Universitat Oberta de Catalunya

uoc.edu

TFG – Representación de *KPI* geolocalizados

Raúl Pérez Sanchiz
Grado en Tecnologías de Telecomunicación
Servicios basados en localización y espacio inteligente

Francesc Puigvert Pell
David Merino Arranz

1/1/2019

Agradecimientos

Gracias a mis hermanos, a mis amigos y a todas aquellas personas que estuvieron a mi lado durante la realización de este grado en Tecnologías de Telecomunicación.

Y, en especial, a Jordi Palà. Excompañero de trabajo, gran amigo y máximo responsable de que hoy esté entregando esta Memoria. Desde que nos conocemos se preocupó por estar en los momentos más difíciles, dándome su apoyo incondicional y ayuda cuando más lo necesitaba. Esta etapa de mi vida no fue una excepción, y por eso le estaré eternamente agradecido.

Queda un último sprint.

Ficha del trabajo final

Título del trabajo:	*Representación de KPI geolocalizados*
Nombre del autor:	*Raúl Pérez Sanchiz*
Nombre del consultor/a:	*Francesc Puigvert Pell*
Nombre del PRA:	*David Merino Arranz*
Fecha de entrega (mm/aaaa):	01/2019
Titulación:	*Grado en Tecnologías de Telecomunicación*
Área del Trabajo Final:	*Servicios basados en localización y espacio inteligente*
Idioma del trabajo:	*Español*
Palabras clave	*Monitorización, KPI, Sistemas*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

El proyecto consiste en la implantación de un sistema de monitorización capaz de obtener datos de rendimiento y estado de diferentes elementos de la infraestructura de una cadena hotelera con más de 30 hoteles ubicados tanto en el territorio español como en Andorra. Concretamente son objeto de monitorización aplicaciones y servicios cuyo correcto funcionamiento es fundamental, el cual anteriormente no era controlado.

La herramienta utilizada para realizar la monitorización es Zabbix, una herramienta de código abierto capaz de registrar estados de servicios de red, servidores y *hardware* mediante la utilización de agentes, SNMP, ICMP, etc. Para albergar esta aplicación se selecciona el sistema operativo CentOS, distribución basada en Red Hat Enterprise Linux conocido por su estabilidad, seguridad y sus ciclos largos de mantenimiento y soporte.

Para realizar la implantación se ha realizado, en primer lugar, en un entorno de desarrollo que la compañía tiene ubicado en su sede Central. Posteriormente, y tras comprobar su correcto funcionamiento, se ha realizado la migración a un entorno de producción de la sede Central para finalmente configurar los puntos de monitorización considerados necesarios para tener más control sobre los sistemas.

El resultado del trabajo ha sido satisfactorio, monitorizando actualmente 72 dispositivos, con 2419 puntos de monitorización recopilando datos a más de 34 valores por segundo con 988 alertas definidas. El estudio posterior de herramientas como Power BI o Grafana han aportado un salto cualitativo en cuanto al producto final de este trabajo permitiendo analizar mejor los datos

recopilados por Zabbix.

En conclusión, la implantación de la herramienta de monitorización ha sido una mejora para la empresa.

Abstract (in English, 250 words or less):

The project consists of the implementation of a monitoring system capable of obtaining performance and status data from different elements of the infrastructure about a hotel chain with 30 hotels located in Spain and Andorra. Specifically, applications and services will be monitored to obtain a correct performance, which was previously not controlled.

The tool used to perform the monitoring is Zabbix, an open-source tool capable of registering states of network services, servers and hardware using agents and SNMP protocol, for example. This application will be installed at CentOS operating system, a Red Hat Enterprise Linux distribution well-known by its stability, security and long maintenance and support cycles.

To carry out the implementation, the application was tested in a development environment that the company has located in its headquarters. Afterwards, and after verifying its correct performance, a migration was made from development to production environment to finally configure monitoring points considered necessary to have more control over the systems the company has.

The results of the work have been satisfactory, currently monitoring 72 devices with 2419 monitoring points collecting data at more than 34 values per second and 988 alerts defined. The subsequent study of tools such as Power BI or Grafana have allowed us to better analyse the data collected by Zabbix, providing a qualitative leap in terms of the final product of this work.

In conclusion, the implementation of the monitoring tool has been an improvement for the company.

Índice

Lista de figuras

Índice de tablas

1. Introducción

Este apartado dará una visión general del trabajo realizado en este trabajo final de grado, definiendo el contexto y justificación del trabajo, los objetivos a alcanzar y tareas e hitos derivados de éstos, las incidencias y riesgos que pueden manifestarse durante la realización del trabajo y los planes de contingencia que tratarán de mitigar éstos posibles contratiempos.

1.1. Contexto y justificación del trabajo

Una empresa hotelera tiene una estructura de más de 30 complejos repartidos por España y Andorra, conectados mediante la solución de cortafuegos *VPN* de la empresa Fortinet a su sede Central y su *Datacenter*, ambos ubicados en la ciudad de Barcelona. En el *Datacenter* se alojan los datos de la aplicación del sistema de gestión de la propiedad (de ahora en adelante, *PMS*) desarrollada por los programadores de la compañía. Esta aplicación es consultada desde los complejos y su correcto funcionamiento tanto a nivel de rendimiento como a nivel de conectividad son puntos críticos. A demás, la aplicación requiere de datos extraídos por la aplicación CHAR, tarificador de llamadas desarrollado por la empresa Barcelonesa CHAR que obtiene datos de las centralitas de los complejos sobre los consumos telefónicos realizados por huéspedes para posteriormente enviar dicha información al *PMS* y facturar los consumos en el *check-out* de los clientes.

La necesidad de controlar el estado de funcionamiento tanto a nivel de conectividad como a nivel de rendimiento es un hecho en cualquier entorno de sistemas: Si se producen cortes en el servicio de conexión a *Internet* o fallos de rendimiento en los distintos puntos de la infraestructura se pueden ver gravemente afectadas operativas críticas como los *chech-in*, los *check-out*, la limpieza de las habitaciones, las tareas del personal de mantenimiento, el servicio de consultas de disponibilidad de alojamientos a turoperadores y agencias de viajes *on-line*, entre otros.

Por ello, tratar de detectar problemas en los sistemas estudiando los posibles motivos que los ocasionan para prevenirlos incluso antes que se produzcan son objetivos que cualquier departamento de *IT* debe alcanzar para ofrecer un mejor servicio tanto a los huéspedes, como al resto de actores que intervienen en la comercialización de los alojamientos de la compañía. También es objetivo de este Trabajo Final de Grado el optimizar recursos tanto a nivel informático como a nivel humano, lo que se traduce en el ahorro de costes y la evolución de los sistemas.

1.2. Objetivos del trabajo

A continuación, se detallan los objetivos a alcanzar mediante la realización de este trabajo final de grado, que son los siguientes:

- Familiarización con los objetos específicos de la monitorización de sistemas.

- Conocer las características y conceptos de la tecnología de sistemas de geoposicionamiento e información geográfica.

y específicamente:

- Justificación de la solución propuesta bajo las condiciones descritas.

- Aprender a utilizar servicios de monitorización y representación mediante un panel web con los indicadores clave de rendimiento (de ahora en adelante, *KPI)* ubicados geolocalizados en un mapa.

- Aprender a desarrollar e implementar el proyecto en entorno de producción que corrobore la viabilidad y utilidad de la solución.

1.3. Tareas e hitos

Respecto a la planificación para llevar a cabo este trabajo, se ha subdividido en las siguiente cuatro tareas:

- Tarea 1: “Definición del entorno”. Se definirá la solución y se analizará la viabilidad de ésta considerando los requisitos de la infraestructura como el tiempo de duración del proyecto. También se determinará el coste del despliegue del entorno escogido. Esta tarea permitirá la preparación del entorno para las siguientes tareas y favorecerá la familiarización de la tecnología elegida. El resultado de esta tarea será una parte introductoria de la memoria final del trabajo.

- Tarea 2: “Puesta en marcha del entorno de desarrollo de los *KPI*”. Incluirá la descripción de la arquitectura del entorno de pruebas, la puesta en marcha del servicio de monitorización en el entorno de desarrollo y la valoración del resultado de la monitorización que corrobore el buen funcionamiento del sistema. Esta tarea proporcionará un servicio web que muestre los *KPI* de diferentes puntos de la infraestructura que debe servir de referencia para la puesta en marcha del entorno en producción. El resultado de esta tarea es un borrador que acabará siendo una parte de la memoria final del trabajo.

- Tarea 3: “Puesta en marcha del entorno de producción de los *KPI*”. Se pondrá en marcha en entorno de producción los *KPI* definidos. Se incluirá una descripción de la arquitectura en entorno de producción, se realizará la migración y puesta en marcha del servicio de monitorización en entorno de producción, se diseñará un sistema de copias de seguridad (de ahora en adelante, *back-up*) de los datos recogidos para garantizar la recuperación del sistema en caso de fallo de la base de datos (de ahora en adelante, *BBDD*), sistema operativo, etc. y se valorará el resultado de la monitorización que corrobore el buen funcionamiento del sistema. Finalmente se obtendrá un documento de diseño que servirá de referencia para la construcción del sistema en entornos de *TI*, además esta tarea proporcionará un borrador que acabará siendo una parte importante de la memoria y del video del final del trabajo.

- Tarea 4: “Estudio y configuración del cuadro de mando con datos geolocalizados”. En esta tarea se estudiarán posibles interfaces de visualización de los *KPI* y de otras posibles propuestas de análisis geográfico. Se configurará el cuadro de mando que mostrará en un mapa los *KPI* de los elementos críticos de sistema recogidos por la herramienta de monitorización. Finalmente se conseguirá el código fuente y/o configuración del cuadro de mando que obtendrá los datos.

- Entrega final: Durante este periodo se realizará el video y documentación final para la entrega del Trabajo Final de Grado.

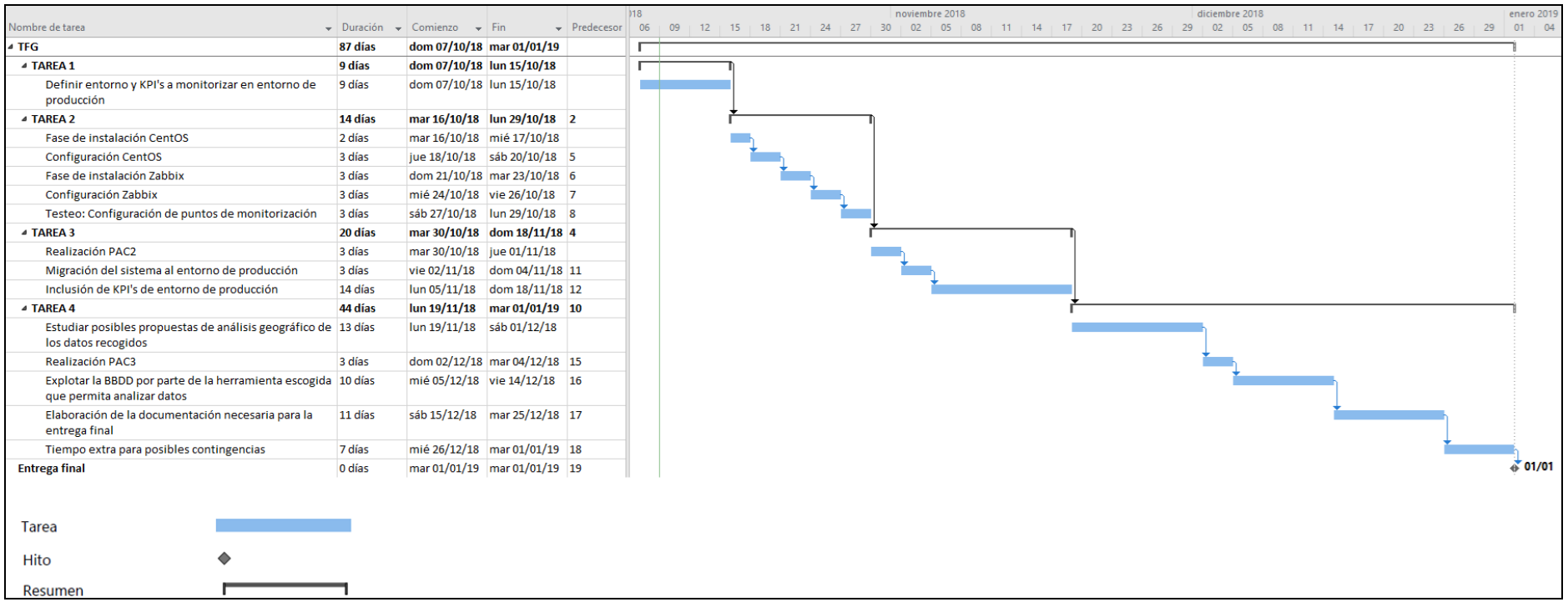
En la Tabla 1 se detallan las tareas mencionadas anteriormente.

Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
Trabajo Final de Grado	**87 días**	**dom 07/10/18**	**mar 01/01/19**	
TAREA 1	**9 días**	**dom 07/10/18**	**lun 15/10/18**	
Definir entorno y *KPI* a monitorizar en entorno de producción	9 días	dom 07/10/18	lun 15/10/18	
TAREA 2	**14 días**	**mar 16/10/18**	**lun 29/10/18**	**2**
Fase de instalación CentOS	2 días	mar 16/10/18	mié 17/10/18	
Configuración CentOS	3 días	jue 18/10/18	sáb 20/10/18	5
Fase de instalación Zabbix	3 días	dom 21/10/18	mar 23/10/18	6
Configuración Zabbix	3 días	mié 24/10/18	vie 26/10/18	7
Validación: Configuración de puntos de monitorización	3 días	sáb 27/10/18	lun 29/10/18	8
TAREA 3	**20 días**	**mar 30/10/18**	**dom 18/11/18**	**4**
Elaboración de documentación	3 días	mar 30/10/18	jue 01/11/18	
Migración del sistema al entorno de producción	3 días	vie 02/11/18	dom 04/11/18	11
Inclusión de *KPI* de entorno de producción	14 días	lun 05/11/18	dom 18/11/18	12
TAREA 4	**44 días**	**lun 19/11/18**	**mar 01/01/19**	**10**
Estudiar posibles propuestas de análisis geográfico de los datos recogidos	13 días	lun 19/11/18	sáb 01/12/18	
Elaboración de documentación	3 días	dom 02/12/18	mar 04/12/18	15
Explotar la BBDD por parte de la herramienta escogida que permita analizar datos	10 días	mié 05/12/18	vie 14/12/18	16
Elaboración de la documentación necesaria para la entrega final	11 días	sáb 15/12/18	mar 25/12/18	17
Tiempo extra para posibles contingencias	7 días	mié 26/12/18	mar 01/01/19	18
Entrega final	0 días	mar 01/01/19	mar 01/01/19	19

Tabla 1 - Planificación de tareas

1.4. Diagrama de Gantt

El gráfico de la Figura 1 muestra la planificación del punto 1.3 de este documento en formato de diagrama de Gantt.



Nombre de tarea	Duración	Comienzo	Fin	Predecesor
TFG	**87 días**	**dom 07/10/18**	**mar 01/01/19**	
TAREA 1	**9 días**	**dom 07/10/18**	**lun 15/10/18**	
Definir entorno y KPI's a monitorizar en entorno de producción	9 días	dom 07/10/18	lun 15/10/18	
TAREA 2	**14 días**	**mar 16/10/18**	**lun 29/10/18**	**2**
Fase de instalación CentOS	2 días	mar 16/10/18	mié 17/10/18	
Configuración CentOS	3 días	jue 18/10/18	sáb 20/10/18	5
Fase de instalación Zabbix	3 días	dom 21/10/18	mar 23/10/18	6
Configuración Zabbix	3 días	mié 24/10/18	vie 26/10/18	7
Testeo: Configuración de puntos de monitorización	3 días	sáb 27/10/18	lun 29/10/18	8
TAREA 3	**20 días**	**mar 30/10/18**	**dom 18/11/18**	**4**
Realización PAC2	3 días	mar 30/10/18	jue 01/11/18	
Migración del sistema al entorno de producción	3 días	vie 02/11/18	dom 04/11/18	11
Inclusión de KPI's de entorno de producción	14 días	lun 05/11/18	dom 18/11/18	12
TAREA 4	**44 días**	**lun 19/11/18**	**mar 01/01/19**	**10**
Estudiar posibles propuestas de análisis geográfico de los datos recogidos	13 días	lun 19/11/18	sáb 01/12/18	
Realización PAC3	3 días	dom 02/12/18	mar 04/12/18	15
Explotar la BBDD por parte de la herramienta escogida que permita analizar datos	10 días	mié 05/12/18	vie 14/12/18	16
Elaboración de la documentación necesaria para la entrega final	11 días	sáb 15/12/18	mar 25/12/18	17
Tiempo extra para posibles contingencias	7 días	mié 26/12/18	mar 01/01/19	18
Entrega final	0 días	mar 01/01/19	mar 01/01/19	19

Figura 1 - Planificación de tareas del proyecto final de carrera

1.5. Incidencias y riesgos

Durante la realización de este trabajo final de grado se pueden dar lugar incidencias o riesgos relacionados con los recursos que se van a utilizar. Los detectados en el desarrollo de este trabajo final de grado son los siguientes:

- Problemas de alojamiento de la máquina virtual de la herramienta de monitorización en entorno de desarrollo o producción

  Es posible que, debido a las máquinas virtuales que están actualmente en funcionamiento y la implantación de otros proyectos que se prevén llevar a cabo durante la realización de este trabajo final de grado y que tienen como ubicación los servidores *ESX*, los recursos que pueda consumir la máquina virtual donde se prevé se realizará la instalación del sistema de monitorización no tenga cabida en los recursos disponibles.

- Necesidad de dedicar más tiempo a otras asignaturas

  Por propia experiencia, en ocasiones es difícil aproximar el tiempo que consumirán las asignaturas durante el semestre. A pesar de contar con ayudas de temporización en los planes de estudio de las asignaturas estas no suelen ser útiles, ya que cada estudiante tiene un ritmo de aprendizaje distinto.

- Imprevistos laborales/enfermedad

  El tiempo disponible para dedicar a tareas de la universidad se ve limitado debido a horas extra, viajes laborales, enfermedades, etc.

- Falta de conocimiento para realizar la implementación de las tecnologías utilizada

  Es posible que la fluidez en la realización de los objetivos de este trabajo final de grado se vea afectada por el desconocimiento para instalar y configurar correctamente los sistemas que se utilizarán.

- Problemas con el ordenador personal o *Internet*

  Se puede dar el caso que los dispositivos o servicios que se utilizan para realizar el trabajo final de grado no funcionen correctamente, lo que puede provocar un retraso en la temporización.

1.6. Plan de contingencia

Para tratar de mitigar las incidencias y riesgos comentados en el punto anterior se proponen diversas soluciones, las cuales quedan recogidas en la Tabla 2:

Incidencia/Riesgo	Plan de contingencia
Problemas de alojamiento de la máquina virtual de desarrollo	Se dispone del alojamiento de tres *ESX* de producción que están conectados en la red del trabajo, a parte del escenario de desarrollo contemplado. Además, la instalación puede realizarse en aplicaciones capaces de ejecutar máquinas virtuales como Oracle Virtualbox o VMWare Player, lo que permitiría la instalación en cualquier ordenador del perteneciente a la empresa.
Problema de alojamiento de la máquina virtual de producción	Se dispone del alojamiento de tres *ESX* de producción que están conectados en la red del trabajo, a parte del escenario de desarrollo. Además, la instalación puede realizarse en aplicaciones capaces de ejecutar máquinas virtuales como Oracle Virtualbox o VMWare Player, lo que permitiría la instalación en cualquier ordenador del perteneciente a la empresa.
Necesidad de dedicar más tiempo a otras asignaturas	Ya que el producto obtenido en el Trabajo Final de Grado será aprovechado por la empresa, se llega a un acuerdo para dedicar horas para el desarrollo de este TFG en horario laboral, siempre y cuando esté justificado.
Imprevistos laborales/enfermedad	En caso de enfermedad, la disponibilidad para hacer el trabajo siempre será completa (lo que permita la enfermedad). En el caso de tener imprevistos laborales, éstos siempre son compensados por la empresa con días de fiesta. Por lo que, si no se cumpliese la fecha de una entrega o de un hito, siempre podrá ser recuperada.
Falta de conocimiento para realizar la implementación de las tecnologías utilizadas	Como última instancia, se puede recurrir a contactos que trabajen en sistemas para poder así pedir soporte en momentos delicados, siempre y cuando éstos comprometan las fechas de entrega.
Problemas con ordenador personal o *Internet*	En el caso de tener problemas con el ordenador principal o la conexión e *Internet* para realizar el trabajo, se podrá realizar de forma provisional desde el puesto de trabajo en la empresa o desde un ordenador portátil en un espacio con *Internet* gratuito.

Tabla 2 - Planes de contingencia

2. Detección de puntos críticos en una infraestructura de *IT*

El objetivo del apartado 2 es resumir los puntos críticos detectados en el entorno objeto de este trabajo final de grado, así como realizar un estudio de herramientas de control y gestión de redes para finalmente escoger la solución que mejor se adapte al entorno que es caso de estudio.

2.1 Estudio de puntos críticos en el entorno dado

La implantación se realizará en una empresa cuya actividad es plenamente hotelera. Con una topología de red en estrella la cual puede ser observada en la Figura 2, la red está orientada a que tanto los complejos como la sede Central se conecten directamente al *Datacenter*, donde se encuentra la información relevante que permite realizar la actividad diaria.

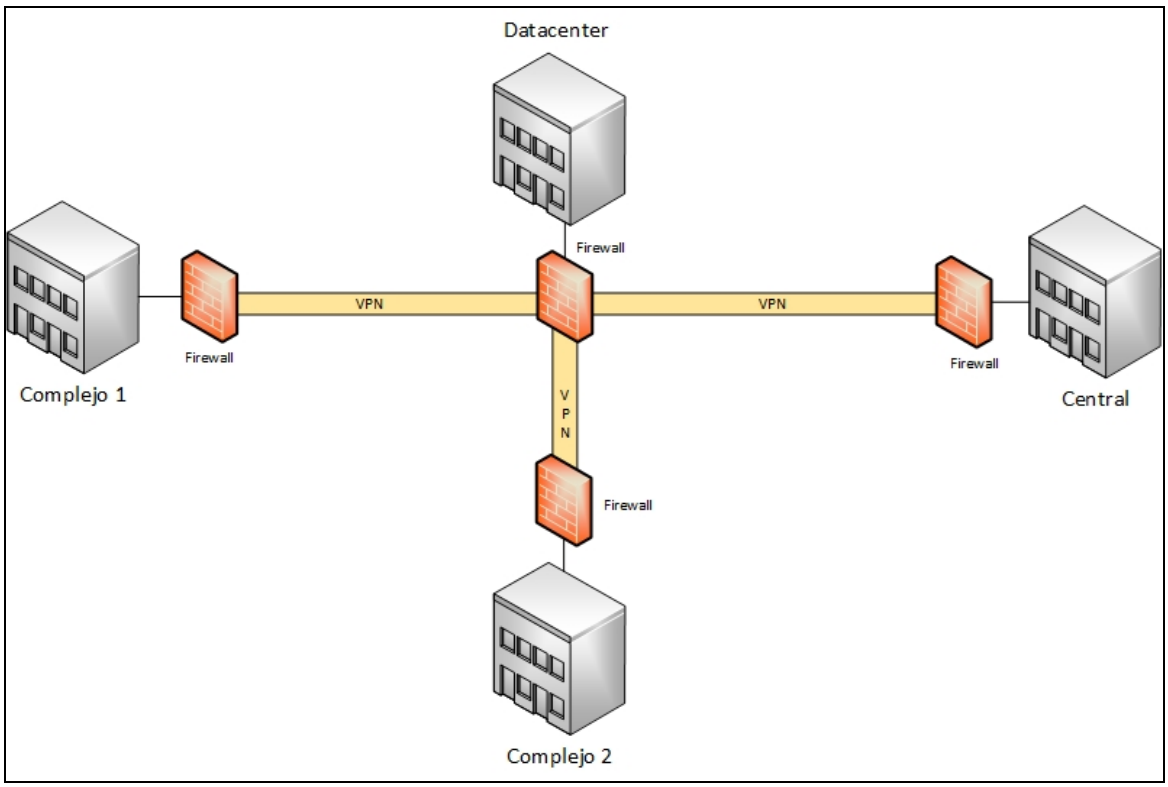


Figura 2 - Esquema de red general de la Organización

En la infraestructura de la organización se pueden diferenciar diversas peculiaridades. A continuación, se detallará la infraestructura:

- *Datacenter*

  Es donde se aloja la información y la capacidad de procesamiento de la aplicación *PMS*. Actualmente consta de tres servidores, dos conmutadores, un cortafuegos FortiGate, un cortafuegos Juniper y un enrutador. Desde el cortafuegos se crea un túnel *VPN* a la sede Central y al resto de complejos, con tipología en estrella, de tal manera que todos los complejos están conectados con el *Datacenter*. La Figura 3 representa el esquema de red de la situación expuesta.

