



**Implementación de plataforma de monitoreo de variables de desempeño  
ópticas de interfaces OpenZR+ sobre plataformas desagregadas por medio de  
Zabbix y Grafana para aplicaciones IPoDWDM**

Mateo Muñoz Arroyave

Informe final para optar al título de Ingeniera de Telecomunicaciones

Semestre de Industria

Asesora Interna

Ana María Cárdenas Soto, PhD

Asesor Externo

Hernán Darío Yepes Montoya,

Msc en Ingeniería de Telecomunicaciones

Universidad de Antioquia

Facultad de Ingeniería

Ingeniería de Telecomunicaciones

Medellín, Antioquia

2024

Cita	Muñoz Arroyave Mateo
<b>Referencia</b>	[1] M. Muñoz Arroyave, “Implementación de plataforma de monitoreo de variables de desempeño ópticas de interfaces OpenZR+ sobre plataformas desagregadas por medio de Zabbix y Grafana para aplicaciones IPoDWDM”, Semestre de Industria, Ingeniería de Telecomunicaciones, Universidad de Antioquia, Medellín, 2024.
Estilo IEEE (2020)	



**Repositorio Institucional:** <http://bibliotecadigital.udea.edu.co>

Universidad de Antioquia - [www.udea.edu.co](http://www.udea.edu.co)

**Rector:** John Jairo Arboleda Céspedes.

**Decano/Director:** Julio César Saldarriaga Molina.

**Jefe departamento:** Eduard Emiro Rodríguez Ramírez.

El contenido de esta obra corresponde al derecho de expresión de los autores y no compromete el pensamiento institucional de la Universidad de Antioquia ni desata su responsabilidad frente a terceros. Los autores asumen la responsabilidad por los derechos de autor y conexos.

## **Dedicatoria**

Dedico este trabajo a Dios, por las enseñanzas y la fortaleza que me ha brindado a lo largo de mi vida académica y personal. A mi familia, por su apoyo incondicional en cada momento difícil, siempre motivándome a no rendirme hasta alcanzar mis metas. A mis profesores desde la escuela, quienes con su paciencia y dedicación despejaron mis dudas durante mi vida académica, compartiendo su valiosa experiencia.

Especialmente, dedico este trabajo a mis padres, quienes han sido el motor de mi vida y un ejemplo a seguir por su lucha y perseverancia, siempre esforzándose por sacar a nuestra familia adelante frente a las adversidades.

## **Agradecimientos**

Quiero expresar mi más profundo agradecimiento a mis padres, quienes, a través de su lucha y perseverancia, me inculcaron valores éticos y morales que han sido fundamentales en toda mi trayectoria académica. Agradezco también a todos los profesores del Departamento de Ingeniería Electrónica y de Telecomunicaciones de la UdeA, a la empresa Padtec y a mis asesores, cuya experiencia y apoyo me han brindado los conocimientos necesarios para desarrollar este documento.

## CONTENIDO

RESUMEN .....	14
ABSTRACT .....	15
I. INTRODUCCIÓN.....	16
II. OBJETIVOS.....	19
1. OBJETIVO GENERAL .....	19
2. OBJETIVOS ESPECÍFICOS .....	20
III. PRESENTACIÓN DE LA EMPRESA .....	20
IV. MARCO TEÓRICO .....	21
1. HISTORIA DE LAS COMUNICACIONES ÓPTICAS.....	21
2. PARÁMETROS DE LA RED DWDM .....	21
2.1. Descripción de las redes DWDM .....	21
2.3. Direcciones de propagación de la señal DWDM .....	22
2.4. Ancho de banda en sistemas DWDM .....	23
2.5. Potencia en sistemas DWDM .....	23
2.6. Tasa de bit de error (BER).....	24
2.7. Ruido óptico.....	24
3. ELEMENTOS DE LA RED DWDM .....	25
3.1. Fuentes de luz .....	25
3.2. Multiplexores.....	25
3.3. Amplificadores ópticos .....	26
3.3.1. Amplificadores EDFA .....	26
4. ROUTER.....	27
5. SWITCH .....	28
6. SERVIDOR.....	29

<b>7. MONITOREO</b> .....	30
<b>7.1. Tipos de monitoreo</b> .....	30
<b>7.2. Protocolos y Técnicas de monitoreo de Redes</b> .....	31
<b>8. SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)</b> .....	31
<b>8.1. Agente SNMP</b> .....	32
<b>9. MIB</b> .....	33
<b>10. ZABBIX</b> .....	34
<b>10.1. Funcionamiento de Zabbix</b> .....	34
<b>10.2. Ventajas de Zabbix</b> .....	35
<b>10.3. Características de Zabbix</b> .....	36
<b>11. ELEMENTOS DE ZABBIX</b> .....	38
<b>11.1. Servidor Zabbix</b> .....	38
<b>11.2. Agente Zabbix</b> .....	39
<b>11.3. Ítems</b> .....	40
<b>11.4. Host y grupos de hosts</b> .....	40
<b>11.5. Plantillas o templates</b> .....	40
<b>11.6. Discovery</b> .....	41
<b>11.7. Interfaz web</b> .....	41
<b>V. METODOLOGÍA</b> .....	42
<b>VI. RESULTADOS</b> .....	43
<b>1. IMPLEMENTACIÓN DEL HYPER-V EN EL SERVIDOR</b> .....	43
<b>2. IMPLEMENTACIÓN DEL SISTEMA DE MONITOREO</b> .....	45
<b>2.1. Instalación del servidor Zabbix 7.0 LTS</b> .....	45
<b>2.1.1. Instalación del repositorio de Zabbix</b> .....	46
<b>2.1.2. Instalación del servidor, la interfaz y el agente de Zabbix</b> .....	46

2.1.3.	<i>Creación de la base de datos inicial</i> .....	47
2.1.4.	<i>Importación del esquema y los datos iniciales</i> .....	48
2.1.5.	<i>Configuración de la base de datos para el servidor Zabbix</i> .....	48
2.1.6.	<i>Iniciación de los procesos del agente y del servidor Zabbix</i> .....	49
2.1.7.	<i>Verificación del estado del servidor Zabbix</i> .....	49
2.1.8.	<i>Configuración de la interfaz web</i> .....	50
2.1.9.	<i>Comprobación de prerrequisitos</i> .....	51
2.1.10.	<i>Configuración de la conexión a la base de datos</i> .....	51
2.1.11.	<i>Ajustes adicionales</i> .....	52
2.1.12.	<i>Resumen de preinstalación</i> .....	53
2.1.13.	<i>Instalación de Zabbix</i> .....	53
2.1.14.	<i>Inicio de sesión al servidor</i> .....	54
2.1.15.	<i>Interfaz web de Zabbix</i> .....	54
2.2.	<b>Creación de grupos de Host y de un Host</b> .....	55
2.2.1.	<i>Configuración grupo de Host</i> .....	55
2.2.2.	<i>Configuración del Host</i> .....	56
2.2.4.	<i>Verificación de la configuración SNMP</i> .....	58
2.2.5.	<i>Parámetros a monitorear</i> .....	58
2.2.6.	<i>Creación de nuevos parámetros</i> .....	59
2.2.7.	<i>Configuración de monitores</i> .....	60
2.2.8.	<i>Configuración de las gráficas</i> .....	62
2.2.9.	<i>Verificación de las gráficas</i> .....	63
3.	<b>RESULTADOS DE LAS GRÁFICAS DE LOS PARÁMETROS PRINCIPALES MONITOREADOS</b> .....	64
3.1.	<i>Monitoreo de potencia de entrada y salida en la interfaz OpenZR+</i> .....	64

3.2.	<i>Monitoreo de OSNR en la interfaz OpenZR+ del router UfiSpace</i> .....	64
3.3.	<i>Monitoreo PREFEC y TEMPERATURA del receptor en la interfaz OpenZR+ </i> .....	65
3.4.	<i>Monitoreo tráfico en la red.</i> .....	66
3.5.	<i>Implementación de Informes y Alarmas</i> .....	66
3.5.1.	<i>Configuración de Informes programados en Zabbix</i> .....	66
4.	<b>DESAGREGACIÓN DE LAS VARIABLES EN GRAFANA</b> .....	71
4.1.	<b>Instalación del servidor Grafana</b> .....	72
4.1.1.	<i>Configuración de los prerequisites</i> .....	72
4.1.2.	<i>Instalación del repositorio Grafana</i> .....	73
4.1.3.	<i>Instalación de Grafana</i> .....	73
4.1.4.	<i>Inicio de los procesos del servidor Grafana</i> .....	74
4.1.5.	<i>Verificación del estado del servidor</i> .....	75
4.1.6.	<i>Configuración de la interfaz web</i> .....	75
4.1.7.	<i>Interfaz web de Grafana</i> .....	76
4.1.8.	<i>Instalación del plugin de Zabbix</i> .....	76
4.1.9.	<i>Habilitación del plugin de Zabbix en Grafana</i> .....	77
4.2.	<b>Creación del Dashboard</b> .....	77
4.2.1.	<i>Configuración de los hosts en Grafana</i> .....	78
4.2.2.	<i>Dashboard de monitoreo</i> .....	79
5.	<b>RESULTADOS DEL MONITOREO EN EL DASHBOARD INTEGRADO</b> .....	79
5.1.	<i>Estado operacional de la interfaz OpenZR+, potencia de entrada y salida</i> .....	80
5.2.	<i>Tasa de transferencia, velocidad, paquetes enviados y recibidos</i> .....	80
5.3.	<i>OSNR, TEMPERATURA Y PRE-FEC</i> .....	81
VII.	<b>CONCLUSIONES</b> .....	82
VIII.	<b>REFERENCIAS</b> .....	83



