only to' is set to 'Email', 'Default message' is checked, and there is a 'Conditions' table with a 'New' button. At the bottom, there are buttons for 'Update', 'Clone', 'Delete', and 'Cancel'.

Para realizar una prueba estresamos la CPU de la máquina Debian para que salte el trigger y se nos mande la información al correo:



The screenshot shows a Zabbix notification email. The subject is "Problem: Carga CPU muy alta en la maquina debian hace 2 minutos". The sender is "root@localhost.localdomain". A yellow banner indicates the message is in spam. The body contains details: "Problem started at 15:08:20 on 2018.06.02", "Problem name: Carga CPU muy alta en la maquina debian hace 2 minutos", "Host: debian", "Severity: Not classified", and "Original problem ID: 67".

## 5.2.5 Configuración de plantillas

La función principal de las plantillas en Zabbix es automatizar la configuración de los Items, Triggers y notificaciones realizadas anteriormente, ya que puede resultar mas sencillo cuando tenemos un número elevado de Hosts que monitorizar.

Las plantillas permiten agrupar Items, Triggers, y otros elementos. Al vincularle un host, este hereda todas los elementos de la plantilla. Zabbix crea por defecto varias plantillas para la mayoría de sistemas operativos.

Para crear una plantilla nos vamos a “**Configuration** → **Templates**” y hacemos clic en “**Create template**”.

Los parámetros necesarios para crearla son:

- **Template name** → Indicamos el nombre de la plantilla.
- **Groups** → Indicamos los grupos a los que va a pertenecer la plantilla.

**ZABBIX** Monitoring Inventory Reports Configuration Administration

Host groups **Templates** Hosts Maintenance Actions Event correlation Discovery Services

### Templates

Template **Linked templates** Macros

Template name:

Visible name:

Groups

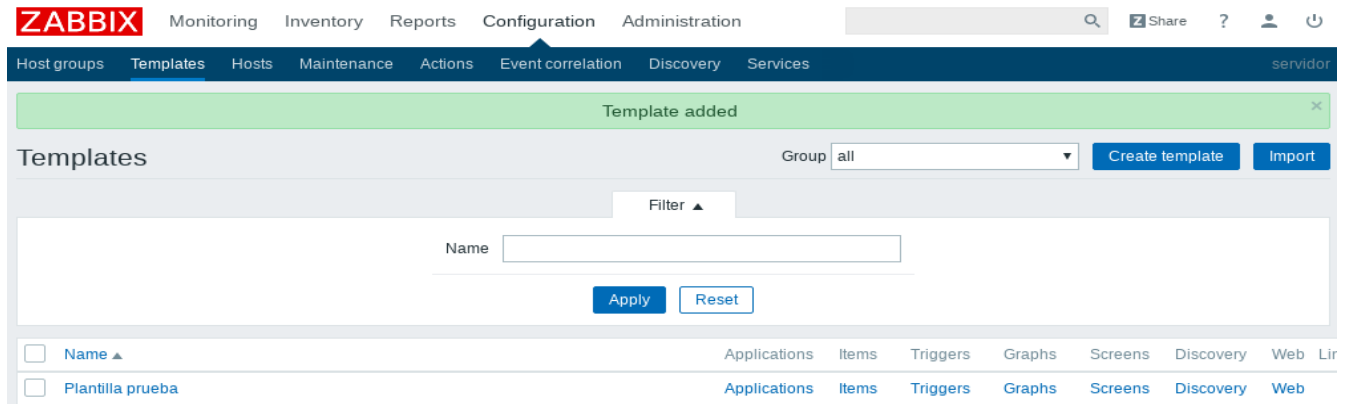
In groups

- Linux servers
- Zabbix servers

Other groups

- Hypervisors
- Templates
- Templates/Applications
- Templates/Databases
- Templates/Modules
- Templates/Network Devices
- Templates/Operating Systems
- Templates/Servers Hardware
- Templates/Virtualization
- Virtual machines

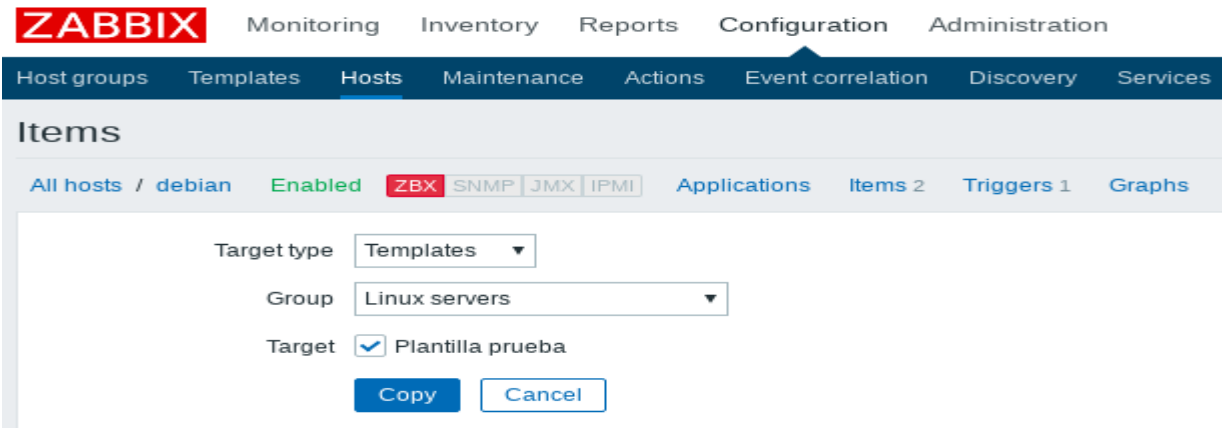
Por último le damos a **“Add”** para tener la plantilla visible en la lista de plantillas.



La plantilla como vemos no contiene ningún Item, por lo que tendremos que agregarlo. Para ello nos vamos a la lista de Items para **“debian”**. En **“Configuration → Hosts”** hacemos clic en **“Items”** junto a host **“debian”**.

Tendríamos que marcar lo siguiente:

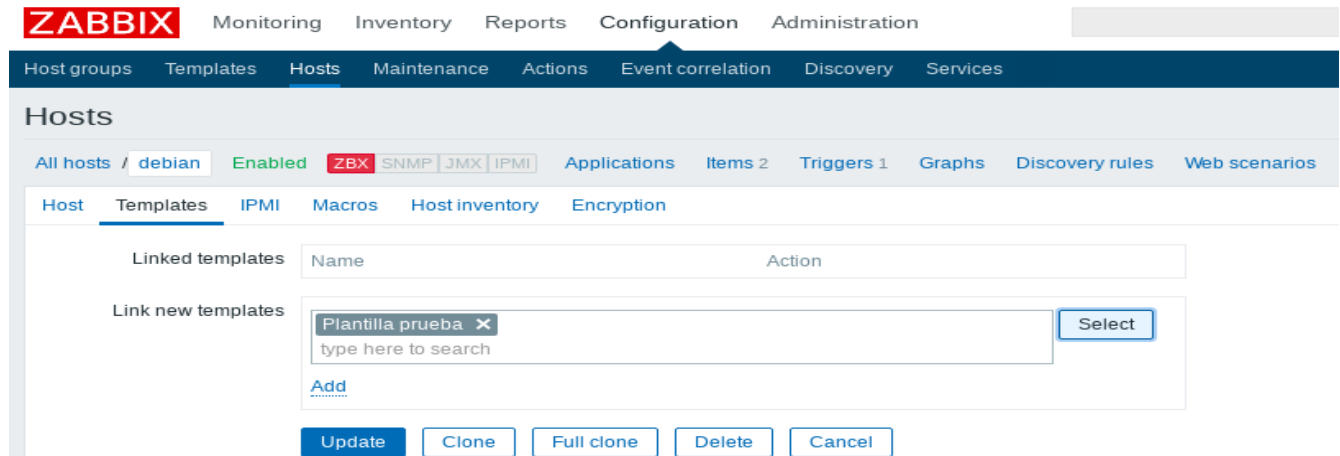
- Checkbox del elemento que queremos agregar.
- Clic sobre Copy debajo de la lista.
- Seleccionamos la plantilla donde copiar el elemento.
- Clic sobre Copy.



Si nos vamos a **“Configuration → Templates”**, nuestra plantilla tiene que tener un nuevo elemento en ella.

Lo que nos quedaría es saber como agregar la plantilla a un host. Para ello dentro de “**Configuration** → **Hosts**” y hacemos clic en “**Create host**” para crear uno nuevo, o seleccionamos un host ya creado. A continuación vamos a la pestaña “**Templates**”.

Le damos a “**Select**”, que está junto a “**Link new templates**”, seleccionamos la plantilla que hemos creado y aceptamos para que aparezca en la lista de plantillas vinculadas:



Por último Actualizamos el formulario para guardar los cambios. Ya tendríamos la plantilla agregada al host.

## 5.2.6 Configuración Auto-registro

Otra de las opciones que tiene Zabbix para monitorizar Hosts y elementos es a través del auto-registro. Esta función permite al servidor Zabbix añadir automáticamente nuevos hosts que tengan un agente zabbix instalado.

En nuestro caso vamos a realizar la configuración de auto-registro para la **máquina Windows**. Para ello el primer paso sería irnos a “**Configuration** → **Actions**” y en la pestaña “**Event source**” indicamos “**Auto registration**”. Después hacemos clic en “**Create action**”.



A continuación indicamos un nombre a la acción y añadimos una nueva condición, en nuestro caso diremos que el Host metadata tiene que ser Windows:

The screenshot shows the ZABBIX web interface. The top navigation bar includes 'Monitoring', 'Inventory', 'Reports', 'Configuration', and 'Administration'. Below it, a secondary navigation bar lists 'Host groups', 'Templates', 'Hosts', 'Maintenance', 'Actions', 'Event correlation', 'Discovery', and 'Services'. The main content area is titled 'Actions' and has two tabs: 'Action' and 'Operations'. The 'Action' tab is active. The 'Name' field contains 'auto-registro Windows'. Below it, the 'Conditions' section has a table with columns 'Label', 'Name', and 'Action'. Under 'New condition', there is a dropdown menu set to 'Host metadata', another dropdown set to 'like', and a text input field containing 'Windows'. There are 'Add' and 'Cancel' buttons at the bottom. An 'Enabled' checkbox is checked.