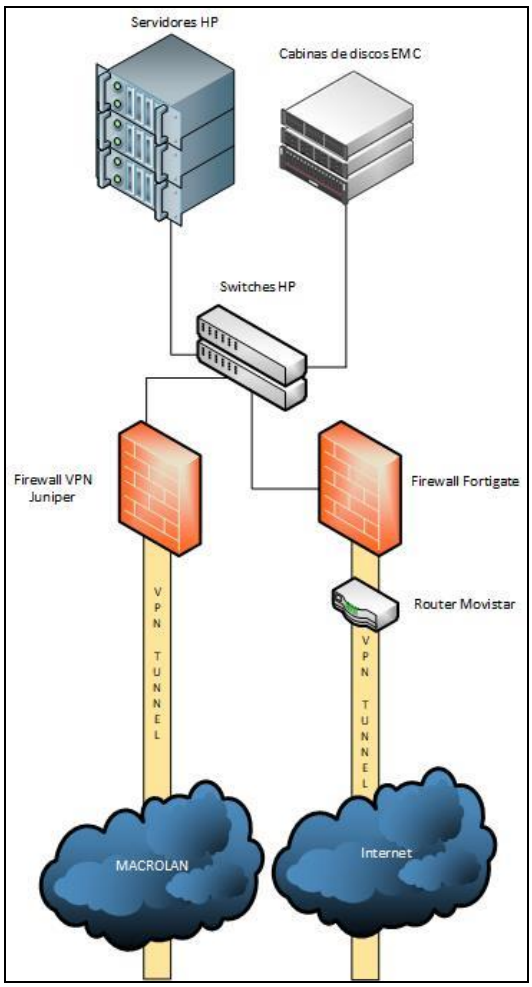


Figura 3 - Esquema de red *Datacenter*

- Sede Central

  Es donde se realizan funciones derivadas de la actividad hotelera como *Marketing, Call center,* soporte informático, etc. La sede Central está compuesta por dos servidores, dos almacenamientos en red (de ahora en adelante, *NAS*), un cortafuegos FortiGate, diversas impresoras, lectores biométricos, diversos ordenadores portátiles y estaciones de trabajo y, por último, dos puntos de acceso a la red de forma inalámbrica (de ahora en adelante, *WiFi*). La Figura 4 representa su esquema de red.

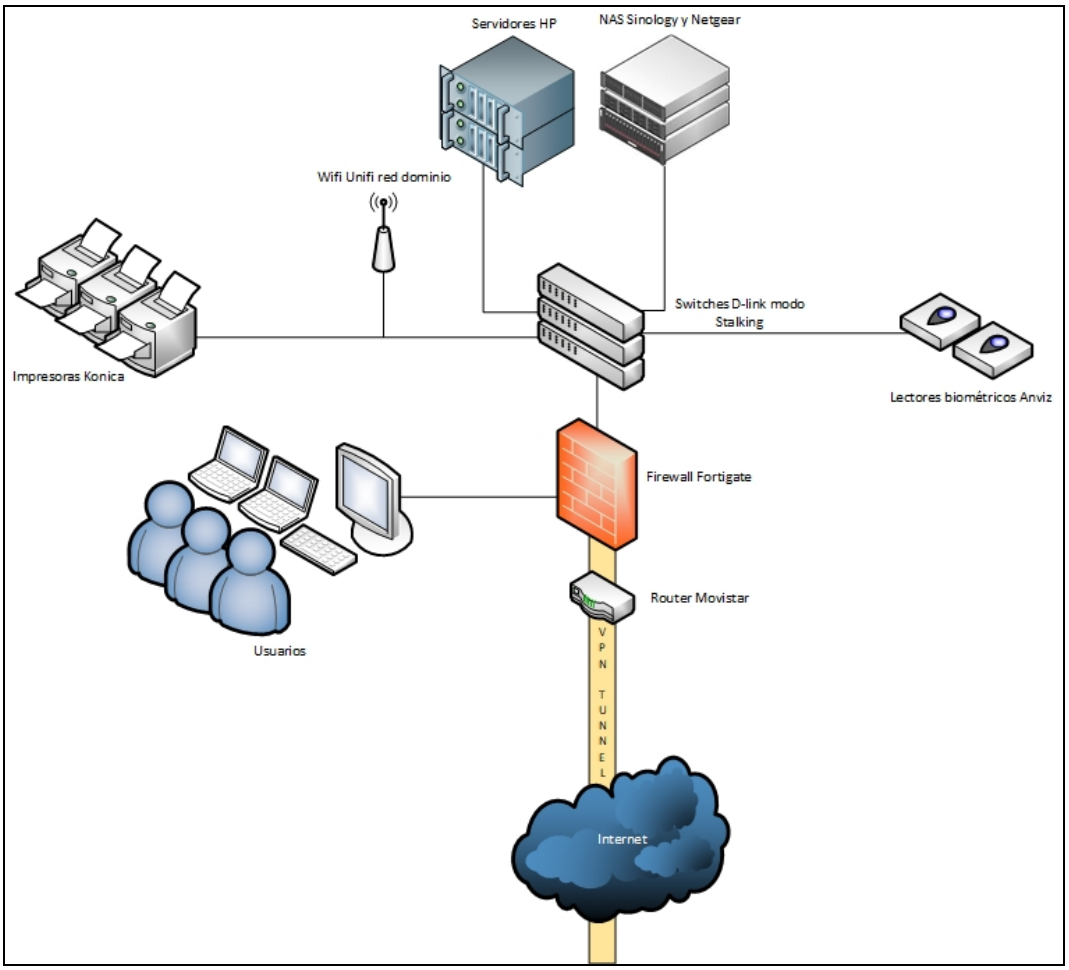


Figura 4 - Esquema de red sede Central

- Complejos

  Existen distintos métodos de conexión y sistemas a monitorizar en cada uno de ellos. Los podemos diferenciar de la siguiente manera:

  - Conexión: Cortafuegos FortiGate / MacroLAN
    En el proceso de expansión de la compañía se han detectado necesidades que han requerido la búsqueda de soluciones. A nivel de conectividad, se ha detectado un coste muy elevado en el servicio de conexión entre los distintos nodos de la organización, el cual se realizaba íntegramente mediante MacroLAN. Para el departamento de tecnologías de información (de ahora en adelante, *IT*) es objetivo desde enero de 2018 la implementación de nuevas tecnologías que permitían la migración de este tipo de conexión a otra solución más económica. Finalmente, se decidió implantar una solución de conexión de fibra óptica simétrica más FortiGate, cortafuegos de la compañía Fortinet capaz de establecer conexiones *VPN* entre extremos de una red. Actualmente el proceso de migración sigue activo, teniendo casi la totalidad de los complejos con la solución FortiGate. La Figura 5

representa el esquema de red de complejos con FortiGate y la Figura 6 muestra el esquema de red de complejos con MacroLan.

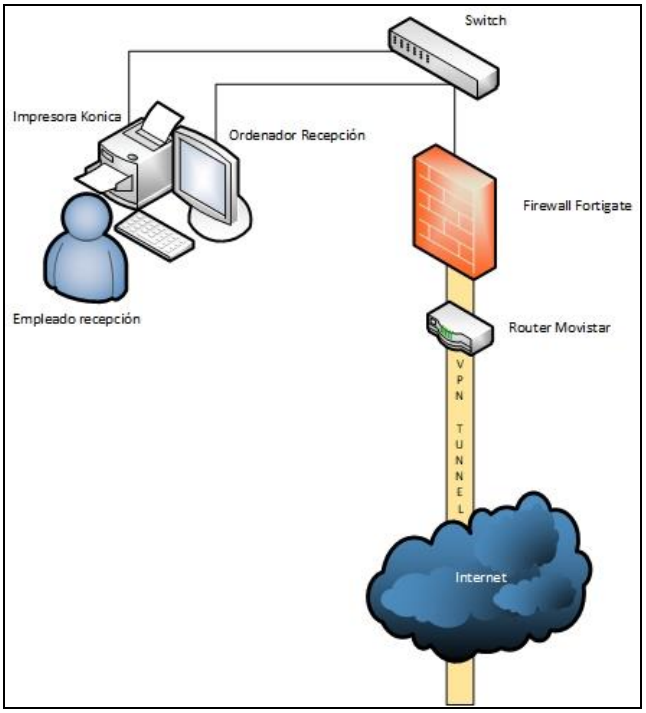


Figura 5 - Esquema de red Complejo con FortiGate

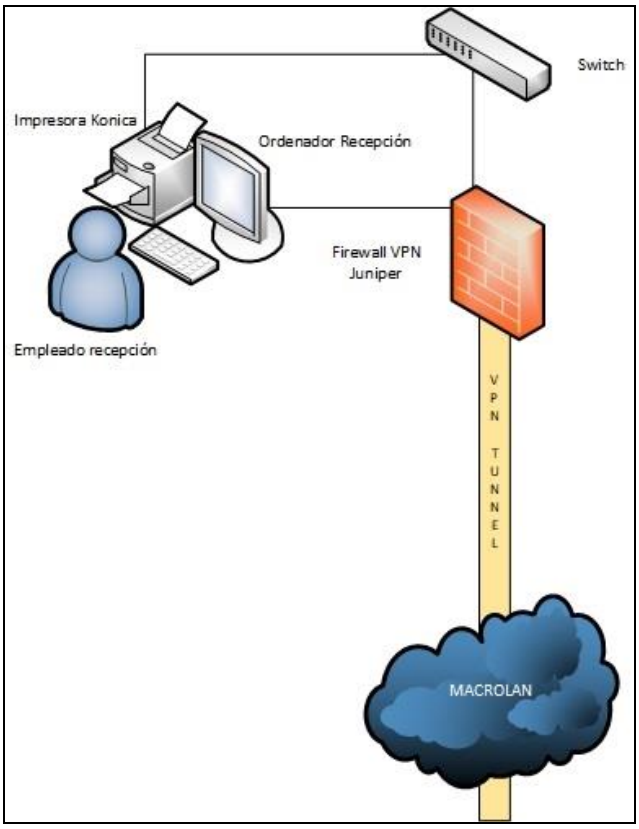


Figura 6 - Esquema de red Complejo con MacroLAN

- Aplicación CHAR
  Software instalado en uno de los equipos de recepción de algunos de los complejos de la compañía, que permite tarificar y controlar las llamadas realizadas por los huéspedes, cargando automáticamente en la reserva de la habitación el consumo telefónico realizado. Desafortunadamente, desde hace unos años se están experimentado problemas de funcionamiento con la aplicación y existe la necesidad de estudiar los motivos.

2.2 Herramientas de control y gestión de redes

Debido a la complejidad y heterogeneidad de los recursos que componen una red de telecomunicaciones, la gestión de éstos tiene una enorme importancia. Por ello, es necesario implementar herramientas en la infraestructura que permitan alcanzar un mayor control en la gestión de los elementos que la conforman.

El objetivo de este trabajo final de carrera es monitorizar, analizar, y controlar comportamientos para alcanzar un correcto funcionamiento tanto de la red de telecomunicaciones como de sus sistemas.

Con la puesta en marcha del servicio de monitorización se conseguirá tener:

- Control del estado de la infraestructura de *IT* monitorizada.
- Visión centralizada.
- Control de sucesos centralizado mediante alertas de monitorización.
- Capacidad de respuesta ante posibles sucesos.
- Capacidad de predicción.
- Estadísticas de rendimiento.
- Histórico de datos.

Los datos más comúnmente monitorizados son servicios de red (*SMTP*, *POP3*, *HTTP* e *ICMP*) y recursos de sistemas (*RAM*, *CPU* y espacio en disco). Los dispositivos más comúnmente monitorizados son servidores, enrutadores, conmutadores y cortafuegos.

2.3 Análisis de herramientas actuales

Algunas de las herramientas de monitorización mejor valoradas en la actualidad son las siguientes:

- Nagios

  Sistema de monitorización de código abierto fundado en 1999 capaz de monitorizar todo tipo de componentes como protocolos de red, sistemas operativos, métricas de sistema, aplicaciones, servicios, servidores web, sitios web, etc. Es implementada por empresas como Bitnetix, Watch communications, Petrofac y Quental, entre otros. La aplicación base (de ahora en adelante, *core*) se puede instalar en distribuciones de Linux basadas en la arquitectura Debian y Red Hat.

  Como características, permite centralizar la visión de la infraestructura de *IT* monitorizada, restablecer automáticamente servicios o aplicaciones que han sufrido fallo. Además, tiene la capacidad de mostrar a cada usuario únicamente cierta parte de la infraestructura, tiene una comunidad activa de 1 millón de usuarios y el sistema es escalable fácilmente.

  Como puntos débiles, el despliegue de los puntos de monitorización requiere mayor tiempo de configuración debido a su complejidad, ya que la configuración la obtiene de archivos de texto debido a la ausencia de interfaz de configuración. Además, requiere complementarse con otros proyectos y módulos para alcanzar el potencial óptimo de la herramienta, debido a que la interfaz web de monitorización es poco intuitiva y ofrece poca información para el análisis tal como se puede ver en la Figura 7.

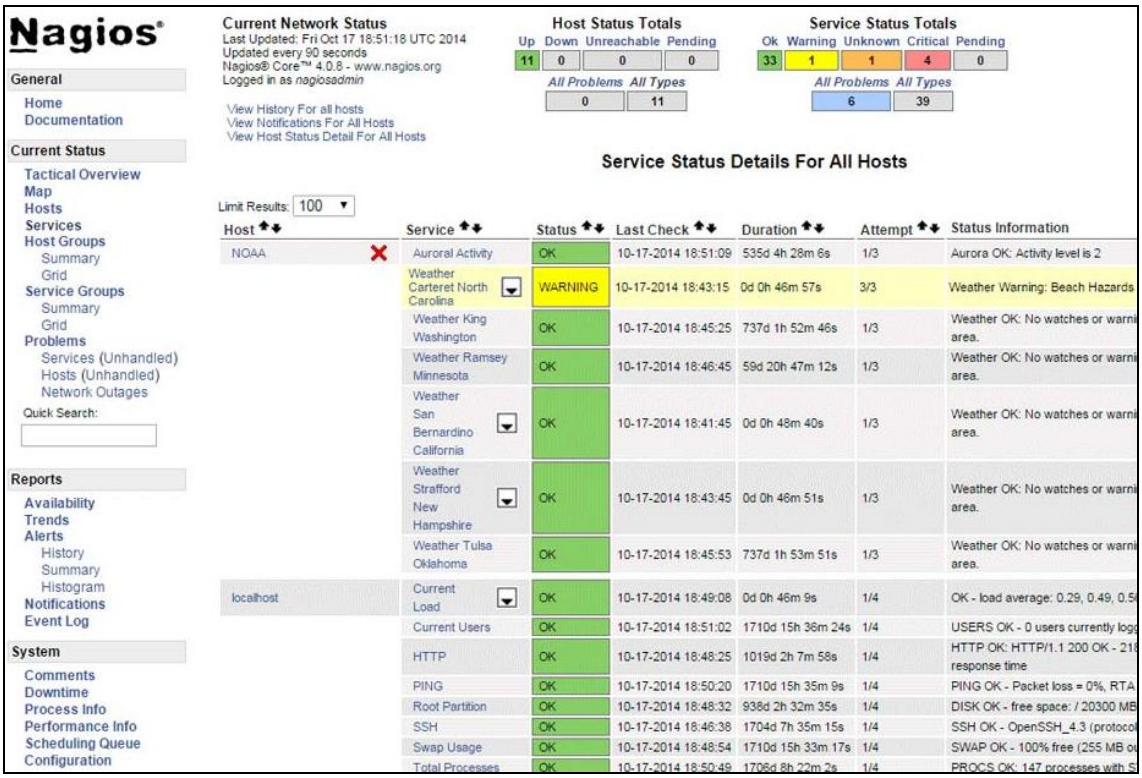


Figura 7 - Ejemplo de la interfaz de monitorización Nagios

- Hostmonitor

  Herramienta que permite monitorizar tanto servicios como sistemas y redes de telecomunicaciones mediante agentes (instalados en cada nodo a monitorizar) y testeos directos (no requieren de instalación de ningún cliente). Para gestionar los puntos de monitorización que se aplican en los agentes se utiliza la aplicación auxiliar RMA Manager.

  El *core* de la aplicación se ejecuta sobre varias distribuciones de la familia Microsoft Windows como Server 2003/2008/2008 R2/2012 R2/2016.

  Como puntos débiles respecto al resto de herramientas estudiadas, Hostmonitor tiene una interfaz de apariencia antigua (véase Figura 8) y es únicamente instalable en ciertas distribuciones de Microsoft Windows, lo que comporta un coste añadido debido a la necesidad de poseer licencia del sistema operativo de Windows.

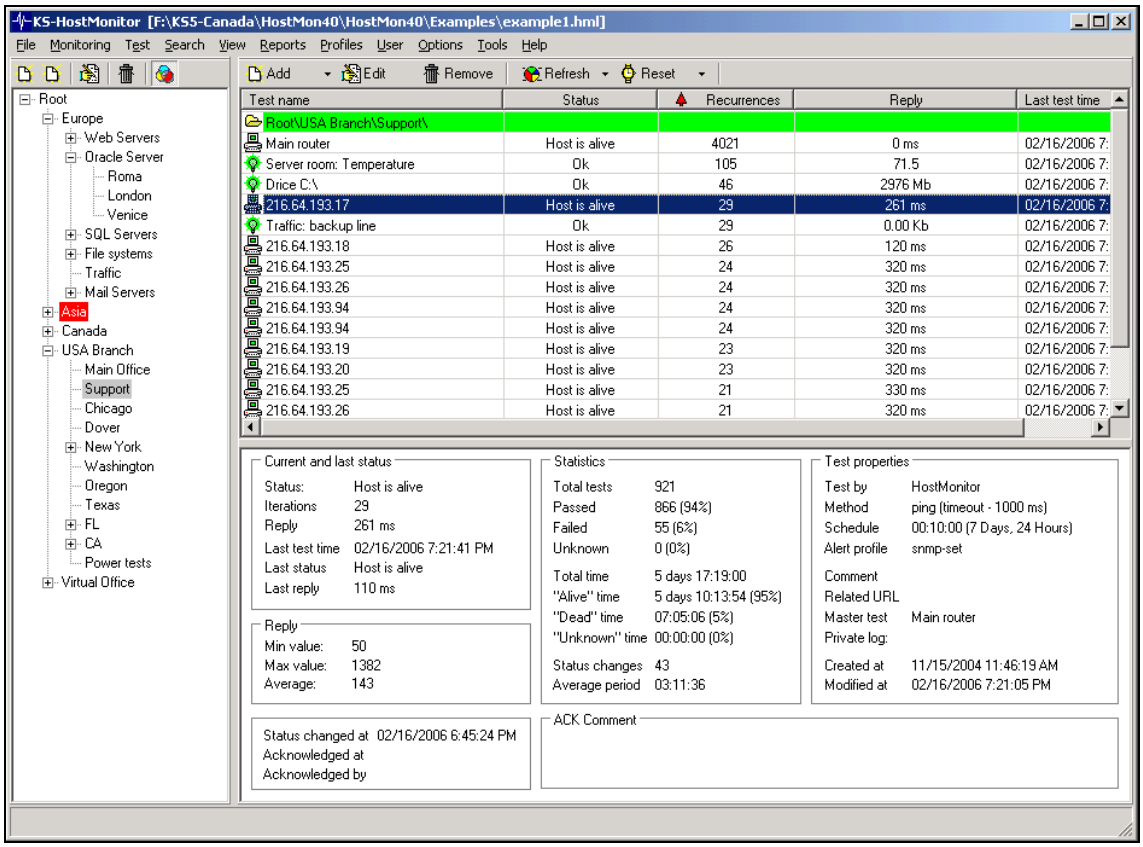


Figura 8 - Ejemplo de la interfaz de monitorización Hostmonitor

- ManageEngine OpManager

  Plataforma de monitorización de redes, servidores y aplicaciones que ofrece funcionalidades avanzadas para monitorizar recursos críticos de *TI* como enrutadores, nodos WAN, conmutadores, cortafuegos, comunicaciones VoIP, servidores físicos y virtuales y otros dispositivos de infraestructura de *TI*.

  Esta herramienta aporta una interfaz intuitiva (véase Figura 9) que permite monitorizar disponibilidad, rendimiento, aplicaciones, tráfico y ancho de banda en más de 40.000 interfaces o 5000 dispositivos en una sola consola de monitorización. También es capaz de mostrar mapas de red en vivo que permite detectar cuellos de botella, realizar correcciones automáticas de fallas mediante uso de scripts y flujos de datos y permite elaborar potentes informes de red capaces de mostrar tendencias de uso y capacidad.

  Como punto débil, la aplicación requiere un pago de cuota mensual además de un pago por la instalación con más de 10 dispositivos monitorizados.

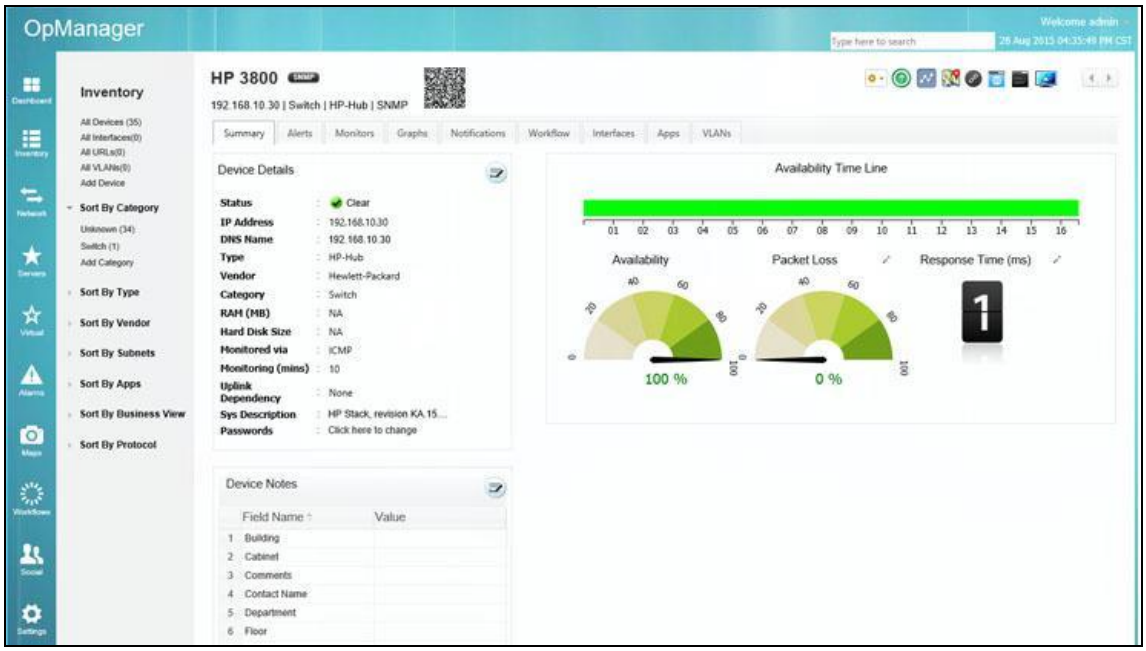


Figura 9 - Ejemplo de la interfaz de monitorización OpManager

- Zabbix

  Aplicación de código abierto diseñada en 1998 por Zabbix LLC para monitorizar aspectos de rendimiento y disponibilidad de servidores, equipos de red, aplicaciones web y bases de datos utilizado por grandes compañías como Dell, Salesforce, ICANN, Orange, entre otros. Realiza sus actividades de monitorización mediante una arquitectura servidor-cliente, pese a que algunos de los servicios no necesitan instalación de agentes, como son los servicios FTP, SSH, HTTP y DNS, entre otros.

  Instalable tanto en CentOS, como Debian, Oracle Linux, Red Hat Enterprise Linux, Ubuntu y Raspbian mediante paquetes pre compilados de Linux, también existe la posibilidad de descargar máquinas virtuales preinstaladas en formato *KVM*, Parallels, VirtualBox, VMWare, Microsoft Hyper-V y Azure, entre otros. Además, el despliegue de los puntos de monitorización es tarea ágil gracias a los agentes autoinstalables y las plantillas predefinidas y configurables a través de su interfaz web (véase Figura 10) que se adaptan perfectamente a los sistemas monitorizados.

  Gracias a ser una aplicación de código abierto, la comunidad de Zabbix desarrolla y publica en la página web https://share.zabbix.com/ plantillas que se adaptan a la gran mayoría de dispositivos que se pueden encontrar en una infraestructura empresarial. También existen aplicaciones informáticas (de ahora en adelante, *software*) de terceros que utilizan la *API* de Zabbix para obtener información recopilada por la herramienta y aportar un valor añadido a la recopilación de datos.

  Como punto débil de esta herramienta, la representación de los valores recogidos en forma de gráficas es simple, por lo que su utilización debería ser complementada con herramientas que permitan explotar,

analizar y visualizar métricas para alcanzar características que otras herramientas del mercado sí incluyen, como la solución la solución de OpManager.

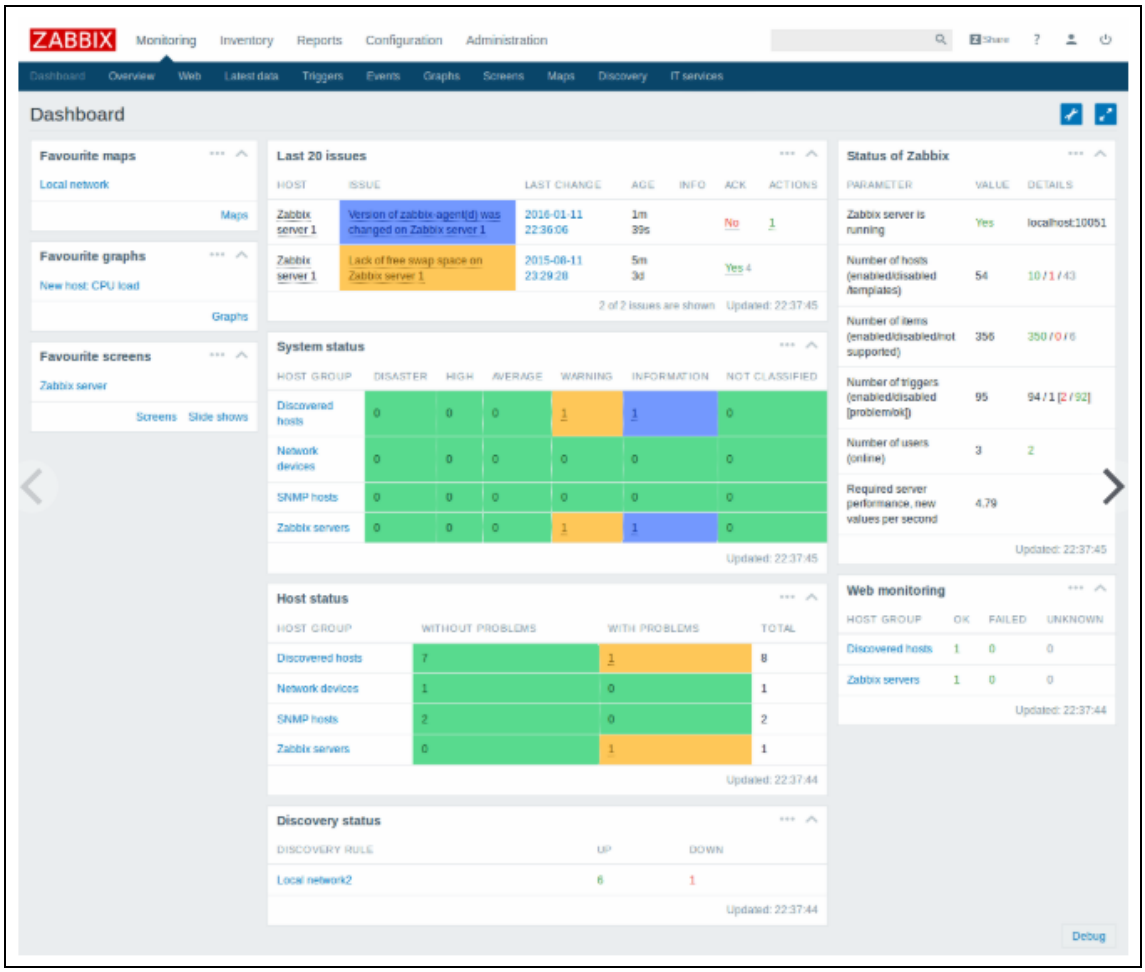


Figura 10 - Ejemplo de la interfaz de monitorización Nagios

2.4 Justificación de la herramienta escogida

Respecto a la elección de la herramienta de monitorización, se considera que la mejor opción es Zabbix por los siguientes motivos:

- Licencia de código libre

  La no repercusión a nivel de costes en la organización es un punto a favor para poder realizar la implantación de la herramienta a modo de toma de contacto. En caso de ser necesario implantar una herramienta más potente, sería valorada una alternativa de pago si fuese necesario.