**IX. ANEXOS** .....84

**ANEXO A:** Características Equipo UfiSpace .....84

**ANEXO B:** Características Switche Datacom.....85

**LISTA DE TABLAS**

**Tabla 1** Metodología a implementar .....42

**Tabla 2** OID que identifica los parámetros. ....60

## LISTA DE FIGURAS

<b>Fig. 1</b> Gestión de monitoreo equipos ópticos.....	16
<b>Fig. 2</b> Visualización de parámetros de los UfiSpace .....	17
<b>Fig. 3</b> Dashboard final soluciones IPoDWDM .....	18
<b>Fig. 4</b> Proceso de configuración.....	19
<b>Fig. 5</b> Esquema de red DWDM.....	22
<b>Fig. 6</b> Tipos de multiplexores ópticos.....	26
<b>Fig. 7</b> Enrutador Ufispac .....	28
<b>Fig. 8</b> Switch DM4370.....	29
<b>Fig. 9</b> Servidor PowerEdge R660xs.....	30
<b>Fig. 10</b> Topología implementada .....	34
<b>Fig. 11</b> Configuración Servidor para gestión de máquinas virtuales .....	43
<b>Fig. 12</b> Configuración Hyper-V Cliente .....	44
<b>Fig. 13</b> Conexión remota al servidor.....	44
<b>Fig. 14</b> Instalación del repositorio de la página oficial.....	46
<b>Fig. 15</b> Instalación de Zabbix server, la interfaz y el agente Zabbix .....	46
<b>Fig. 16</b> Creación de la base de datos inicial MySQL.....	47
<b>Fig. 17</b> Configuración de la base de datos .....	48
<b>Fig. 18</b> Inicio de los procesos del agente y del servidor Zabbix.....	49
<b>Fig. 19</b> Estado del servidor Zabbix .....	49
<b>Fig. 20</b> Estado del agente Zabbix.....	50
<b>Fig. 21</b> Interfaz de bienvenida.....	50
<b>Fig. 22</b> Verificación de prerequisites en la interfaz web .....	51
<b>Fig. 23</b> Configuración de la conexión a la base de datos .....	52
<b>Fig. 24</b> Ajustes adicionales del servidor .....	52
<b>Fig. 25</b> Resumen de la preinstalación .....	53
<b>Fig. 26</b> Instalación exitosa de la interfaz web.....	53
<b>Fig. 27</b> Inicio de sesión Zabbix.....	54
<b>Fig. 28</b> Panel de control del servidor .....	55
<b>Fig. 29</b> Creación del grupo de host “Proyecto” .....	56
<b>Fig. 30</b> Configuración del host.....	57

<b>Fig. 31</b> Dispositivos enlazados con SNMP.....	58
<b>Fig. 32</b> Parámetros determinados por la plantilla .....	59
<b>Fig. 33</b> Configuración del monitor.....	61
<b>Fig. 34</b> Preprocesamiento de la variable .....	61
<b>Fig. 35</b> Verificación del valor recopilado .....	62
<b>Fig. 36</b> Potencia de salida desde el router.....	62
<b>Fig. 37</b> Configuración de la gráfica .....	63
<b>Fig. 38</b> Potencia de entrada y Potencia de salida de la interfaz OpenZR+ del router.....	64
<b>Fig. 39</b> OSNR de la interfaz OpenZR+ del router .....	65
<b>Fig. 40</b> Pre-FEC y Temperatura del módulo en la interfaz OpenZR+ del router .....	65
<b>Fig. 41</b> Parámetros obtenidos por la plantilla predeterminada.....	66
<b>Fig. 42</b> Configuración del Web Service.....	68
<b>Fig. 43</b> Configuración de los servicios.....	68
<b>Fig. 44</b> Configuración de la URL.....	69
<b>Fig. 45</b> Configuración del reporte periódico.....	70
<b>Fig. 46</b> Envío del reporte.....	70
<b>Fig. 47</b> Correo recibido .....	71
<b>Fig. 48</b> Instalación de prerequisites servidor Grafana .....	72
<b>Fig. 49</b> Configuración de los Key GPG .....	73
<b>Fig. 50</b> Instalación del repositorio de la página oficial Grafana .....	73
<b>Fig. 51</b> Instalación de Grafana .....	74
<b>Fig. 52</b> Inicio de los procesos del servidor Grafana.....	74
<b>Fig. 53</b> Habilidad del servidor.....	74
<b>Fig. 54</b> Verificación del estado del servidor .....	75
<b>Fig. 55</b> Inicio de sesión de Grafana.....	75
<b>Fig. 56</b> Interfaz web de Grafana.....	76
<b>Fig. 57</b> Instalación del plugin.....	76
<b>Fig. 58</b> Reinicio del servidor.....	77
<b>Fig. 59</b> Habilidad del Plugin en Grafana.....	77
<b>Fig. 60</b> Creación del Dashboard.....	78
<b>Fig. 61</b> Configuración del host en Grafana .....	79

**Fig. 62** Visualización de las variables en Grafana (1), .....80  
**Fig. 63** Visualización de las variables en Grafana (2) .....81  
**Fig. 64** visualización de las variables en Grafana (3) .....81

## SIGLAS, ACRÓNIMOS Y ABREVIATURAS

<b>AWG</b>	Rejilla de guía de ondas en matriz
<b>BER</b>	Bit Error Rate
<b>CPU</b>	Central Processing Unit
<b>DEMUX</b>	Demultiplexor
<b>DWDM</b>	Dense Wavelength Division Multiplexing
<b>ICMP</b>	Internet Control Message Protocol
<b>IPoDWDM</b>	Internet Protocol Over Dense Wavelength Division Multiplexing
<b>MAC</b>	Media Access Control
<b>MIB</b>	Management Information Base
<b>MUX</b>	Multiplexor
<b>MySQL</b>	My Structured Query Language
<b>NMS</b>	Network Management System
<b>OSNR</b>	Optical Signal Noise Ration
<b>OSPF</b>	Open Shortest Path First
<b>RTT</b>	Round Trip Time
<b>SNMP</b>	Simple Network Management Protocol
<b>TCP</b>	Transmission Control Protocol
<b>UDP</b>	User Datagram Protocol
<b>VLAN</b>	Virtual Local Area Networks

## RESUMEN

Al momento de implementar soluciones IPoDWDM, resulta complicado evaluar las variables de desempeño debido a la ausencia de un sistema de monitoreo adecuado en las interfaces de los routers. La empresa Padtec realiza un monitoreo constante de puntos críticos en su gestión para asegurar la calidad del servicio ofrecido a sus clientes. Actualmente, el software de monitoreo que utiliza es compatible solo con sus equipos ópticos. La empresa trabaja con equipos como; transponder, amplificadoras, multiplexores, demultiplexores, compensadores de dispersión cromática, sin embargo, no le es posible monitorear routers, switches, que igualmente forman parte de la red entre otros. Dado que cualquier incidente puede causar la interrupción del servicio y generar pérdidas significativas, el objetivo del presente trabajo es implementar una plataforma de monitoreo en tiempo real para las interfaces OpenZR+ en sus routers, utilizando el protocolo simple de administración de red SNMP y el software de monitoreo Zabbix, asegurando el correcto funcionamiento de las aplicaciones IPoDWDM.

Se empleó una metodología aplicada, en la que las instrucciones de control del software desarrollado, se prueban en equipos instalados en entornos reales. Se hizo uso del software de código abierto (Open Source) Zabbix para desagregar datos y realizar pruebas de control. Esta metodología permitió garantizar una plataforma de monitoreo de las variables más relevantes para detectar anomalías o fallas en la transmisión extremo a extremo. Gracias a la interfaz web, la plataforma permite acceder desde cualquier navegador mediante la dirección IP del servidor y utilizar diversas herramientas para el control y monitoreo. Se concluye que la plataforma implementada mejora el rendimiento de las aplicaciones IPoDWDM y asegura un control eficaz de las fallas y degradaciones en las interfaces OpenZR+.

***Palabras clave*** — **OpenZR+, IPoDWDM, Open Source, SNMP, Zabbix, Equipos ópticos de transporte.**

## ABSTRACT

When implementing IPoDWDM solutions, it becomes difficult to evaluate performance variables due to the lack of an adequate monitoring system on the router interfaces. The company Padtec performs constant monitoring of critical points in its management to ensure the quality of the service offered to its customers. Currently, the monitoring software it uses is only compatible with its optical equipment. The company works with equipment such as transponders, amplifiers, multiplexers, demultiplexers, chromatic dispersion compensators; however, it is not able to monitor routers, switches, which are also part of the network, among others. Since any incident can cause service interruptions and generate significant losses, the objective of this work is to implement a real-time monitoring platform for OpenZR+ interfaces on its routers, using the Simple Network Management Protocol (SNMP) and the Zabbix monitoring software, ensuring the proper functioning of IPoDWDM applications.

It was used an applied methodology, in which the control instructions of the developed software are tested on equipment installed in real-world environments. The open-source software Zabbix was used to disaggregate data and conduct control tests. This methodology allowed for the establishment of a monitoring platform for the most relevant variable to detect anomalies or failures in transmission. Thanks to the web interface, the platform allows access from any browser via the server's IP address and provides various tools for control and monitoring. It is concluded that the implemented platform enhances the performance of IPoDWDM applications and ensures effective control of failures and degradations in OpenZR+ interfaces.

***Keywords* — OpenZR+, IPoDWDM, Open Source, SNMP, Zabbix, Optical transport equipment.**

## I. INTRODUCCIÓN

Las telecomunicaciones en la sociedad actual desempeñan un papel muy importante, especialmente en lo que respecta al acceso a internet. En los últimos años y durante la pandemia, la demanda de conectividad creció significativamente, lo que llevo a los proveedores de servicios de internet a aumentar sus capacidades. Tanto proveedores grandes como pequeños expandieron sus redes de fibra óptica por todo el territorio, lo que resultó en un crecimiento de sus infraestructuras y una mayor complejidad en su administración.