Después nos vamos a la pestaña “**Operations**” y en el apartado “**Operation details**” marcamos como tipo de operación “**Link to template**”. Seleccionamos la plantilla que hace referencia al Sistema Operativo Windows. Con esto lo que hacemos es añadirle al host toda la información(items, triggers, gráficos,... ) configurada en esa plantilla:

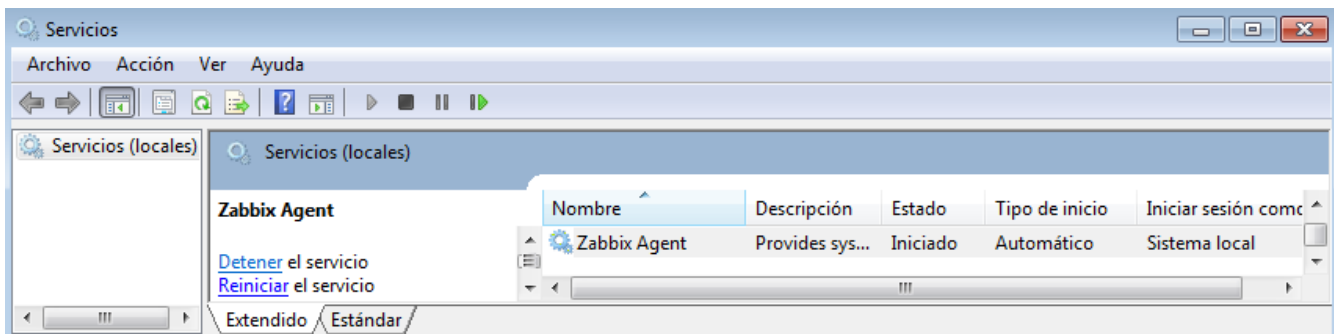
The screenshot shows the ZABBIX web interface, similar to the previous one. The 'Operations' tab is now active. The 'Default subject' field contains 'Auto registration: {HOST.HOST}'. The 'Default message' field contains 'Host name: {HOST.HOST}', 'Host IP: {HOST.IP}', and 'Agent port: {HOST.PORT}'. Below this, the 'Operations' section has a table with columns 'Details' and 'Action'. Under 'Operation details', the 'Operation type' dropdown is set to 'Link to template'. The 'Templates' field shows a search box with 'Template OS Windows' selected and a 'Select' button. There are 'Update' and 'Cancel' links below the search box. At the bottom, there are 'Add' and 'Cancel' buttons.

Por último le damos a “**Add**” para añadir la acción.

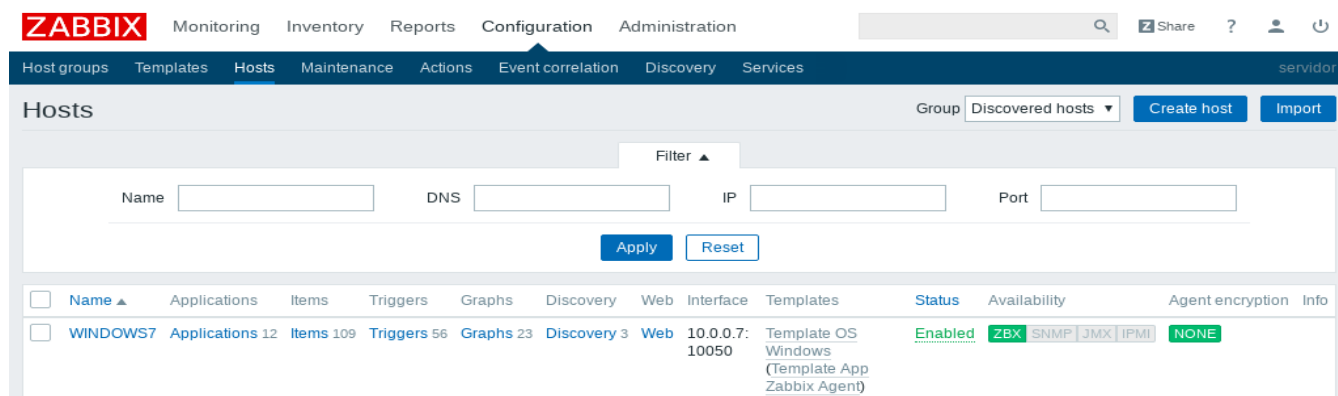
El siguiente paso sería configurar el agente. Para ello nos vamos al fichero de configuración del agente Windows y añadimos la siguiente línea en el apartado de HostMetadata:

```
C:\zabbix\zabbix_agentd.win.conf  
  
HostMetadata=Windows Server Web
```

Reiniciamos el servicio del cliente Windows:



Si en el panel web de Zabbix nos vamos a “**Configuration** → **Hosts**” ya veríamos la máquina Windows ya añadida con todos los elementos pertenecientes a la plantilla del SO Windows:



## 6. Introducción Pandora FMS

### 6.1 ¿Qué es Pandora FMS?

Pandora FMS es un software de monitorización orientado a todo tipo de entornos. FMS es el acrónimo de "Sistema de Monitorización Flexible". Se emplea para monitorizar sistemas, aplicaciones o dispositivos de red.

Esta herramienta está orientada a grandes entornos, y permite gestionar con y sin agentes, miles de sistemas, por lo que se puede emplear en grandes clusters, centros de datos y redes de todo tipo.

Pandora FMS dispone de agentes para todos los sistemas operativos del mercado.

Permite conocer el estado de cada elemento de un sistema a lo largo del tiempo, ya que dispone de histórico de datos y eventos.

Pandora FMS está publicado bajo licencia GPL2. Es Open Source aunque dispone de una versión específica para empresas, con una licencia comercial, llamada Enterprise.



### 6.2 Funcionalidades de Pandora FMS

Las principales funcionalidades de Pandora FMS son las siguientes:

#### **Monitorización de rendimiento y disponibilidad:**

Pandora monitoriza los recursos claves a través de la infraestructura, para asegurarse de que todos los dispositivos están funcionando correctamente. Las pruebas de monitorización se ejecutan mediante un agente que recoge información local de la máquina donde está instalado.

Los agentes son capaces de monitorizar los siguientes elementos:

- Latencia de red
- Uso de CPU, Disco, Memoria, etc.
- Operaciones entrada-salida en un disco.
- Número de usuarios conectados a un servidor
- Disponibilidad de servicios o procesos en ejecución

### **Creación de Informes:**

Pandora puede crear informes HTML, PDF y XML para cualquier elemento monitorizado. A estos informes se le pueden añadir datos como gráficas, métricas o eventos. Los informes se crean para un límite de tiempo configurable, que va desde una hora hasta seis meses.

### **Gestión de errores y eventos:**

El sistema de eventos de Pandora FMS mantiene un log de todo lo que ha sucedido: cuando un servicio o un host se cae, cuando se recupera, cuando se dispara una alerta, cuando se descubren nuevos hosts en la red, etc.

Es posible buscar eventos, filtrándolos por grupo, tipo, severidad o status. Todo esto se hace desde la consola Web.

### **Alta disponibilidad:**

Pandora FMS tiene redundancia sobre todos sus sistemas. Se puede crear cualquier cantidad de servidores o equipos. Los agentes también disponen de mecanismos para poder enviar a varios servidores, por si falla uno de ellos.

### **Geolocalización GIS:**

Pandora FMS proporciona información de localizaciones y mapas interactivos que muestren la posición de los agentes. También puede mostrar un tracking del recorrido de cada agente a lo largo del tiempo, haciendo una geolocalización inversa y traduciendo las coordenadas en direcciones legibles.

### **Control remoto de equipos:**

Mediante la integración con eHorus es posible controlar equipos remotamente, tanto por escritorio remoto, como por terminal.

También permite copia de archivos bidireccional, gestión de procesos y de servicios. Todo esto se encuentra integrado en la consola de Pandora FMS.



## **Monitorización WMI:**

Con la monitorización WMI se puede obtener información de cualquier Servidor Windows sin tener que instalar software. Esto incluye tanto disponibilidad, rendimiento como información de inventario.

Pandora soporta WMI de forma nativa, incluyendo el escaneo de servidores para obtener información común (CPU, Disco, Memoria) de forma automatizada.

## **6.3 Funcionamiento de Pandora FMS**

El servidor de Pandora es el encargado de mostrar la información que recoge a través los agentes instalados en cada una de los servidores o equipos que queremos monitorizar.

Estos agentes obtienen la información de sus máquinas mediante comandos. Los datos obtenidos son mandados al servidor de Pandora cuando este lo requiere, y podemos acceder a ellos a través del panel web instalado en el Servidor.

El funcionamiento de Pandora sería el siguiente:

1. El agente debe de estar instalado en las máquinas de las que recopilaremos datos.
2. A través de la interfaz web del servidor de Pandora se añaden manualmente o mediante un reconocimiento de la red las máquinas con los agentes instalados, o sin agente si queremos conocer solo su estado.
3. Cada elemento encontrado en el paso anterior recibe el nombre de “Agente”.
4. A estos agentes se le añaden los elementos encargados de recopilar información, que reciben el nombre de “Módulos”.
5. En Pandora las “Alertas” son los elementos compuestos por la unión de la operación que se ejecuta cuando salta esta alerta y la acción que se realiza. Se relacionan a uno o varios módulos. Estas alertas se hacen visibles en la interfaz web de Pandora.
6. Pandora permite enviar estas alertas mediante “Notificaciones” a través de correo electrónico.

## 7. Instalación de Pandora FMS

### 7.1 Requisitos Mínimos

El primer requisito sería tener PHP, un servidor WEB y servidor MySQL funcionando. Para ello instalamos los siguientes paquetes:

```
[root@pandora usuario]# yum install httpd mariadb mariadb-server php
```

A parte de esto, también necesitamos instalar los siguientes paquetes:

```
[root@pandora usuario]# yum install net-snmp nmap
```

### 7.2 Creación base de datos

Primero iniciamos el servicio de mariadb y nos creamos una base de datos para el servidor:

```
[root@pandora usuario]# systemctl start mariadb

[root@pandora usuario]# mysql -u root -p
MariaDB [(none)]> create database pandora character set utf8 collate
utf8_bin;
MariaDB [(none)]> grant all privileges on pandora.* to pandora@localhost
identified by 'pandora';
MariaDB [(none)]> quit;
```

### 7.3 Instalación Pandora FMS en Centos7

Es recomendable instalar primero la consola y después el servidor, ya que la base de datos MySQL que usa el servidor se crea en el proceso de configuración inicial de la consola.