- Rápido despliegue del servidor

  La posibilidad de realizar el despliegue mediante paquetes pre compilados de Linux o máquinas virtuales preconfiguradas ofrece distintas formas de obtener un resultado final satisfactorio en la tarea de instalación.

- Disponibilidad del entorno de despliegue requerido

  Debido a la versatilidad de métodos de instalación del servidor, se pueden establecer diversos entornos que podrían albergar la aplicación que se adaptase más a la organización.

- Rápido despliegue de puntos de monitorización

  Gracias a las plantillas predefinidas, establecer un punto de monitorización de un dispositivo (de ahora en adelante, nodo) es tan sencillo como aplicar una plantilla predefinida.

- Interfaz web de administración intuitiva

  Gracias a la posibilidad de gestionar las configuraciones del servidor vía interfaz web, se consigue una mayor perspectiva del alcance de administración de la herramienta.

- Posibilidad de conectar a la herramienta *software* de terceros

  Mediante el uso de la *API*, se permite que otras herramientas interconecten con los datos recogidos por la herramienta, lo que abre un abanico de nuevas posibilidades de analizar los datos.

- Comunidad activa

  Este hecho permite detectar posibles errores de programación en la herramienta, obtener ayuda en foros ante dificultad o errores de monitorización y disponer de una amplia gama plantillas de monitorización realizadas por la comunidad.

3. Definición y despliegue de la arquitectura

3.1 Objetivos de la sección

Durante el desarrollo del apartado 3 se describirán las actividades realizadas, se detallará la implementación en entorno de producción y se mostrarán los resultados previstos y obtenidos respecto al Plan de Trabajo.

3.2 Relación de las actividades realizadas

Las actividades previstas en el Plan de Trabajo que se han llevado a cabo son las siguientes:

- Definición del entorno y los *KPI* a monitorizar en entorno de producción.
- Fase de instalación CentOS.
- Configuración CentOS.
- Fase de instalación Zabbix.
- Configuración Zabbix.
- Validación: Configuración de puntos de monitorización.

3.3 Implementación en entorno de producción

Indicadores de monitorización

Una vez analizado el entorno de implementación del sistema de monitorización y tras realizar una reunión con el departamento de *IT* de la compañía se define que los puntos críticos a monitorizar en entorno de producción incluidos en este trabajo final de grado son los siguientes:

- Latencias

  Este valor nos proporciona información del estado de la red. Mide el tiempo que se requiere en responder a una petición entre dos extremos. En el entorno estudiado, el tiempo de respuesta es un punto crítico debido a las consultas que realiza el *PMS* hotelero tanto desde la sede Central como desde los complejos al *Datacenter*, donde se encuentra su base de datos. Dada la experiencia, hemos detectado que una latencia superior a 40ms conlleva una experiencia negativa para las recepciones de los hoteles, en los que se prioriza una máxima agilidad en gestiones con los huéspedes. Debido a esto, se establecen cláusulas de latencia máxima en los contratos de conexiones a *Internet* y, por ello, el objetivo de esta monitorización será supervisar que los requisitos de latencia se cumplan.

- Tasas de transferencia de datos de *Internet*

  Un dimensionamiento erróneo del ancho de banda de *Internet* o un uso indebido del mismo pueden provocar problemas de lentitud y altas latencias en la red. Debido a esto, es necesario esclarecer cuáles son los consumos normales de ancho de banda en puntos críticos de la red y vigilar su correcto funcionamiento para evitar que se puedan formar cuellos de botella, en este caso en las conexiones *WAN*.

- Disponibilidad de elementos críticos

  Los *enrutadores* y cortafuegos que dotan de conexión a *Internet* y VPN respectivamente a las redes locales tanto de complejos como de Central y Datacenter, los conmutadores y ordenadores de los complejos con el cliente de la aplicación de tarificación de llamadas CHAR deben ser monitorizados para ser conocedores en todo momento de posibles fallos de funcionamiento o falta de disponibilidad de servicio. Con ello se podrán analizar patrones de errores, establecer y ejecutar planes de contingencia de forma más fácil, entre otros.

- Rendimiento de servidores virtualizados con aplicaciones críticas

  Las máquinas virtuales que albergan aplicaciones críticas como el *PMS*, el servidor de la aplicación tarificadora de llamadas CHAR, el servidor de impresiones Papercut y el servidor con la base de datos de la aplicación de contabilidad Datisa serán objeto de monitorización.

- Monitorización de estado de copias de seguridad de la información de la herramienta Zabbix

  Debido a que los sistemas actuales de copias de seguridad de la compañía son limitados, se decide realizar una copia de respaldo de la base de datos que contiene información recopilada por la herramienta. Dicha información será guardada en el almacenamiento en red que la compañía dispone.

Instalación de Zabbix

Esta fase se desarrolla primeramente en entorno de desarrollo, el cual se conforma con la conexión de un miniordenador *NUC* Intel con el sistema operativo *VMware ESXi* 6.7 (de ahora en adelante, *ESXi*) preinstalado al enrutador de fibra óptica de la sede Central. Para acceder a la página de gestión de *ESXi* se debe conectar un ordenador directamente al mismo enrutador, por lo que se genera una conexión de red local con conexión a *Internet* donde están conectados tanto el *ESXi* como un terminal de trabajo estándar.

A continuación, se muestra el montaje del entorno provisional de desarrollo, que se puede ver en la parte inferior derecha del esquema de red de la sede Central original (véase Figura 11).

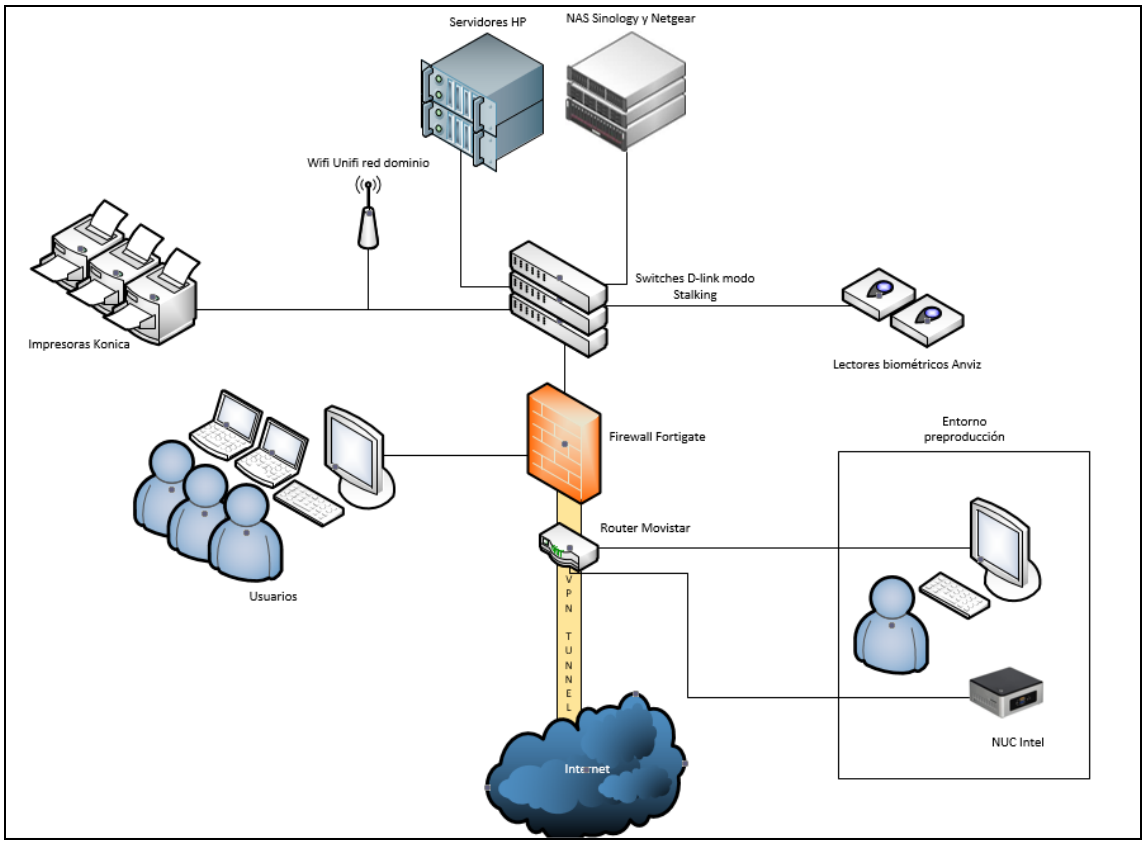


Figura 11 - Diagrama de red del entorno de desarrollo

Fase de instalación Zabbix en CentOS:

En primer lugar, se crea una máquina virtual en el *ESXi* de desarrollo con las características de *CPU y RAM* detalladas en la Figura 12:

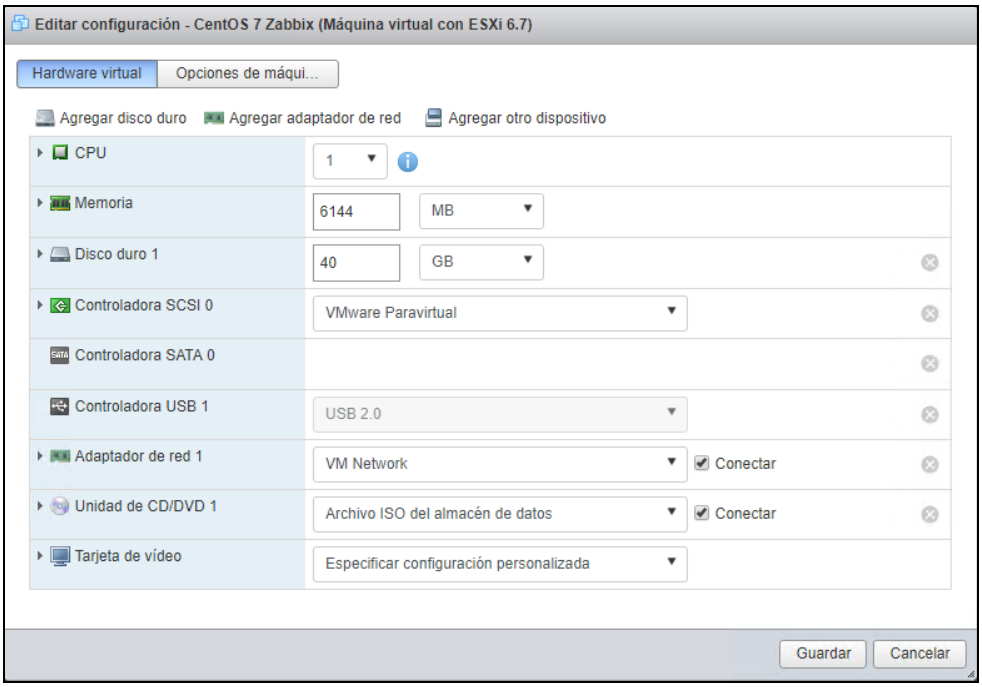


Figura 12 - Definición de *CPU* y *RAM* de la nueva máquina virtual

A continuación, se añade la imagen de CentOS 7 en la unidad de disco compacto (de ahora en adelante, *CD*) de la máquina virtual, la cual ha sido descargada a de la página oficial de CentOS https://www.centos.org/ (véase Figura 13).

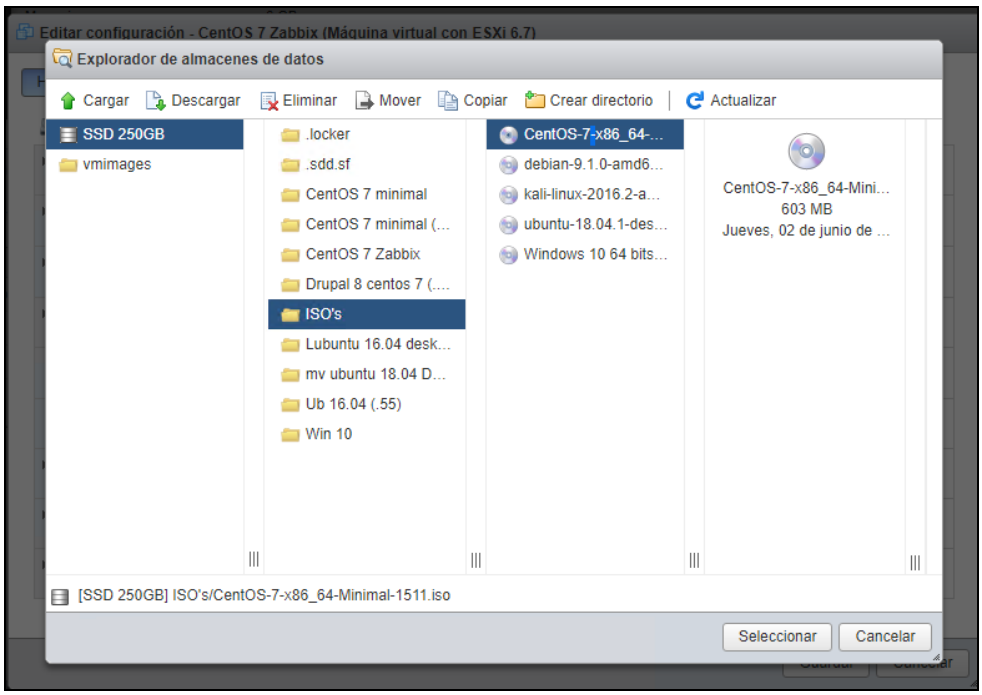


Figura 13 - Montaje de la ISO de CentOS en la máquina virtual

Posteriormente, se abre la consola de la máquina virtual (de ahora en adelante, MV) y se prosigue con la instalación (véase Figura 14):

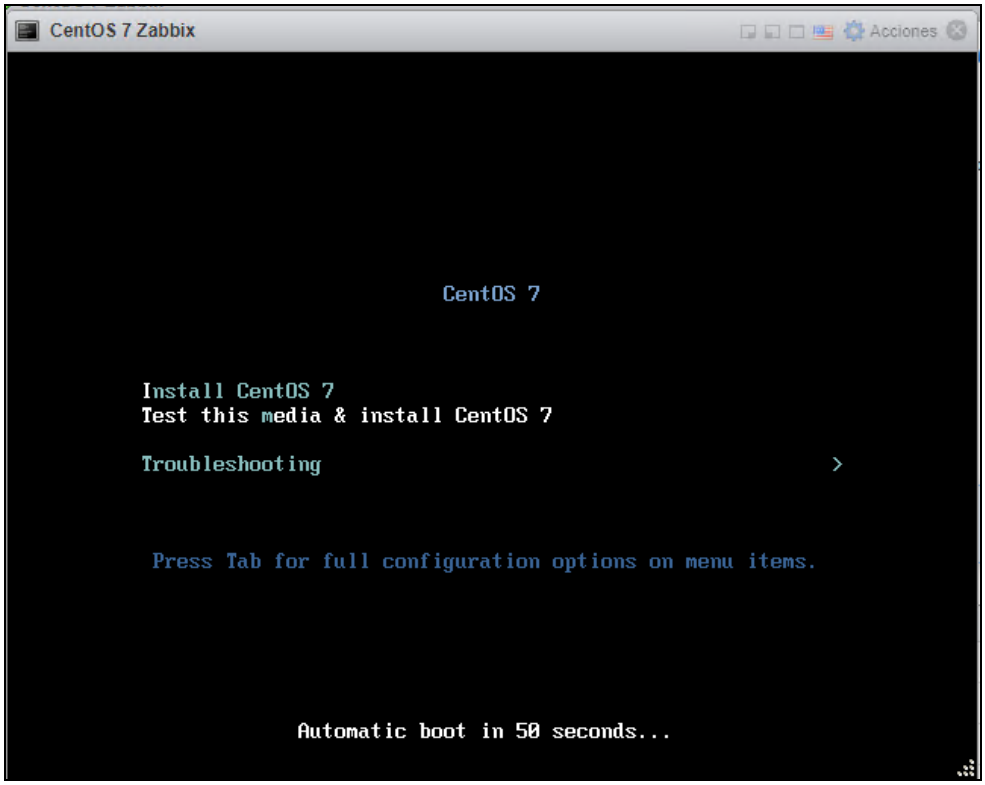


Figura 14 - Pantalla de inicio de instalación de CentOS 7

Tras seleccionar la opción "*Install CentOS 7*", se detalla el destino de instalación (véase Figura 15):

Figura 15 - Definición de la partición del sistema operativo

El paso siguiente consiste renombrar la máquina virtual a nivel de sistema operativo a "*zabbix*" (véase Figura 16):

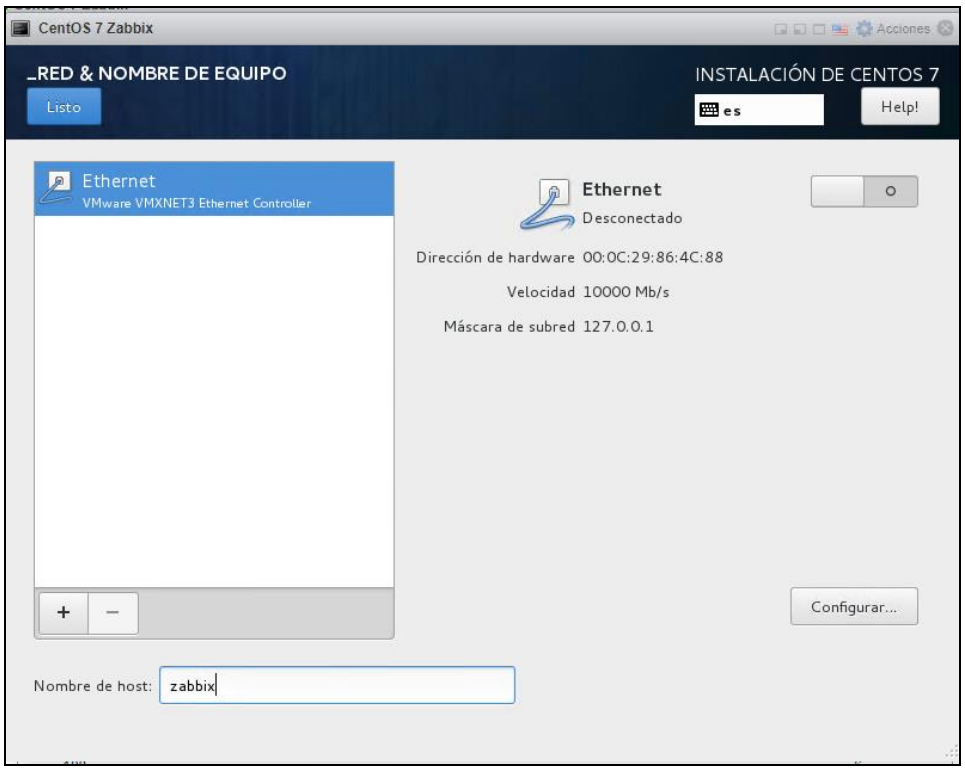


Figura 16 - Configuración del nombre del host

A continuación, se establece la contraseña con permisos de administrador (de ahora en adelante, *root)*. Una vez finalizada la instalación (véase Figura 17) se da por finalizado el proceso de instalación y se reinicia la máquina virtual.

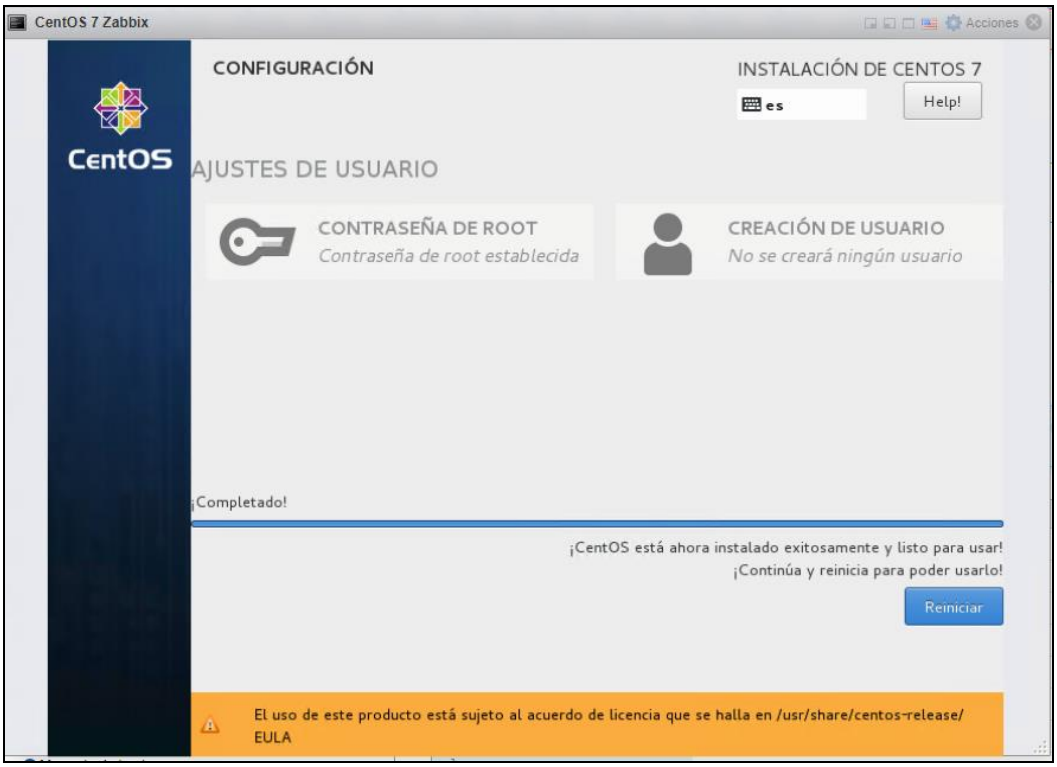


Figura 17 - Finalización de la instalación de CentOS 7

Configuración CentOS

Para llevar a cabo la configuración se debe encender la máquina virtual anteriormente mencionada y acceder al sistema con el usuario *root* (véase Figura 18):

Figura 18 - Pantalla inicial tras acceder con credenciales al sistema

A continuación, se modifica el archivo que define la configuración de la tarjeta de red para cambiar el tipo de conexión a *IP* estática, realizando previamente una copia de seguridad de la información que éste contiene:

```
# cp /etc/sysconfig/network-scripts/ifcfg-eno16780032 /etc/sysconfig/network-scripts/ifcfg-eno16780032.bkp

# vi /etc/sysconfig/network-scripts/ifcfg-eno16780032
```

Una vez dentro del archivo, se deben cambiar los siguientes parámetros tal y como se muestra a continuación:

```
BOOTPROTO="static"

ONBOOT="yes"

DNS1="8.8.8.8"

DNS2="1.1.1.1"

IPADDR="192.168.0.10"

NETMASK="255.255.255.0"

GATEWAY="192.168.0.1"

NN_CONTROLLED="no"
```

Se guardan las modificaciones y se reinicia el servicio de interfaz de red:

```
# /etc/init.d/network restart
```

```
[root@zabbix ~]# /etc/init.d/network restart
Restarting network (via systemctl):                        [  OK  ]
[root@zabbix ~]# fping www.google.es
-bash: fping: no se encontró la orden
[root@zabbix ~]# ping www.google.es
PING www.google.es (172.217.16.227) 56(84) bytes of data.
64 bytes from mad08s04-in-f3.1e100.net (172.217.16.227): icmp_seq=1 ttl=55 time=13.4 ms
64 bytes from mad08s04-in-f3.1e100.net (172.217.16.227): icmp_seq=2 ttl=55 time=12.8 ms
^C
--- www.google.es ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 12.811/13.121/13.432/0.330 ms
[root@zabbix ~]#
```

Figura 19 - Reinicio del servicio de interfaz de red y prueba de ping

En la Figura 19 se puede comprobar que, al realizar un test de tiempo de respuesta *ping* a la dirección www.google.es, éste responde a dicha petición, lo que indica que hay conexión a *Internet*.

