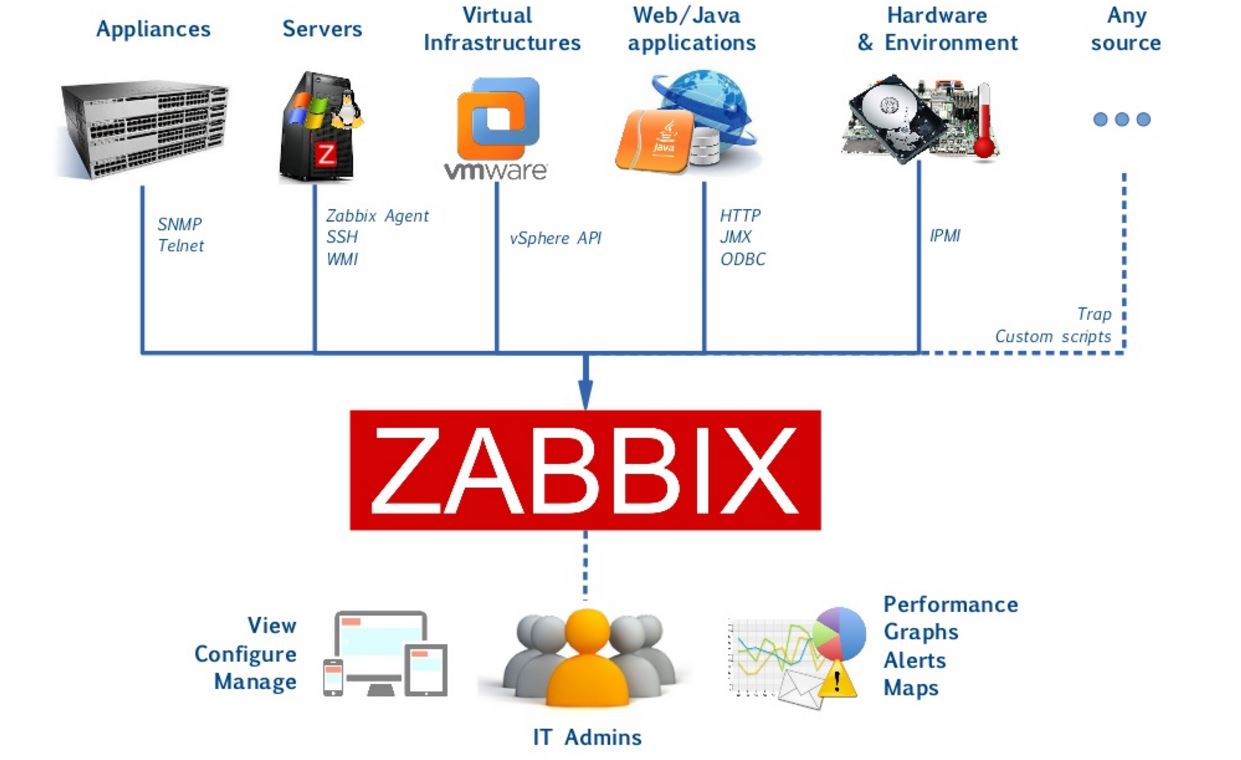
**Implantación de un sistema de monitorización con Zabbix**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Introducción**](#_g59i8ewd3ed3) **2**

[**3. Requisitos previos**](#_65bkbeaoxp9w) **2**

[**4. Añadir usuarios y grupos al sistema**](#_p81vn68osmpu) **6**

[**5. Añadir host a Zabbix**](#_8tihsr2is52z) **8**

[**6. Notificaciones por correo electrónico**](#_jmx7bss60sbl) **15**

# **2. Introducción**

Zabbix es un software de monitorización de código abierto para redes y aplicaciones. Ofrece

monitorización en tiempo real de miles de métricas recogidas de servidores, equipos virtuales, dispositivos de red y aplicaciones web.

Zabbix usa varias opciones para recoger métricas, incluyendo la monitorización sin agente de los servicios del usuario y de la arquitectura cliente-servidor. Para recoger métricas del servidor, utiliza un agente pequeño en el cliente monitorizado para recopilar datos y enviarlos al servidor Zabbix.

Zabbix admite la comunicación cifrada entre el servidor y los clientes conectados, de forma que sus datos están protegidos mientras recorren redes inseguras.

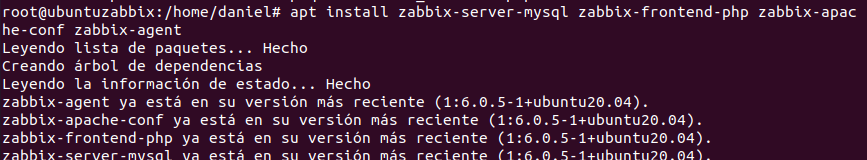
El servidor Zabbix almacena sus datos en una base de datos relacional alimentada con MySQL o PostgreSQL. También puede almacenar datos históricos en bases de datos NoSQL como Elasticsearch.

# **3. Requisitos previos**

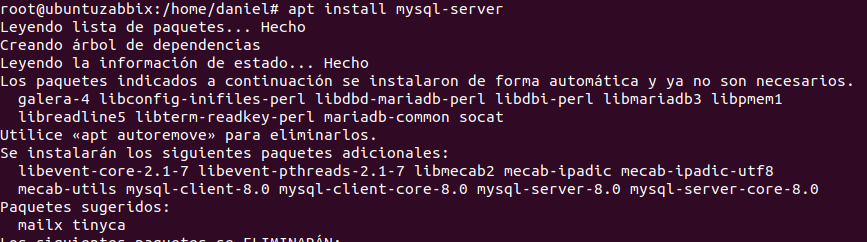
Zabbix está disponible en el administrador de paquetes de Ubuntu, pero está obsoleto, de forma que utilizaremos el repositorio oficial de Zabbix para instalar la última versión estable.