Lo primero que haremos será activar los siguientes repositorios oficiales de Centos para instalar dependencias, modificando el fichero `/etc/yum.repos.d/CentOS-Base.repo`:

```
[root@pandora usuario]# nano /etc/yum.repos.d/CentOS-Base.repo

[updates]
name=CentOS-$releasever - Updates
mirrorlist=http://mirrorlist.centos.org/?
release=\$releasever&arch=\$basearch&repo=updates
gpgcheck=0

[extras]
name=CentOS-$releasever - Extras
mirrorlist=http://mirrorlist.centos.org/?
release=\$releasever&arch=\$basearch&repo=extras
gpgcheck=0
```

Añadimos a continuación el repositorio EPEL:

```
[root@pandora usuario]# nano /etc/yum.repos.d/CentOS-Base.repo

[EPEL]
Name = EPEL
baseurl = http://dl.fedoraproject.org/pub/epel/\$releasever/\$basearch/
enabled = 1
gpgcheck = 0
```

Actualizamos la información de los repositorios:

```
[root@pandora usuario]# yum makecache
```

## 7.4 Instalación de paquetes

Instalaremos la herramienta mediante el repositorio oficial de Pandora FMS. Para ello nos creamos el repositorio oficial y le añadimos las siguientes líneas:

```
[root@pandora usuario]# nano /etc/yum.repos.d/pandorafms.repo

[artica_pandorafms]
name=CentOS7 - PandoraFMS official repo
baseurl=http://firefly.artica.es/centos7
gpgcheck=0
enabled=1
```

Actualizamos de nuevo los repositorios:

```
[root@pandora usuario]# yum makecache
```

Instalamos ahora los paquetes de Pandora FMS:

```
[root@pandora usuario]# yum install pandorafms_console pandorafms_server
```

## 7.5 Configuración inicial

### 7.5.1 Pasos iniciales

Antes de comenzar con la configuración de Pandora tendríamos que realizar algunos cambios en Centos.

Primero deshabilitaremos el firewall, utilizando los comandos:

```
[root@pandora usuario]# systemctl stop firewalld

[root@pandora usuario]# systemctl disable firewalld
```

Tendríamos que deshabilitar también SELinux:

```
[root@pandora usuario]# setenforce 0

[root@pandora usuario]# sed -i 's/enforcing/disabled/g'
/etc/selinux/config /etc/selinux/config
```

A continuación habilitamos los servicios para que arranquen automáticamente al iniciar el sistema:

```
[root@pandora usuario]# systemctl start httpd

[root@pandora usuario]# systemctl enable httpd

[root@pandora usuario]# systemctl enable mariadb
```

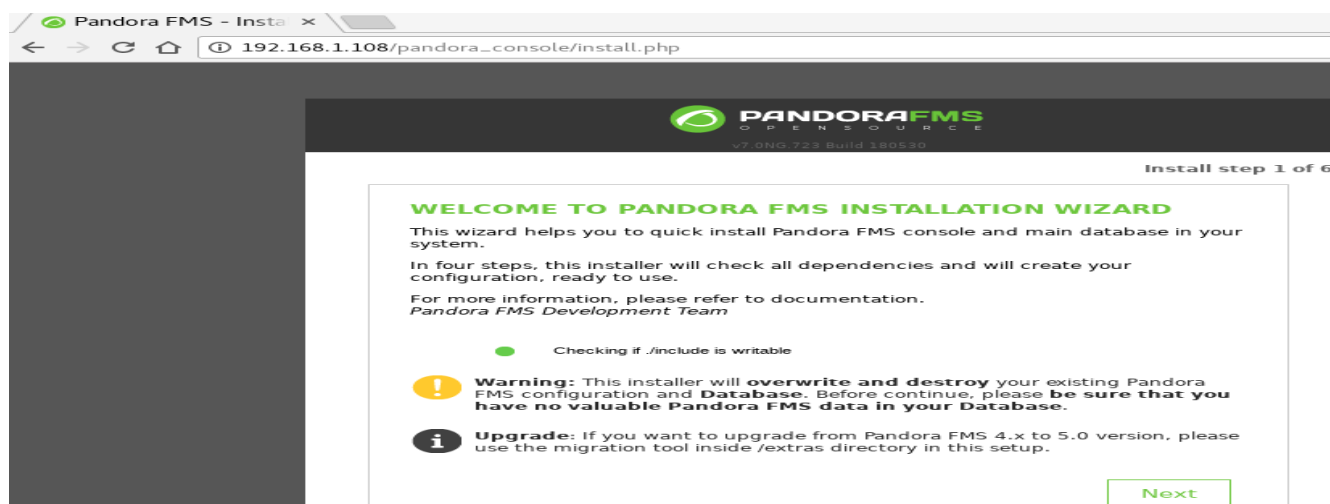
Quitamos el private tmp del systemd en apache:

```
[root@pandora usuario]# sed -i 's/PrivateTmp=true/PrivateTmp=false/g'
/etc/systemd/system/multi-user.target.wants/httpd.service
```

## 7.5.2 Configuración inicial de la Consola:

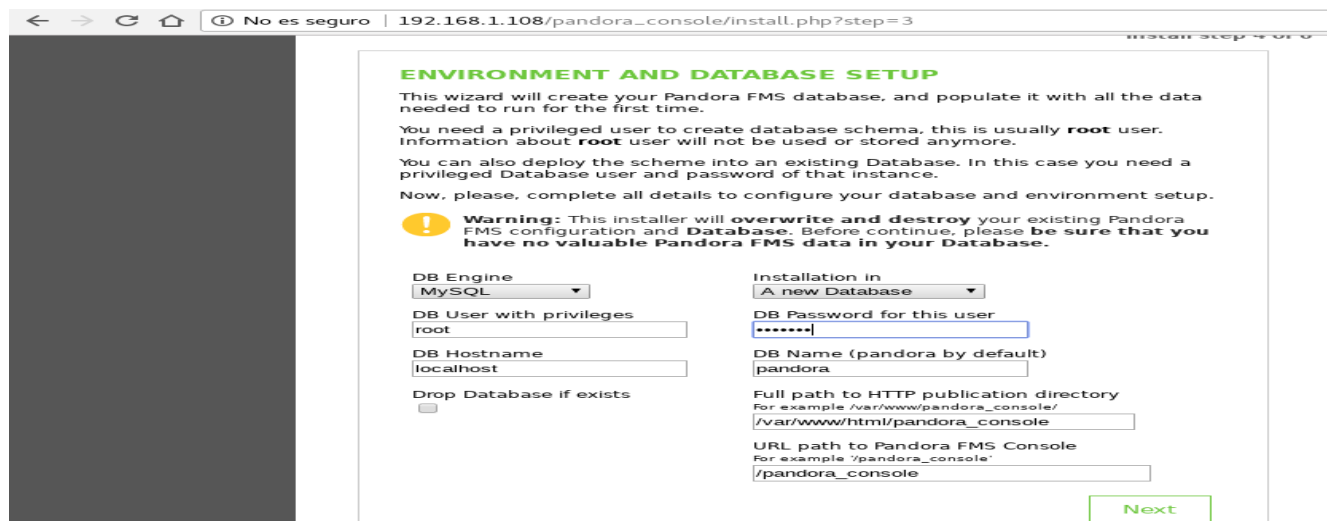
Introducimos en el navegador la siguiente URL para comenzar con la configuración gráfica de Pandora:

[http://IPservidorPandora/pandora\\_console/install.php](http://IPservidorPandora/pandora_console/install.php)

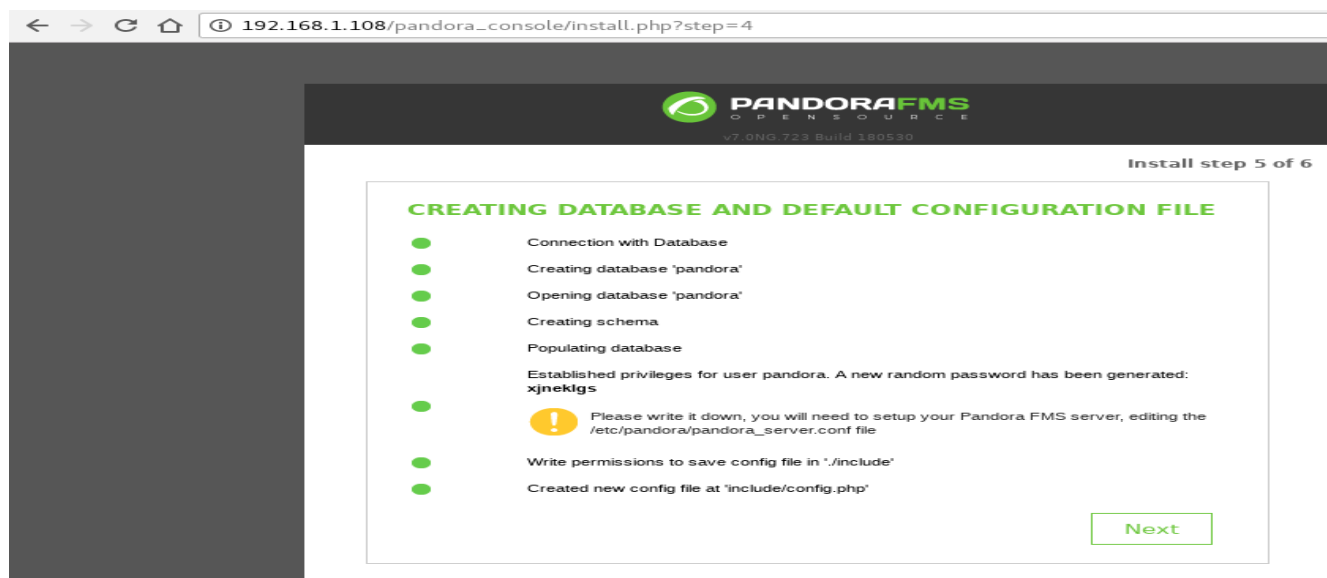


The screenshot shows a web browser window with the address bar displaying "192.168.1.108/pandora\_console/install.php". The page content includes the Pandora FMS logo and the text "v7.0.0-723 build 180530". The main heading is "WELCOME TO PANDORA FMS INSTALLATION WIZARD". Below this, there is a welcome message and instructions: "This wizard helps you to quick install Pandora FMS console and main database in your system. In four steps, this installer will check all dependencies and will create your configuration, ready to use. For more information, please refer to documentation. Pandora FMS Development Team". A progress indicator shows a green dot for "Checking if /include is writable". There are two warning messages: one with a yellow exclamation mark icon stating "Warning: This installer will overwrite and destroy your existing Pandora FMS configuration and Database. Before continue, please be sure that you have no valuable Pandora FMS data in your Database." and another with an information icon stating "Upgrade: If you want to upgrade from Pandora FMS 4.x to 5.0 version, please use the migration tool inside /extras directory in this setup." A "Next" button is visible at the bottom right.