Para trabajar con más comodidad se accederá vía *SSH* al servidor, utilizando el cliente de conexión *SSH* y *Telnet* para plataforma Windows llamado Putty. Una vez descargada la aplicación, se establece conexión con la máquina virtual de CentOS 7 con credenciales de *root*, la cual tiene dirección IP XXX.XXX.0.10 (véase Figura 20):

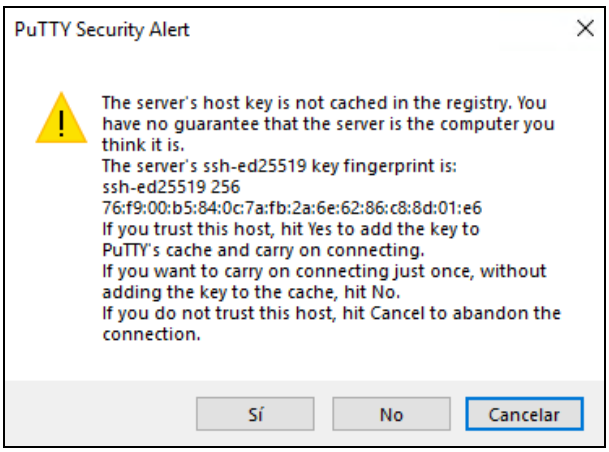


Figura 20 - Aceptación del *fingerprint* de la conexión *SSH*

Se acepta el cuadro de diálogo de la Figura 9 en el que aceptamos el nuevo identificador del servidor que trata de establecer la conexión, llamado también *fingerprint,* con el resultado de acceso satisfactorio (véase Figura 21):

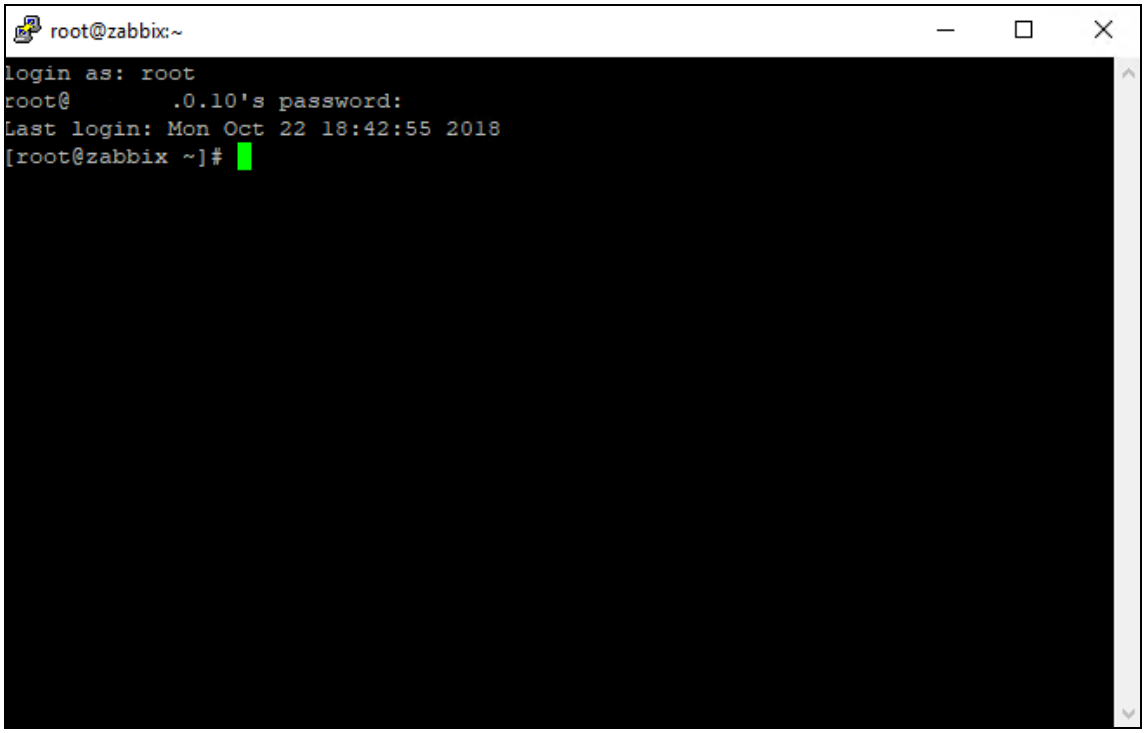


Figura 21 - Acceso mediante *SSH* a la máquina virtual CentOS 7

Fase de instalación Zabbix

Para realizar la instalación de la aplicación, se aplicarán los siguientes pasos.

Instalación del paquete del servidor web Apache, el paquete *PHP* y el paquete del servidor MariaDB para la base de datos:

```
# yum install httpd php
# yum install mariadb-server
```

Para permitir que la base de datos se ejecute tras iniciar la máquina virtual se añade a la ejecución de inicio del sistema el servicio MariaDB.

```
# systemctl enable mariadb
```

Tras ello, se instala el paquete de Red Hat Package Manager (de ahora en adelante, *RPM*) de *Zabbix* y se accede por primera vez a la base de datos.

```
# rpm -ivh http://repo.zabbix.com/zabbix/3.4/rhel/7/x86_64/zabbix-release-3.4-2.el7.noarch.rpm
# yum install zabbix-server-mysql zabbix-web-mysql
# mysql -uroot -p
```

Una vez se accede a la MariaDB, se crea una base de datos llamada Zabbix y se proporcionan permisos de edición al usuario “zabbix”.

```
# MariaDB [(none)]> CREATE DATABASE zabbix CHARACTER SET utf8;
# MariaDB [(none)]> GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost' IDENTIFIED BY 'zabbix_passwd';
# MariaDB [(none)]> FLUSH PRIVILEGES;
# MariaDB [(none)]> \q
```

Tras crear la base de datos, se vuelca la información inicial de la base de datos que proporciona Zabbix con las tablas necesarias para poder funcionar:

```
# zcat /usr/share/doc/zabbix-server-mysql-*/create.sql.gz | mysql -u zabbix -p Zabbix
```

El paso por seguir después de esta última operación es editar el archivo “zabbix_server.conf”, donde se deberá des-comentar la línea “DBPassword” y añadir la contraseña de la BBDD:

```
# vi /etc/zabbix/zabbix_server.conf
DBPassword=XXXXX
```

También se deberá modificar la línea “php_value” del archivo “zabbix.conf” con la configuración regional “Europe/Madrid”.

```
# vi /etc/httpd/conf.d/zabbix.conf
php_value date.timezone Europe/Madrid
```

Para aplicar estos cambios, se deberá reiniciar tanto el servicio de Apache como el servicio del servidor de Zabbix:

```
# systemctl restart httpd

# systemctl start zabbix-server
```

Por último, se cambia el nombre de la máquina virtual:

```
# hostnamectl set-hostname “onazbx”
```

Configuración *Zabbix*

La dirección web http://XXX.XXX.0.10/zabbix/setup.php permite configurar la conexión de *BBDD*, el nombre del servidor y el nombre visible de la herramienta en el navegador (véase Figura 22). Con ello la preinstalación será finalizada (véase Figura 23).

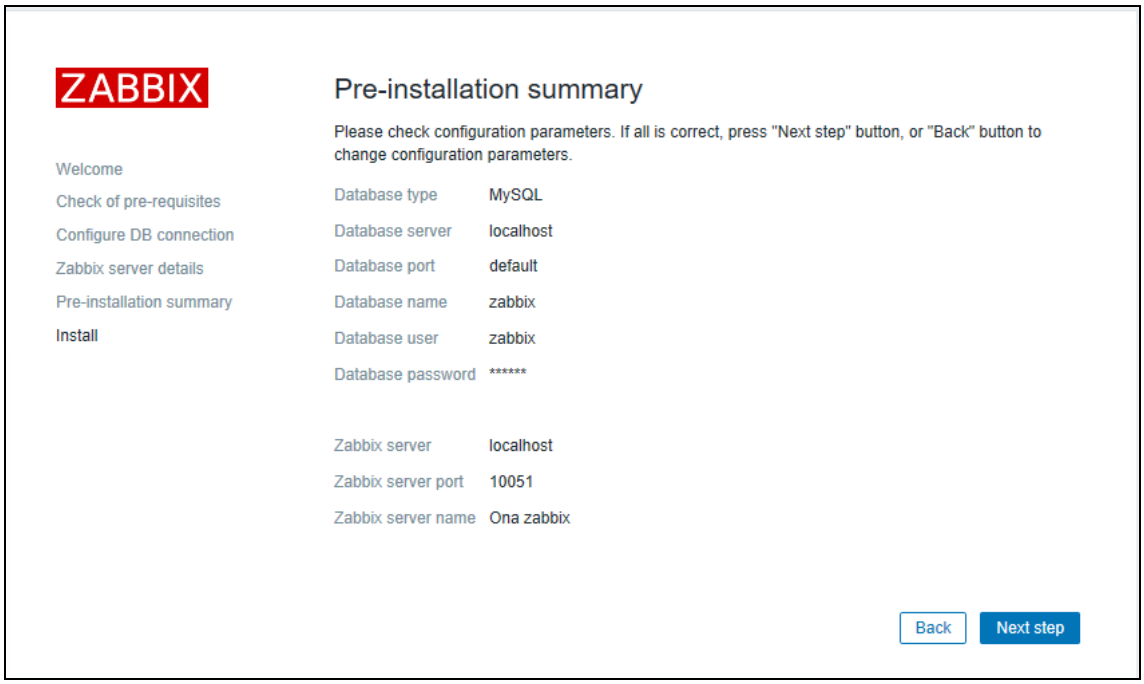


Figura 22 - Sumario previo de la configuración de Zabbix

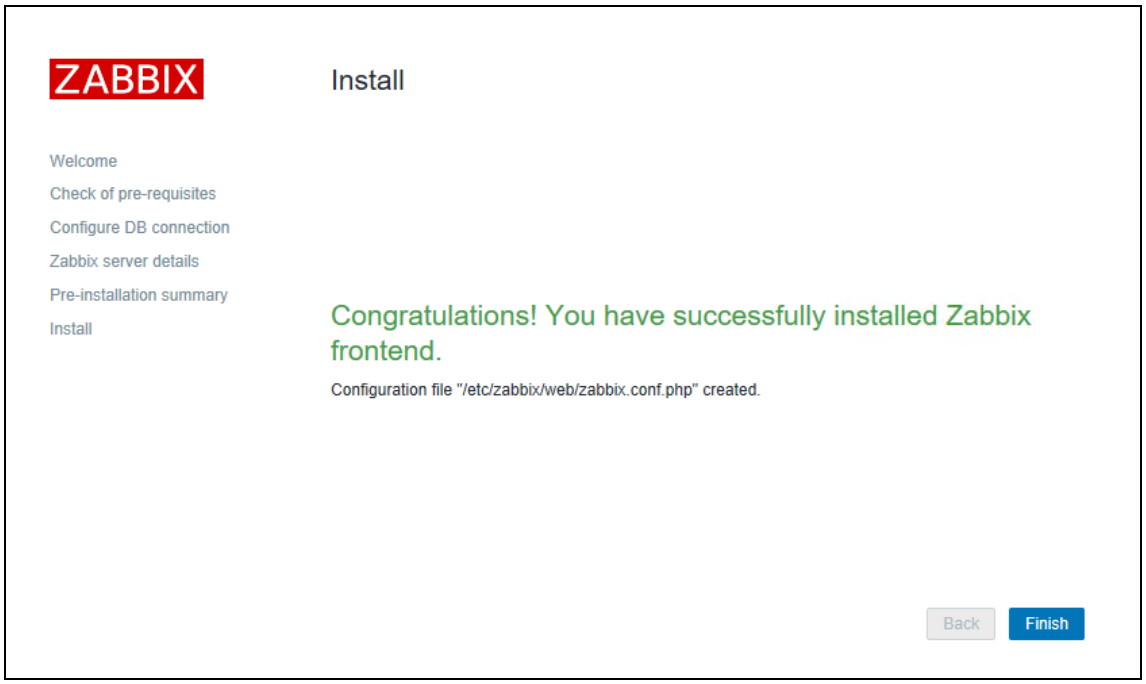


Figura 23 - Configuración básica satisfactoria de la herramienta Zabbix

Configuración de puntos de monitorización

En este punto se configurará la monitorización del propio servidor de Zabbix para validar que el servicio funciona recogiendo datos.

Para acceder a la interfaz de monitorización se utiliza la siguiente dirección web http://XXX.XXX.0.10/zabbix (véase Figura 24). El usuario con acceso por defecto es "*admin"* y la contraseña "*zabbix*", la cual deberá ser cambiada más adelante.

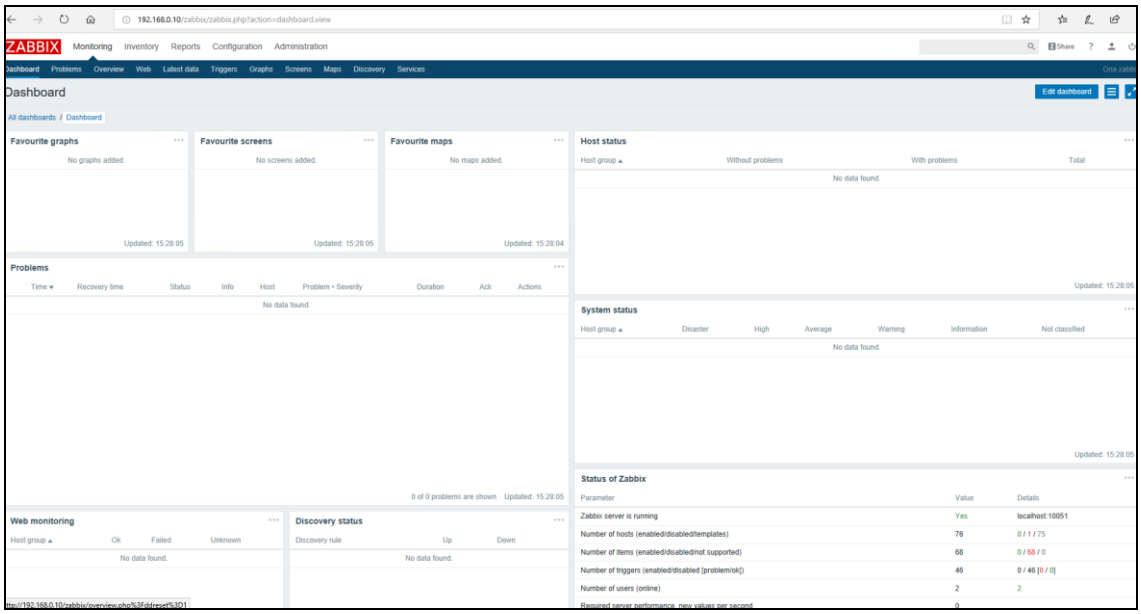


Figura 24 - Interfaz de la página principal de Zabbix

Para comprobar el correcto funcionamiento de la herramienta, se comprobará si recolecta datos monitorizando el propio servidor de Zabbix. Para ello se tendrá que instalar el agente de Zabbix en el servidor, cuya función es recopilar y enviar información del objeto monitorizado al servidor de Zabbix:

```
# yum install zabbix-agent
```

Se modifica la configuración del agente con el editor de textos *vi*:

```
# vi /etc/zabbix/zabbix_agentd.conf

hostname=onazbx
```

y finalmente se reinicia el servicio del agente "*Zabbix Agent":*

```
# service zabbix-agent restart
```

Validación: Configuración de puntos de monitorización

Posteriormente, se añade a la monitorización el servidor de Zabbix. Para realizar este proceso se debe acceder al menú "*Configuration"→"Hosts"* (véase Figura 25), donde aparece añadido por defecto el servidor Zabbix en modo deshabilitado. Por tanto, únicamente será necesario habilitar la monitorización y el nombre del servidor:

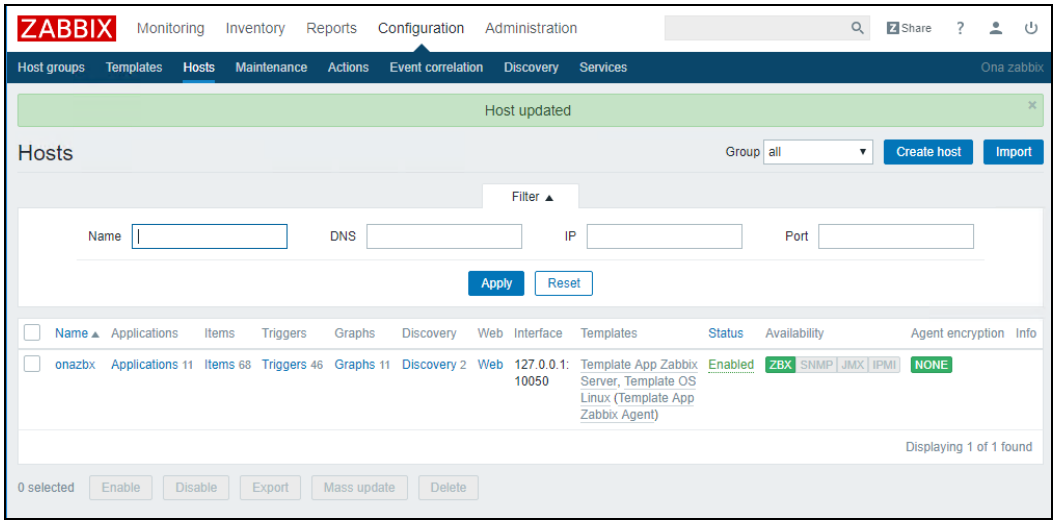


Figura 25 - Adición del servidor a la herramienta de monitorización

En la columna "Availability" aparece el campo *ZBX en color* verde, indicando el correcto estado de la monitorización a través del agente. Ya que el host tiene una plantilla de monitorización asignada, se deben estar recolectando datos de los puntos de monitorización que tiene dicha plantilla. Por ello, en el apartado "*Monitoring"→"Latest Data"* (véase Figura 26) debe permitir la visualización de información recabada por la herramienta.

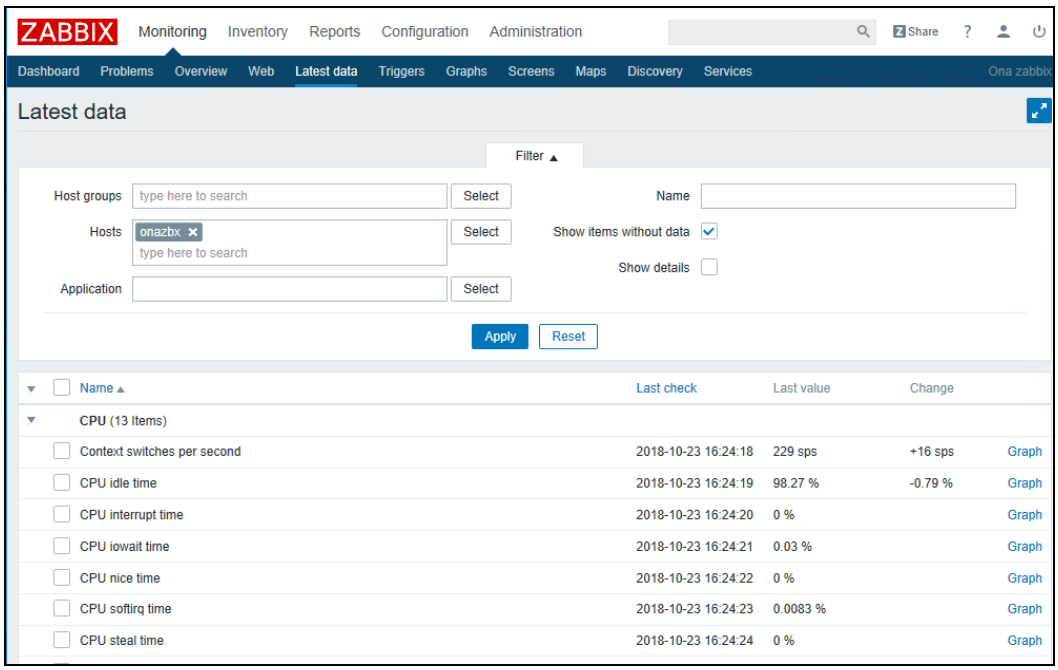


Figura 26 - Valores recogidos por la herramienta de monitorización

Si, por ejemplo, se analizan valores del punto de monitorización (de ahora en adelante, *item)* "*CPU idle time"* se muestra la gráfica de la Figura 27:

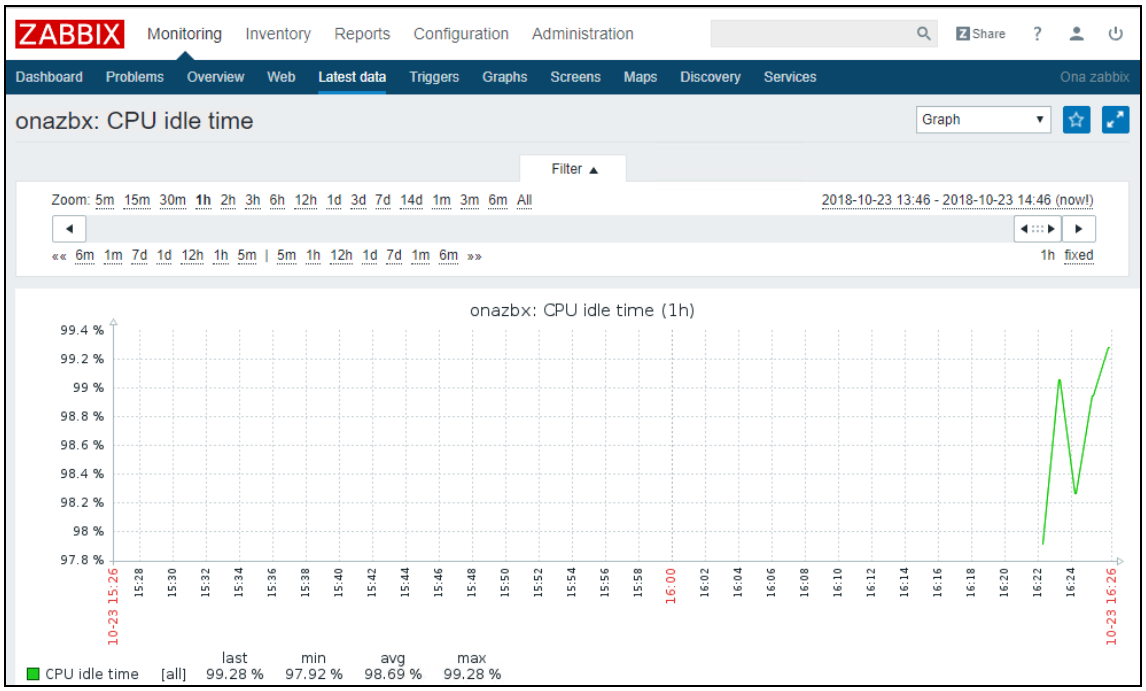


Figura 27 - Gráfica de rendimiento *CPU* idle time

Por lo tanto, la herramienta de monitorización funciona, siendo capaz de recabar información relativa a la máquina virtual que alberga Zabbix.

Migración de la máquina virtual CentOS:

Para realizar la migración desde la versión de *ESXi 6.5* en entorno de desarrollo es necesario detener la máquina virtual, ya que las versiones utilizadas no permiten hacer una migración en caliente. La migración se realizará al entorno de *producción* en el *ESXi* de la sede Central en Barcelona, en el servidor *HP ESX 2* con *IP* XXX.XXX.100.9.

Los pasos realizados son los siguientes:

Apagado de la máquina virtual: Para detener la máquina virtual se debe acceder al panel web de *ESXi 6.5*, desplegar con el botón derecho del ratón el menú el siguiente menú y seleccionar "*Energía"→"Apagar*" (véase Figura 28).

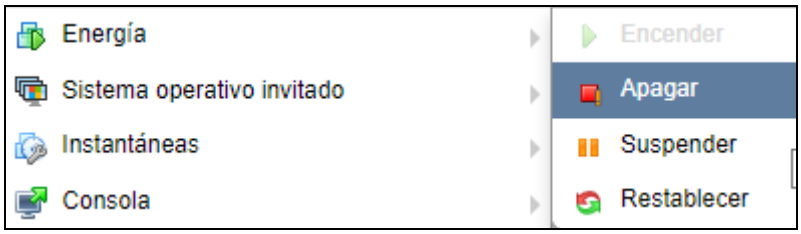


Figura 28 - Apagado de la máquina virtual en *ESXi*

Exportar la máquina virtual: Para realizar esta operación, se debe seleccionar la opción "Exportar" (véase Figura 29):

Figura 29 - Exportación de la máquina virtual como plantilla *OVF*

A continuación, aparece un cuadro de diálogo que permite descargar dos archivos que conforman la máquina virtual (véase Figura 30): El archivo con extensión *OVF* contiene la configuración de la máquina virtual y el archivo con extensión V*MDK* es el disco duro virtual de la máquina.

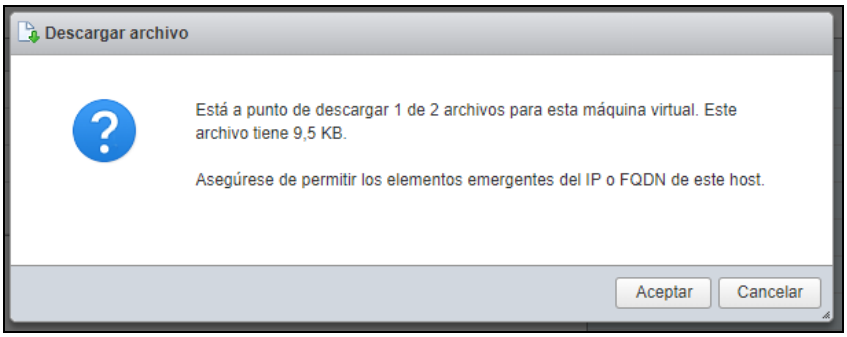


Figura 30 - Descarga del archivo de la máquina virtual

Importar la máquina virtual: Para realizar este proceso se accede a la aplicación *VMware vSphere Client 5.0* y se escoge la opción "*File"→"Deploy OVF Template"* (véase Figura 31).