El mantenimiento de una infraestructura eficiente y el adecuado desempeño de la red son factores clave para el funcionamiento óptimo de un proveedor. La gestión y monitoreo remoto de los dispositivos deben ser confiables y precisos para asegurar la integridad de la red y proporcionar un servicio de calidad.

Actualmente, la empresa utiliza la gestión de monitoreo de manera exclusiva para los equipos ópticos, como los transponder, amplificadores, entre otros. A través de esta gestión, es posible visualizar los parámetros de monitoreo a través de la siguiente interfaz mostrada en la Fig 1. En esta figura se observa por ejemplo en LINE 2 los parámetros más relevantes, los cuales nos ayudan a mejorar significativamente un enlace DWDM, como lo son OSNR, Pin, Pout, entre otros.

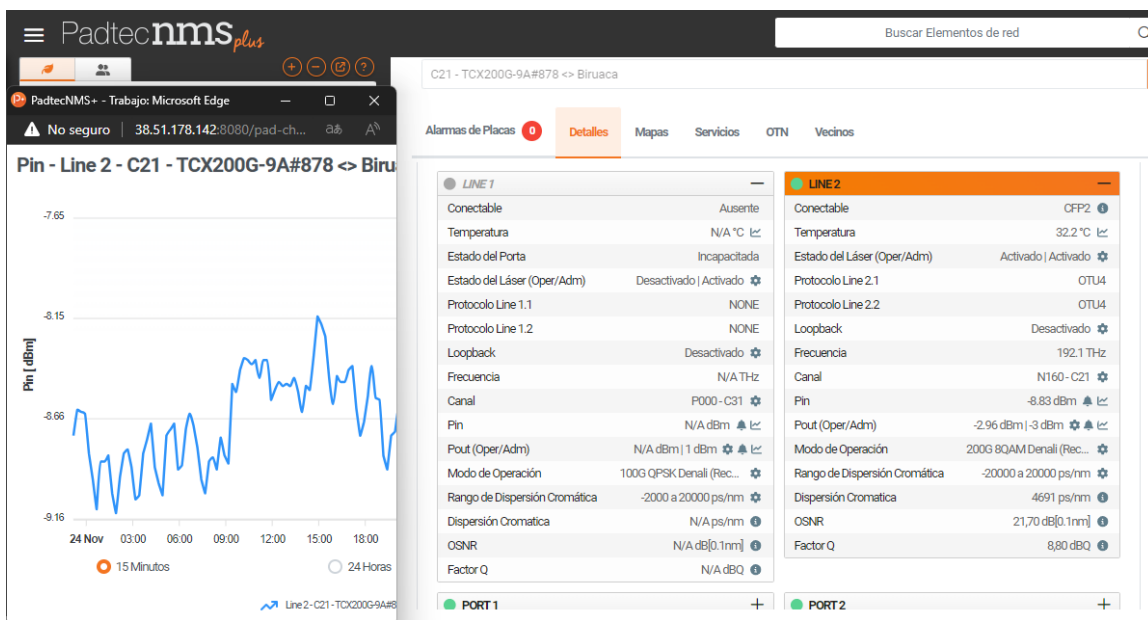


Fig. 1 Gestión de monitoreo equipos ópticos



El monitoreo de equipos de red como los routers y switches presentan un mayor desafío, ya que estos dispositivos generalmente solo proporcionan información en tiempo real, accesible únicamente a través de comandos específicos. Estas limitaciones dificultan la posibilidad de obtener un historial de parámetros, lo que complica la tarea de realizar un monitoreo efectivo para la detección de fallas o la identificación de posibles problemas de desagregación en las interfaces. La figura 2 muestra los valores arrojados por el router UfiSpace sobre la interfaz OpenZR+, siendo un poco difícil de leer y no tan llamativo. Además, no cuenta con los valores históricos el cual son muy importantes a la hora de solucionar adversidades en la red.

```

Router#show qsfp-dd 0 monitors media
Port Number : 0

Alarm Codes: TFIFO - Tx FIFO Error, TLOLDS - Tx Deskew Loss of Lock
              TLOLRC - Tx Reference Clock Loss of Lock, TLOLCMU - Tx CMU Loss of Lock
              TODA - Tx Out of Alignment, TLOA - Tx Loss of Alignment
              RFIFO - Rx FIFO Error, RLOLDS - Tx Deskew Loss of Lock
              ROOA - Rx Out of Alignment, RLOA - Rx Loss of Alignment
              RLOLCD - Rx Chromatic Dispersion Compensation Loss of Lock
              RLOLD - Tx Demodulator Loss of Lock, RLOM - Rx Loss of Multi Frame
              RLOF - Rx Loss of Frame, FDD - FEC Detected Degrade
              FED - FEC Excessive Degrade, RPF - Remote Phy Fault
              LD - Local Degrade, RD - Remote Degrade

Codes: [HA : High Alarm], [LA : Low Alarm], [HW : High Warning], [LW : Low Warning]

Port Number          : 0
-----
| Monitors          | Lane | Value      | High Alarm | High Warning | Low Warning | Low Alarm |
|-----|-----|-----|-----|-----|-----|-----|
| Rx Optical Power | 1    | -32.2 [LW] | 8.0        | 6.0         | -28.2      | -32.2     |
| dBm              |      |            |            |            |            |            |
| Tx Optical Power | 1    | 0.0        | 6.0        | 4.0         | -16.0      | -18.0     |
| dBm              |      |            |            |            |            |            |
| Tx Bias          | 1    | 254.4      | 0.0        | 0.0         | 0.0        | 0.0       |
| mA              |      |            |            |            |            |            |
|-----|-----|-----|-----|-----|-----|
| VDM              | Lane | Value      | High Alarm | High Warning | Low Warning | Low Alarm |
|-----|-----|-----|-----|-----|-----|
| eSNR Input      | 1    | 6.0        | 255.0      | 230.0       | 0.0        | 0.0       |
| dB              |      |            |            |            |            |            |
|-----|-----|-----|-----|-----|-----|
| Monitors          | Lane | Status      |
|-----|-----|-----|
| Tx Output         | 1    | Valid       |
|-----|-----|-----|
| Flag              | Lane | Status (L)  |
|-----|-----|-----|
| Rx LOS            | 1    | True        |
| Tx Failure        | 1    | False       |
| Rx CDR LOL        | 1    | False       |
|-----|-----|-----|
| Link Performance  | Lane | Average     | Minimum   | Maximum   | Unit       |
|-----|-----|-----|-----|-----|-----|
| Rx DSP CCD        | 1    | 0           | 0         | 0         | ps/nm     |
| Rx DSP DGD        | 1    | 2.00        | 2.00      | 2.00      | ps        |
| Rx Low Granularity SOPMD | 1    | 9600.0      | 9600.0    | 9600.0    | ps^2      |
| Rx PDL            | 1    | 0.8         | 0.8       | 0.8       | dB        |
| Rx OSNR           | 1    | 35.4        | 35.4      | 35.4      | dB        |
| Rx ESNR           | 1    | 6.3         | 6.3       | 6.3       | dB        |
| Rx CFO            | 1    | -10         | -108      | 72        | MHz       |
| Tx Power          | 1    | 0.00        | 0.00      | 0.00      | dBm       |
| Rx Input Optical Power | 1    | -31.72      | -31.75    | -31.70    | dBm       |
| Rx Input Optical Signal Power | 1    | -40.00      | -40.00    | -40.00    | dBm       |
| Rx SOPCR          | 1    | 0           | 0         | 0         | krads/s   |
| Rx High Granularity SOPMD | 1    | 1.0         | 1.0       | 1.0       | ps^2      |
    
```

Fig. 2 Visualización de parámetros de los UfiSpace

Este proyecto se centra en las redes IPoDWDM y la desagregación de las variables de las interfaces OpenZR+ mediante la plataforma Zabbix. Esta tecnología es importante para la distribución de