Seguimos los pasos que nos indican hasta llegar a la pestaña de la Base de Datos, donde indicaremos los parámetros de conexión a la base de datos de Pandora antes creada:



Nos mostrará la contraseña de acceso a la base de datos y le daremos a siguiente, y renombraremos el fichero install.php para finalizar la instalación:



### 7.5.3 Configuración inicial básica del Servidor:

Tras configurar la base de datos de pandora tendremos que cambiar la contraseña predefinida. Para ello nos vamos al fichero `/etc/pandora/pandora_server.conf` y dejamos la línea “**dbpass**” con la contraseña generada en el instalador:

```
[root@pandora usuario]# nano /etc/pandora/pandora_server.conf  
dbpass xjneklgs
```

Ahora arrancamos y habilitamos el servicio del servidor de Pandora FMS para que inicie al arrancar el sistema con el comando:

```
[root@pandora usuario]# systemctl start pandora_server  
[root@pandora usuario]# systemctl enable pandora_server
```

Nos logeamos con el usuario “admin” y contraseña “pandora”. Configuramos el idioma, la región horaria y un correo electrónico para el envío de alertas. Después de esto ya podríamos ver el panel web de Pandora correctamente:

Usuario	Acción	Fecha	IP origen	Comentarios
admin	Logon	★ 2 s	192.168.1.107	Logged in
admin	Logon Failed	★ 10 s	192.168.1.107	Invalid login: admin
admin	Logoff	★ 2 m 05 s	192.168.1.107	Logged out
admin	Logon	★ 19 m 48 s	192.168.1.107	Logged in
admin	Logoff	★ 20 m 01 s	192.168.1.107	Logged out
admin	Logon	★ 27 m 08 s	192.168.1.107	Logged in
admin	Logon Failed	★ 4 d	192.168.1.107	Invalid login: admin

## 8. Configuración Pandora FMS

### 8.1 Configuración Agentes

El agente en Pandora es un software que se instala en un sistema operativo y se ejecuta para extraer información de monitorización y enviarla al servidor de Pandora regularmente.

Los agentes utilizan los comandos y herramientas del sistema operativo para obtener la información. Conforman los datos en un fichero en formato XML y los envían al servidor de datos del servidor Pandora, que los procesa y almacena en la base de datos.

Cada uno de los chequeos individuales es denominado Módulo. Su funcionamiento se determina en el fichero de configuración, llamado **pandora\_agent.conf**.

#### 8.1.1 Configuración agente en CentOS

Al tener activado el repositorio de Centos podemos instalar el agente mediante el comando:

```
[root@pandora usuario]# yum install pandorafms_agent_unix.noarch
```

Iniciamos y habilitamos el servicio para que arranque automáticamente al iniciar el sistema:

```
[root@pandora usuario]# systemctl start pandora_agent_daemon  
[root@pandora usuario]# systemctl enable pandora_agent_daemon
```

#### 8.1.2 Configuración agente Debian

De igual manera que en CentOS podemos instalar el agente a través de la paquetería mediante el comando:

```
root@debian:/home/usuario# apt install pandorafms-agent
```

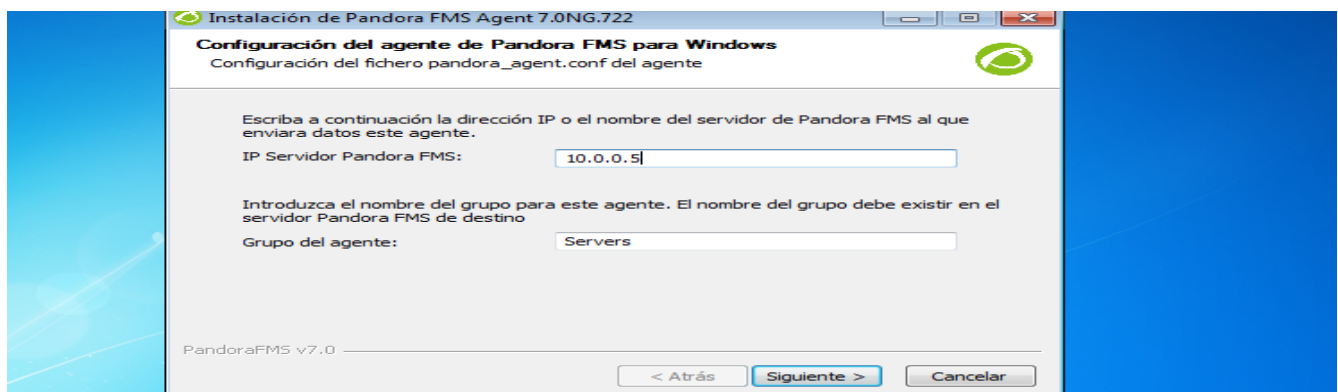


### 8.1.3 Configuración agente Windows

Lo primero que tenemos que hacer es descargarnos el siguiente fichero para nuestra versión de Windows para a continuación ejecutarlo:

[https://sourceforge.net/projects/pandora/files/Pandora%20FMS%207.0NG/722/Windows/Pandora%20FMS%20Windows%20Agent%20v7.0NG.722\\_x86\\_64.exe/download](https://sourceforge.net/projects/pandora/files/Pandora%20FMS%207.0NG/722/Windows/Pandora%20FMS%20Windows%20Agent%20v7.0NG.722_x86_64.exe/download)

Lo siguiente será indicar el idioma y una ruta donde instalar el agente. Después indicamos en la configuración del agente la IP del servidor, para que reciba los datos del agente:



Para cambiar otros parámetros del agente, como por ejemplo el nombre o la ruta de los ficheros tendríamos que modificar a mano el fichero **pandora\_agent.conf**.

Para terminar la instalación indicaríamos que se inicie el agente este momento en lugar de hacerlo manualmente más adelante.

## 8.2 Configuración principal Pandora FMS

### 8.2.1 Configuración de equipos

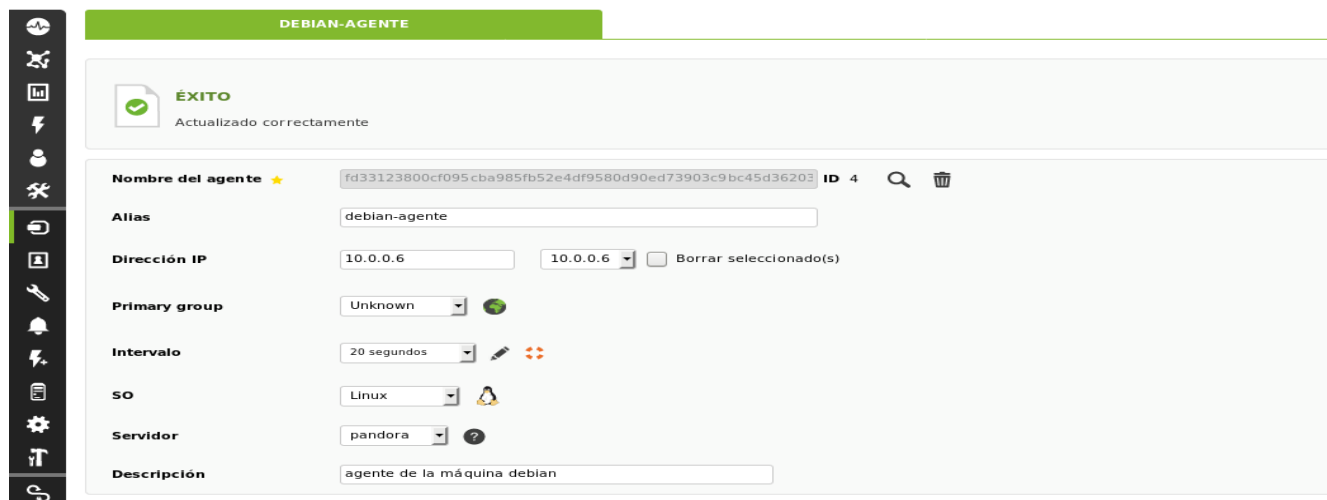
En Pandora se monitoriza cualquier dispositivo o equipo a través de los agentes.

Para agregar un nuevo equipo tendríamos que irnos a “**Resources** → **Gestionar agentes**” y hacer clic sobre la pestaña crear agente.

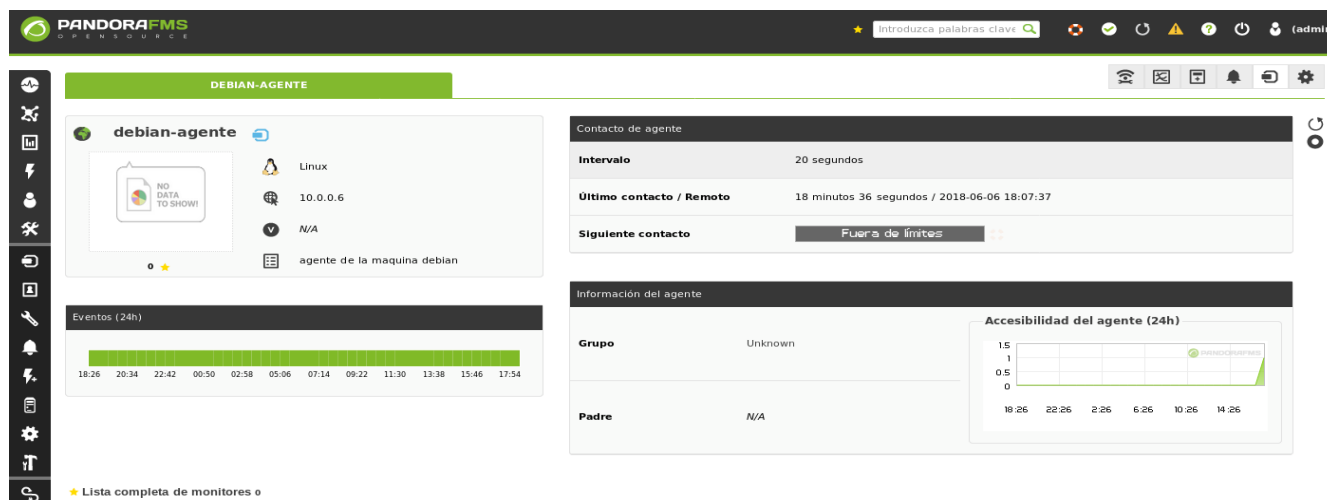
Tendríamos que indicarle la siguiente información:

- Alias con el que haremos referencia al agente.
- Dirección IP de la máquina que vamos a monitorizar.
- Intervalo de tiempo en el que se actualizará la información del equipo.
- Sistema Operativo del dispositivo.
- Servidor al que estará relacionado.
- Descripción del equipo.