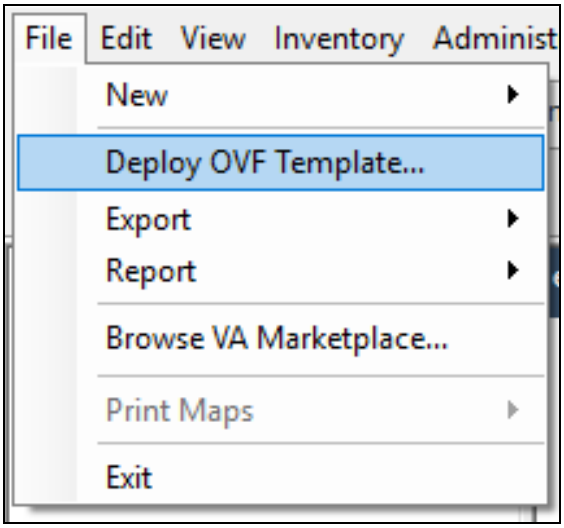


Figura 31 - Despliegue de la máquina virtual

Posteriormente se seleccionan los archivos relativos a la máquina virtual CentOS con extensiones *OVF* y *VMDK* descargados anteriormente y automáticamente se realiza el despliegue de la máquina virtual en el nuevo entorno *ESXi*.

Poner en marcha la máquina virtual: Una vez finalizado el proceso de despliegue, se desactiva la tarjeta de red de la máquina virtual en el menú configuración. Con ello se evita que ésta realice intentos de conexión a la red con una dirección *IP* que no pertenece al segmento de red al que se quiere conectar. Posteriormente, se enciende la máquina virtual con normalidad y se accede mediante la pestaña "Console" a la consola de la máquina virtual (véase Figura 32) para comprobar que se ha iniciado correctamente.

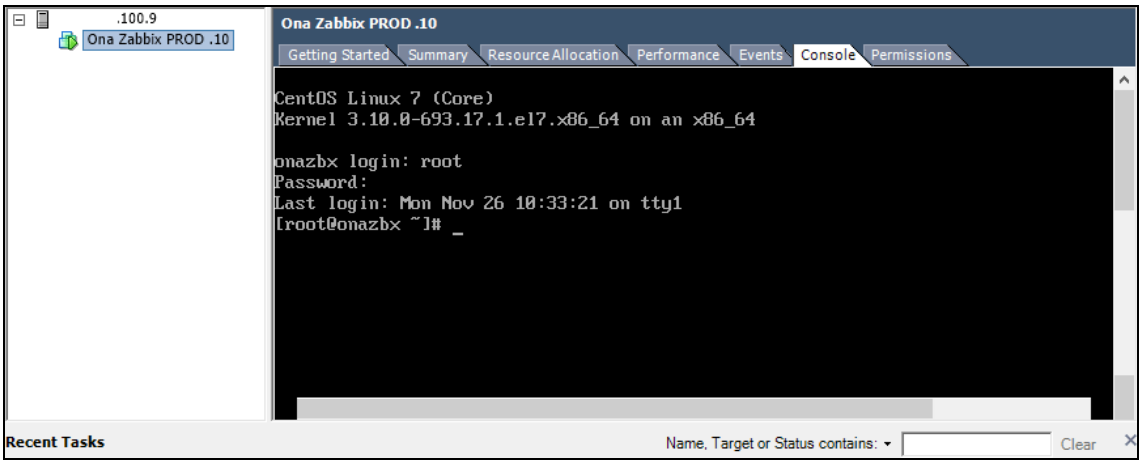


Figura 32 - Visualización de la consola de la máquina virtual

Cambio de configuración de red del servidor: A continuación, se accede al archivo de configuración de la tarjeta de red y se modifica la dirección *IP* con la nueva dirección XXX.XXX.100.10 y el DNS primario con la nueva dirección XXX.XXX.10.20, la cual pertenece al servidor primario de DNS del dominio.

```
# vi /etc/sysconfig/network-scripts/ifcfg-eno*
```

Una vez dentro del archivo, se deben cambiar los siguientes parámetros tal como se muestra a continuación:

```
DNS1="192.168.10.20"

IPADDR="192.168.100.10"
```

Posteriormente, se guardan los cambios realizados y se apaga la máquina virtual para volver conectar la tarjeta de red en el menú de configuración. Entonces, se enciende nuevamente la máquina virtual y se comprueba que el acceso tanto el acceso SSH mediante Putty como la dirección web http://XXX.XXX.100.10/zabbix están operativos. En este último caso, si se consulta la gráfica del servidor de Zabbix *item* "*Interrupts per second*" en *"Monitoring"→"Latest data"* se puede visualizar la siguiente gráfica:

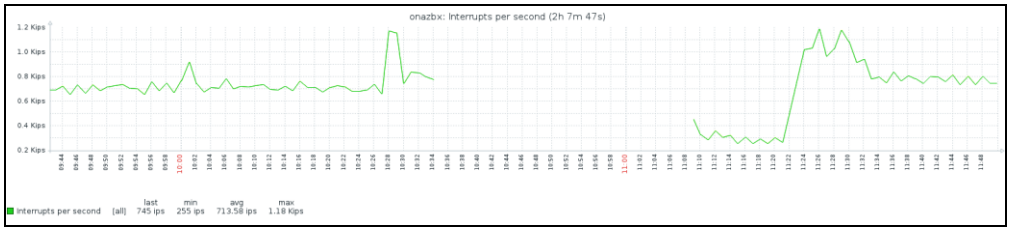


Figura 33 - Gráfica servidor onazbx: Interrupts per second

En la Figura 33 se aprecia el periodo de tiempo en que la máquina virtual ha estado detenida y no ha recogido datos. Además, se puede ver como nuevamente ha retomado la monitorización del propio servidor, por lo que la migración se ha realizado satisfactoriamente.

Configuración de *KPI* a monitorizar en producción

Por defecto, *Zabbix* recoge en su herramienta de monitorización unas plantillas con *items* y alertas de monitorización (de ahora en adelante, *triggers*) predefinidos, los cuales serán utilizados para realizar una monitorización estándar en los entornos Windows y Linux.

Además, permite monitorizar mediante la creación manual de plantillas formadas por *items y triggers*, o mediante la descarga de plantillas de monitorización preconfiguradas tanto por Zabbix como por la comunidad. Para monitorizaciones más específicas se pueden encontrar plantillas que se ajustan al *hardware* a monitorizar en https://share.zabbix.com.

Una vez se descarga una plantilla se puede añadir a la herramienta de monitorización haciendo clic en *"Configuration"→"Templates"→"Import"* (véase Figura 34).

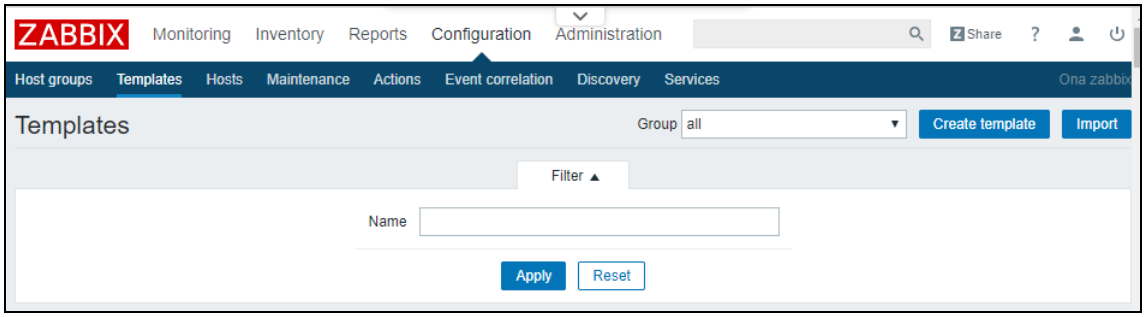


Figura 34 - Configuración de plantillas de monitorización

A modo de ejemplo, para añadir a la monitorización los servidores *ESXi* se realizará el siguiente proceso:

- Se busca en la página web https://share.zabbix.com la palabra *ESXi.*
- Se escoge la plantilla "*ESXi SNMP only for Zabbix 3.0*".
- Se accede a la pestaña "*Configuration"→"Templates"→"Import*" y se selecciona la plantilla descargada (véase Figura 35).

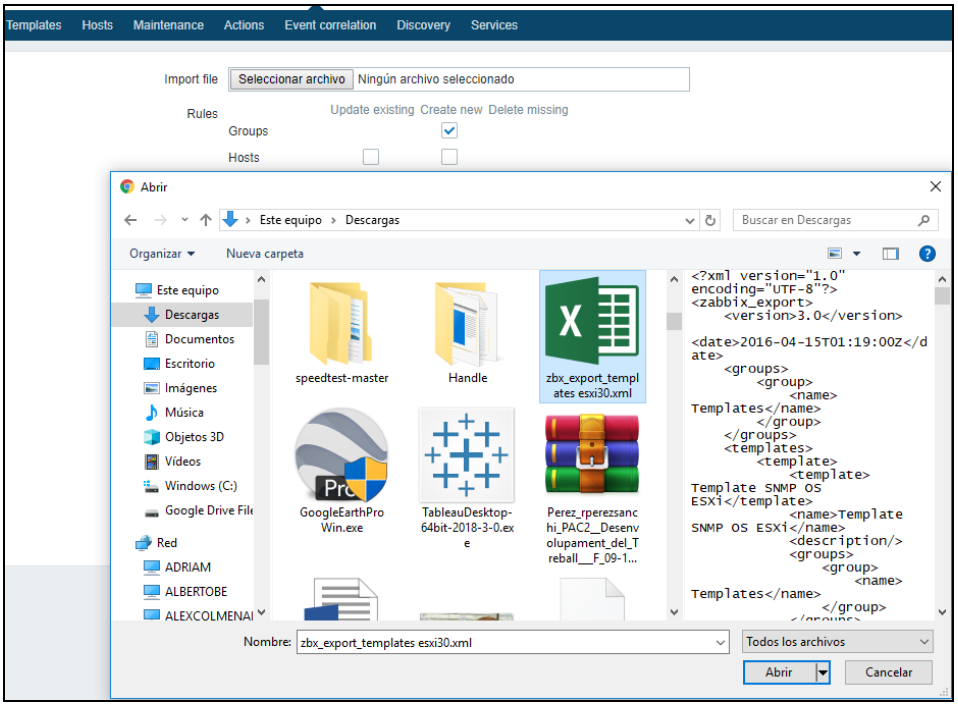


Figura 35 - Selección de una plantilla customizada para añadir a Zabbix

Aparecerá un menú donde se permite seleccionar las opciones de importación. En este caso, se importan las opciones por defecto (véase Figura 36). Posteriormente, la plantilla quedará en la herramienta.

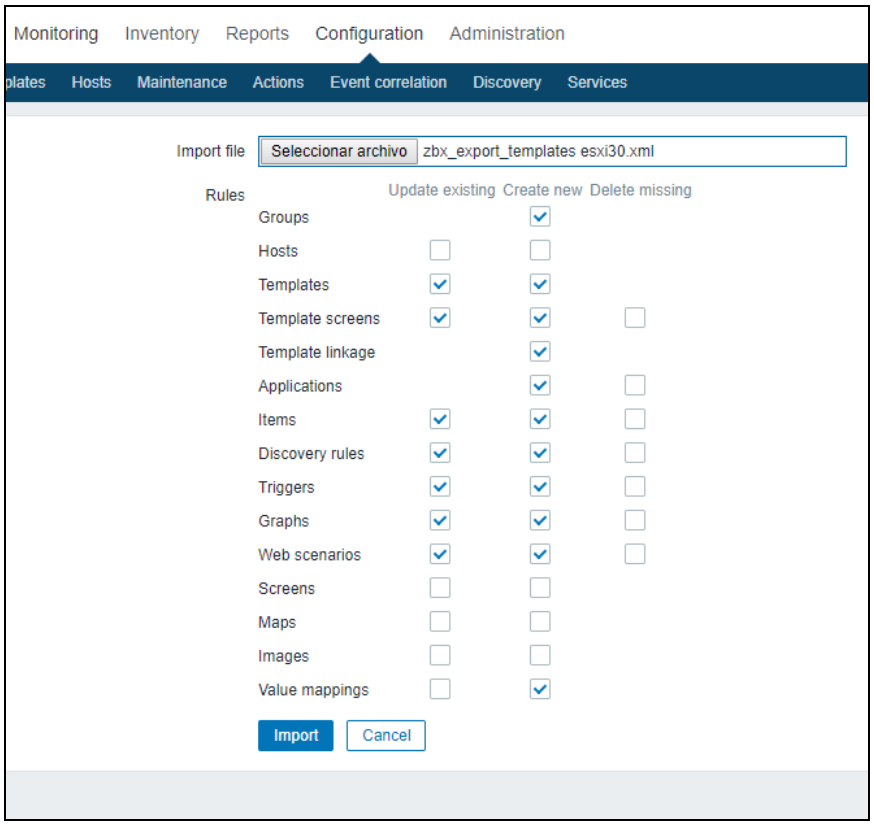


Figura 36 - Selección de la información que se copiará de la plantilla.

Finalmente, para monitorizar dispositivos se necesita instalar un agente, enviar datos a través de un ejecutable o habilitar el agente *SNMP* en la configuración del dispositivo, entre otros. A modo de ejemplo se mostrará el proceso de instalación del agente de Zabbix en una máquina virtual Linux, en una máquina Windows y en uno de los cortafuegos FortiGate a través del protocolo *SNMP*.

- Instalación agente de Zabbix:

Para instalar el agente de Zabbix se descarga el paquete de software con formato ".deb" de los repositorios de Zabbix:

```
#wget http://repo.zabbix.com/zabbix/3.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_3.4-1%2Bbionic_all.deb
```

Se descomprime el archivo descargado:

```
#sudo dpkg -i zabbix-release_3.4-1+trusty_all.deb
```

Se actualiza el Sistema de gestión de paquetes *APT*:

```
#sudo apt-get update
```

Se instala el programa *zabbix-agent*:

```
#sudo apt-get install zabbix-agent
```

Tras realizar la instalación, se modifica el archivo de configuración "/etc/zabbix/zabbix_agentd.conf" con el editor *vi* de la siguiente manera:

```
#vi /etc/zabbix/zabbix_agentd.conf

server=XXX.XXX.100.10

serveractive=XXX.XXX.100.10

hostname=Nombre_del_host_local
```

Se guarda el documento escribiendo el comando ":wq" y se reinicia el agente de Zabbix para que se aplique la configuración:

```
#sudo service zabbix-agent restart
```

Tras este último paso, el agente queda instalado satisfactoriamente.

- Aplicación *"*zabbix_sender*"* en Windows*:*

Para descargar el ejecutable "zabbix_sender" se debe descargar el paquete de agente pre compilado para Windows de Zabbix disponible en el siguiente enlace https://www.zabbix.com/downloads/4.0.0/zabbix_agents-4.0.0-win-amd64.zip.

Una vez descargado, se descomprime el archivo y se localiza el ejecutable "zabbix-sender" dentro de la carpeta *bin*. Para realizar envíos de información únicamente se debe abrir una consola de Powershell de Windows y ejecutar los siguientes comandos:

```
$commandline="c:\zabbix\zabbix_sender.exe -z 192.168.100.10 -s 'nombre_host' -k ""nombre_item"" -o valoraenviar"

Invoke-Expression -command $commandline
```

Donde "*nombre_host"* pertenece al nombre del *host* al que hace referencia el ítem que va a recibir el valor monitorizado, "*nombre_item"* hace referencia al *item* que recibe la modificación con del último valor recibido y "*valoraenviar"* contiene un valor numérico.

Para probar este tipo de recepción de valores se envían valores binarios desde un host Windows con Powershell y el ejecutable "zabbix_sender" a un host de prueba llamado "Prueba", con un punto de monitorización configurado, cuyo *item* es llamado "prueba". En primer lugar, se realizará un envío con valor "1", y posteriormente, será enviado un valor "0".

```
$commandline="c:\zabbix\zabbix_sender.exe -z 192.168.100.10 -s 'Prueba' -k ""prueba"" -o 1"

Invoke-Expression -command $commandline


$commandline="c:\zabbix\zabbix_sender.exe -z 192.168.100.10 -s 'Prueba' -k ""prueba"" -o 0"

Invoke-Expression -command $commandline
```

Como se puede ver en la Figura 37, se visualiza que la gráfica del *item* "*prueba"* del host *"Prueba"* que aparece en *Monitoring→Latest data* muestra tanto el valor "1" como el valor "0" enviados en los pasos anteriores:

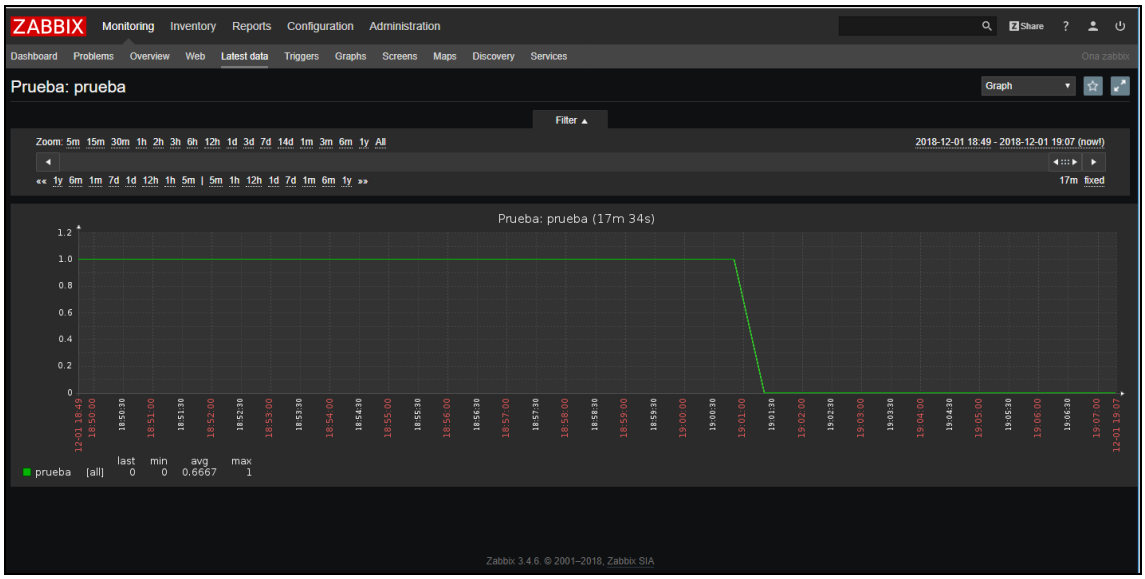


Figura 37 - Gráfica de verificación de monitorización con *trappers*

- *SNMP* en cortafuegos FortiGate:

Para monitorizar el cortafuegos FortiGate a través del protocolo *SNMP* es necesario acceder al menú "*System*"→"*SNMP*". Posteriormente se crea una nueva *Community Name* (similar a un identificador de acceso) al que se permite captar información de estadísticas del dispositivo FortiGate (véase Figura 38). Se configura la dirección *IP* que va a consultar la información y la máscara de red, además de especificar el tipo de comunicación que se establecerá.

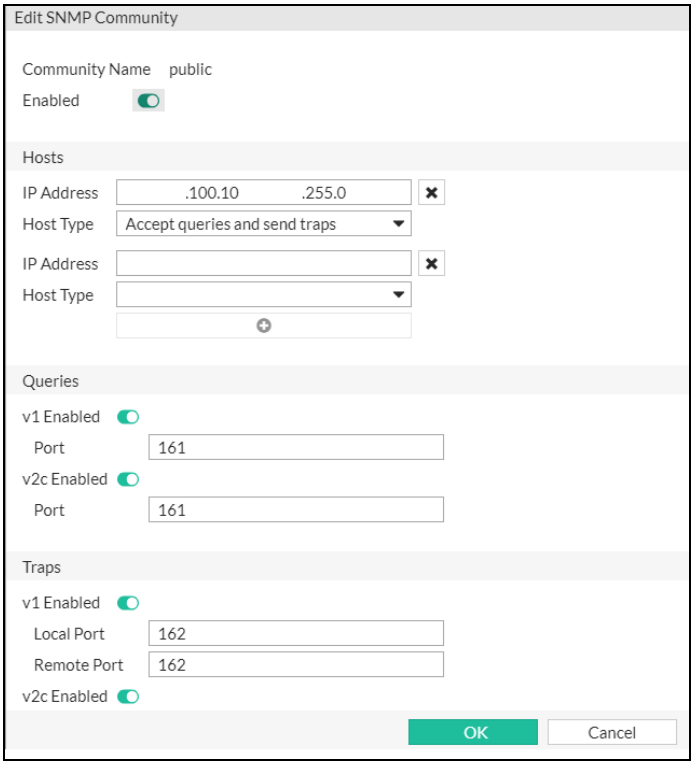


Figura 38 - Configuración de *SNMP* de FortiGate

Tras aplicar la plantilla "*PROD – Template SNMP Fortinet Devices*" al host *FortiGate Central* y transcurridos unos minutos, Zabbix muestra información relativa al dispositivo, la cual se puede consultar en "*Monitoring*"→"*Latest data*" (véase Figura 39):

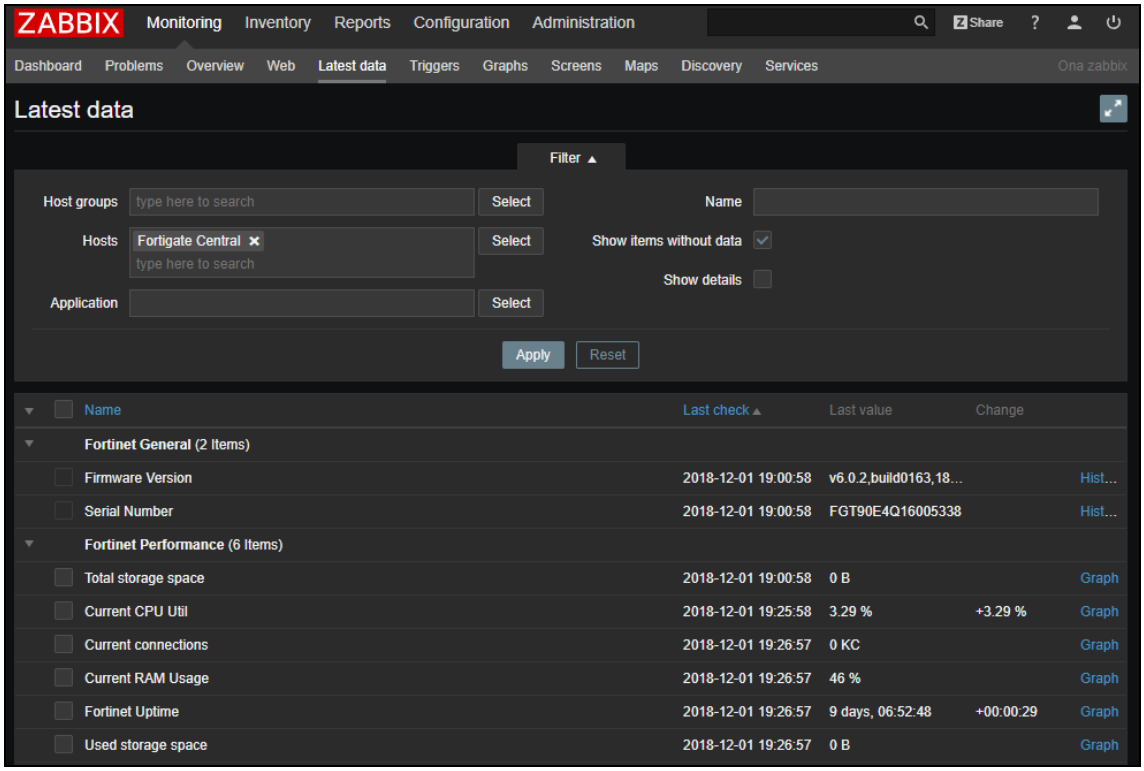


Figura 39 - Datos de rendimiento de FortiGate recopilada mediante *SNMP*

Es importante tener en cuenta que algunas de las plantillas aplicadas contienen más puntos de monitorización de los que trata de alcanzar este Trabajo Final de Grado. Por tanto, se valorará en un futuro la funcionalidad y/o utilidad de estos puntos de monitorización suplementarios para ajustarlos o suprimirlos y así obtener una mejor optimización de la monitorización.

3.4 Resultados obtenidos de la fase

Como se puede apreciar en el apartado anterior, los resultados previstos de las tareas 1, 2 y 3 detallados en el punto 1.3 “*Tareas e hitos*” de este mismo documento se han cumplido satisfactoriamente, quedando definido tanto el entorno de producción como los puntos de monitorización donde se realiza la implantación, así como la puesta en marcha de la máquina virtual CentOS 7 con la herramienta de monitorización Zabbix, cuyo funcionamiento ha sido validado satisfactoriamente. Posteriormente, se han configurado los puntos de monitorización definidos previamente para así dar por finalizado el proceso de configuración.

4. Representación de *KPI* geolocalizados

4.1 Objetivos de la sección

Durante el desarrollo de esta sección se analizan posibles soluciones para explotar información recogida por la herramienta Zabbix relativa a los sistemas del entorno monitorizado. Posteriormente se escogerá una de las herramientas estudiadas y se elaborará un cuadro de mando que permita visualizar datos importantes para el desarrollo de las actividades de la empresa, ofreciendo una visión geolocalizada de los datos recogidos.

4.2 Herramientas utilizadas

Las herramientas utilizadas para analizar la viabilidad de realizar un cuadro de mando con *KPI* geolocalizados son las siguientes:

Tableau:

Es una plataforma de análisis visual desarrollada por Tableau Software. La herramienta se define como eficaz, segura y flexible. Es capaz de facilitar el análisis visual en tiempo real, permitiendo así analizar patrones y datos relevantes de forma rápida y ágil. Permite combinar datos de Big Data, bases de datos SQL y MySQL, hojas de cálculo y aplicaciones en la nube como Google Analytics y Salesforce.

Tableau ofrece cuatro tipos de productos:

- Tableau *Desktop*: Solución de escritorio. Permite conectar a los datos desde un ordenador personal y analizarlos.