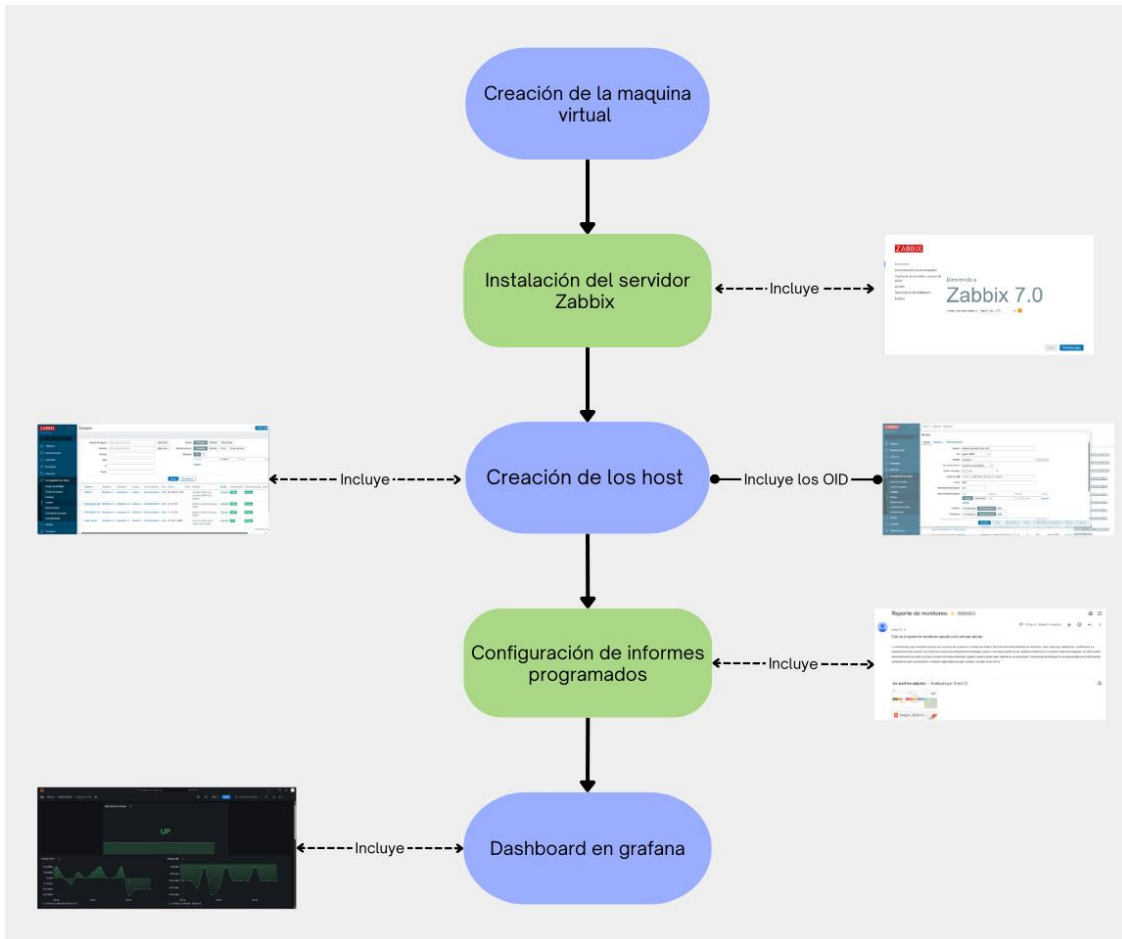
capacidades en enlaces de larga distancia, lo que hace necesario el monitoreo de las interfaces OpenZR+, permitiendo al equipo de operaciones tener un control efectivo sobre la gestión de la red.

Existen diversas aplicaciones de monitoreo de red de código abierto en el mercado, y se ha seleccionado Zabbix como la herramienta más adecuada para este proyecto. Zabbix fue elegida por su facilidad de uso de programación, la disponibilidad de plantillas para distintos dispositivos, su compatibilidad con todas las versiones de SNMP, su capacidad para generar gráficos en tiempo real, así como chequeos de disponibilidad y rendimiento. Además, cuenta con una interfaz web que permite controlar cualquier dispositivo compatible con el protocolo SNMP y con una fácil vinculación al software de Grafana.



**Fig. 3** Dashboard final soluciones IPoDWDM

La solución implementada para alcanzar el objetivo principal del proyecto se detalla en el diagrama de flujo mostrado en la figura 4. Este diagrama describe de manera secuencial los pasos y procesos clave llevados a cabo para desarrollar el Dashboard ideal, destacando las fases de planificación, desarrollo y validación de cada Software instalado.



**Fig. 4** Proceso de configuración

## II. OBJETIVOS

### 1. OBJETIVO GENERAL

Implementar una plataforma de monitoreo que permita visualizar el comportamiento de las variables de desempeño óptico en las interfaces OpenZR+ sobre plataformas desagregadas, utilizando Zabbix y Grafana, para proveer los datos que permitan al equipo de operación de redes IPoDWDM mejorar su disponibilidad, eficiencia y calidad del servicio.

## **2. OBJETIVOS ESPECÍFICOS**

- Configurar y adaptar el servidor para la implementación de la plataforma mediante Zabbix a través de una máquina virtual, permitiendo la captura y visualización en tiempo real de las variables de desempeño óptico en las interfaces OpenZR+.
- Implementar la plataforma Zabbix en la máquina virtual del servidor ya configurado.
- Hacer pruebas de captura de datos de la plataforma Zabbix sobre un montaje de red IPoDWDM en los laboratorios de Padtec.
- Analizar los datos recopilados por la plataforma de monitoreo para identificar puntos de mejora en el sistema que se está monitoreando, emitiendo alertas y recomendaciones operativas con base en la información extraída de las interfaces OpenZR+, con el fin de aumentar la estabilidad y calidad de los servicios implementados sobre la red desagregada.
- Generar informes periódicos en Zabbix para la detección temprana de anomalías y el seguimiento continuo del desempeño de las redes IPoDWDM.

## **III. PRESENTACIÓN DE LA EMPRESA**

Padtec S.A. es una multinacional brasileña, establecida en 2001, con sede principal en Campinas, São Paulo. La empresa se especializa en ofrecer soluciones flexibles y de alta capacidad para transmisiones ópticas de larga distancia, utilizando tecnología de Multiplexación por División en Longitud de Onda Densa (DWDM). Padtec cuenta con una amplia gama de productos diseñados para redes que satisfacen las demandas integrales de grandes operadores, integradores, carriers de carriers, proveedores de servicios, y otros actores clave en el sector. Impulsada por una fuerte orientación hacia la investigación y el desarrollo, la tecnología innovadora de Padtec se destaca por superar grandes distancias y romper barreras, conectando el mundo de manera eficiente e inteligente.

## IV. MARCO TEÓRICO

### 1. HISTORIA DE LAS COMUNICACIONES ÓPTICAS

El avance significativo en las comunicaciones ópticas no se estableció hasta mediados del siglo XX, cuando Albert Einstein introdujo el concepto de emisión estimulada. Esta teoría, junto con los esfuerzos de los investigadores Bird y Houssel, quienes lograron la primera transmisión de información a través de fibra óptica, marcó el inicio de una nueva era en las telecomunicaciones. Antes de estos avances las transmisiones de voz se realizaban de manera analógica, utilizando multiplexación en frecuencia a través de cables coaxiales. Sin embargo, este método presentaba un problema importante, debido a la elevada atenuación del medio de transmisión que aumentaba con la frecuencia.

La creciente demanda de mayor ancho de banda, impulsada por la expansión global de las redes telefónicas, se convirtió en un fuerte motivador para el desarrollo de los sistemas ópticos. Para aumentar el ancho de banda, era necesario elevar la frecuencia de la señal portadora, lo que a su vez aumentaba la atenuación de la señal. Para mantener una comunicación efectiva punto a punto, se requería la instalación de repetidores en la red para amplificar la señal, lo que a su vez aumentaba considerablemente los costos. Este desafío técnico fue uno de los principales impulsores del desarrollo de las comunicaciones ópticas, que ofrecían una solución más eficiente y económica para satisfacer la creciente demanda de capacidad de transmisión [1].

### 2. PARÁMETROS DE LA RED DWDM

#### *2.1. Descripción de las redes DWDM*

La tecnología DWDM (Dense Wavelength Division Multiplexing) es fundamental en las redes ópticas modernas, permitiendo la transmisión simultánea de múltiples señales ópticas a través de una sola fibra óptica, como se muestra en la figura 5. Esta tecnología combina la salida de varios transmisores ópticos con diferentes longitudes de onda, permitiendo que múltiples canales ópticos ocupen un solo hilo de fibra, esto se logra usando, además de los transmisores mencionados, receptores ópticos, filtros y multiplexores/demultiplexores DWDM,

multiplexores ópticos de adición/extracción (OADM) y amplificadores ópticos que convierten las señales a las longitudes de onda adecuadas. DWDM mejora significativamente la capacidad y eficiencia de las comunicaciones, al permitir la transmisión de datos en diversos formatos y velocidades. Las redes basadas en DWDM pueden transmitir datos en formatos como IP, ATM, SONET y Ethernet, facilitado la transmisión simultánea de diferentes tipos de tráfico (voz, video, datos) a diferentes velocidades. Factores relevantes como la atenuación, dispersión y la relación señal/ruido óptico (OSNR) son importantes para mantener la calidad de la señal en larga distancia [2].

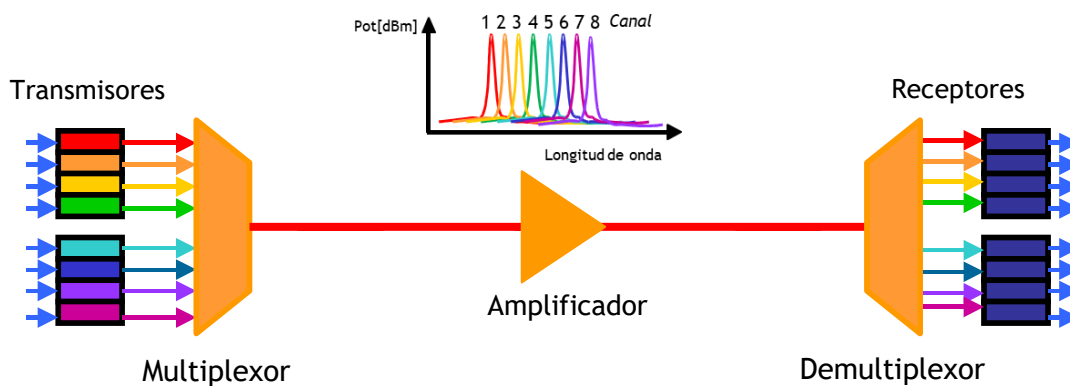


Fig. 5 Esquema de red DWDM

## 2.2. Espacio entre canales

El espaciamiento de canales se define a la separación mínima en frecuencia entre las señales multiplexadas dentro de la fibra óptica. Este valor de espaciamiento puede ser de 200, 100, 50, 25 o 12.5 GHz. La Unión Internacional de Telecomunicaciones (UIT) ha estandarizado los espaciamientos de 50 y 100 GHz, según la recomendación G.694.1. A medida que el espaciamiento entre canales se reduce, la velocidad máxima de transmisión de datos por cada longitud de onda también se ve limitada, dependiendo de las capacidades del equipo utilizado, dado que se tiene menos tolerancia a las dispersiones y efectos no lineales [3].