Le daríamos clic a “**Crear**” y nos mostraría un panel informando de que se ha realizado correctamente:



Por último si marcamos “**Vista**”, junto al nombre del equipo creado situado en la pestaña “**Gestionar agentes**” veríamos su información relevante, aunque todavía no tenga ningún modulo configurado:



## 8.2.2 Configuración de tarea de reconocimiento

Pandora también es capaz de localizar automáticamente los host con un agente instalado a través de nuestra red. Esto se hace mediante la Tarea de reconocimiento y es muy útil sobre todo para las ocasiones en las que queramos monitorizar una gran cantidad de equipos de una red.




Para realizar esta configuración nos dirigimos “**Servidores** → **Tarea de reconocimiento**”. Hacemos clic sobre “**Crear**” y modificamos la tarea indicando un nombre, nuestra red, un grupo y una plantilla de monitorización básica, entre otros parámetros:

The screenshot shows the configuration form for a network discovery task. The form is titled 'GESTIONAR TAREA RECON' and contains the following fields:

- Nombre de la tarea:** ReconRed
- Servidor de exploración de red:** pandora
- Modo:** Barrido de red
- Red:** 10.0.0.0/24
- Intervalo:** Manual
- Plantilla de módulos:** Basic Monitoring
- SO:** Cualquier
- Puertos:** (empty field)
- Grupo:** Network
- Incidente:** Sí

Añadimos la tarea y hacemos clic sobre el icono de la lupa para ejecutar la tarea:

The screenshot shows the Pandora interface after the task has been created. A success message is displayed: 'ÉXITO Tarea de reconocimiento creada correctamente'. Below the message is a table listing the tasks:

Nombre	Red	Modo	Grupo	Incidente	SO	Intervalo	Puertos	Acción
ReconRed	10.0.0.0/24	Basic Monitoring		Sí	Cualquier	Manual		  

Cuando la barra de progreso termine nos dirigimos a “**Monitorización** → **Vistas** → **Detalle de agente**” para ver todos los agentes de la red que ha localizado y añadido:

Agente	Descripción	Remoto	SO	Intervalo	Grupo	Tipo	Módulos	Estado	Alertas	Último contacto
10.0.0.7	Created by pandora			5 minutos			3 : 3	Verde	Verde	2 minutos 57 segundos
WINDOWS7	Created by pandora			5 minutos			2 : 2	Verde	Verde	5 segundos
centos-agente	agente del servidor			5 minutos			10 : 1 : 9	Verde	Verde	58 segundos
debian-agente	agente de la máquina debian			20 segundos			7 : 2 : 5 : 5	Verde	Verde	15 segundos
servidor-pandora	Pandora FMS Server version 7.0NG.723			5 minutos			8 : 8	Verde	Verde	2 minutos 37 segundos

### 8.2.3 Configuración de módulos

Pandora llama módulos a cada uno de los elementos que se monitorizan y se llevan a cabo a través de comandos o scripts. Podemos añadir módulos a una máquina a través del panel web o modificando el fichero de configuración del agente.

A través de ésta segunda opción crearemos un nuevo módulo que nos calcule la memoria libre de la máquina donde se encuentra el servidor. Para ello nos vamos al fichero de configuración del agente y añadimos las siguientes líneas:

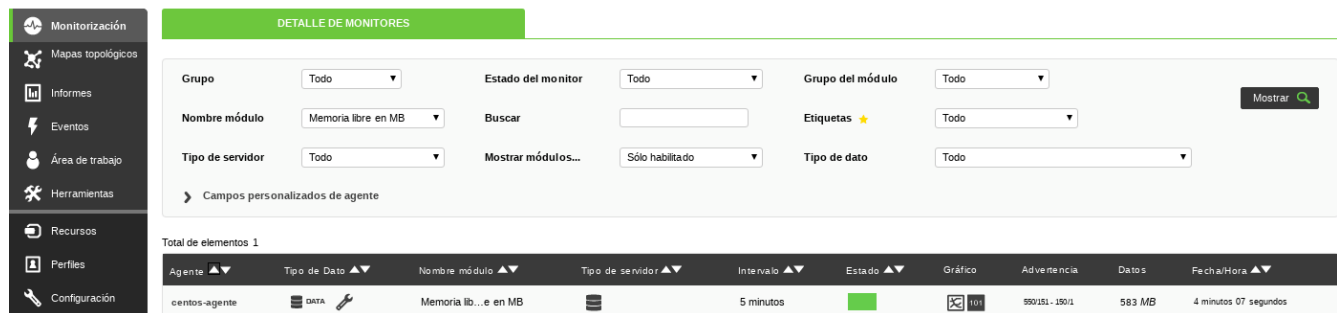
```
[root@pandora usuario]# nano /etc/pandora/pandora_agent.conf


#Memoria Libre en MB
module_begin
module_name Memoria libre en MB
module_type generic_data
module_exec free -m | grep Mem | awk '{print $4}'
module_description Memoria libre en MB en el agente
module_min_warning 151
module_max_warning 550
module_min_critical 1
module_max_critical 150
module_unit MB
module_end
```

Reiniciamos el servicio del agente:

```
[root@pandora usuario]# systemctl restart pandora_agent
```

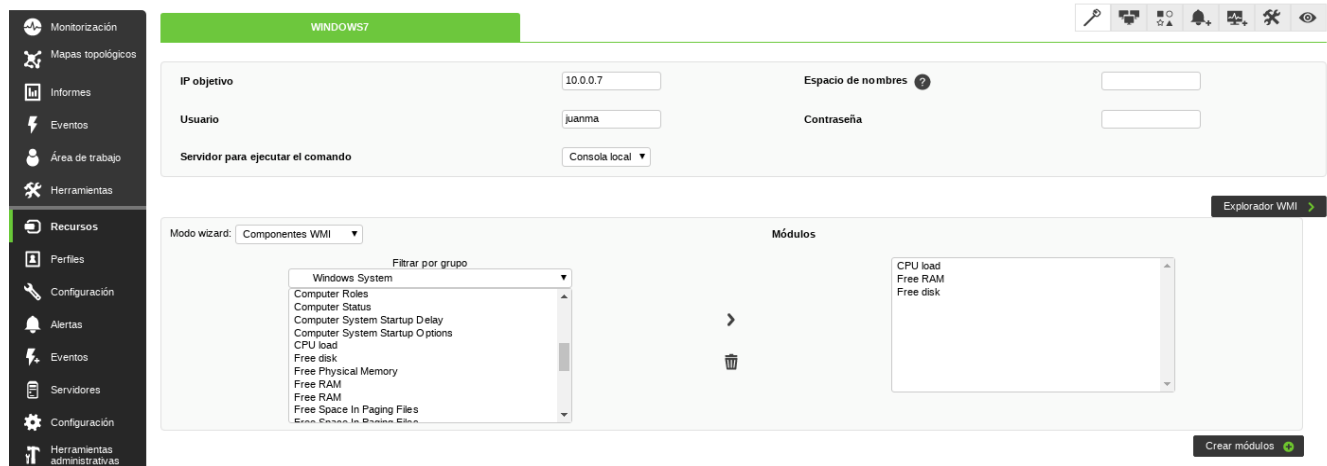
Si nos vamos al panel web y entramos en la máquina donde hemos creado el módulo veríamos que ya se encuentra añadido:



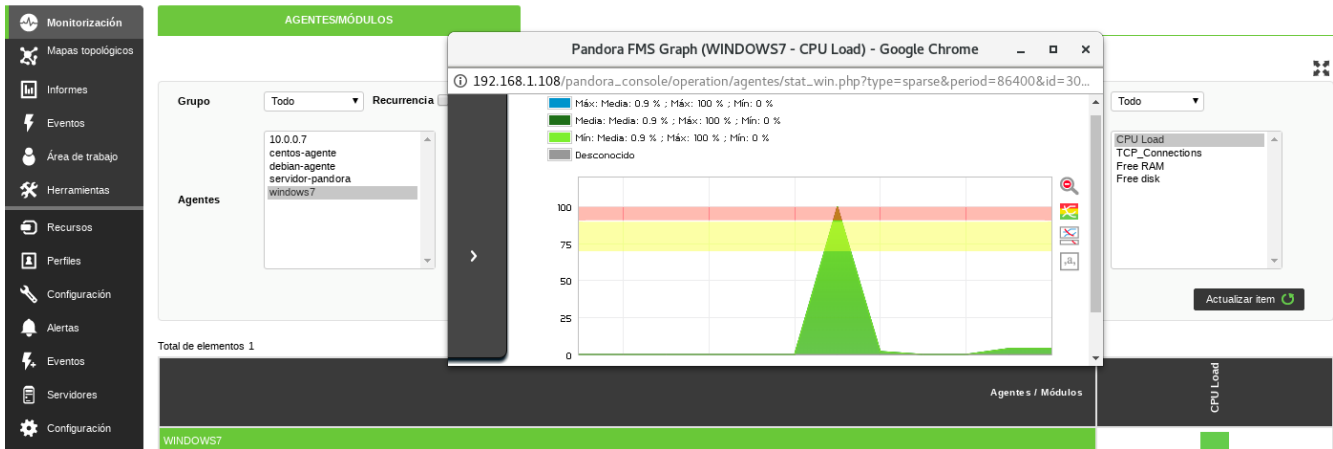
Añadimos ahora varios módulos a través del panel web a la máquina Windows. Para ello en la lista de agentes seleccionamos el agente Windows y hacemos click en “**Gestionar**” 

Hacemos clic en “**Wizard WMI**” e indicamos la IP objetivo, el usuario con privilegios y la contraseña si la tuviera.

Nos vamos al apartado “**Modo wizard**” y seleccionamos los componentes de los que queremos hacer un módulo:



Le damos a “**Crear módulos**” y ya tendríamos los módulos con sus gráficas disponibles para su visualización. Por ejemplo nos dirigimos a “**Monitorización** → **Vistas** → **Vista de agentes/módulos**” y observamos la carga de la CPU de la máquina Windows con sus umbrales de alerta:



## 8.2.4 Configuración de alertas

Las alertas en Pandora están compuestas por tres elementos: Comando, Acción y Plantilla.