- Tableau *Server*: Es capaz de concentrar datos de diversas procedencias y plataformas en un único servidor que puede ser consultado por diversos usuarios, publicando así datos para su análisis.

- Tableau *Online*: Plataforma de análisis completamente hospedada en la nube.

- Tableau *Prep*: Nuevo producto que permite preparar datos de un modo más visual y directo.

Entre estas cuatro soluciones, se decide realizar pruebas con la versión de *Desktop* que se muestra en la Figura 40:

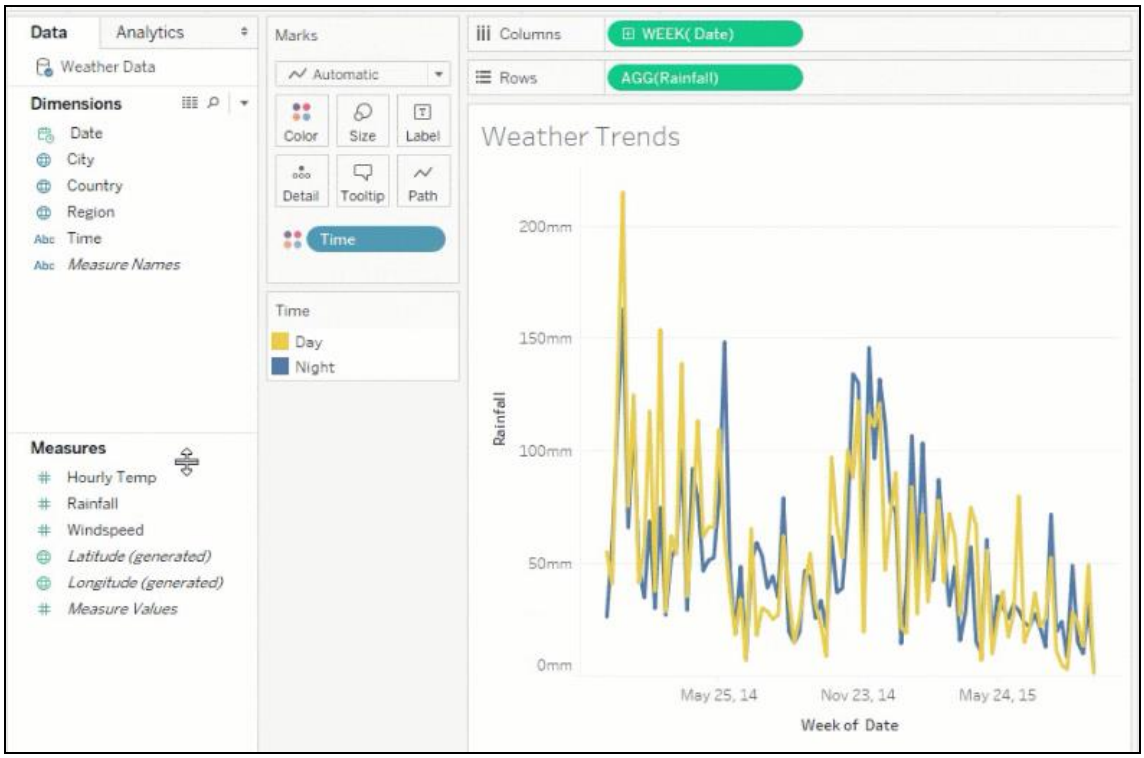


Figura 40 - Gráfica bidimensional con Tableau disponible en www.tableau.com

Además, como se puede ver en la Figura 41, Tableau permite la creación de mapas interactivos nativos donde se pueden geolocalizar datos para tener información representada sobre el mapa.

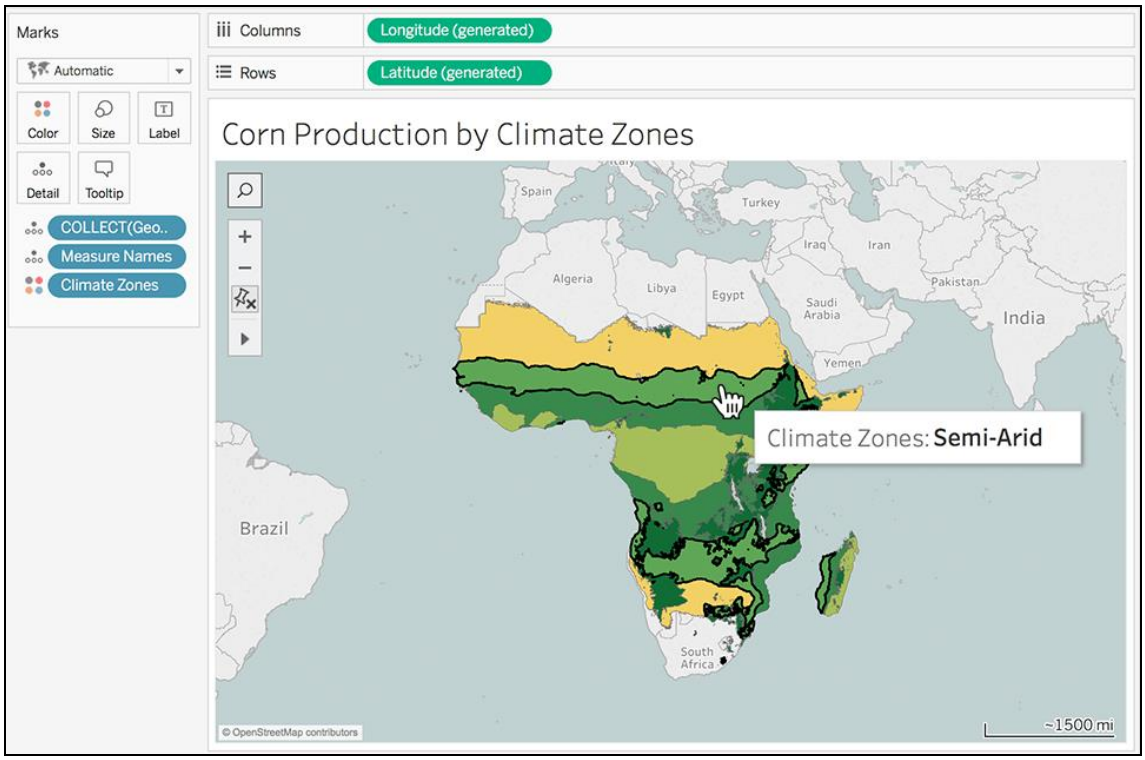


Figura 41 - Representación de datos geolocalizados con Tableau disponible en https://taiphanmemfull.com

Respecto al tipo de licencia de uso, Tableau es una herramienta de pago, con una versión de prueba de 14 días.

Power BI

Power BI se define como una colección de servicios de *software*, aplicaciones y conectores que funcionan conjuntamente para convertir orígenes de datos sin relación entre sí en información coherente, interactiva y visual. Permite conectar fácilmente con orígenes de datos de archivos como Excel y CSV, paquetes de contenido como Google Analytics, Marketo y Salesforce, Bases de datos en la nube como Azure SQL y locales como SQL server y MySQL. En concreto, Power BI Desktop tiene una aplicación para representar valores geolocalizados, además de poder agregar el módulo ArcGIS Maps for Power BI que proporciona una segunda opción para realizar representaciones de datos geolocalizados en un mapa (véase Figura 42).

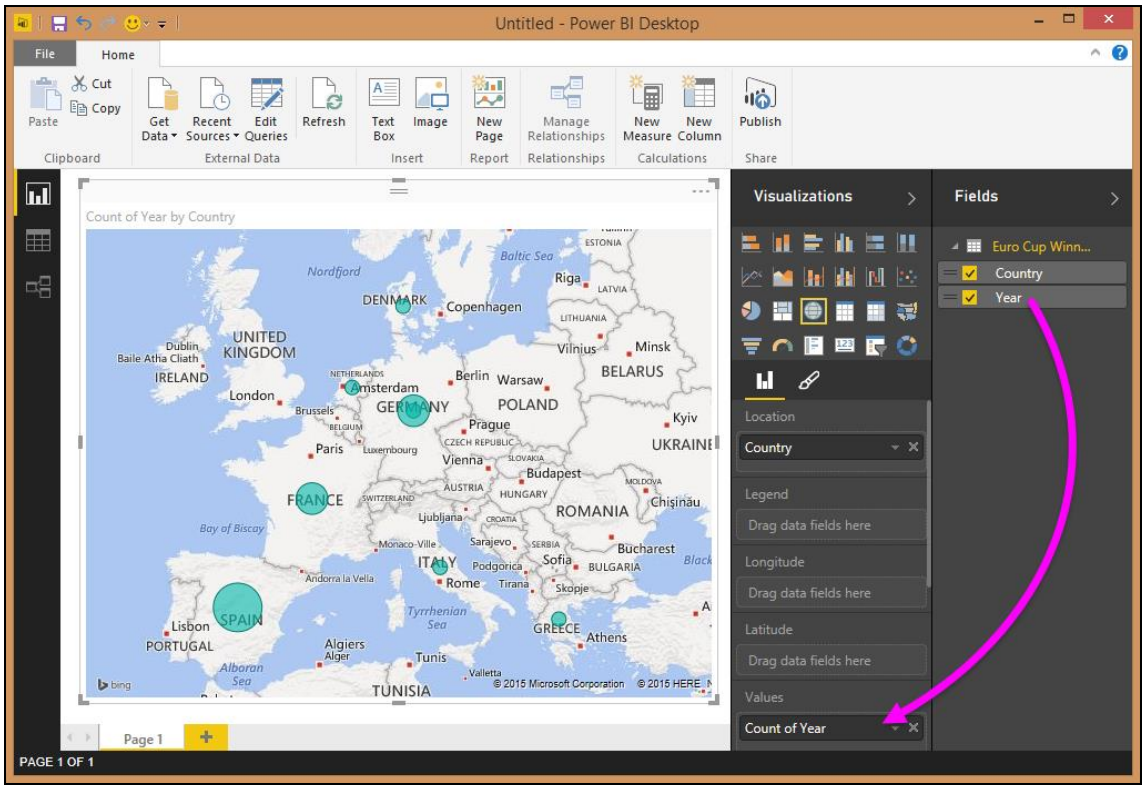


Figura 42 - Representación de datos geolocalizados con Power BI disponible en https://pbiwebprod.trafficmanager.net

Respecto al tipo de licencia de uso, Power BI es una herramienta de pago, con una versión de prueba de 60 días. Sin embargo, en el departamento de *IT* de la organización donde se realiza la implantación del Trabajo Final de Grado cuenta con una licencia, por lo que se podría añadir a las actividades diarias de la organización sin coste adicional.

Grafana

Herramienta que permite el análisis y visualización de métricas. Se utiliza frecuentemente para visualizar de forma elegante series de datos en el análisis de infraestructuras y aplicaciones. Contiene un sistema de alertas de monitorización e integración directa con Zabbix y permite consultar datos de estados de recursos (*CPU, RAM*, disco duro) de detalles de servicios como MySQL, PostgreSQL, Apache, Redis, etc. Gracias a ser una herramienta de código abierto, la Comunidad pueda desarrollar aplicaciones de terceros que aporten nuevas e interesantes funcionalidades como el módulo Worldmap, que permite geolocalizar datos analizados (véase Figura 43).

Figura 43 - Ejemplo de representación de datos geolocalizados con Grafana disponible en https://github.com/grafana/worldmap-panel

4.3 Justificación de solución escogida

Se realiza una primera toma de contacto de aproximadamente dos horas de duración con las tres herramientas para tomar primeras impresiones.

Tableau

Se descarga la versión Tableau *Desktop* de la aplicación y se consigue conectar a la base de datos MySQL XXX.XXX.100.10 de Zabbix. Sin embargo, no se consigue representar información en los módulos de mapas de la aplicación. Además, al ser una herramienta de pago y no poseer licencia resulta menos atractiva que Power BI o Grafana.

Power BI

Se descarga la versión Desktop de la aplicación y se consigue representar mediante una consulta directa a la base de datos MySQL de Zabbix la información relativa al valor de tiempo de respuesta de dispositivos FortiGate (véase Figura 44).

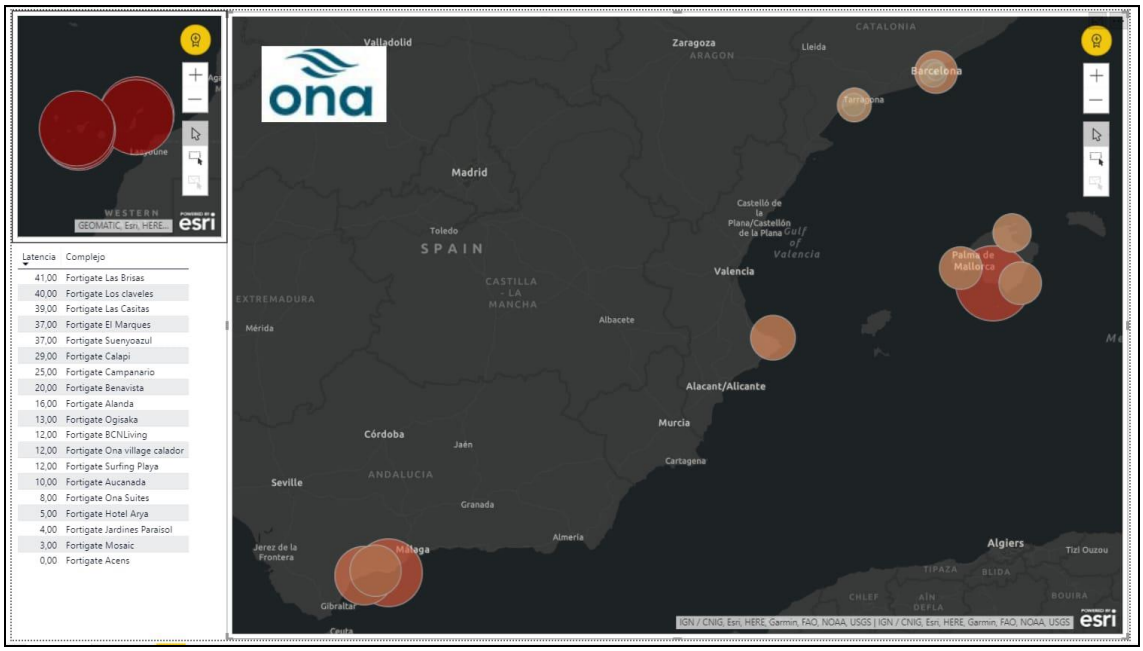


Figura 44 - Test de geolocalización de datos en Power BI

Cabe destacar que el resultado obtenido se puede publicar en forma de informe en la web de Power BI. Sin embargo, cualquier usuario puede ver en *Internet* el informe o el objeto visual que se publique por lo que la confidencialidad de los datos queda rota, permitiendo la fuga de datos sensibles de la organización.

Grafana

Se descarga una versión de escritorio de la aplicación ejecutable en Windows, se añade el módulo WorldMap y se obtiene el mismo resultado que con la aplicación Power BI (véase Figura 45), con una imagen ligeramente más atractiva de los datos tal como se muestra en la siguiente imagen.

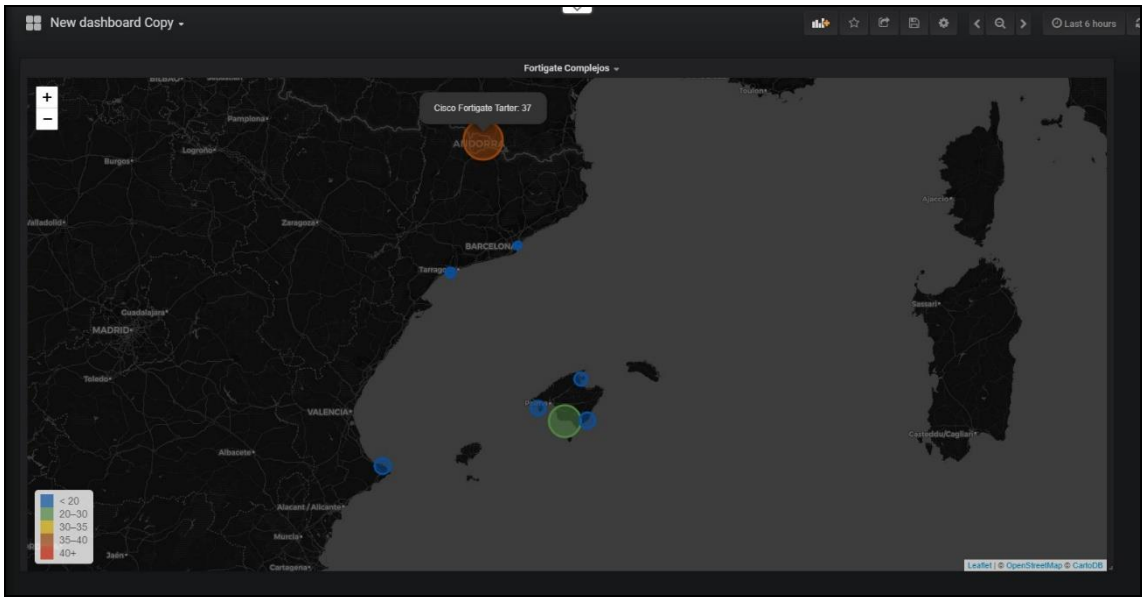


Figura 45 - Grafana: Test de geolocalización de datos

Cabe destacar que la aplicación Grafana es accesible vía web, por lo que puede ser consultada a nivel de red local. Ello habilita la posibilidad de mostrar datos representados en Grafana en cualquier dispositivo que tenga acceso a la red local, como televisores y dispositivos móviles, entre otros.

Dado el resultado final obtenido, se decide utilizar Grafana por los siguientes motivos:

- Herramienta gratuita
- Fácil despliegue
- Multiplataforma (instalable en sistemas operativos Windows y Linux)
- Integración mediante un módulo con la herramienta Zabbix
- Buena apariencia de representación de gráficos
- Fácil acceso a nivel de red local desde cualquier dispositivo con navegador web.

4.4 Relación de las actividades realizadas

Debido a que Grafana únicamente consulta los datos recogidos por la herramienta Zabbix, puede ejecutarse únicamente cuando se deseen consultar datos, por lo que se realizará una instalación en un ordenador con sistema operativo Windows 10 que a nivel de conectividad estará dentro de la misma red local que el servidor de Zabbix.

Posteriormente, se realizarán las configuraciones necesarias para obtener un cuadro de mando el cual permita obtener una visión general y avanzada del estado de la infraestructura de *TI* monitorizada.

4.5 Implementación

Se descarga la última versión de Grafana para Windows desde el sitio web oficial https://grafana.com/grafana/download?platform=windows mediante el siguiente enlace:

https://dl.grafana.com/oss/release/grafana-5.2.4.windows-amd64.zip

Se descomprime el archivo descargado y se ejecuta el archivo grafana-server.exe (véase Figura 46) presente en la dirección de archivos \grafana-5.2.4\bin.

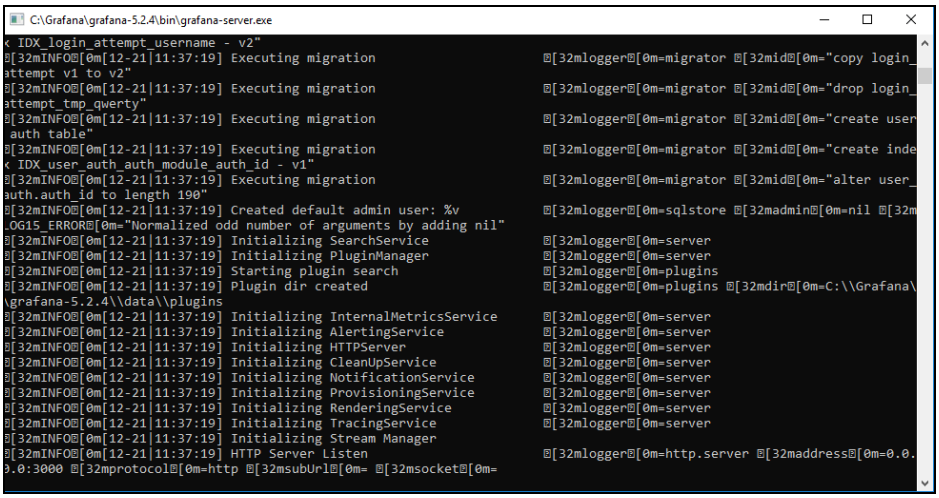


Figura 46 - Ejecución del servidor de Grafana en Windows

Posteriormente, la aplicación queda en ejecución y es accesible desde la dirección web http//localhost:3000 (véase Figura 47):

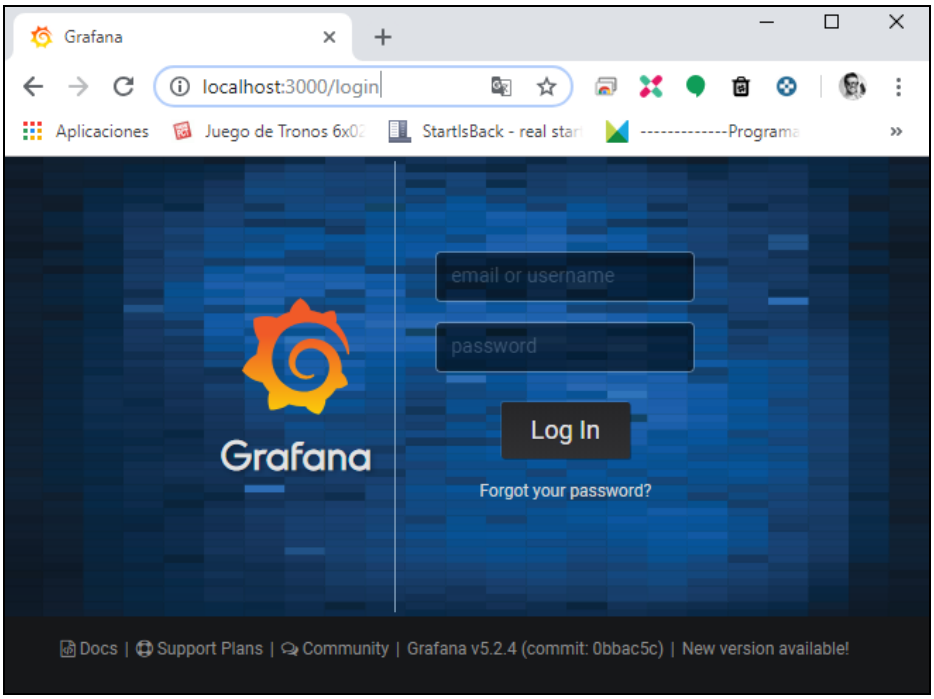


Figura 47 - Pantalla de inicio de sesión a Grafana

4.6 Análisis e implementación de herramientas de explotación de datos

Por un lado, se necesita el módulo de Zabbix para Grafana, el cual está disponible en https://grafana.com/plugins/alexanderzobnin-zabbix-app. Una vez descargado se configura para que Grafana tenga conexión con Zabbix (véase Figura 48).

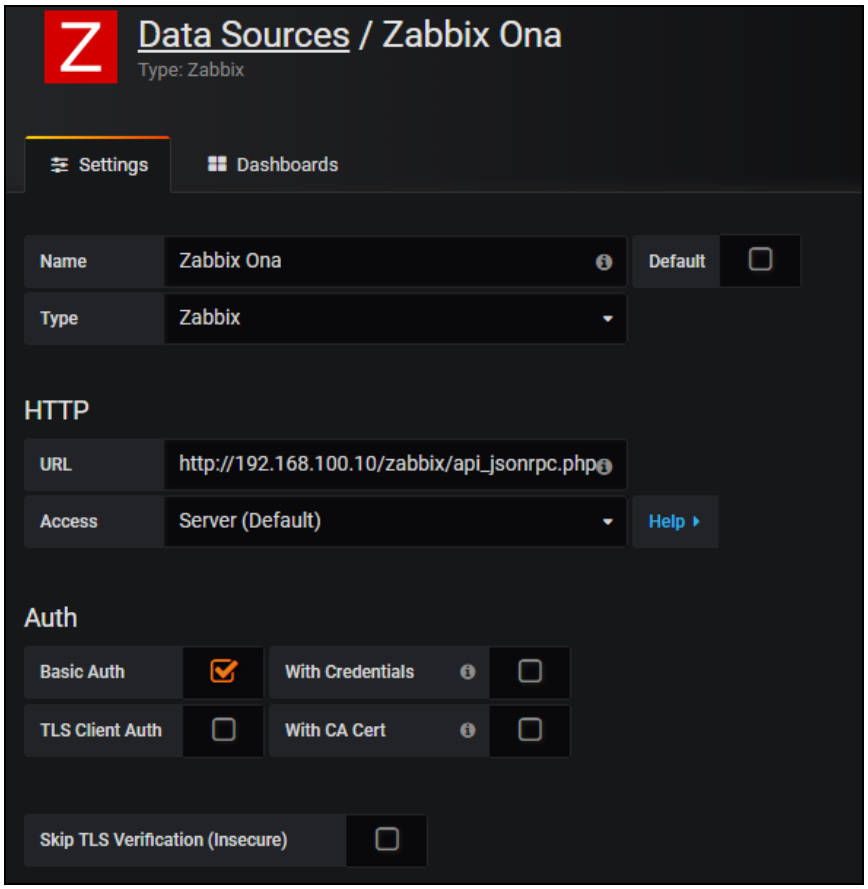


Figura 48 - Configuración de la fuente de datos Zabbix en Grafana

Se testea la configuración y, tal como muestra la Figura 49, se confirma que la conexión es satisfactoria.