## 2.3. Direcciones de propagación de la señal DWDM

Los sistemas DWDM pueden configurarse de dos formas: unidireccional y bidireccional.

En las configuraciones unidireccionales, se emplean dos fibras ópticas: una dedicada al canal de subida y otra al canal de bajada. Por otro lado, en los sistemas bidireccionales, ambos canales, tanto de subida como de bajada, comparten una única fibra óptica. Aunque esta configuración elimina la necesidad de una segunda fibra, reduce la capacidad total de ancho de banda disponible.

Esta diferencia en la configuración conlleva diversas ventajas e inconvenientes. Los sistemas unidireccionales son más eficientes, ya que ofrecen el doble de canales que los sistemas bidireccionales. Además, la amplificación es más sencilla en estos sistemas, resultando en una mejor ganancia y niveles de potencia más altos a la salida, en comparación con los sistemas bidireccionales [2]. El inconveniente es el uso de una fibra adicional.

#### ***2.4. Ancho de banda en sistemas DWDM***

Los sistemas DWDM han avanzado significativamente, permitiendo ahora el transporte de señales ópticas con anchos de banda mucho mayores.

Actualmente, estos sistemas pueden soportar capacidades de transmisión de datos que un sistema puede manejar simultáneamente a través de diferentes longitudes de onda de luz en una sola fibra óptica. Cada longitud de onda transporta un canal de información independiente, permitiendo que múltiples señales se transmitan de manera concurrente. Esto maximiza la eficiencia del uso de la infraestructura de fibra, permitiendo la transmisión de grandes volúmenes de datos a larga distancia sin necesidad de amplificación constante, lo que la convierte en una tecnología clave para satisfacer la creciente demanda de ancho de banda en redes de telecomunicaciones modernas. Estos desarrollos dependen de la calidad de la fibra óptica y de la capacidad de los sistemas de conmutación para manejar estas elevadas tasas de datos, asegurando así una transmisión eficiente y confiable en redes de alta capacidad [4].

#### ***2.5. Potencia en sistemas DWDM***

La potencia de la señal en los sistemas ópticos DWDM está conformada por la suma de las potencias de los transmisores de forma individual. Es justamente esta suma de potencias las que pueden excitar los fenómenos no lineales en las fibras ópticas. La potencia disminuye de manera exponencial a medida que aumenta la distancia. La potencia inicial proviene directamente del conjunto de láseres emisores, mientras que la potencia de salida se ve afectada por diversos fenómenos a lo largo del enlace óptico, tales como la atenuación, dispersión, efectos no lineales en las fibras ópticas, amplificación óptica, entre otros.

### **2.6. Tasa de bit de error (BER)**

La tasa de errores de bits (BER) se refiere a la proporción de bits erróneos en relación con el total de bits transmitidos. En las redes DWDM, especialmente en aquellas de larga distancia, es común encontrar valores de BER del orden de  $10^{-15}$ , lo que significa que se produce un error en  $10^{15}$  bits transmitidos [3].

### **2.7. Ruido óptico**

El ruido aparece en sistemas ópticos que incorporan procesos de amplificación. El OSNR (relación señal a ruido óptico) define la proporción entre la potencia neta de la señal y la potencia neta del ruido. Este valor se calcula a la entrada de cada amplificadora (EDFA) a lo largo de la transmisión de la señal en el enlace. Para determinar el OSNR óptico en la entrada de un amplificador EDFA, se utiliza la ecuación 1. Para obtener la ecuación 2 se aplica el logaritmo a la ecuación 1, lo que nos proporciona una forma más práctica para calcular el OSNR.

$$OSNR = \frac{P_{in}}{N_F h\nu \Delta f} \quad (1)$$

$$OSNR(\text{dB}) = P_{in}(\text{dBm}) - NF(\text{dB}) + 58 \quad (2)$$

El término  $h\nu$  representa la energía de un fotón, por otro lado  $N_F$  es la figura de ruido del EDFA, el término  $\Delta f$  es correspondiente al ancho de banda óptico, donde se estable en 12.5 GHz y  $P_{in}$  es referente a la potencia de entrada de la amplificadora.



### **3. ELEMENTOS DE LA RED DWDM**

#### ***3.1. Fuentes de luz***

Una propiedad clave de un haz de luz es que las ondas de luz con diferentes longitudes de onda no se interfieran entre sí dentro de un medio.

Un láser puede generar pulsos de luz con una longitud de onda muy precisa. Cada una de estas longitudes de onda puede actuar como un canal de información independiente. Al combinar pulsos de diferentes longitudes de onda, es posible transmitir simultáneamente múltiples canales a través de una única fibra óptica, lo que maximiza la capacidad de transmisión y la eficiencia del sistema. Es clave en estos elementos su potencia, longitud de onda central y ancho espectral muy fino, para evitar que interfieran entre sí en sistemas DWDM.

#### ***3.2. Multiplexores***

El multiplexor es el equipo encargado de combinar las señales de entrada, y después dividir esta señal dentro del sistema DWDM. El MUX combina diferentes señales de los clientes, que pueden variar en protocolo y velocidad. A estas señales se les asignan dos longitudes de onda específicas (una para transmisión y otra para recepción) y se unifican en un solo haz de luz para ser transmitidas a través de una única fibra óptica.

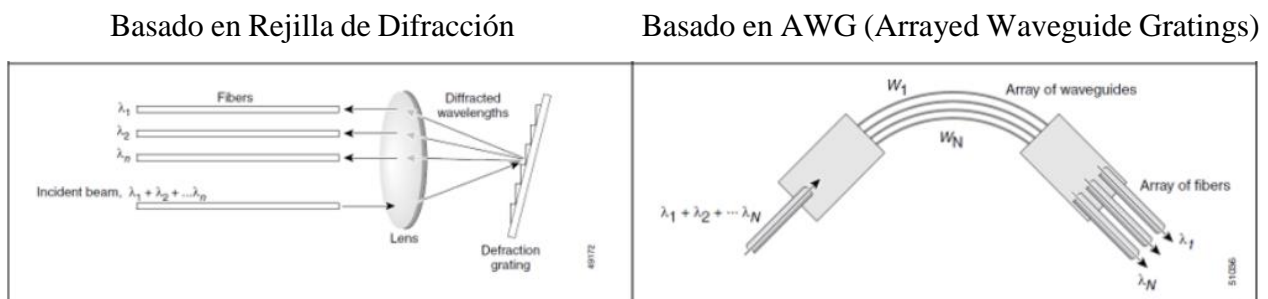
En el extremo receptor, el demultiplexor (DEMUX) separa los componentes de la luz para entregar cada servicio de manera individual. Tanto los multiplexores como los demultiplexores pueden ser diseñados con tecnología pasiva o activa (ver figura 5).

Existen según la tecnología utilizada para combinar o separar señales.

Los multiplexores y demultiplexores más tradicionales son los basados en la difracción, como los que se muestran en la figura 6, que funcionan mediante el fenómeno de la difracción de Bragg. En este proceso, la señal de entrada se refleja en una rejilla de difracción (grating), la cual separa espacialmente las diferentes longitudes de onda de la señal. Luego, estas señales son enfocadas en fibras ópticas individuales utilizando una lente. El uso de lentes de índice

gradual en lugar de lentes convencionales facilita el alineamiento de las señales y permite un diseño más compacto del dispositivo.

Otro tipo de multiplexor es el basado en guías de onda, conocido como multiplexor/demultiplexor AWG (Arrayed Waveguide Grating). Este dispositivo está compuesto por una guía de onda de entrada, un acoplador de guía de onda de entrada, un arreglo de guía de onda, un acoplador de guías de onda de salida y las guías de onda de salida, todos montados sobre un sustrato. En la figura se ilustra el funcionamiento básico de un AWG. La señal WDM, que incluye longitudes de onda como  $\lambda_1, \lambda_2, \dots, \lambda_N$ , ingresa por la guía de onda de entrada, donde es difractada y distribuida a través del acoplador de entrada hacia cada una de las guías de onda del arreglo.



**Fig. 6** Tipos de multiplexores ópticos.

**Fuente:** Optical Networks, A Practical Perspective, 3rd Ed. Rajiv Ramaswami

### 3.3. Amplificadores ópticos

Estos dispositivos son fundamentales en los sistemas DWDM, ya que su función principal es amplificar las señales que se propagan a través de la fibra, contrarrestando así los efectos de la atenuación. Los dos tipos de amplificadores ópticos más utilizados son el EDFA (Erbium-Doped Fiber Amplifier) y el amplificador Raman [5].

#### 3.3.1. Amplificadores EDFA

Los amplificadores de fibras dopados con erbio (EDFA) son particularmente populares, operando en la región de 1550 nm, que es la ventana principal para sistemas DWDM. Estos

dispositivos amplifican señales mediante un proceso llamado “emisión estimulada”, donde se utilizan diodo laser de bombeo para excitar electrones en la fibra. Los amplificadores EDFA pueden alcanzar ganancias de hasta 30 dB con potencias de bombeo relativamente bajas. Por otro lado, los amplificadores tipo Raman utilizan el efecto de dispersión estimulada Raman (SRS) para amplificar señales directamente en la fibra, aunque requieren potencias más altas y son más costosos de operar. Ambos tipos de amplificadores son importantes para mejorar la capacidad y el alcance de las comunicaciones ópticas.

#### **4. ROUTER**

Un Router es un dispositivo que enruta la información a través de distintos caminos, asegurando el cumplimiento de políticas, protocolos y medidas de seguridad. Su función principal es facilitar la comunicación eficiente entre el emisor y el receptor, contribuyendo a la creación de amplias redes de comunicación.