- El **comando** define la operación que se ejecuta cuando se dispara la alerta, por ejemplo el envío de un correo.
- La **acción** relaciona el comando con una plantilla y personaliza la ejecución del comando.
- La **plantilla** define las condiciones de disparo de la alerta, la acción a ejecutar y la acción de recuperación.

Una de las maneras de crear una alerta es irnos a “**Alertas** → **Lista de alertas**” y hacer click en “**Crear**”. Le tendríamos que indicar el agente del que realizar la alerta, el módulo, la acción que se realizará, y la plantilla. En este caso crearemos una alerta para que nos indique cuando falla el servicio web de la máquina Debian:

A continuación nos vamos a “**Monitorización** → **Vistas** → **Detalle de alertas**” y validamos la alerta creada.

Hacemos la prueba parando el servidor web de la máquina Debian y viendo como se dispara la alerta en el panel web:

Lista completa de alertas

Total de elementos 1

S.	F.	Módulo	Plantilla	Acción	Disparada por última vez	Estado	Validar
○		Check HTTP Server	🔍 Critical condition	Monitoring Event	39 segundos	🟡	☐

Validar ✓

▼ Últimos eventos para este agente

Mostrar todos los eventos en las últimas 24h

V.	S.	Tipo	Nombre del evento	Fecha/Hora
★	●	🔴	Module 'Check HTTP Server' is going to CRITICAL (0)	39 segundos
★	●	🔔	debian-agente Check HTTP Server generated an event alert (0)	39 segundos

## 8.2.5 Configuración de notificaciones

Para que Pandora pueda mandar la información sobre el estado de un módulo o cualquier otro elemento a través de correo electrónico es necesario tener instalado y configurado un servidor de correo en la máquina donde se encuentra el servidor Pandora.

En nuestro caso utilizaremos como servidor de correo Postfix y lo configuraremos siguiendo la guía que nos ofrece Pandora a través del siguiente enlace:

[https://wiki.pandorafms.com/index.php?title=Pandora:Configuracion\\_alertas\\_emails#Configuraci.C3.B3n\\_Postfix](https://wiki.pandorafms.com/index.php?title=Pandora:Configuracion_alertas_emails#Configuraci.C3.B3n_Postfix)



Realizamos una prueba modificando la alerta creada en el apartado anterior y añadiéndole una nueva acción para que envíe un correo al administrador de Pandora. Para ello nos vamos a “**Alertas** → **Lista de alertas** → **Añadir acción**”. (+)


Previamente tenemos que comprobar el correo del administrador, ya que este paso se configura en la instalación. Esto se encuentra en “Alertas → Acciones → Mail to admin → Destination address”. En este apartado también se puede modificar la información que se mandará en el correo.

Detenemos el servicio web del agente y comprobamos que se nos envía un correo electrónico con la información referente al módulo:

[PANDORA] Alerta del agente debian-agente en el modulo Check HTTP Server Recibidos x

---

 **juanma.cj.10@gmail.com**  
para mí 




**Pandora FMS alert system**

Dear customer,

We have **bad news** for you. Something is on **CRITICAL** status!

[Go to Pandora FMS Console](#)



---

**Monitoring details**



<b>Data</b>	0 (Critical)
<b>Agent</b>	debian-agente 10.0.0.6
<b>Module</b>	Check HTTP Server Creado mediante la plantilla Basic DMZ Server monitoring . Test APACHE2 HTTP service remotely (Protocol response, not only openport)
<b>Timestamp</b>	2018-06-10 14:15:46


This is a graph of latest 24hr data for this module:

Cuando el servicio vuelve ha estar bien Pandora nos envía un nuevo correo informándonos de la situación:

[PANDORA] Alert RECOVERED for CRITICAL status on debian-agente / Check HTTP Server Recibidos x

---

 **juanma.cj.10@gmail.com**  
para mí 




**Pandora FMS alert system**

Dear customer,

We have **good news** for you. Alert has been **RECOVERED** status!

[Go to Pandora FMS Console](#)



---

**Monitoring details**

<b>Data</b>	1 (Normal)
<b>Agent</b>	debian-agente 10.0.0.6
<b>Module</b>	Check HTTP Server Creado mediante la plantilla Basic DMZ Server monitoring . Test APACHE2 HTTP service remotely (Protocol response, not only openport)
<b>Timestamp</b>	2018-06-10 14:54:55

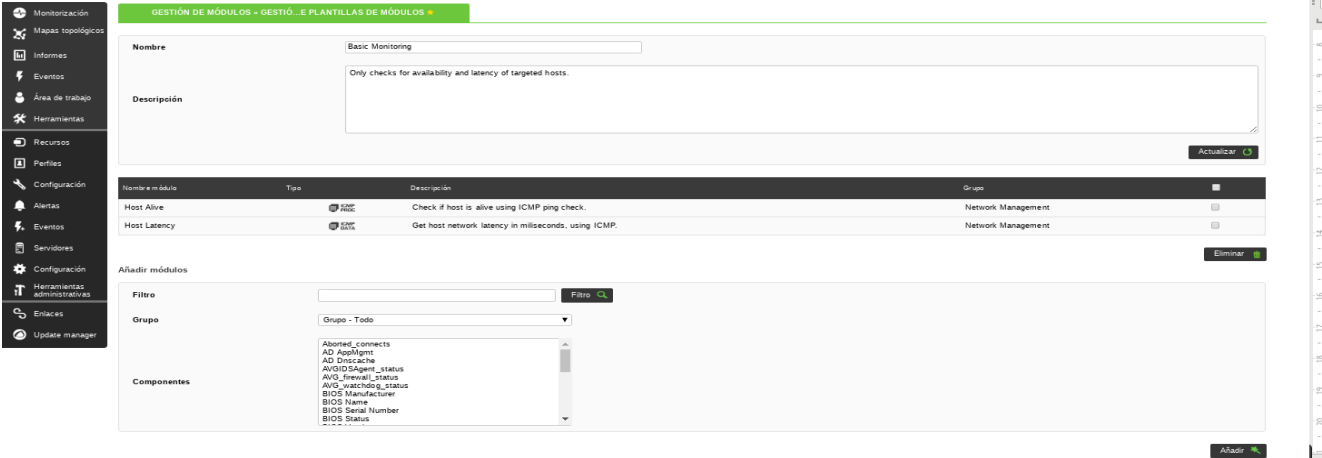
This is a graph of latest 24hr data for this module:



## 8.2.6 Configuración de plantillas

Pandora FMS ofrece la posibilidad de crear plantillas de módulos. Esto hace que sea más sencillo aplicar un grupo de módulos a través de una plantilla a un agente, en lugar de asignar esos módulos uno a uno y repetidas veces.

Para ver y gestionar las plantillas de módulos existentes nos vamos a “**Configuración** → **Plantillas de módulos**”. Si entramos en una plantilla creada vemos una descripción de la plantilla, los módulos que la componen y la posibilidad de añadir nuevos módulos.



Nombre módulo	Tipo	Descripción	Grupo
Host Alive	TCP	Check if host is alive using ICMP ping check.	Network Management
Host Latency	TCP	Get host network latency in milliseconds, using ICMP.	Network Management

Añadir módulos

Filtro:  Filtro

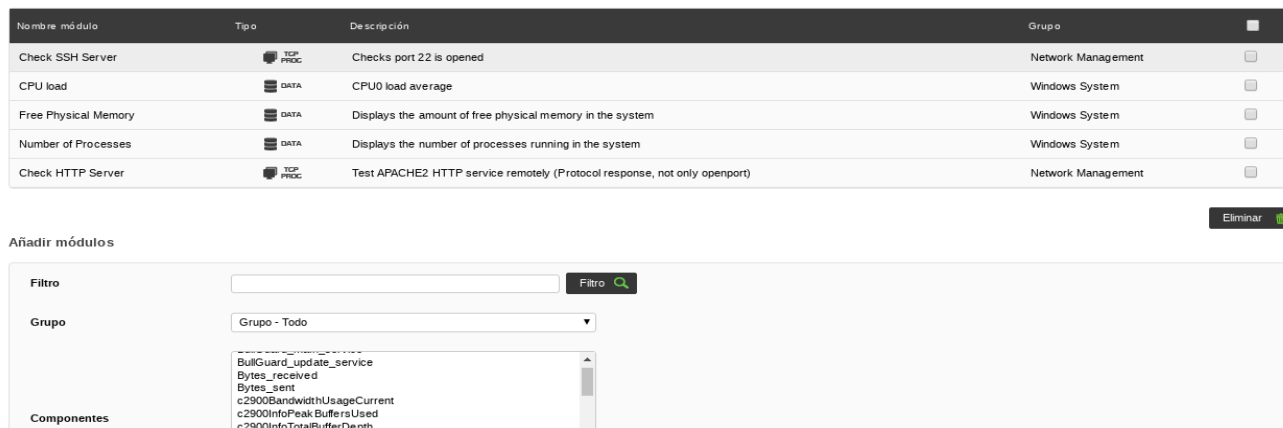
Grupo: Grupo - Todo

Componentes

- Aborted\_connects
- AD Application
- AD\_DnsCache
- AD\_SID\_Signtool\_status
- AVG\_firewall\_status
- AVG\_install\_status
- BIOS\_Manufacturer
- BIOS\_Name
- BIOS\_Serial\_Number
- BIOS\_Status

Lo que haremos será crearnos una plantilla nueva. Para ello en el apartado “**Plantilla de módulos**” hacemos clic en “**Crear**”. Definimos un nombre, una descripción de la plantilla y creamos.