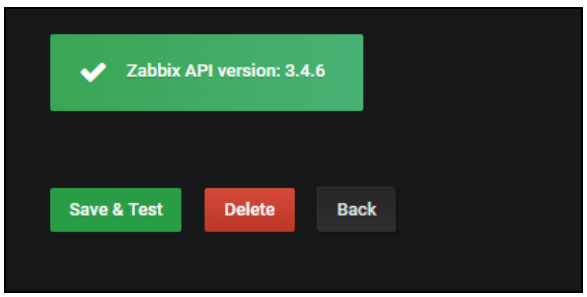


Figura 49 - Test conexión entre Grafana y Zabbix

Con ello se podrán mostrar datos recogidos por Zabbix en Grafana. Como ejemplo de configuración de un cuadro de mando con Grafana, se realiza la monitorización del ancho de banda tanto de carga como de descarga de los complejos. Para ello, se crea una nueva pantalla (de ahora en adelante,

Dashboard) que muestre información de Zabbix. Una vez creada, se selecciona el tipo de información que se desea representar. Tal como muestra la Figura 50, existen diversos tipos como gráficos, estados simples, tablas, texto, mapas de calor, listas de alertas, columnas, fotos, entre otros.

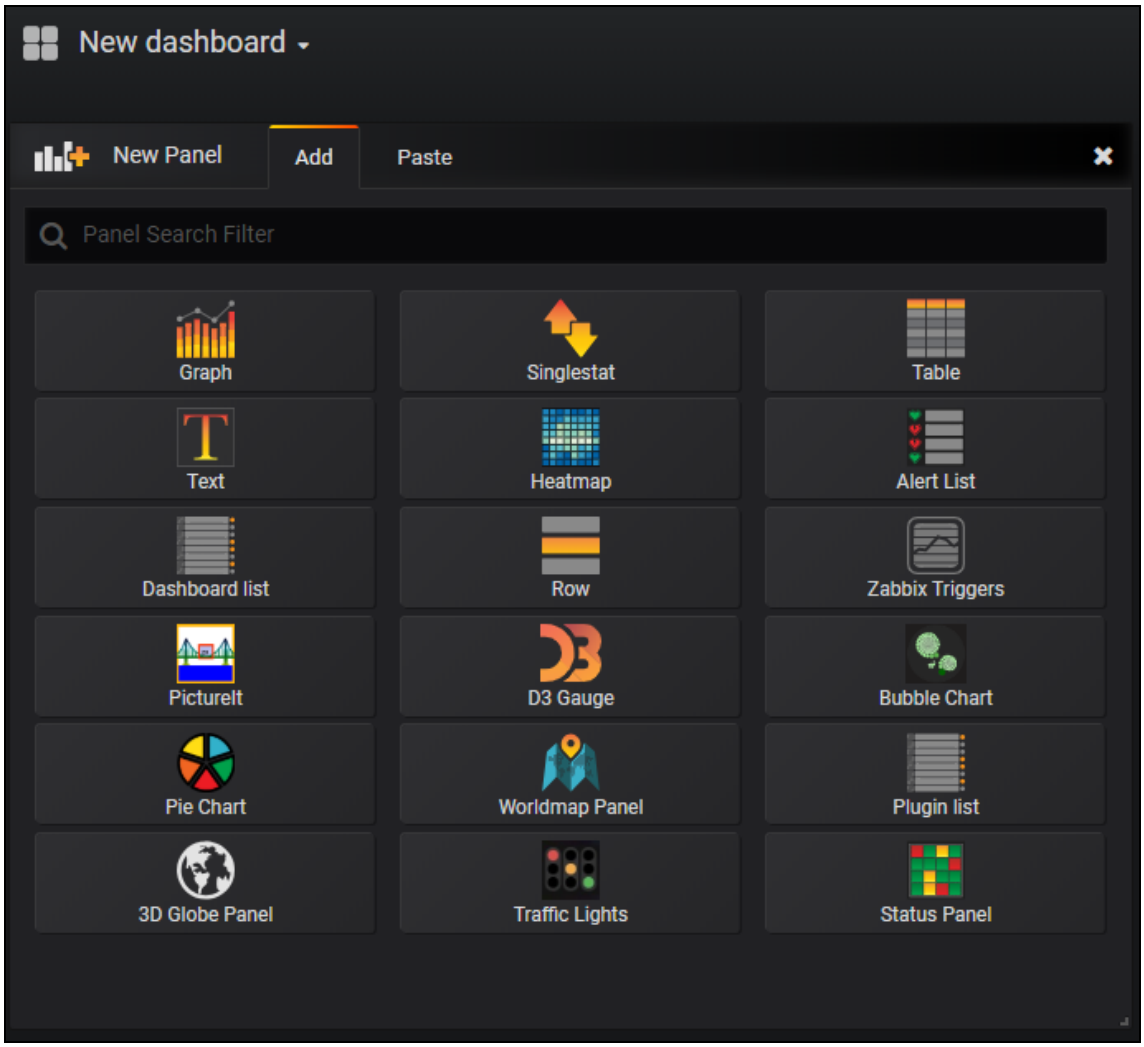


Figura 50 - Tipos de panel disponibles en Grafana

En esta ocasión utilizaremos gráficos de tipo estado simple (de ahora en adelante, *Singlestat*), de tipo gráfico (de ahora en adelante, *Graph*) y de mapa de calor (de ahora en adelante, *Heatmap*). Ello nos permitirá tener una visión general de posibles excesos de consumos de ancho de banda de la conexión a *Internet* en los complejos, lo que puede provocar cuellos de botella y bajos rendimientos en el *PMS* hotelero.

Para visualizar la descarga del complejo Aucanada, se crea un nuevo panel en el *Dashboard* de tipo *Singlestat* de la siguiente manera:

Se selecciona la pestaña *Metrics* y se selecciona la fuente de datos “Zabbix Ona”. A continuación, se selecciona la descarga del dispositivo FortiGate Aucanada tal como se muestra en la Figura 51:

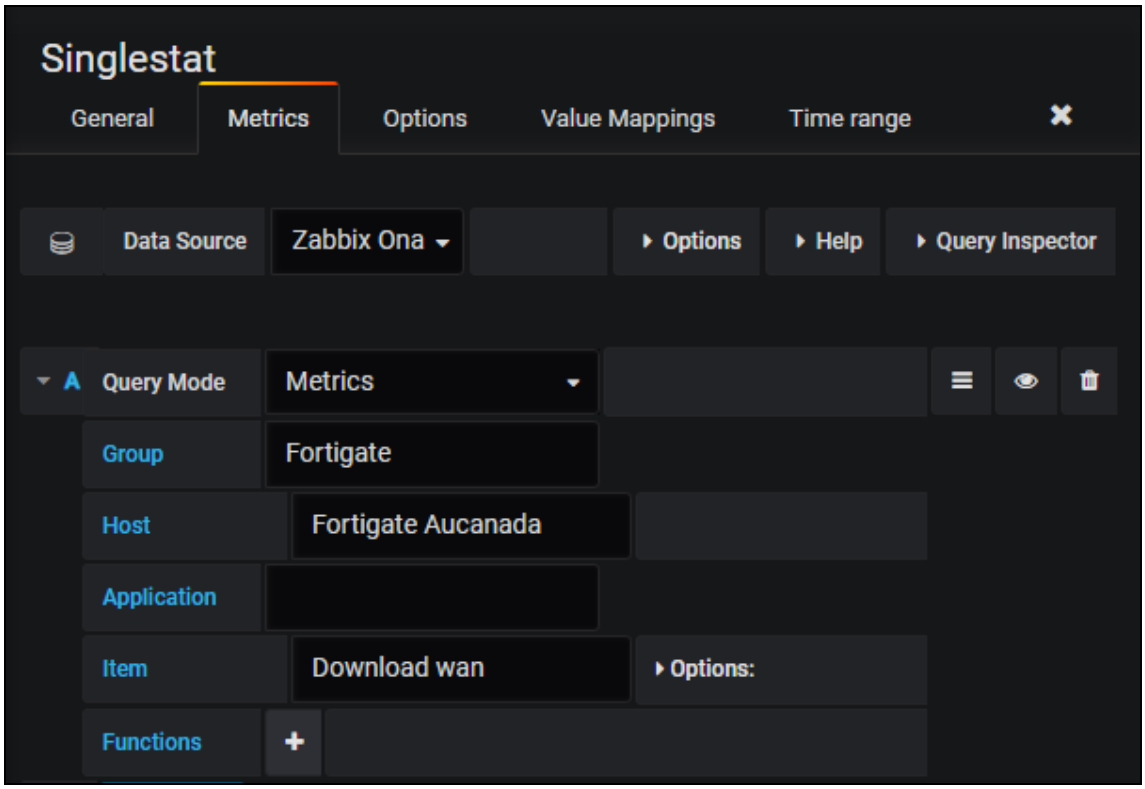


Figura 51 - Ejemplo de configuración de métricas del panel tipo Singlestat

En la pestaña “Options” se define el umbral en el cual el color del gráfico cambiará (véase Figura 52). Se establece un código de colores verde-naranja-rojo para mostrar la cantidad de descarga realizada, de tal forma que, para valores por debajo de 15 MB el color del gráfico será verde, entre 15MB y 20MB será naranja y para valores que superen 20MB serán de color rojo. Para el caso de los paneles con gráficos de carga, se establecerá un color fijo azul, ya que no es crítico para la organización la saturación de la subida de información.

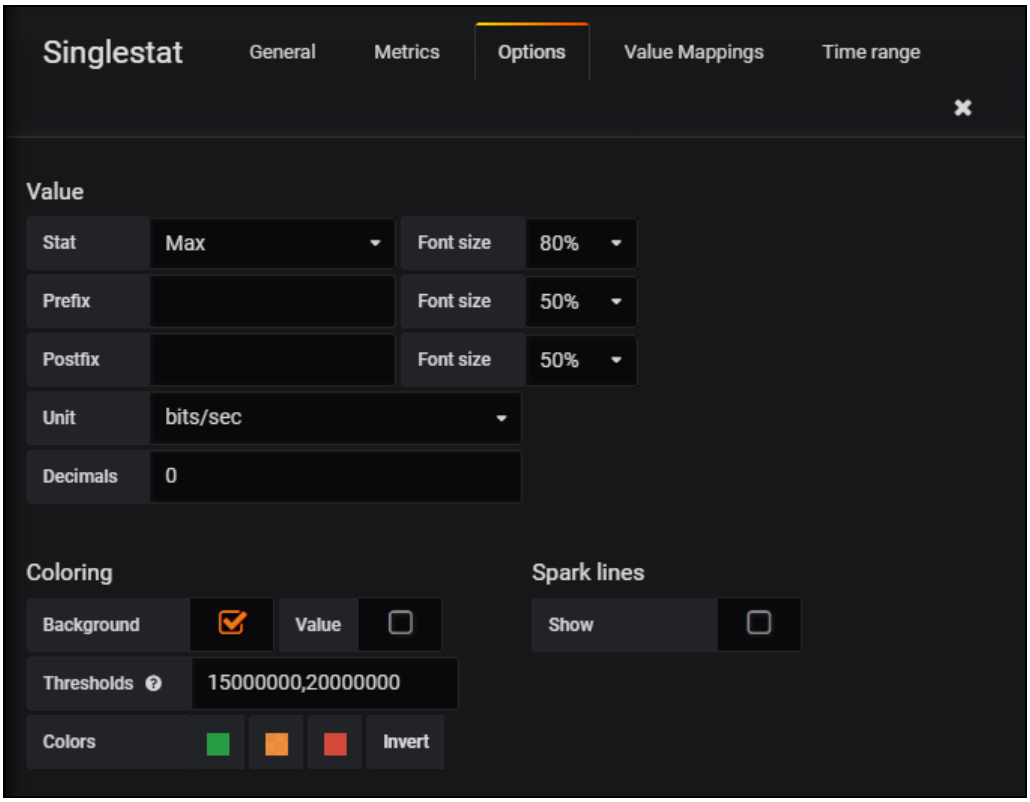


Figura 52 - Ejemplo de configuración de pestaña *Singlestat* - *Options*

Por otro lado, el panel *Heatmap* mostrará con un color más intenso cuales son los valores de tasa de carga y descarga que más se producen en todos los complejos. Para poder visualizar esta información, se requiere realizar la siguiente configuración en la pestaña *Metrics*, tal como muestra la Figura 53:

En ella se puede apreciar que los valores registrados más comunes son de 0 y 10 Megabytes de carga y descarga, ya que lo habitual es que no exista apenas consumo en los complejos.

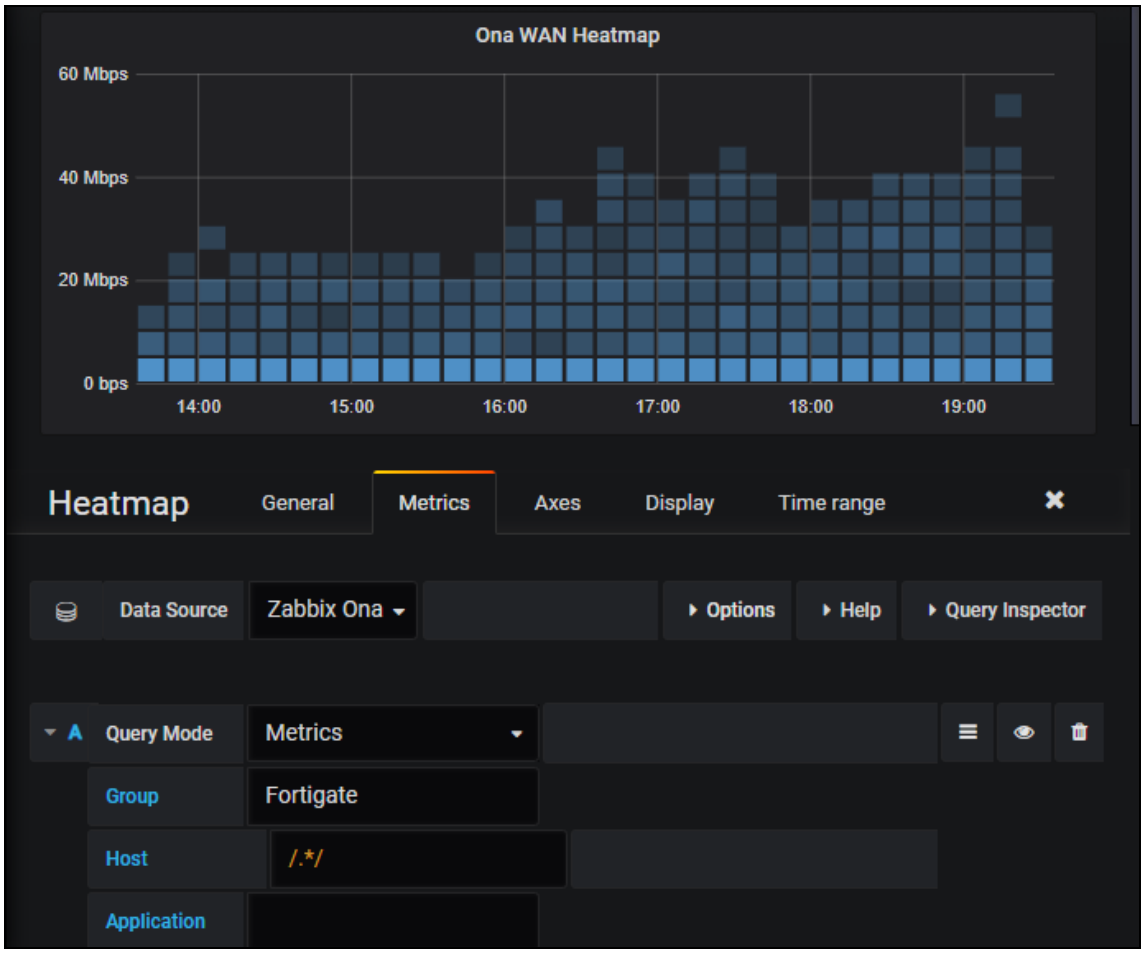


Figura 53 - Ejemplo de configuración de métricas del panel Heatmap

Por último, se mostrará una gráfica a modo histórico de los consumos tanto de carga como de descarga de los complejos. Para ello, se requiere añadir un nuevo panel de tipo *Graph* (gráfico 2D), el cual se configura tal como muestra la Figura 54:

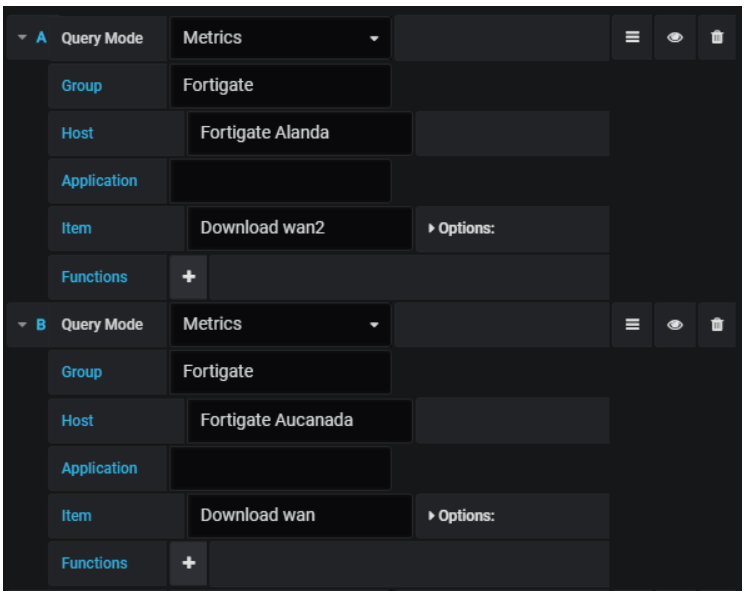


Figura 54 - Ejemplo de configuración de métricas del panel

En esta ocasión se muestran dos consultas realizadas a la descarga de FortiGate de dos complejos, concretamente Alanda y Aucanada. Para que se muestren todos los complejos se deberá replicar esta configuración en todos ellos. El resultado se muestra en la Figura 55:

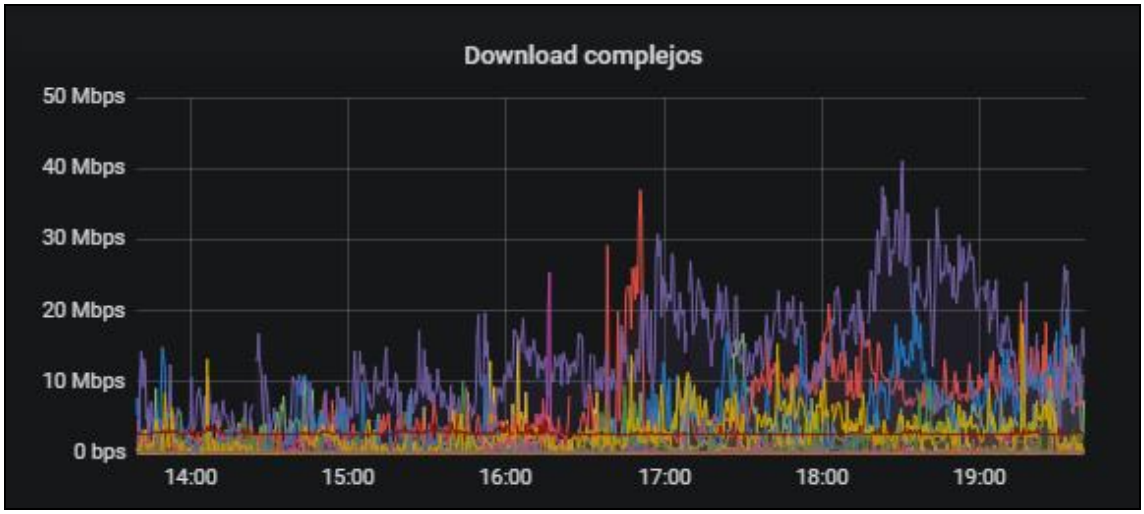


Figura 55 - Tasa de descarga de complejos en Grafana

Para reproducir la misma configuración en el caso de la tasa de carga de todos los complejos se debe replicar la configuración que muestra la Figura 54, utilizando el *item* de tipo "Upload WAN". El resultado se visualiza en la Figura 56):

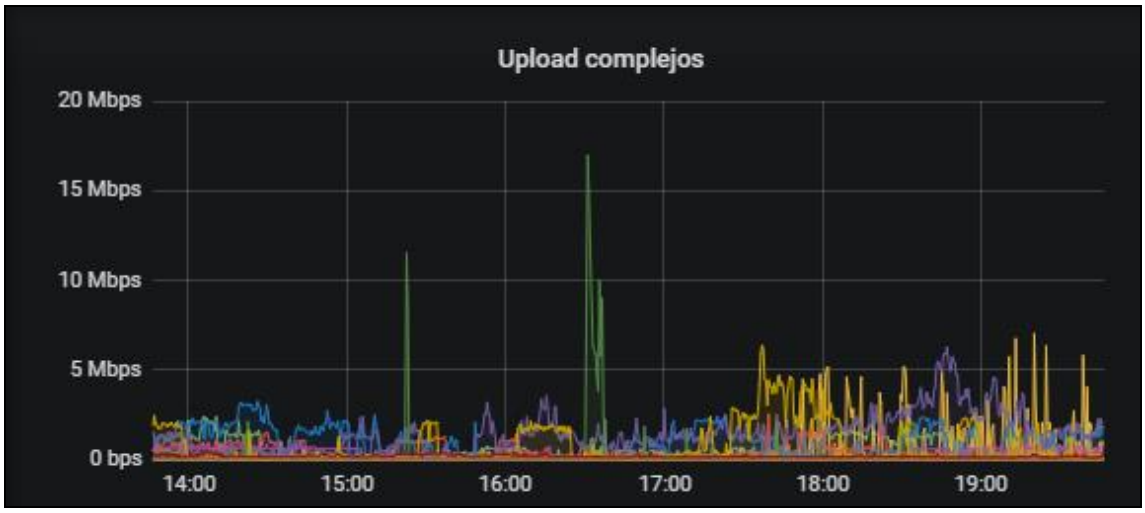


Figura 56 - Tasa de carga de complejos en Grafana

En él podemos observar que, a niveles generales, la tasa de descarga de datos en los complejos es mucho mayor que la tasa de subida de datos, además de experimentar más actividad en la segunda mitad del día.

Posteriormente, para realizar la monitorización de los *KPI* geolocalizados se utiliza el módulo Worlmap Panel, disponible en la dirección

https://grafana.com/plugins/grafana-worldmap-panel/installation. Para la utilización de este módulo se requerirá realizar una consulta directa a la base de datos de Zabbix, debido a que ni el módulo de Zabbix contemplan la representación geolocalizada ni el módulo Worlmap conecta directamente con la base de datos de Zabbix.

La consulta en base de datos, tal como especifica el propio módulo en la aplicación Grafana, debe cumplir los siguientes requisitos:

- Tener formato de tabla de datos.
- Contener la latitud de la ubicación del dispositivo.
- Contener la longitud de la ubicación del dispositivo.
- Contener la columna de métrica numérica del dispositivo.
- Tener el nombre de la localización del dispositivo.

Tal como se puede ver en la Tabla 3, Será necesario consultar las tablas "*history_text*", "*hosts*", "*items*" y "*host_inventory*" para obtener la información requerida. Se utiliza un código de colores para identificar las relaciones de las claves primarias entre las tablas.

Tabla BBDD	Columna 1	Columna 2	Columna 3
history_text	itemid	clock	value
hosts	hostid	hostname	
items	itemid	name	hostid
host_inventory	hostid	location_lon	location_lat

Tabla 3 - Relación de tablas y columnas de la *BBDD* de Zabbix

Por lo tanto, la consulta finalmente obtendrá los siguientes valores:

- Tabla "*history_text*", valores "*clock*" y "*value*".
- Tabla "*hosts*", valor "*name*".
- Tabla "*host_inventory"*, valores "*location_lon*" y "*location_lat*".

Se decide configurar un cuadro de mando en el que se visualice geo posicionar los últimos valores recogidos de latencias entre cada uno de los complejos (en concreto, las *IP* públicas de los dispositivos FortiGate) y el *Datancenter*, por lo que la consulta en base de datos requerida para mostrar esta información es la siguiente:

```
SELECT TBL.clock as time_sec, TBL.NOMBRE_HOST as name, CAST(TBL.value as UNSIGNED) as value, HI.location_lat, HI.location_lon
FROM
        (SELECT HI.*, H.NOMBRE_HOST, H.hostid
        FROM history_text HI
        INNER JOIN (SELECT itemid, MAX(clock) AS MAX_CLOCK FROM history_text GROUP BY itemid) HI1 ON HI.itemid = HI1.itemid AND HI.clock = HI1.MAX_CLOCK
        LEFT JOIN (SELECT H.hostid, H.host AS NOMBRE_HOST, I.itemid FROM hosts H INNER JOIN (SELECT hostid, itemid FROM items WHERE name = 'latencia') I ON H.hostid = I.hostid WHERE H.host like '%forti%') H ON HI.itemid = H.itemid

        WHERE H.NOMBRE_HOST IS NOT NULL
        ) TBL
        INNER JOIN host_inventory HI on TBL.hostid=HI.hostid
```

Por último, en forma de tabla los últimos valores de latencias de complejos recibidos con una estructura Dispositivo-Latencia, se requiere realizar modificaciones a la hora de obtener la información, de tal forma que la consulta utilizada es:

```
SELECT TBL.NOMBRE_HOST as Dispositivo, TBL.value as 'Latencia (ms)'
FROM
        (SELECT HI.*, H.NOMBRE_HOST, H.hostid
        FROM history_text HI
        INNER JOIN (SELECT itemid, MAX(clock) AS MAX_CLOCK FROM history_text GROUP BY itemid) HI1 ON HI.itemid = HI1.itemid AND HI.clock = HI1.MAX_CLOCK
        LEFT JOIN (SELECT H.hostid, H.host AS NOMBRE_HOST, I.itemid FROM hosts H INNER JOIN (SELECT hostid, itemid FROM items WHERE name = 'latencia') I ON H.hostid = I.hostid WHERE H.host like '%forti%') H ON HI.itemid = H.itemid

        WHERE H.NOMBRE_HOST IS NOT NULL
        ) TBL
        INNER JOIN host_inventory HI on TBL.hostid=HI.hostid
```

4.7 Resultados obtenidos en la fase

Con Grafana se han realizado dos cuadros de mando, que muestran la siguiente información:

- Tasa de carga/descarga en complejos:

  Tal como se muestra en la Figura 57, ésta representa las tasas de descarga con formato de título “Nombre_Complejo DW”, el cual camba de color verde a rojo cuando se superan los 20Mbps de descarga en el ancho de banda de la conexión a *Internet*.
  En el caso de las tasas de subida se representan en color azul, con formato de título “Nombre_Complejo UP”. No existe variación de representación de color en estos paneles debido a que se considera no crítico el ancho de banda de subida en los complejos.