En el ámbito de las telecomunicaciones, los Routers a menudo se confunden con otros dispositivos como concentradores de red, módems o switches. Sin embargo, gracias a su capacidad avanzada de procesamiento de datos, los Routers pueden integrar las funciones de estos dispositivos y conectarse con ellos para optimizar el acceso a internet o para configurar redes empresariales más robustas.

Estos dispositivos también están equipados para realizar operaciones como el intercambio de etiquetas (label swapping), la adición de etiquetas (label push) y la eliminación de etiquetas (label pop).

El funcionamiento de un router se basa en la gestión de datos de la red mediante paquetes. Estos paquetes contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples, como interacciones web. Cada paquete de datos está compuesto por varias capas, una de las cuales transporta información importante, como el emisor, el tipo de datos, el tamaño y, lo más importante, la dirección IP, que es fundamental para el protocolo de internet. El router es capaz de leer esta capa, priorizar los datos y seleccionar la ruta óptima para la transmisión de cada paquete de datos [6].

Para este proyecto se utilizarán los enrutadores Ufispaces como hardware principal (ver figura 7). Estos enrutadores de acceso abierto son resistentes a la temperatura y cuentan con capacidades que admiten tráfico móvil, fijo y óptico cuando son combinados con transceptores OpenZR+ [7]. La gestión de estos enrutadores se realiza a través del software OcNOS (Open Compute Network Operating System) de IP Infusion, que ofrece una solución flexible para la administración de redes desagregadas. OcNOS proporciona soluciones basadas en software para conmutadores y enrutadores de red, facilitando una gestión por medio del protocolo SNMP eficiente y adaptable [8]. La combinación del hardware Ufispaces y el software OcNOS garantizan un entorno eficaz, capaz de gestionar y optimizar el desempeño de redes IPoDWDM, asegurando la disponibilidad, eficiencia y calidad del servicio.



**Fig. 7** Enrutador Ufispaces

**Fuente:** UfiSpace. Productos de telecomunicaciones [7]

## 5. SWITCH

Los switches son dispositivos esenciales en cualquier red, ya que su función principal es conectar múltiples dispositivos, como computadoras, puntos de acceso inalámbricos, impresoras y servidores, dentro de la misma red. Un switch facilita la comunicación y el intercambio de información entre los dispositivos conectados, permitiendo que operen de manera coordinada y eficiente.

Además de conectar dispositivos, los switches gestionan el flujo de datos en la red mediante la segmentación de tráfico, lo que reduce la congestión y mejora el rendimiento general. Utilizan direcciones MAC (Media Access Control) para dirigir los datos al dispositivo correcto, lo que garantiza una transmisión eficiente y segura. Los switches también pueden ser configurados para manejar tráfico de red más avanzado, como la priorización de ciertos tipos de datos o la creación

de VLANs (Virtual Local Area Networks), que segmentan una red física en varias redes lógicas para mejorar la seguridad y la gestión del tráfico. En este proyecto se hizo uso del switch Datacom DM4370 (Ver figura 8), el cual es el encargado de hacer paso a la comunicación, entre el servidor con los routers UfiSpace.



**Fig. 8** Switch DM4370

**Fuente:** DATACOM. Productos switches.

## 6. SERVIDOR

Un servidor es un equipo de cómputo diseñado para manejar, procesar y almacenar grandes cantidades de datos, además de proporcionar servicios a otros dispositivos en una red. Los servidores son fundamentales en infraestructuras tecnológicas, ya que soportan aplicaciones críticas, gestionan bases de datos, alojan sitios web y permiten la comunicación y colaboración entre diferentes sistemas y usuarios.

Para este proyecto, se utilizará el servidor Dell PowerEdge R660xs (ver figura 9), diseñado para ofrecer un alto rendimiento con una combinación equilibrada de recursos de procesamiento, memoria y almacenamiento. Este servidor es ideal para aplicaciones exigentes como el monitoreo de redes, ya que cuenta con procesadores escalables que proporcionan una robusta capacidad de procesamiento, garantizando un desempeño óptimo. Su arquitectura está optimizada para maximizar la eficiencia energética y la capacidad de enfriamiento, aspectos importantes para la operación continua y fiable en entornos de centros de datos. La capacidad de expansión del servidor permite la incorporación de múltiples unidades de almacenamiento y tarjetas de red de alta velocidad, facilitando el manejo de grandes volúmenes de datos y monitoreo en tiempo real de múltiples variables de desempeño. Al utilizar Zabbix en este servidor, se garantiza una plataforma de monitoreo potente y escalable, capaz de gestionar de manera eficiente las necesidades de supervisión de redes complejas, proporcionando alertas precisas y análisis detallados que son

esenciales para mantener la disponibilidad y calidad del servicio en infraestructuras de telecomunicaciones.



**Fig. 9** Servidor PowerEdge R660xs

**Fuente:** DELL Technologies [14]

## 7. MONITOREO

El monitoreo de la red, tiene como gran objetivo proporcionar la información adecuada a los administradores de las redes, en tiempo real, para diagnosticar si la red está funcionando de manera óptima y según los estándares de cada empresa. El monitoreo se realizará en este proyecto mediante la plataforma de desagregación Zabbix con el fin de detectar fallas en la red.

La monitorización involucra dos factores importantes, el tiempo de duración del monitoreo y el uso de recursos de la red. Mientras mayor sea el tiempo de monitoreo más efectiva será la detección de problemas [9].

### *7.1. Tipos de monitoreo*

- **Monitoreo activo:** El monitoreo activo se realiza insertando paquetes de prueba en la red, o en otras palabras enviando paquetes a determinadas aplicaciones midiendo los tiempos de respuesta, la técnica tiene la particularidad de agregar tráfico a la red y que será utilizado para medir el rendimiento de la misma red [9].
- **Monitoreo pasivo:** Este método se basa principalmente en obtener datos a partir de recolectar en una base de datos y analizar el tráfico que circula por la red, empleando diversos dispositivos que soporten SNMP.

El uso de SNMP para el monitoreo pasivo es una técnica que utiliza estadísticas sobre el ancho de banda en los dispositivos de red, con el respectivo acceso a dichos dispositivos. Este protocolo genera paquetes llamados TRAPS que indican que un evento inusual se ha producido [9]. En este proyecto se empleará el monitoreo pasivo.

## **7.2. Protocolos y Técnicas de monitoreo de Redes**

### **o UDP**

El protocolo UDP se utiliza para medir la pérdida de paquetes en una dirección unidireccional. Esto es útil para evaluar la integridad de la comunicación en una sola dirección. Además, el tiempo de ida y vuelta (RTT) se puede medir mediante técnicas como el trazado de rutas (trace route), lo que ayuda a identificar la latencia en la red.

### **o ICMP**

ICMP es fundamental para verificar la disponibilidad de host y red. Este protocolo permite detectar problemas en la red, así como medir retardos y pérdidas de paquetes. Gracias a su capacidad para enviar mensajes de error y de consulta, ICMP se convierte en una herramienta clave para el diagnóstico de conectividad.

### **o TCP**

El protocolo TCP se centra en la tasa de transferencia de datos, lo que permite evaluar el rendimiento de la comunicación. También es útil para diagnosticar problemas en la capa de aplicación, ayudando a identificar cuellos de botella y otros inconvenientes que puedan afectar el flujo de información en la red.

## **8. SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)**

El protocolo simple de gestión de red, es un protocolo de la capa de aplicación basado en IP que permite el intercambio de información entre una solución de administración de red y cualquier dispositivo compatible con SNMP.

La gestión de redes es un aspecto crítico para los proveedores de servicios de Internet, ya que es esencial para administrar el rendimiento de la red, resolver problemas y gestionar su expansión. SNMP es considerado el "lenguaje" de la administración de redes, ya que los dispositivos de red deben ser compatibles con SNMP para integrarse eficientemente con software de monitoreo de red, como las soluciones Zabbix.

En esencia, SNMP es un protocolo de nivel de aplicación diseñado para supervisar toda la infraestructura de red de un proveedor. Proporciona al administrador una visión detallada del equipo que está siendo monitoreado. Una de las ventajas clave de SNMP es su compatibilidad con dispositivos de múltiples marcas, lo que facilita la integración de diferentes equipos dentro del mismo entorno de monitoreo utilizando el mismo software.

El funcionamiento de SNMP se basa en la recopilación de información mediante sondeos. El software de monitoreo de red actúa como cliente, enviando paquetes de sondeo al servidor SNMP o agente, que es un fragmento de código ejecutado en el dispositivo monitorizado. El agente responde al sondeo enviando un paquete SNMP con las configuraciones y métricas predefinidas al cliente. El software de monitoreo procesa, recopila, revisa y analiza la información proveniente de diversos dispositivos, lo que permite una gestión eficiente y un análisis estadístico de los datos recopilados.

### ***8.1. Agente SNMP***

Un agente SNMP es un programa o módulo de software integrado en un dispositivo que está bajo gestión en una red. Este agente permite la recopilación local de información de administración en una base de datos, que está organizada de manera jerárquica. Cuando el administrador SNMP lo solicita, el agente proporciona acceso a esta información estructurada.

Las principales funciones del agente SNMP son:



- El agente SNMP recopila datos de administración sobre su entorno local, incluyendo métricas como la memoria libre, el número de paquetes IP recibidos, las rutas de red, caídas, tráfico, velocidad, ancho de banda, temperatura, entre otros.
- El agente recupera y almacena información de gestión en la MIB (Management Information Base), que es una base de datos jerárquica que contiene todas las variables que el agente puede reportar y gestionar.
- El agente tiene la capacidad de señalar al administrador cualquier evento inusual o crítico en la red, como fallos o anomalías, permitiendo una respuesta rápida para evitar interrupciones o problemas mayores.