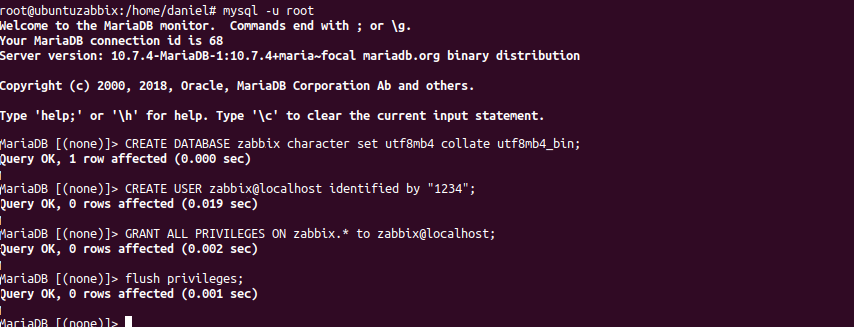
Instalamos el servidor, la interfaz y el agente de Zabbix





Ahora instalamos mysql, realizamos la configuración de seguridad inicial y creamos la base de datos inicial

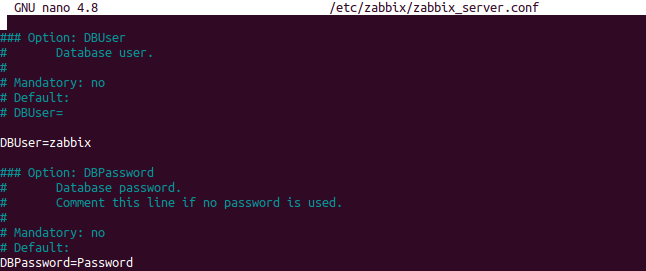




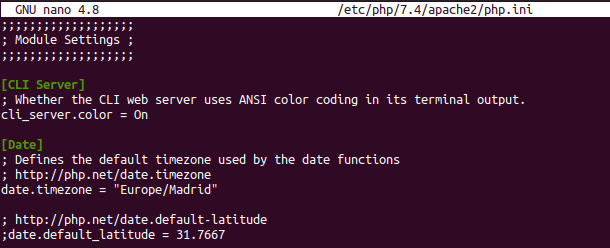
Ahora importamos el esquema y los datos iniciales que se encuentran en /usr/share/doc/



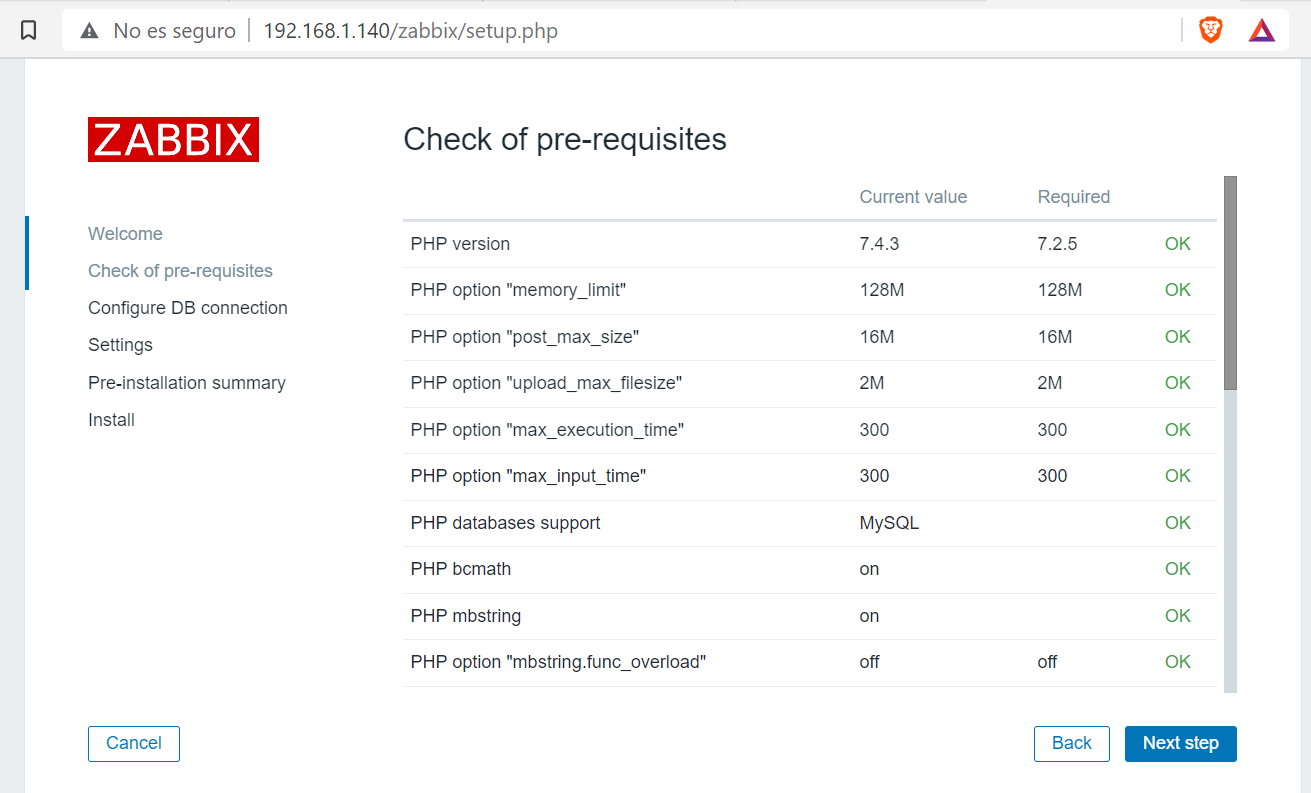
Y configuramos la base de datos para el servidor Zabbix