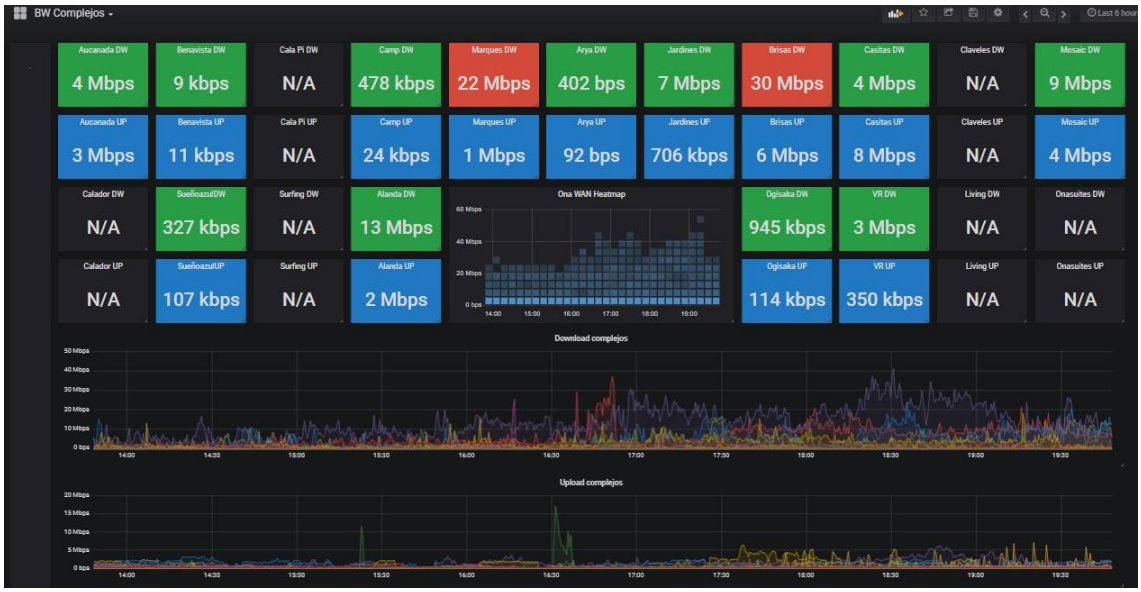


Figura 57 - Tasa de carga y descarga de FortiGate de la organización

Cabe destacar que los paneles que muestran información (N/A) es debido a que los complejos permanecen cerrados, por lo que la monitorización de los dispositivos en la herramienta Zabbix están deshabilitados y Grafana no consigue recabar información para mostrar.

- Latencias geolocalizadas:

  Como se puede ver en la Figura 58, se ha configurado un cuadro de mando que habilita visualizar las latencias de conexión entre los complejos y el *Datacenter*.

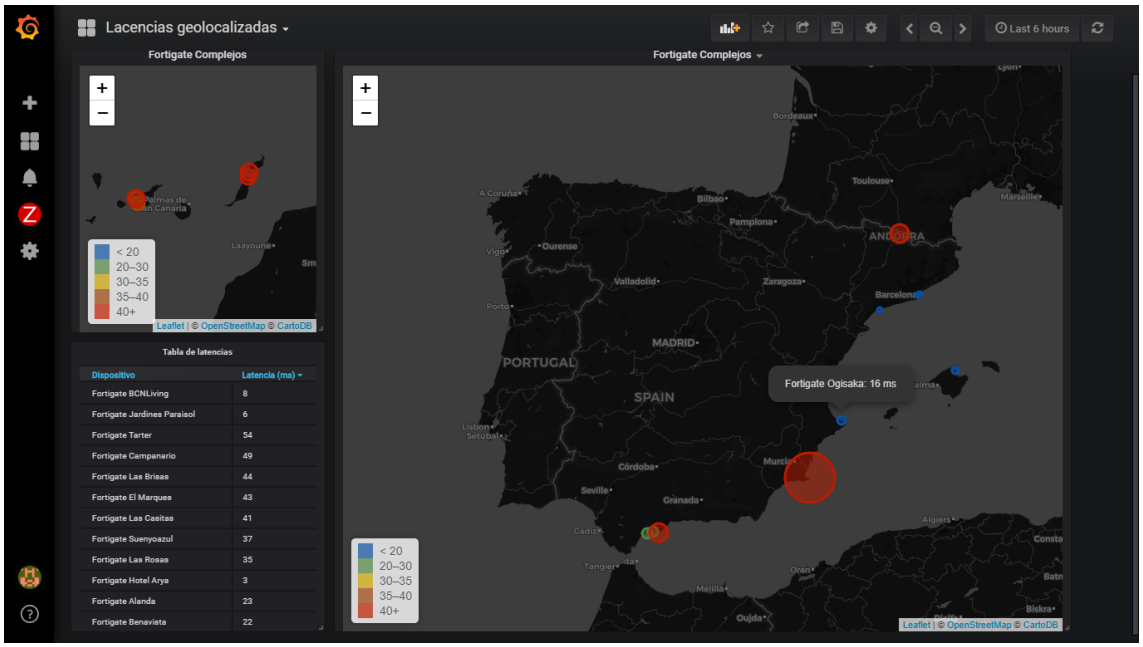


Figura 58 - Gráfica de latencias entre complejos y Central geolocalizadas

Las combinaciones de estos dos cuadros de mando habilitan la posibilidad de analizar con mayor precisión los sucesos que puedan ocurrir en la operativa diaria de la organización. Por ejemplo, permiten detectar el motivo por el cual se experimentan tiempos de espera elevados en la ejecución de operaciones con el *PMS* hotelero ya que:

- Si el valor de latencia es alta y la tasa de subida o descarga son altas, el problema probablemente radique en un consumo excesivo por alguno de los dispositivos del complejo afectado

- Si el valor de latencia es alta y las tasas de subida o descarga no han sufrido una variación significativa, probablemente existan problemas de servicio de la operadora de conexión a *Internet*.

Es evidente pues, la capacidad de control y análisis que proporciona tanto la herramienta de monitorización Zabbix como la herramienta de análisis y visualización de métricas Grafana.

5. Material

El material utilizado durante la realización de este trabajo final de grado es el siguiente:

A nivel de *hardware*:

- Entorno de desarrollo: Intel NUC I7 16GB RAM 256GB SSD

- Entorno de producción: HP Proliant DL 380GB 32GB RAM y 2 procesadores con ocho núcleos de 2Ghz.

A nivel de *software*:

- Entorno de desarrollo: Entorno VMWare *ESXi* 6.7, CentOS 7, Zabbix 4.0, Grafana, Microsoft Power BI, Tableau.

- Entorno de producción: VMware vSphere 5.5 Essentials Plus, CentOS 7, Zabbix 4.0, Herramientas de análisis geolocalizado de *KPI*.

6. Previsión del coste económico

A pesar de que Zabbix, Grafana y CentOS no comportan un coste para la implantación de este proyecto, la previsión del coste económico de la puesta en marcha de este sistema de monitorización en una organización puede diferir por el alojamiento del *software*.

Cabe la posibilidad de ejecutar tanto Zabbix como Grafana en un único dispositivo que ejecute el sistema operativo CentOS, por lo que sólo será necesario definir en qué dispositivo y en qué modo se ejecutará el sistema. Existen las siguientes posibilidades:

- Ejecución en local mediante *software* virtualizador:

  Este tipo de *software* permite visualizar un segundo sistema operativo compartiendo los recursos disponibles por el sistema operativo anfitrión. Si se posee el recurso previamente, el coste de implantación será cero. Existen soluciones gratuitas, como Oracle VM Virtualbox.

- Ejecución en local mediante la instalación en una máquina física:

  La instalación directa del sistema operativo sobre el dispositivo aportará un mayor rendimiento respecto a la ejecución en local mediante *software* virtualizador. Sin embargo, si no se posee un dispositivo para realizar la instalación tendrá que ser adquirido uno con recursos similares a los de un ordenador personal de gama media-alta, con un coste aproximado de 500-800€.

- Ejecución en la nube mediante servicios de hosting

  Permitir que las tareas de computación se realicen desde la nube liberan al departamento de *IT* del mantenimiento derivado de la utilización de una máquina física. Sin embargo, comporta un coste mensual y la instalación de Zabbix sería más compleja, requiriendo una máquina virtual con Zabbix Proxy que recabase toda la información de la red y la enviase al servidor de Zabbix, que se alojaría fuera de los límites de la red local. Por ello, con la situación dada no es viable esta solución.

- Ejecución en un servidor virtualizador dedicado:

  Ejecutar el sistema operativo en una máquina virtual alojada en un servidor físico que ofrece servicios de virtualización es la mejor opción en el caso estudiado. Sin embargo, para ello se requiere un servidor, por

lo que el coste normalmente supera los 1000 euros, y por tanto es superior a la solución de ejecución local mediante una máquina física.

Teniendo en cuenta que se promueve la utilización de *software* libre, y dadas las opciones anteriormente mencionadas, si la implantación debe hacerse sin tener en cuenta la utilización de recursos existentes previamente, únicamente se requerirá la compra de un ordenador personal que se ajuste a los requisitos de *hardware* y tamaño de infraestructura mostrados en la Tabla 4, considerando que Zabbix es la herramienta que más recursos utilizará:

Tipo de Empresa	Plataforma OS	CPU/Memoria	Base de datos	Hosts monitorizados
Pequeño	CentOS	Aplicación virtual	MySQL InnoDB	100
Medio	CentOS	2 núcleos CPU /2GB	MySQL InnoDB	500
Grande	RedHat Enterprise Linux	4 núcleos CPU /8GB	RAID10 MySQL InnoDB or PostgreSQL	>1000
Muy grande	RedHat Enterprise Linux	4 núcleos CPU /16GB	Fast RAID10 MySQL InnoDB or PostgreSQL	>10000

Tabla 4 - Requisitos de instalación de Zabbix

Actualmente se están monitorizando 72 hosts, lo que está comprendido en una organización de tipo pequeña. Dada la previsión de crecimiento de la infraestructura y la ejecución de varias aplicaciones en el mismo *hardware*, debería elegirse una configuración de *hardware* de tipo grande con 4 núcleos y 8GB de memoria *RAM*.

Por ello, se puede decir que el coste de la implantación de este proyecto es el derivado de la compra de un ordenador de gama media-alta, con un coste aproximado de 500-800€.

7. Líneas futuras de trabajo

Tal como se ha comentado anteriormente en este trabajo final de grado, la herramienta de monitorización Zabbix contiene plantillas con puntos de monitorización y alertas predefinidas. Ello permite un rápido despliegue de la herramienta, pero tras unas semanas en funcionamiento se ha podido detectar la necesidad de ajustar con mayor exactitud tanto como los puntos de monitorización y las alertas de los elementos que son monitorizados, ya que la criticidad de cada sistema cambia según su uso y las capacidades de cada sistema varían según el *hardware* que lo soporta.

Se considera pues, que para poder ajustar correctamente la herramienta de monitorización se necesita tiempo para recopilar información, ser estudiada y valorar si los puntos de monitorización o alertas deberían ser ajustados correctamente o ser eliminados. Por ello, como línea de trabajo futura se revisarán mensualmente las alertas de monitorización detectadas, para así poder identificar y analizar la necesidad de realizar ajustes en la configuración de la herramienta.

8. Conclusiones

Tras la realización de este Trabajo Final de Grado, la conclusión extraída es la necesidad evidente de implantar un sistema de monitorización, siempre que las dimensiones del entorno a monitorizar así lo requieran. Ello permite tomar más control de los sucesos de la infraestructura, detectando fallos y proporcionando la capacidad de analizar y mejorar rendimientos y disponibilidades. Además, teniendo como aspecto positivo el bajo coste de implantación y los altos beneficios que aporta.

Como ejemplo práctico de la necesidad de la implantación de la herramienta durante el proceso de elaboración de este Trabajo Final de Grado se han dado los siguientes casos prácticos:

- Disponibilidad de red: Se han detectado en varias ocasiones fallos de disponibilidad de servicio de *Internet* en algunos de los complejos monitorizados permitiéndonos agilizar los trámites de reclamo de avería.

- Se han detectado alertas de consumo de memoria *RAM* en el dispositivo FortiGate de la sede Central, lo cual nos ha llevado en ocasiones anteriores a perder la conectividad con el resto de la red. Gracias al sistema de monitorización se detectó el aumento significativo de *RAM* del dispositivo, se pudo analizar cuál era el problema que causaba el problema y permitió buscar soluciones.

Además, mediante el uso de Grafana y Power BI se ha conseguido representar sobre un mapa del mundo los *KPI* geolocalizados, proporcionando así un valor añadido para la organización, que está en plena fase de expansión y la visualización geolocalizada será importante para futuras reuniones del equipo de *IT*.

La metodología y el seguimiento de la planificación ha sido la correcta, dado que se han conseguido tanto el resultado final esperado como se han cumplido los plazos establecidos.

9. Glosario

A continuación, se muestran las definiciones de los términos y acrónimos más relevantes utilizados dentro de la Memoria.

- *KPI*: Indicador de clave de rendimiento de un recurso informático que permiten medir la eficacia de este.

- CentOS 7: Sistema operativo con licencia de *software* libre Linux basado en la distribución Red Hat Enterprise Linux.

- Zabbix: Solución para la monitorización en tiempo real de servicios de red, servidores y *hardware* de red.

- Monitorización: Proceso de recopilación, agregación y análisis de valores para mejorar el conocimiento y el comportamiento de un sistema.

- PDF: Formato de documento que permite almacenar documentos digitales independientemente de las plataformas de *software* o *hardware*.

- Entorno desarrollo: Entorno teóricamente con características similares al entorno de producción que se utiliza para probar aplicaciones.

- Entorno producción: Entorno donde se realizan todas las transacciones reales de la organización.

- *Datacenter*: Centro donde, en un lugar con condiciones y rendimiento óptimo, se almacenan, se tratan y se distribuyen los datos de la empresa al personal o procesos autorizados.

- Enrutador: Dispositivo o mecanismo que permite direccionar la información o comunicaciones entre distintos sistemas de información o aplicaciones.

- CHAR: Tarificador y control de llamadas telefónico.

- *VPN*: Red Privada Virtual que permite, mediante un túnel donde las comunicaciones son cifradas, una conexión a través de *Internet* a una red local.

- MS SQL: Sistema de base de datos desarrollado por la empresa Microsoft.

- Rack: Estructura que permite sostener o albergar un dispositivo tecnológico.

- SSH: Protocolo que facilita las comunicaciones seguras entre dos sistemas utilizando una arquitectura cliente/servidor y mediante una sesión de conexión encriptada.

- WAN: Red privada distribuida de telecomunicaciones que permite interconectar redes de área local entre sí.

- NAS: Dispositivo que ofrece servicio de almacenamiento en red.

- MacroLAN: Solución que permite construir redes privadas virtuales de banda ancha con las mismas velocidades y prestaciones que si estuviesen ubicadas localmente.

- Fingerprint: Tecnología capaz de identificar de manera precisa y única a una persona por medio de su huella digital.

- MariaDB: Servidor de código libre de base de datos.

- Hostmonitor: Herramienta de monitorización remota de servidores, red y sistemas similar a Zabbix.

- OPManager: Herramienta de monitorización remota de servidores, red y sistemas similar a Zabbix.

- Nagios: Herramienta de monitorización remota de servidores, red y sistemas similar a Zabbix.

- Grafana: Herramienta de código abierto para el análisis y visualización de métricas de herramientas de monitorización.

- *API*: Conjunto de protocolos y herramientas usadas por desarrolladores para crear programas específicos para ciertos sistemas operativos.

- Máquina virtual: *software* que simula un sistema de computación y que puede ejecutar programas como si fuese una computadora real.

- *ESXi*: Es una capa de virtualización que pertenece a VMware y que permite ejecutar diversos sistemas operativos sobre la misma máquina física

- Datastore: Espacio de almacenamiento de un Host de VMware para almacenar Máquinas Virtuales, Plantillas y/o ficheros ISO. Pueden tener formato NFS o VMFS

- BBDD: Es un almacén de datos que permite guardar grandes cantidades de información de forma organizada para poder encontrarla fácilmente.

- *Back-up*: Copia de seguridad de información.

- *OVF*: Mecanismo de transporte de plantillas de máquinas virtuales.

- *VMDK*: Disco duro virtual que almacena el contenido del disco duro de la máquina virtual

- *IP*: Es una matrícula identificativa que define un dispositivo en la red.

- *Items*: Elementos que recopilan información de monitorización.

- *Triggers*: Alertas de monitorización que aparecen tras superar un umbral definido.

- Conmutador (Switch): Dispositivo de interconexión de redes informáticas, también llamado conmutador.

- Agente: Permite realizar operaciones como recopilar información para enviarlas o almacenarlas.

- Powershell: Consola de sistema orientada a administradoras que permite realizar tareas con un mayor control sobre el sistema.

- Cortafuegos: Primera línea de defensa ante un ataque desde *Internet* a la red que se desea proteger.

- *Bash*: Intérprete de comandos que ejecuta las instrucciones introducidas por el usuario o contenidas en un script y devuelve los resultados.

- *CIFS*: Protocolo de compartición de archivos.

- Script: Código de programación que contiene comandos u órdenes normalmente sencillas que se ejecutan de manera secuencial para controlar el comportamiento de un programa específico o interactuar con el sistema operativo.

- *Crontab*: Archivo de texto que posee una lista con los scripts a ejecutar.

- *Log*: es un registro donde se graban los acontecimientos (eventos o acciones) que explican el comportamiento de sistemas o programas.

- *ACK*: Indica que la información ha sido recibida y leída.

10. Bibliografía

- COMPUTERWOLD (2009). *Cómo medir el rendimiento de las TI en la empresa*. Recuperado el día 12/10/2018 de https://www.computerworld.es/archive/como-medir-el-rendimiento-de-las-ti-en-la-empresa

- Sethi, A. (2015). *Nagios Vs. Zabbix Vs. PRTG Vs. Spiceworks Vs. Solarwinds Network Performance Monitor*. Recuperado el día 12/10/2018 de https://www.itcentralstation.com/product_reviews/zabbix-review-32935-by-anuj-sethi

- Nagios (2018). *Case Studies – Nagios*. Recuperado el día 12/10/2018 de https://www.nagios.com/casestudies/#Testimonials

- Kumar, C. (2018). *5 Best Open Source Monitoring Software for IT Infrastructure*. Recuperado el día 12/10/2018 de https://geekflare.com/best-open-source-monitoring-software/

- Digital Guide (2017). *¿Qué es CentOS? Versiones CentOS y requisitos de sistema*. Recuperado el día 12/10/2018 de https://www.1and1.es/digitalguide/servidores/know-how/que-es-centos-versiones-y-requisitos-del-sistema/

- Javier (2017). *Las 16 mejores herramientas de monitoreo de Redes de 2016*. Recuperado el día 12/10/2018 de https://blog.pandorafms.org/es/herramientas-de-monitoreo-de-redes/

- Vidmar, A. (2007). *Zabbix: State-of-the-art network monitoring*. Recuperado el día 12/10/2018 de https://www.linux.com/news/zabbix-state-art-network-monitoring?tid=129

- Ks-Soft (2018). *Advanced Host Monitor*. Recuperado el día 13/10/2018 de https://www.ks-soft.net/hostmon.eng/index.htm

- FinancesOnline (2018). *Compare Zabbix vs. ManageEngine OpManager*. Recuperado el día 13/10/2018 de https://comparisons.financesonline.com/manageengine-opmanager-vs-zabbix

- ITConsultants Colombia S.A.S (2018). *OpManager*. Recuperado el día 13/10/2018 de https://www.itcc.com.co/opmanager.html

- RoseHosting (2018). *How To Install Zabbix 3.4 Server On CentOS 7*. Recuperado el día 13/10/2018 de https://www.rosehosting.com/blog/how-to-install-zabbix-3-4-server-on-centos-7/

- Elliongwood, J. (2017). *An Introduction to Metrics, Monitoring, and Alerting*. Recuperado el día 13/10/2018 de https://www.digitalocean.com/community/tutorials/an-introduction-to-metrics-monitoring-and-alerting

- SUSHAIN (2017). *5 ways to add or change hostname in RHEL/CentOS 7*. Recuperado el día 16/10/2018 de https://linuxtechlab.com/5-ways-add-hostname-rhel-centos/

- Adobe (2018). *¿Qué es el formato PDF?* Recuperado el día 26/10/2018 de https://acrobat.adobe.com/es/es/acrobat/about-adobe-pdf.html

- Jummp. *Un buen entorno de preproducción*. Recuperado el día 26/10/2018 de https://jummp.wordpress.com/2009/06/24/un-buen-entorno-de-preproduccion/

- acensBlog (2008). *¿Qué es un Datacenter?* Recuperado el día 26/10/2018 de https://blog.acens.com/acens/que-es-un-data-center/

- Sanchez Iglesias, A (2016). *¿Qué es un router?* Recuperado el día 26/10/2018 de https://www.aboutespanol.com/que-es-un-router-841387

- CHAR. Soluciones hoteleras. Recuperado el día 26/10/2018 de http://www.char.es/soluciones-hoteleras/

- Ramírez, I (2016). *¿Qué es una conexión VPN, para qué sirve y qué ventajas tiene?* Recuperado el día 27/10/2018 de: https://www.xataka.com/seguridad/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

- Rouse, M. (2017). *Microsoft SQL Server*. Recuperado el día 27/10/2018 de https://searchsqlserver.techtarget.com/definition/SQL-Server

- Perez Porto, J. Gardey, A. (2013). *Definición de rack*. Recuperado el día 27/10/2018 de https://definicion.de/rack/

- MIT. Red Hat Enterprise Linux 4: Manual de referencia. Recuperado el día 27/10/2018 de https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html

- Rouse, M. (2016). *WAN (wide area network).* Recuperado el día 27/10/2018 de https://searchenterprisewan.techtarget.com/definition/WAN

- TIREA (2018). *Soluciones para: Acceso / MacroLAN*. Recuperado el día 28/10/2018 de https://www.tirea.es/Menu/Entidades-Aseguradoras/Diversos/Redes-y-Correo/Acceso/MicroLan.aspx

- Mariadb (2018). *About MariaDB*. Recuperado el día 28/10/2018 de https://mariadb.org/about

- Wikipedia (2018). *Fingerprint (computing)*. Recuperado el día 28/10/2018 de https://en.wikipedia.org/wiki/Fingerprint_(computing)

- ABC (2015). *¿Qué es una API y para qué sirve?* Recuperado el día 09/11/2018 de https://www.abc.es/tecnologia/consultorio/20150216/abci-201502132105.html

- Reichardt, J. (2014). *Introduction to Grafana*. Recuperado el día 09/11/2018 de https://thepracticalsysadmin.com/introduction-to-grafana/

- Leonhardt, L. (2016) *¿Qué es ESXi y cómo es una máquina virtual?* Recuperado el día 09/11/2018 de https://www.ymant.com/blog/que-es-esxi-y-como-es-una-maquina-virtual

- Penalva, J. (2018) *Intel NUC (Core I7 e Intel Octane), análisis: un PC configurable en formato compacto para el salón o el trabajo*. Recuperado el día 09/11/2018 de https://www.xataka.com/analisis/intel-nuc-core-i7-e-intel-octane-analisis-un-pc-configurable-en-formato-compacto-para-el-salon-o-el-trabajo

- Diaz, A. (2017) *¿Qué son los LOGS y por qué deben interesarte?* Recuperado el día 25/11/2018 de https://dbi.io/es/blog/que-son-los-logs/

- Leonhardt, L (2017) *¿Qué es ESXi y cómo es una máquina virtual?* Recuperado el día 25/11/2018 de https://www.ymant.com/blog/que-es-esxi-y-como-es-una-maquina-virtual

- Cinalli, F (2012). *50 Conceptos de VMware para los que recién comienzan con la virtualización*. Recuperado el día 25/11/2018 de http://federicocinalli.com/blog/item/98-50-conceptos-de-vmware-para-los-que-recien-comienzan-con-virtualizacion

- Pérez Valdés, D (2007). *¿Qué son las bases de datos?* Recuperado el día 26/11/2018 de http://www.maestrosdelweb.com/que-son-las-bases-de-datos/

- Selva, G (2018) *Backup ¿Qué es? Y, ¿Cuáles son los beneficios de realizarlo?* Recuperado el día 26/11/2018 de https://www.clavei.es/blog/backup-que-es/

- Dawson, T (2016) *Introduction to the Windows Command Line with Powershell.* Recuperado el día 26/11/2018 de https://programminghistorian.org/en/lessons/intro-to-powershell

- Mon, A. Estanyo, M. Lopez Gil, F. De Maria, E. (2018) *Definición de un proceso de implantación de sistemas*. Recuperado el día 26/11/2018 de http://sedici.unlp.edu.ar/handle/10915/20124

- Murillo, F (2011) *¿Qué es el Open Virtualization Format?* Recuperado el día 26/11/2018 de https://www.josemariagonzalez.es/cloud-computing/que-es-open-virtualization-format.html

- Carbajo, A. (2018) *La IP ¿Qué es? ¿Cómo funciona? ¿Puedo ocultarla?* Recuperado el día 27/11/2018 de https://www.nobbot.com/tecnologia/mi-conexion/cuarto-especial-sobre-los-routers-la-ip-que-es-como-funciona-puedo-ocultarla/

- Serra Pujadas, O. (2009) *Explicación Tablas de la BBDD de Zabbix*. Recuperado el día 27/11/2018 de http://zabbix-es.blogspot.com/2009/06/explicacion-tablas-de-la-bbdd-de-zabbix.html

- Zabbix (2018). *Requirements*. Recuperado el día 24/12/2018 de https://www.zabbix.com/documentation/3.4/manual/installation/requirements