## **9. MIB**

La Management Information Base (MIB) es una base de administración que organiza de manera jerárquica la información sobre los parámetros de un dispositivo gestionado. Esta base de datos permite que el administrador, utilizando el protocolo SNMP, acceda a información específica del dispositivo según las necesidades del Sistema de Administración de Red (NMS). La MIB contiene valores estadísticos y de control configurados para los diferentes nodos de hardware dentro de la red.

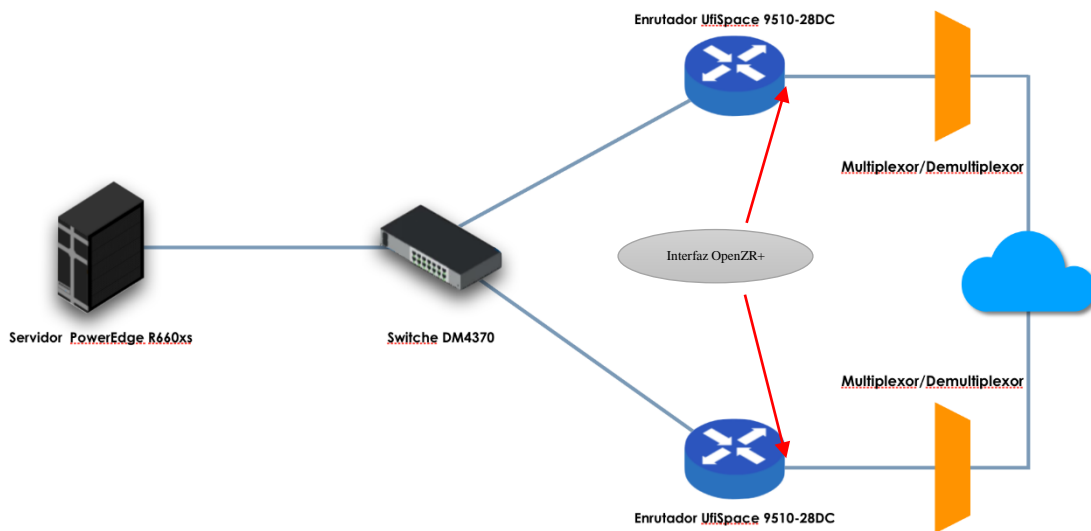
SNMP facilita la extensión de los valores estándar de la MIB con valores específicos a través del uso de agentes y MIB privadas. El agente, encargado de recopilar datos localmente, almacena esta información según las definiciones establecidas en la MIB, lo que permite una gestión precisa y personalizada de los dispositivos en la red.

En un entorno de monitoreo avanzado, como el que se implementa con Zabbix en servidores Dell PowerEdge R660xs, la MIB es fundamental para el seguimiento detallado de la infraestructura de red. Proporciona al administrador una visión completa de los parámetros operativos, permitiendo una administración eficiente y la capacidad de respuesta ante cualquier eventualidad en el sistema.

## 10. ZABBIX

La creación de Zabbix fue realizado por Alexei Vladishev y actualmente está desarrollado por Zabbix SIA. El objetivo de Zabbix es dar una solución al monitoreo de redes, equipos, máquinas virtuales, servidores, bases de datos, sitios web, la nube, aplicaciones, etc. Esta aplicación nos va a permitir registrar y conocer en tiempo real el estado e historial de las interfaces OpenZR+. Cabe destacar que es un software de código abierto (open source) de clase empresarial, quiere decir que su código fuente se distribuye gratuitamente y está disponible para el público en general [10].

Además, utiliza un mecanismo de notificación flexible que permitirá a los usuarios la configuración de alertas basadas en correos electrónicos y mensajes de Telegram o WhatsApp para cualquier evento que esté fuera de lo normal, lo que permitirá reaccionar rápidamente a los problemas del servidor o los equipos que se estén monitoreando. En la figura 10, se muestra el esquema de conexión para la plataforma de monitoreo.



**Fig. 10** Topología implementada

### 10.1. *Funcionamiento de Zabbix*

Para este proyecto, Zabbix se ha instalado en el servidor Dell PowerEdge R660xs, con un sistema operativo en la máquina virtual Ubuntu 24.04 (Noble), para recolectar y monitorear la información de las interfaces OpenZR+ utilizando el protocolo SNMP. Este servidor, diseñado para ofrecer un alto rendimiento y eficiencia, facilita la recopilación de datos y proporciona

una interfaz web que presenta gráficamente toda la información recolectada y almacenada de los dispositivos administrados.

Zabbix es compatible con agentes para sistemas operativos como Linux, Mac y Windows, que se instalan en los servidores y estaciones de trabajos a ser monitoreados. También permite la supervisión en tiempo real de una variedad de dispositivos, incluidos impresoras, routers, switches, y sensores de temperatura y humedad. Entre las funciones claves de Zabbix se destacan:

- **Alertas configurables:** Ofrece la capacidad de configurar notificaciones personalizadas para eventos específicos en la red.
- **Gráficos en tiempo real:** Proporciona visualizaciones actualizadas al instante de los datos monitorizados, facilitando la interpretación y análisis.
- **Capacidad de monitoreo:** Permite una supervisión detallada de múltiples dispositivos y servicios en la red.
- **Almacenamiento de datos históricos:** Conserva un registro de los datos monitorizados para análisis y referencias futuras.
- **Configuración dinámica:** Facilita ajustes en tiempo real para adaptarse a las necesidades cambiantes de la red.

### **10.2. Ventajas de Zabbix**

Utilizar Zabbix para el monitoreo de red en este proyecto presenta varias ventajas significativas:

- **Código abierto y seguridad:** Zabbix es una solución de código abierto, lo que permite su uso sin restricciones y ofrece seguridad mediante la disponibilidad de su código fuente. Además de Zabbix, se incluyen todos los componentes necesarios, como Linux, Apache, MySQL/PostgreSQL y PHP.

- **Administración centralizada:** Zabbix cuenta con un sistema de administración centralizado, accesible a través de una interfaz web que permite gestionar todos los dispositivos de la red desde un único lugar, facilitando la supervisión y el control.
- **Gestión de usuarios:** El sistema incluye un manejo robusto de usuarios, con autenticación mediante contraseñas, asegurando que solo personal autorizado pueda acceder y gestionar la red.
- **Alertas automatizadas:** Zabbix permite configurar alertas automáticas, que se envían a dispositivos específicos a través de correo electrónico o SMS cuando se detecta un problema en la red, asegurando una respuesta rápida a cualquier incidente.
- **Detección de dispositivos:** Tiene la capacidad de identificar y monitorear una amplia variedad de dispositivos de red, como routers, switches, servidores, impresoras y otros periféricos, utilizando varios protocolos como SNMP (versiones 1, 2 y 3).
- **Visualización de datos:** Zabbix integra capacidades avanzadas de visualización que facilitan el trabajo con los datos de la red, permitiendo análisis más rápidos e inteligentes.
- **Mantenimiento de datos:** Incluye un sistema de limpieza que mantiene los datos actualizados y organizados, lo que es importante para una gestión eficiente y precisa de la red.

### **10.3. Características de Zabbix**

- **Funciones de administración**
  - Zabbix incorpora herramientas de administración como Ping y Trace route para diagnosticar y solucionar problemas de conectividad en la red, facilitando la gestión y mantenimiento de la infraestructura de telecomunicaciones [11].
- **Seguridad**
  - Zabbix proporciona permisos flexibles para cada usuario, garantizando un acceso controlado a las funciones de monitoreo.

- La autenticación por IP añade una capa adicional de seguridad, asegurando que solo direcciones IP autorizadas puedan acceder al sistema.
- Incluye protección contra ataques de fuerza bruta, salvaguardando la integridad del sistema de monitoreo [11].
- **Monitorización**
  - Zabbix ofrece una configuración centralizada que facilita la gestión unificada de la red.
  - Proporciona acceso centralizado a toda la información relevante, permitiendo a los administradores gestionar los datos desde una única interfaz.
  - Es capaz de soportar hasta 1,000 nodos Zabbix, lo que lo hace adecuado para redes de gran tamaño.
  - Permite la integración de un número ilimitado de proxies, asegurando la flexibilidad y expansión de la red sin limitaciones [12].
- **Escalabilidad**
  - Estudios han demostrado que Zabbix puede monitorizar hasta 100,000 dispositivos y servidores, destacando su capacidad para manejar grandes infraestructuras [12].
  - Las pruebas realizadas por la organización Zabbix han validado su capacidad para ejecutar hasta 1,000,000 de chequeos de rendimiento y disponibilidad.
  - Es capaz de procesar miles de chequeos de rendimiento y disponibilidad en segundo plano, garantizando un monitoreo continuo y eficiente.
- **Monitorización en tiempo real**
  - Zabbix supervisa el rendimiento y la disponibilidad de la red en tiempo real, lo que permite una detección rápida de problemas.
  - Ofrece notificaciones flexibles basadas en condiciones predefinidas, asegurando que los administradores estén informados de cualquier incidencia.

- Las alertas se pueden enviar a los usuarios a través de SMS o correo electrónico, facilitando una respuesta inmediata.
- Zabbix también mantiene registros detallados de logs para un análisis posterior.
  
- **Auto detección**
  - Zabbix es capaz de detectar dispositivos automáticamente mediante SNMP (versiones 1, 2, 3), rangos IP y servicios, simplificando la integración de nuevos equipos.
  - Monitorea automáticamente los dispositivos que se auto detectan, asegurando que todos los componentes de la red estén bajo supervisión sin necesidad de intervención manual.
  - Soporta tanto IPv4 como IPv6, ofreciendo flexibilidad en el manejo de diferentes tipos de direcciones IP.
  - Los agentes nativos de Zabbix proporcionan una integración más profunda y eficiente con los dispositivos monitorizados.
  