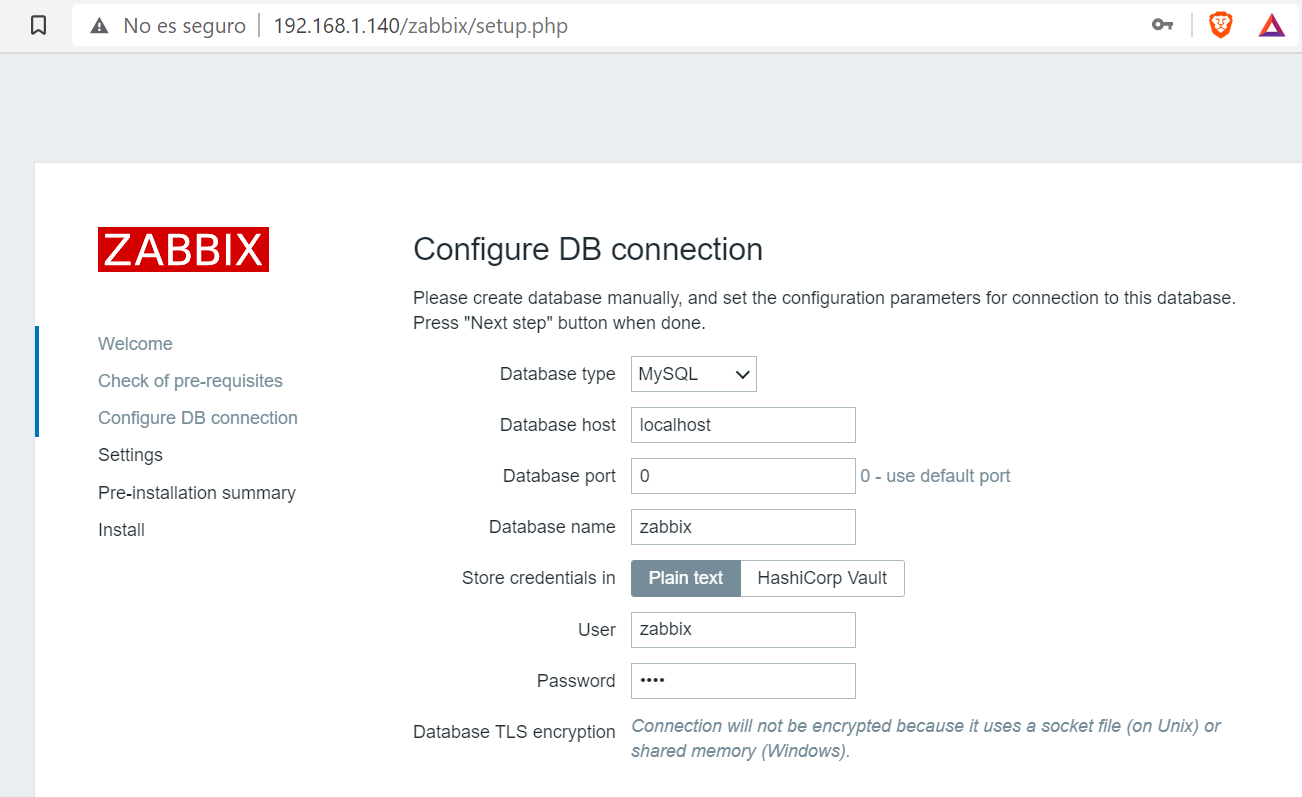


El siguiente paso será iniciar el agente y el servidor de Zabbix y los configuramos para que se inicien con el Sistema.Ahora modificamos el fichero php.ini de apache y fijamos la zona en Europe/Madrid y reiniciamos apache

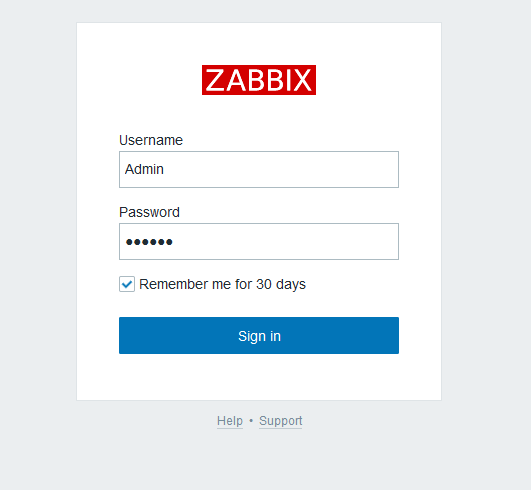


Abrimos un explorador web e introducimos la dirección ip del servidor seguido de /zabbix y configuramos la conexión a la base de datos





Para finalizar nos aparecerá la pantalla de acceso.