Ahora pasamos a añadir uno a uno los módulos a la plantilla:



Nombre módulo	Tipo	Descripción	Grupo
Check SSH Server	TCP	Checks port 22 is opened	Network Management
CPU load	DATA	CPU0 load average	Windows System
Free Physical Memory	DATA	Displays the amount of free physical memory in the system	Windows System
Number of Processes	DATA	Displays the number of processes running in the system	Windows System
Check HTTP Server	TCP	Test APACHE2 HTTP service remotely (Protocol response, not only openport)	Network Management


Añadir módulos

Filtro:  Filtro

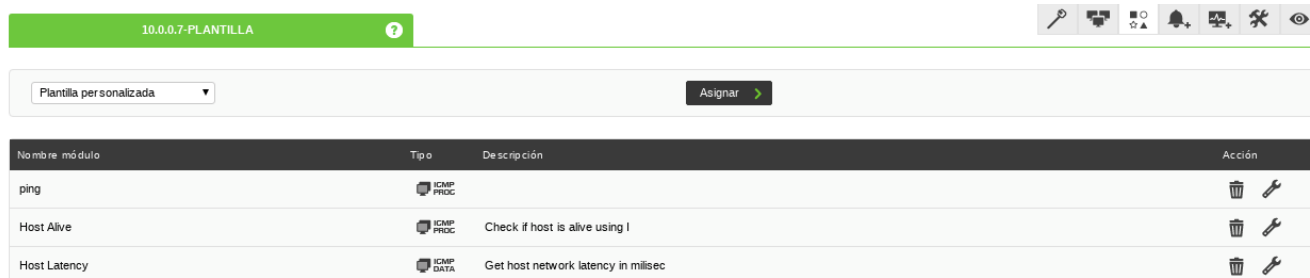
Grupo: Grupo - Todo










Componentes

- BullGuard\_update\_service
- Bytes\_received
- Bytes\_sent
- c2900BandwidthUsageCurrent
- c2900InfoPeakBuffersUsed
- c2900InfoTotalBufferDepth

Con los módulos añadidos ya podríamos asignar la plantilla creada a los distintos agentes. Para ello nos vamos “**Monitorización** → **Vistas** → **Detalle de agente**”, seleccionamos un agente y hacemos clic en “**Gestionar**”. 

A continuación marcamos “**Plantillas de módulos**”, seleccionamos la plantilla creada y la asignamos:



Nombre módulo	Tipo	Descripción	Acción
ping			 
Host Alive		Check if host is alive using I	 
Host Latency		Get host network latency in milisec	 

## 9. Comparativa de herramientas

A continuación se analizarán y compararán algunos de los aspectos que me han parecido más relevantes sobre la implantación de este proyecto realizado con Zabbix y con la versión OpenSource de Pandora:

### Instalación y configuración inicial

Ambas herramientas se caracterizan por una instalación y configuración inicial no muy complicadas siguiendo sus páginas oficiales, aunque Zabbix requiere una mayor cantidad de pasos a realizar.

Con respecto a los agentes, Pandora no necesita realizar ninguna configuración adicional a parte de la instalación para poder trabajar con ellos. En cambio Zabbix si requiere algunas modificaciones en el fichero de configuración de los agentes para su correcto funcionamiento.

### Consumo de recursos

En este apartado Pandora tiene un poco de ventaja pero no significativa, ya que nuestro escenario es demasiado simple como para apreciar la diferencia de consumo que pueden tener estas herramientas.

Si nos vamos a escenarios reales con una gran cantidad de equipos si se podrían comprobar las cifras de consumo. En los siguientes enlaces se especifican los recursos aproximados que se pueden requerir, siguiendo los manuales de instalación de las herramientas:

*Zabbix:*

<https://www.zabbix.com/documentation/3.0/manual/installation/requirements>

*Pandora FMS:*

[https://wiki.pandorafms.com/index.php?title=Pandora:Documentation\\_es:Instalacion#Requisitos\\_minimos\\_de\\_software](https://wiki.pandorafms.com/index.php?title=Pandora:Documentation_es:Instalacion#Requisitos_minimos_de_software)

### Configuración y gestión

Ambas herramientas son capaces de realizar toda su configuración y gestión a través de la interfaz web.

A partir de esto, me ha resultado más sencillo la administración de la herramienta Zabbix debido a que presenta un conjunto amplio de menús, sub menú y pestañas que permiten realizar los distintos cambios de manera más intuitiva.

## **Funcionalidades**

En este caso la limitación de funcionalidades, como pueden ser la recolección de log, autenticación LDAP o la personalización de la interfaz, que tiene la versión OpenSource de Pandora con respecto a Zabbix hace que este último tenga ventaja en este aspecto.

Hay que decir también que la mayor parte de las funciones básicas están disponibles en ambas herramientas.

## **Visualización del panel web**

En este apartado gana Zabbix, ya que presenta un panel más sencillo y organizado, además de contar también con la posibilidad de personalizar su aspecto.

Zabbix tiene también la ventaja de poder clonar o crear nuevos dashboards, y añadirle la información relevante para el usuario.

## **Coste**

Aunque las versiones que hemos utilizado en este proyecto son gratuitas, las dos herramientas presentan servicios de soporte de pago para sus clientes.

Además en el caso de Pandora presenta versiones adicionales como por ejemplo la versión NMS, que incluye las funcionalidades enfocadas en la monitorización remota, o la versión Enterprise, que está compuesta por el paquete completo de funcionalidades.

## **Comunidad**

En este aspecto ambas herramientas tienen su punto a favor aunque para mí Zabbix tienen una mejor opinión. Esto es debido a dos puntos:

- Zabbix presenta una documentación oficial más clara y concisa que la de Pandora, aunque también hay que decir que al ser esta una herramienta hecha en España tiene la ventaja de tener en Español todos sus documentos y enlaces.
- A la hora de resolver los distintos problemas encontrados tanto en la instalación como en la configuración de ambas herramientas, Zabbix presenta una cantidad de foros y usuarios bastante mayor que en Pandora.

En conclusión, me ha parecido que ambas herramientas pueden ser semejantes en cuanto las funciones realizadas en el proyecto pero si me tengo que elegir una, me quedaría con **Zabbix**.

Aunque todo depende del tipo de monitorización que se quiera realizar porque como sabemos, Pandora FMS está orientado a grandes proyectos debido a su alta capacidad de escalabilidad.

## 10. Configuración adicional Zabbix

A continuación se mostrarán las configuraciones de algunas de las funcionalidades de Zabbix que no están soportadas en la versión OpenSource de Pandora.

### 10.1 Configuración aplicación Java

Zabbix proporciona soporte para monitorizar aplicaciones basadas en java, o también llamado JMX. Esto se lleva a cabo a través de un demonio llamado Zabbix Java gateway.

En este caso utilizaré como aplicación un gestor de contenido basado en Java llamado OpenCms. Lo descargamos a través de su página oficial:

<http://www.opencms.org/en/download/opencms.html>

Es necesario tener los siguientes paquetes instalados para mostrar la aplicación:

```
root@debian:/home/usuario# apt install tomcat8
root@debian:/home/usuario# apt install openjdk-8-jre openjdk-8-jre-headless apache2 mysql-server
```

Cuando ya tengamos instalada la aplicación empezaremos con la configuración. El primer paso será irnos al fichero catalina.sh y añadir las siguientes líneas para que java escuche las conexiones JMX:

```
root@debian:/home/usuario# nano /usr/share/tomcat8/bin/catalina.sh
JAVA_OPTS="{JAVA_OPTS} -Dcom.sun.management.jmxremote"
JAVA_OPTS="{JAVA_OPTS} -Djava.rmi.server.hostname=10.0.0.6"
JAVA_OPTS="{JAVA_OPTS} -Dcom.sun.management.jmxremote.port=10052"
JAVA_OPTS="{JAVA_OPTS} -Dcom.sun.management.jmxremote.authenticate=false"
JAVA_OPTS="{JAVA_OPTS} -Dcom.sun.management.jmxremote.registry.ssl=false"
JAVA_OPTS="{JAVA_OPTS} -Dcom.sun.management.jmxremote.ssl=false"
```

Tras esto reiniciamos la aplicación:

```
root@debian:/home/usuario# systemctl restart tomcat8
```

Comprobamos desde el servidor que el puerto está escuchando:

```
[root@zabbix usuario]# telnet 10.0.0.6 10052
Trying 10.0.0.6...
Connected to 10.0.0.6.
```

A continuación nos vamos al servidor zabbix e instalamos el paquete zabbix java gateway con el comando:

```
[root@zabbix usuario]# yum install zabbix-java-gateway
```

Configuramos el fichero de zabbix\_java\_gateway y modificamos las siguientes líneas:

```
[root@zabbix usuario]# nano /etc/zabbix/zabbix_java_gateway.conf

LISTEN_PORT=10052
START_POLLERS=2
TIMEOUT=3
```

- La opción START\_POLLERS indica los hilos con los que iniciará la puerta de enlace java.
- La opción TIMEOUT establece el tiempo de espera para las operaciones de red JMX.

Configuramos también el fichero de zabbix\_server de la siguiente manera:

```
[root@zabbix usuario]# nano /etc/zabbix/zabbix_server.conf

JavaGateway=127.0.0.1
JavaGatewayPort=10052
StartJavaPollers=2
```


- La opción StartJavaPollers controla el tipo específico de procesos que se conectan a la puerta de enlace Java.  
Se sugiere que la opción StartJavaPollers sea inferior o igual a la opción START\_POLLERS del fichero de zabbix\_java\_gateway.

Reiniciamos los servicios del servidor zabbix y de la puerta de enlace java. Habilitamos también el servicio de java para que arranque con el sistema:

```
[root@zabbix usuario]# systemctl restart zabbix-server
[root@zabbix usuario]# systemctl restart zabbix-java-gateway
[root@zabbix usuario]# systemctl enable zabbix-java-gateway
```

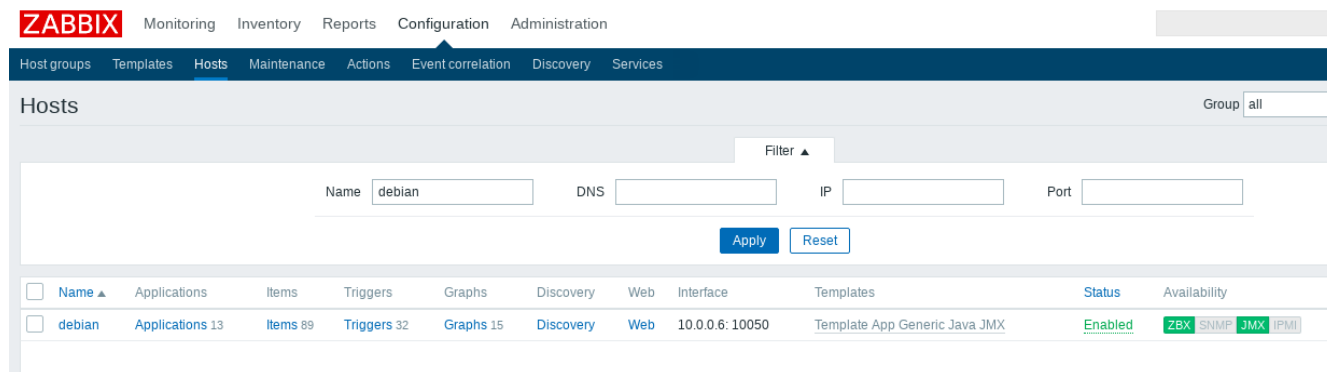
Tras esto nos vamos al panel web de Zabbix para añadir la configuración realizada al host. Para ello nos vamos a la pestaña “**Configuration** → **Hosts**” y seleccionamos la máquina “**debian**”, que es la que contiene la aplicación java.