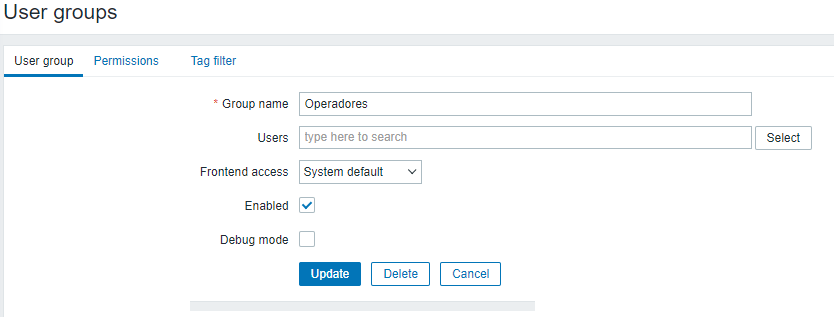


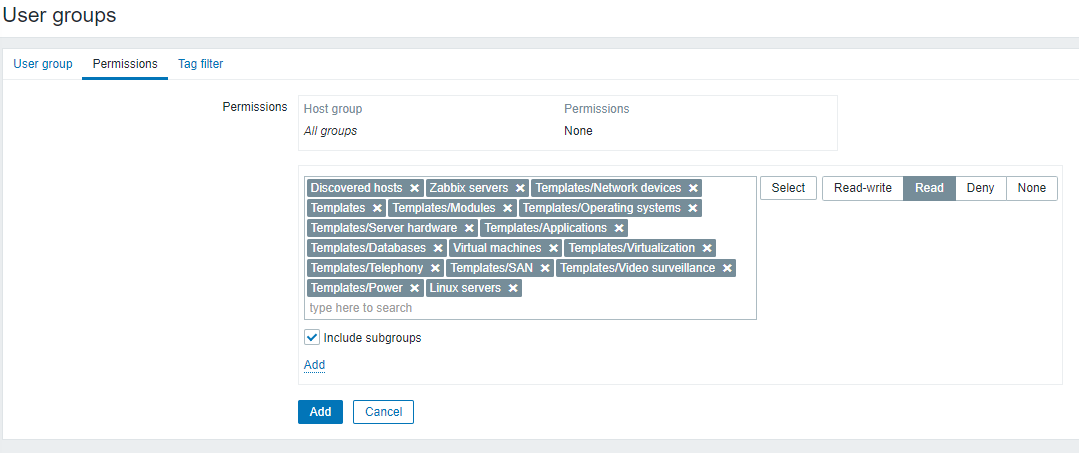
El usuario es “Admin” y la contraseña es “zabbix”.

# **4. Añadir usuarios y grupos al sistema**

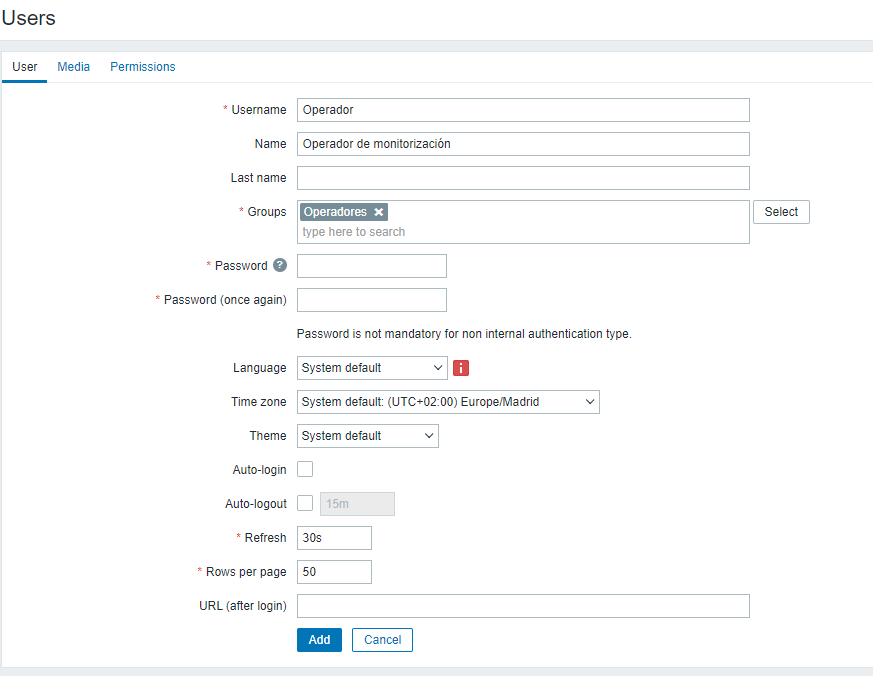
Si queremos crear usuarios para que puedan monitorizar los dispositivos nos dirigimos a “Administration” ”Users

También podemos añadir grupos y de esta manera tener clasificados los usuarios y asignarles permisos según al grupo al que pertenezcan. Por ejemplo, podemos crear el grupo “Operadores” y darle permisos de solo lectura a todos los objetos monitorizados.

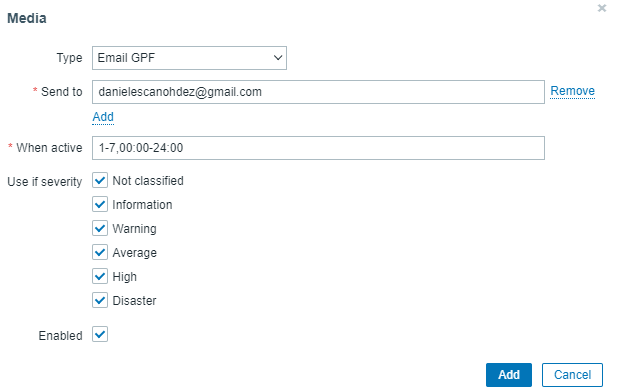


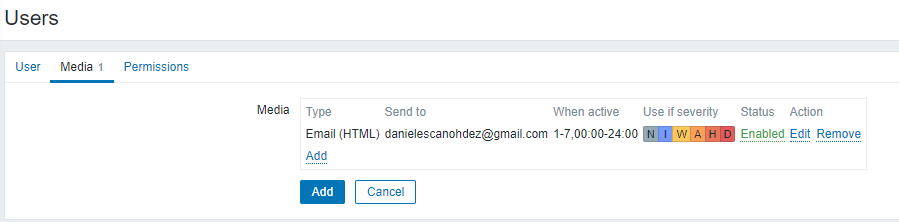


Y ahora creamos un usuario que pertenezca al grupo.

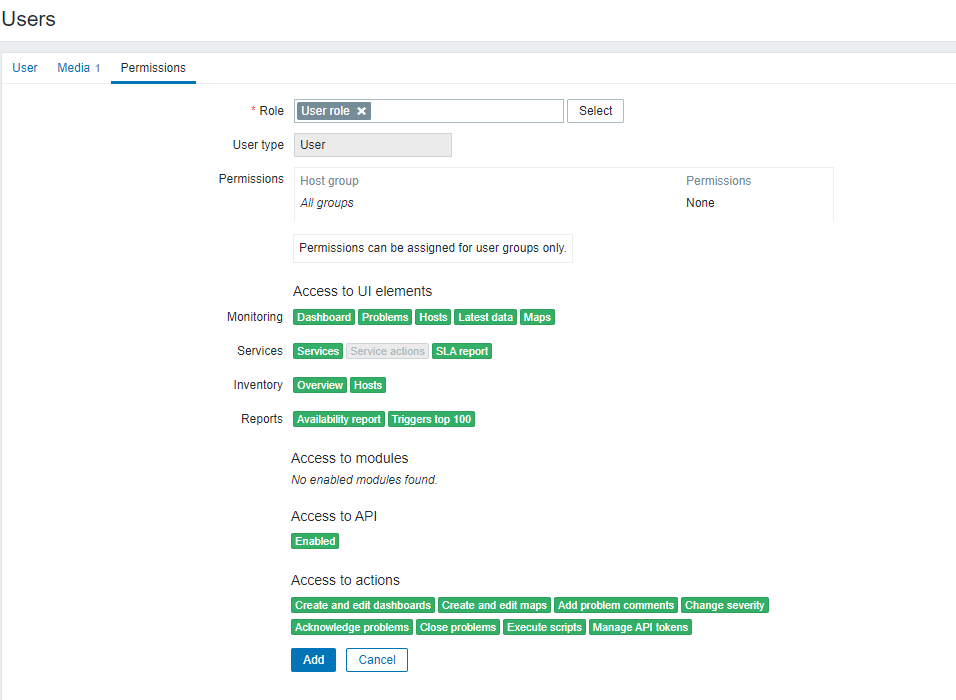


En la pestaña “Media” podemos asignarle un método de notificación. En nuestro caso crearemos uno de tipo “Email”





Y en la pestaña “Permissions” le asignamos el rol de usuario.

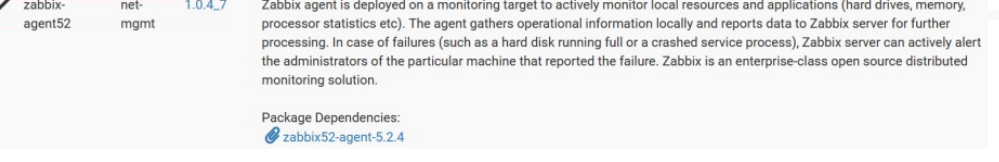


# **5. Añadir host a Zabbix**

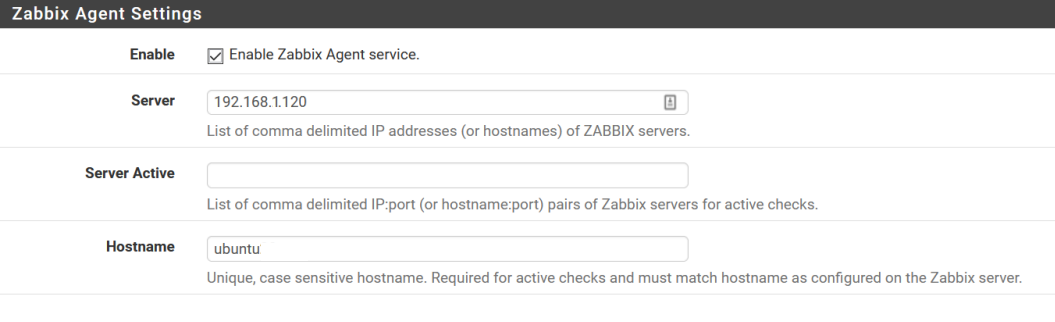
En este apartado veremos como añadir un nuevo host a Zabbix. En Zabbix, un host es una entidad física o virtual que queremos monitorizar. Nos dirigiremos a “Configuration” ”Hosts” para crear un nuevo host

Podemos encender una máquina virtual y configurarla en Zabbix para monitorizar. A continuación, se muestra como monitorizar un firewall pfsense, una máquina Windows y un servidor Linux.

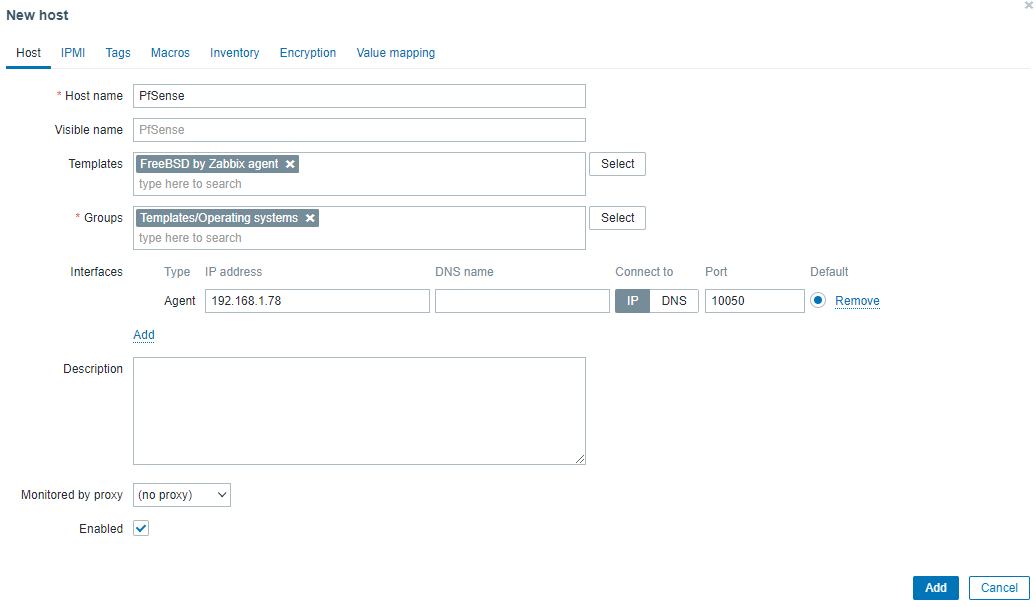
Para monitorizar pfsense vamos a instalar el agente que viene preparado como paquete en el firewall. Instalaremos el paquete zabbix-agent52



Configuramos los parámetros necesarios y activamos el servicio.