En el apartado “**JMX interfaces**” indicamos la IP del equipo con la aplicación java junto con su puerto:



A continuación nos dirigimos a la pestaña “**Templates**” y añadimos al host una nueva plantilla para la aplicación java, llamada “**Generic Java JMX**”. Hacemos clic en “**Update**” para guardar los cambios.

Ya tendríamos disponible la monitorización de la aplicación Java:





Por último si nos vamos a “**Monitoring** → **Latest data**” veríamos los cambios que van teniendo los datos:

Name	Last check	Last value	Change
Classes (3 Items)			
ci Unloaded Class Count	2018-06-10 22:34:05	0	Graph
ci Total Loaded Class Count	2018-06-10 22:34:05	8417	Graph
ci Loaded Class Count	2018-06-10 22:34:05	8417	Graph
Compilation (1 Item)			
comp Accumulated time spent in compilation	2018-06-10 22:34:05	32s 989ms	+10ms Graph
Garbage Collector (4 Items)			
gc ParNew number of collections per second	2018-06-10 22:34:05	0	Graph

## 10.2 Monitorización de Logs

Zabbix es capaz de analizar los ficheros de log de nuestros equipos. Para ello es necesario tener un agente ejecutándose en la máquina de la que queremos recoger la información con el parámetro *ServerActive* indicando la IP del servidor Zabbix, y configurar un nuevo elemento que nos haga esta función.

Para crear el nuevo Item nos vamos a “**Configuration** → **Hosts**” y hacemos clic en la pestaña “**Items**” dentro de la máquina en la que queramos guardar el log.

A continuación marcamos “**Create Items**” y añadimos los siguientes parámetros:

- Nombre del elemento
- Tipo Xabbix agent(active)
- Fichero de log a monitorizar
- Tipo de información Log
- Formato de tiempo del log

Item: Preprocessing

Name: Log java

Type: Zabbix agent (active)

Key: log[/var/log/zabbix/zabbix\_java\_gateway.log]

Type of information: Log

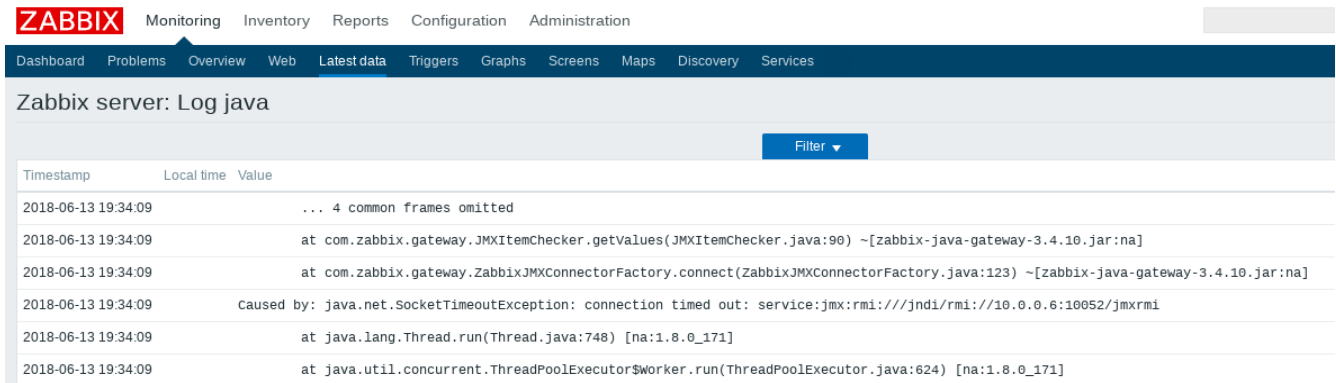
Update interval: 30s

History storage period: 90d

Log time format: ppppddphh:mm:ss

Al terminar hacemos clic en “**Update**” para que se nos cree el elemento.

Por último si nos vamos a “**Monitoring** → **Latest data**” y marcamos el Item creado observamos como nos está recogiendo la información del fichero de log antes indicado:



ZABBIX Monitoring Inventory Reports Configuration Administration

Dashboard Problems Overview Web Latest data Triggers Graphs Screens Maps Discovery Services

### Zabbix server: Log java

Filter ▼

Timestamp	Local time	Value
2018-06-13 19:34:09		... 4 common frames omitted
2018-06-13 19:34:09		at com.zabbix.gateway.JMXItemChecker.getValues(JMXItemChecker.java:90) ~[zabbix-java-gateway-3.4.10.jar:na]
2018-06-13 19:34:09		at com.zabbix.gateway.ZabbixJMXConnectorFactory.connect(ZabbixJMXConnectorFactory.java:123) ~[zabbix-java-gateway-3.4.10.jar:na]
2018-06-13 19:34:09		Caused by: java.net.SocketTimeoutException: connection timed out: service:jmx:rmi:///jndi/rmi://10.0.0.6:10052/jmxrmi
2018-06-13 19:34:09		at java.lang.Thread.run(Thread.java:748) [na:1.8.0_171]
2018-06-13 19:34:09		at java.util.concurrent.ThreadPoolExecutor\$Worker.run(ThreadPoolExecutor.java:624) [na:1.8.0_171]

## 11. Conclusión

En este proyecto hemos conocido el funcionamiento y las características de dos de las herramientas de monitorización más importantes de hoy en día.

Ambas herramientas han resultado muy útiles y fáciles de configurar a la hora de intentar simular algunos de los problemas reales que se puede encontrar cualquier persona al usarlas.

También hemos entendido cuales son las principales ventajas e inconvenientes de cada una, por ejemplo la sencilla gestión a través del panel web de ambas, la falta de una librería de plugins en Zabbix o las limitaciones de la versión OpenSource de Pandora FMS con respecto a la versión Enterprise.

Por último, para seguir ampliando este proyecto se podrían realizar algunas de las siguientes funcionalidades:

- Configuración del proceso Zabbix proxy, que recolecta los datos de una monitorización en varios dispositivos y que después envía la información al servidor Zabbix.
- Configuración de autenticación a Zabbix a través de LDAP.
- Monitorización de una base de datos MySQL en Pandora.
- Creación y modificación de informes en Pandora.

## 12. Referencias y bibliografía

[https://www.zabbix.com/documentation/3.4/manual/installation/install\\_from\\_packages/rhel\\_centos](https://www.zabbix.com/documentation/3.4/manual/installation/install_from_packages/rhel_centos)  
[https://www.zabbix.com/download?zabbix=3.4&os\\_distribution=centos&os\\_version=7&db=MySQL](https://www.zabbix.com/download?zabbix=3.4&os_distribution=centos&os_version=7&db=MySQL)  
[https://www.zabbix.com/documentation/3.4/manual/appendix/install/db\\_scripts#mysql](https://www.zabbix.com/documentation/3.4/manual/appendix/install/db_scripts#mysql)  
<https://www.zabbix.com/documentation/3.4/manual/quickstart/notification>  
<http://bitagorin.blogspot.com.es/2015/11/instalacion-de-los-agentes-zabbix-en.html>  
<http://www.ingdiaz.org/instalacion-agente-zabbix-ubuntu-windows/>  
[https://www.zabbix.com/documentation/3.4/manual/appendix/install/windows\\_agent](https://www.zabbix.com/documentation/3.4/manual/appendix/install/windows_agent)  
<https://clouding.io/kb/zabbix-auto-registration-vs-auto-discovery/>  
[https://www.zabbix.com/documentation/3.4/manual/config/items/itemtypes/jmx\\_monitoring](https://www.zabbix.com/documentation/3.4/manual/config/items/itemtypes/jmx_monitoring)  
<https://www.zabbix.com/documentation/3.4/manual/concepts/java>  
[https://www.zabbix.com/documentation/3.4/manual/config/items/itemtypes/log\\_items](https://www.zabbix.com/documentation/3.4/manual/config/items/itemtypes/log_items)

<https://pandorafms.org/es/producto/introduccion-a-pandora-fms/>  
<https://pandorafms.org/es/producto/funcionalidades-monitorizacion/>  
[https://pandorafms.com/downloads/PDF/funcionalidades\\_DEF\\_ES.pdf](https://pandorafms.com/downloads/PDF/funcionalidades_DEF_ES.pdf)  
[https://pandorafms.com/downloads/PDF/guias\\_rapidas\\_ES.pdf](https://pandorafms.com/downloads/PDF/guias_rapidas_ES.pdf)  
<https://wiki.pandorafms.com/index.php?title=Pandora:Documentation>  
[https://wiki.pandorafms.com/index.php?title=Pandora:QuickGuides\\_ES:Guia\\_Rapida\\_General#Introducci.C3.B3n\\_a\\_esta\\_gu.C3.ADa](https://wiki.pandorafms.com/index.php?title=Pandora:QuickGuides_ES:Guia_Rapida_General#Introducci.C3.B3n_a_esta_gu.C3.ADa)  
[https://wiki.pandorafms.com/index.php?title=Pandora:Documentation\\_es:Instalacion](https://wiki.pandorafms.com/index.php?title=Pandora:Documentation_es:Instalacion)  
[https://wiki.pandorafms.com/index.php?title=Pandora:QuickGuides\\_ES:Configuracion\\_de\\_alertas](https://wiki.pandorafms.com/index.php?title=Pandora:QuickGuides_ES:Configuracion_de_alertas)  
[https://wiki.pandorafms.com/index.php?title=Pandora:Configuracion\\_alertas\\_emails](https://wiki.pandorafms.com/index.php?title=Pandora:Configuracion_alertas_emails)  
[https://wiki.pandorafms.com/index.php?title=Pandora:QuickGuides\\_ES:Guia\\_Rapida\\_General#A.C3.B1adir\\_una\\_alerta\\_.28env.C3.ADo\\_de\\_email.29\\_ante\\_un\\_problema](https://wiki.pandorafms.com/index.php?title=Pandora:QuickGuides_ES:Guia_Rapida_General#A.C3.B1adir_una_alerta_.28env.C3.ADo_de_email.29_ante_un_problema)  
[https://wiki.pandorafms.com/index.php?title=Pandora:Documentation\\_es:Plantillas\\_y\\_Componentes](https://wiki.pandorafms.com/index.php?title=Pandora:Documentation_es:Plantillas_y_Componentes)