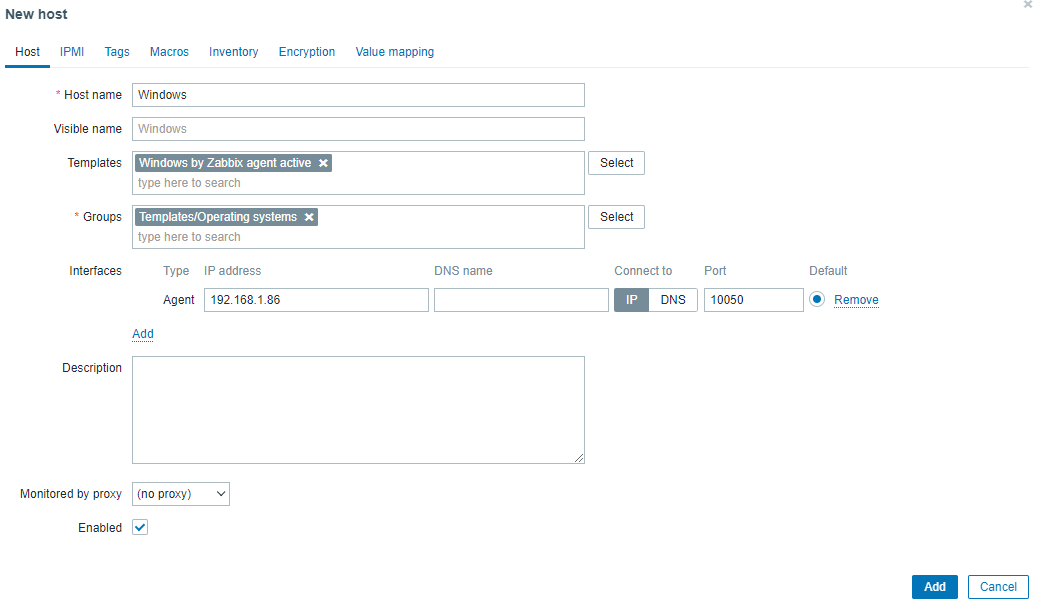


Dentro de Zabbix, en el apartado hosts configuramos la conexión. Como grupo seleccionamos Templates/Operating systems y en templates seleccionamos FreeBSD



Ahora procedemos a configurar el host para la máquina de windows7. Desde la página de zabbix descargamos el agente e instalamos

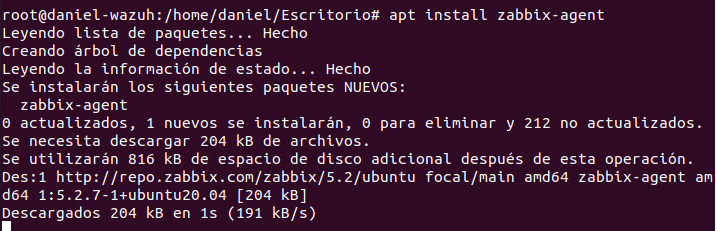




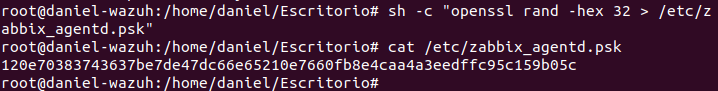
Para monitorizar una máquina con Linux podemos instalar el cliente correspondiente.

Descargamos el paquete debian necesario. Actualizamos e instalamos





En este caso vamos a utilizar claves precompartidas (PSK) para proteger la conexión entre el servidor y el agente. Primero generamos una PSK:

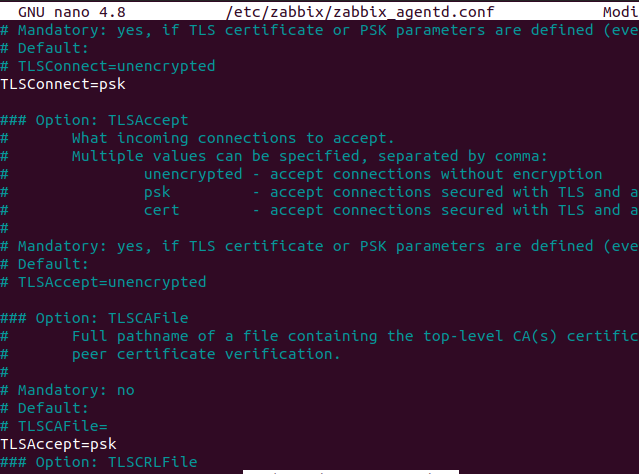


El código generado lo utilizaremos en la configuración. Ahora editamos el fichero de configuración del agente para especificar los datos de conexión. Cambiamos las variables Server y ServerActive poniendo la dirección ip del servidor. En la variable Hostname ponemos el nombre de nuestro hosts Ubuntu.



A continuación, buscamos la sección que configura la conexión segura con el servidor Zabbix y habilitamos el soporte con clave precompartida. Buscamos la sección TLSConnect y añadimos esta línea para configurar el soporte de clave precompartida:

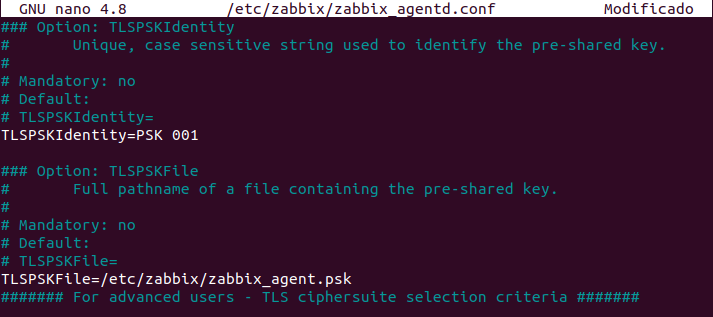
Luego, localizamos la sección TLSAccept,



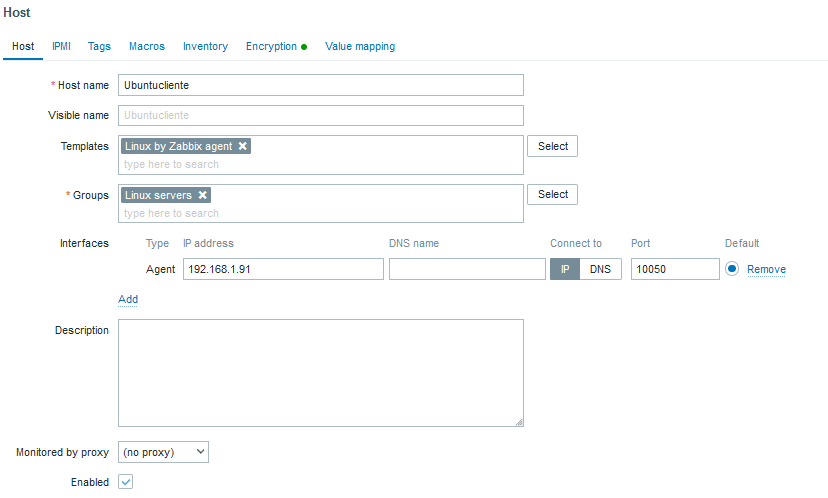
Ahora, localizamos la sección TLSPSKIdentity y elegimos un nombre único para identificar su clave precompartida añadiendo esta línea:

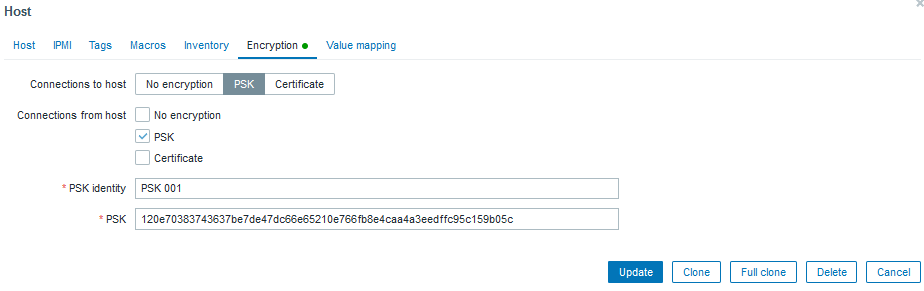
Usaremos esto como el PSK ID cuando añadamos su host a través de la interfaz web de Zabbix. A continuación, establecemos la opción que apunta a su clave precompartida creada previamente. Buscamos la opción TLSPSKFile:

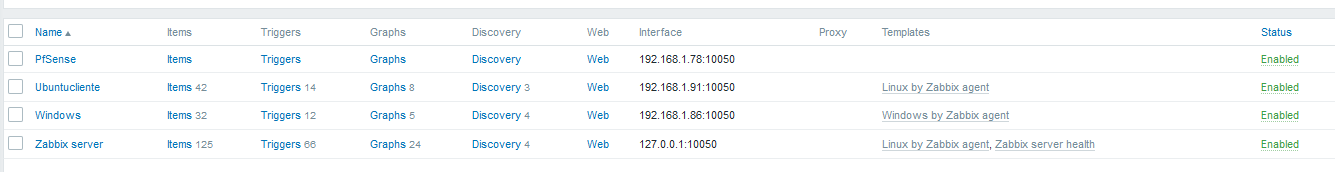
Y seleccionamos el fichero que tiene la clave precompartida:



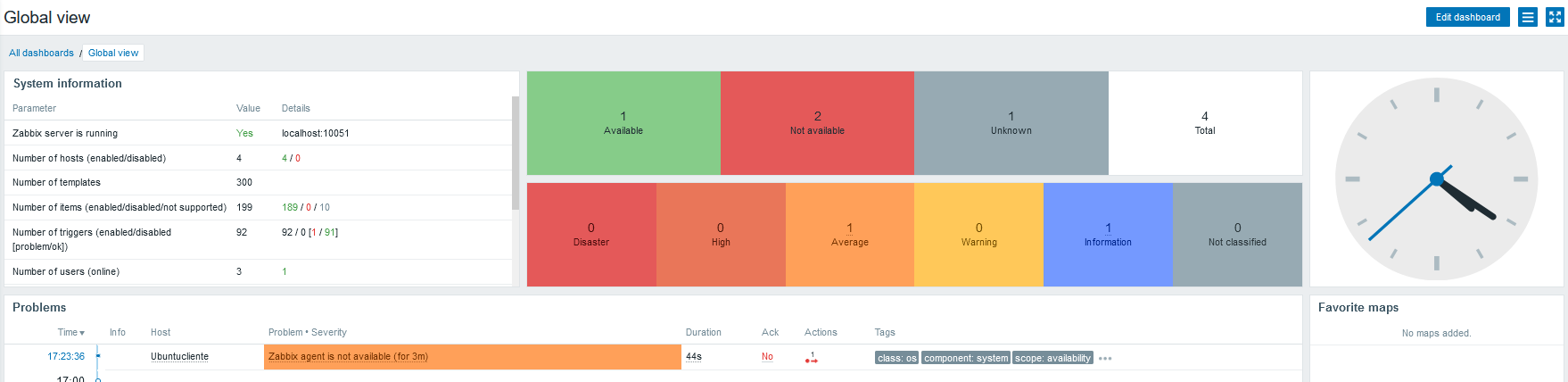
Ahora añadimos el nuevo host en el servidor Zabbix.







Si ahora apagamos las máquinas y esperamos el tiempo necesario para que salten los disparadores de las alarmas veremos el resultado en el dashboard

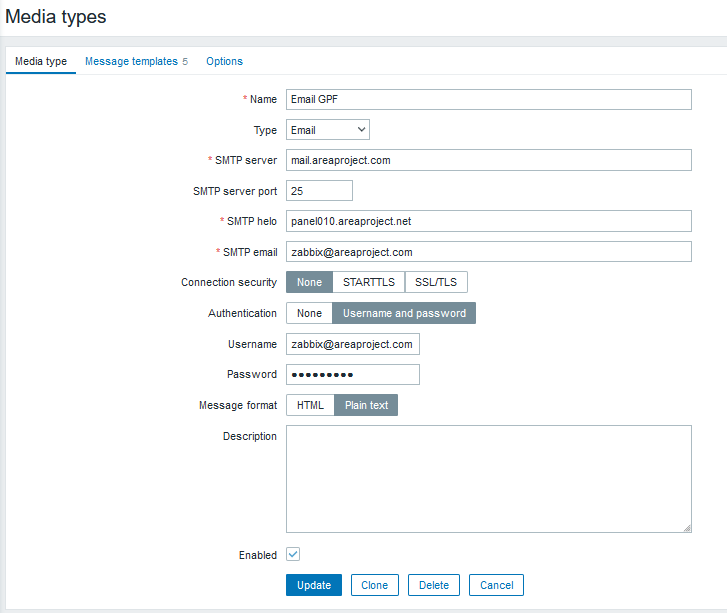


# **6. Notificaciones por correo electrónico**

Zabbix admite automáticamente muchos tipos de notificaciones: correo electrónico, OTRS, Slack, Telegram, SMS, etc.

Hacemos clic en Administración, y a continuación en Tipos de medio en la barra de navegación izquierda. Veremos la lista de todos los tipos de medios. Existen dos opciones preconfiguradas para correos electrónicos: para la notificación de texto sin formato y para las notificaciones HTML. En este tutorial, usará la notificación de texto sin formato. Hacemos clic en Correo electrónico

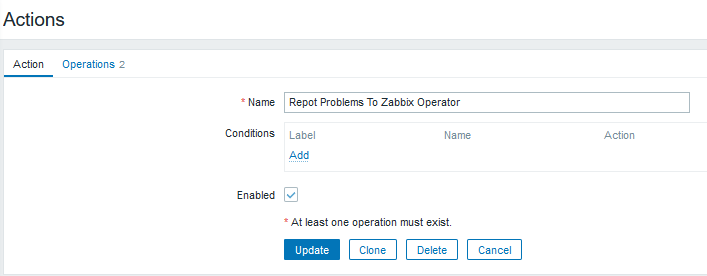
Configuramos los parámetros de conexión a una de nuestras cuentas de email.

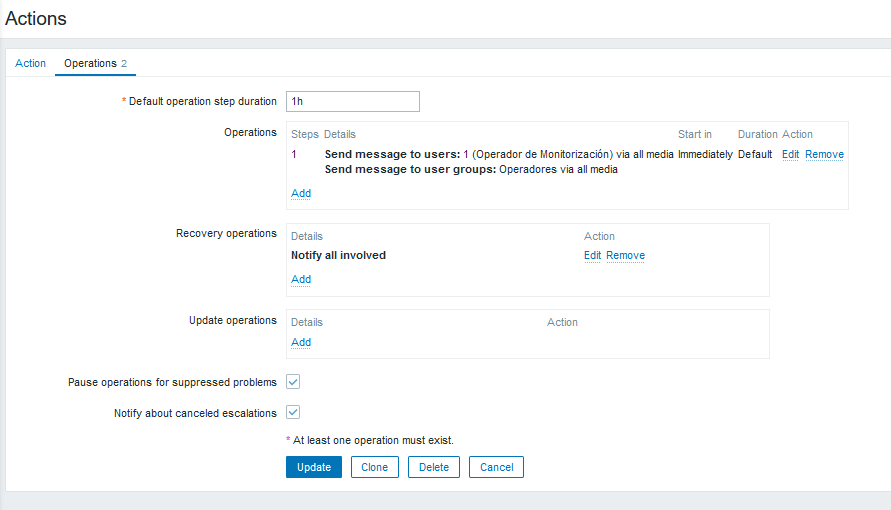


En la pestaña Plantillas de mensaje, podemos ver la lista de mensajes predefinidos para varios tipos de notificaciones. Finalmente, hacemos clic en el botón Actualizar en la parte inferior del formulario para actualizar los parámetros del correo electrónico

Ahora vamos a habilitar las notificaciones. Hacemos clic en la pestaña Configuración y a continuación en Acciones en la barra de navegación izquierda. Veremos una acción preconfigurada, que es responsable de enviar notificaciones a todos los administradores Zabbix. Podemos revisar y cambiar los ajustes haciendo clic en su nombre.

A efectos de este tutorial, utilizaremos esta acción para crearnos una nueva para el grupo de usuarios de operadores





Comprobamos que esté activa la acción.