- **Monitorización proactiva**
  - Zabbix permite la monitorización sin agente, lo que significa que puede supervisar dispositivos y servicios sin necesidad de instalar software adicional.
  - Puede monitorizar servicios remotos como FTP, SSH, HTTP, entre otros, asegurando la disponibilidad y rendimiento de aplicaciones críticas.
  - Ofrece soporte completo para el protocolo SNMP en sus versiones 1, 2 y 3, incluyendo la gestión de traps SNMP.

## 11. ELEMENTOS DE ZABBIX

### 11.1. *Servidor Zabbix*

El servidor de Zabbix es el componente más crítico de todo el sistema, ya que permite realizar comprobaciones remotas de los servidores en la red a través de verificaciones de servicio simples. Los agentes desplegados en los dispositivos de la red envían continuamente información detallada, incluidas estadísticas de disponibilidad e integridad, al servidor de Zabbix. Esta capacidad de centralizar la recopilación y almacenamiento de datos de configuración, operativos y estadísticos convierte al servidor de Zabbix en el núcleo de toda la operación de monitoreo [11].

Además de estas funciones de almacenamiento y organización, el servidor de Zabbix también desempeña un papel importante en la gestión de alertas. Cuando se detecta un problema en cualquiera de los sistemas monitoreados, el servidor alerta activamente a los administradores, permitiéndoles tomar medidas correctivas de manera inmediata.

El servidor no solo centraliza las operaciones de monitoreo, sino que también aloja la consola de administración y la base de datos principal de Zabbix, desde donde se gestiona y organiza toda la información recopilada de los dispositivos bajo supervisión. Esto incluye la configuración de las políticas de monitoreo, la visualización de datos históricos y en tiempo real, y la gestión de usuarios y permisos.

### **11.2.     *Agente Zabbix***

Un componente esencial de Zabbix es su capacidad para monitorear recursos de red en tiempo real, utilizando el protocolo SNMP. El agente nativo de Zabbix, desarrollado en lenguaje C, está diseñado para ejecutarse en múltiples plataformas compatibles, como Linux y Windows. Este agente es responsable de recopilar datos cruciales sobre el rendimiento de los dispositivos en la red, incluyendo el uso de CPU, memoria, capacidad de disco, interfaces de red, y la velocidad de transmisión de datos.

La versatilidad del agente permite a Zabbix integrar y supervisar diversos sistemas operativos y dispositivos de manera eficiente, asegurando que todos los aspectos críticos de la red sean monitorizados continuamente. Esto garantiza que los administradores de red tengan acceso a

información detallada y precisa en tiempo real, facilitando la toma de decisiones informadas y la rápida resolución de problemas.

### **11.3.     *Ítems***

Los elementos en Zabbix son módulos que recopilan datos de un host. Al configurar un nuevo host, es necesario agregar estos elementos para iniciar la recopilación de datos en tiempo real. Esto permite un monitoreo continuo y preciso del rendimiento y estado del host, asegurando una supervisión efectiva de la red.

### **11.4.     *Host y grupos de hosts***

Los hosts en Zabbix representan los dispositivos que se van a monitorear, como servidores, estaciones de trabajo, routers, y switches. Para una mejor organización, estos dispositivos pueden agruparse en "group hosts", lo que facilita la gestión y supervisión de múltiples equipos dentro de una misma categoría o función. Esta estructura organizada permite un monitoreo más eficiente y centralizado de los dispositivos en la red.

### **11.5.     *Plantillas o templates***

En Zabbix, el uso de plantillas es una estrategia eficiente para optimizar la configuración y reducir la carga de trabajo. Una plantilla es un conjunto predefinido de entidades que pueden aplicarse a varios hosts de manera conveniente. Estas entidades incluyen elementos (ítems), disparadores (triggers), gráficos, tableros (dashboards), reglas de descubrimiento de bajo nivel (low-level discovery rules), y escenarios web.

Dado que muchos dispositivos en el mercado son idénticos o muy similares, una plantilla creada para uno de ellos puede reutilizarse en otros con características similares. Al vincular una plantilla a un host o dispositivo, todas las entidades incluidas se añaden automáticamente al host, lo que facilita el monitoreo y asegura una configuración consistente y eficiente en toda la infraestructura de red.



### **11.6.     *Discovery***

Zabbix ofrece una funcionalidad de descubrimiento automático de redes que es tanto flexible como eficaz, diseñada para acelerar la implementación del sistema y simplificar su gestión. Este proceso de descubrimiento en Zabbix se basa en varios métodos:

- **Información del agente SNMP:** Emplea datos obtenidos a través del protocolo SNMP para descubrir y agregar dispositivos a la red.
- **Información del agente de Zabbix:** Utiliza los datos recopilados por los agentes de Zabbix instalados en los dispositivos para identificar nuevos hosts y servicios.
- **Rangos de IP:** Permite identificar y agregar dispositivos en un rango específico de direcciones IP.
- **Disponibilidad de servicios externos:** Detecta dispositivos y servicios externos que están disponibles en la red.

Este enfoque integral permite a Zabbix automatizar la detección de dispositivos y servicios, reduciendo el tiempo necesario para la configuración inicial y garantizando una administración más eficiente de la red.

### **11.7.     *Interfaz web***

Zabbix facilita el acceso a los datos de monitoreo y configuraciones a través de una interfaz web accesible desde cualquier plataforma. Esta interfaz basada en la web permite a los administradores gestionar y visualizar la información de monitoreo de manera eficiente, sin importar el sistema operativo o dispositivo que estén utilizando.

**V. METODOLOGÍA**

Objetivo	Actividad
<p>1. Configurar y adaptar el servidor para la implementación de la plataforma mediante Zabbix a través de una máquina virtual, permitiendo la captura y visualización en tiempo real de las variables de desempeño óptico en las interfaces OpenZR+.</p>	<p>1.1. Configuración e instalación del hypervisor en el servidor para implementar Zabbix por medio de una máquina virtual. 1.2. Documentación de la plataforma Zabbix para la instalación en la máquina virtual</p>
<p>2. Implementar la plataforma Zabbix en la máquina virtual del servidor ya configurado.</p>	<p>2.1. Configuración e instalación de la plataforma en la máquina virtual del servidor.</p>
<p>3. Hacer pruebas de captura de datos de la plataforma Zabbix sobre un montaje de red IPoDWDM en los laboratorios de Padtec</p>	<p>3.1. Configurar la plataforma de Zabbix para integrar los equipos Ufispac. 3.2. Implementar el entorno de laboratorio con una solución IPoDWDM. 3.3 Identificar los datos y los parámetros a que correspondan, arrojados por la plataforma Zabbix.</p>
<p>4. Analizar los datos recopilados por la plataforma de monitoreo para identificar puntos de mejora en el sistema que se está monitoreando, emitiendo alertas y recomendaciones operativas con base en la información extraída de las interfaces OpenZR+, con el fin de aumentar la estabilidad y calidad de los servicios implementados sobre la red desagregada.</p>	<p>4.1. Priorizar las variables que aporten mayor información para los operadores, con base en la experiencia de la empresa PADTEC. 4.2. Identificar mejoras a partir del análisis de los datos recopilados. 4.3. Determinar un ajuste óptimo de parámetros para asegurar que las redes IPoDWDM cumplan con los estándares de calidad del servicio y sirva para implementar alarmas.</p>
<p>5. Generar informes periódicos en Zabbix para la detección temprana de anomalías y el seguimiento continuo del desempeño de las redes IPoDWDM.</p>	<p>5.1. Definir con la empresa el dashboard, la plantilla o esquema de los informes de seguimiento y su periodicidad. 5.2. Implementar el dashboard y la plantilla de informes definida. 5.3. Evaluar con el equipo técnico de PADTEC la aplicación de usuario y hacer los ajustes correspondientes.</p>

**Tabla 1** Metodología a implementar

## VI. RESULTADOS

### 1. IMPLEMENTACIÓN DEL HYPER-V EN EL SERVIDOR

Para instalar el hypervisor donde se gestionarán las máquinas virtuales, se utilizó el aplicativo Hyper-V de Windows. Para ello, es necesario descargar la imagen ISO y proceder a su instalación en el servidor a través de una unidad USB de arranque que contenga dicha imagen. Al finalizar muestra las siguientes opciones (figura 11).

```
Windows Update actualmente establecido en: Automáticas
Seleccionar actualizaciones (a)utomáticas, de solo (d)escarga o (m)anuales:m

Estableciendo actualizaciones en Manual...

=====
                          Configuración del servidor
=====

1) Dominio o grupo de trabajo:          Dominio: 
2) Nombre de equipo:                    [redacted]
3) Agregar administrador local
4) Configurar administración remota      Habilitado

5) Configuración de Windows Update:     Manual
6) Descargar e instalar actualizaciones
7) Escritorio remoto:                   Habilitado (solo los clientes más seguros)

8) Configuración de red
9) Fecha y hora
10) Configuración de telemetría          Desconocido
11) Activación de Windows

12) Cerrar sesión del usuario
13) Reiniciar servidor
14) Apagar servidor
15) Salir a la línea de comandos
```

**Fig. 11** Configuración Servidor para gestión de máquinas virtuales

Para configurar de forma remota la máquina virtual desde el Hyper-V, primero es necesario habilitar el escritorio remoto en el servidor (ítem 7). Luego, accedemos a la consola de comandos (ítem 14), donde iniciamos la consola PowerShell y ejecutamos los siguientes comandos para permitir que el servidor Hyper-V reciba comandos remotos de PowerShell y habilitar la autenticación CredSSP para acceder a la máquina virtual remotamente:

*Enable-PSRemoting*

*Enable-WSManCredSSP -Role server*

Ahora en el lado del computador cliente que va a contar con la conexión al servidor para la gestión y administración del Hyper-V, habilitamos las funciones Hyper-V como se observa en la fig 12.

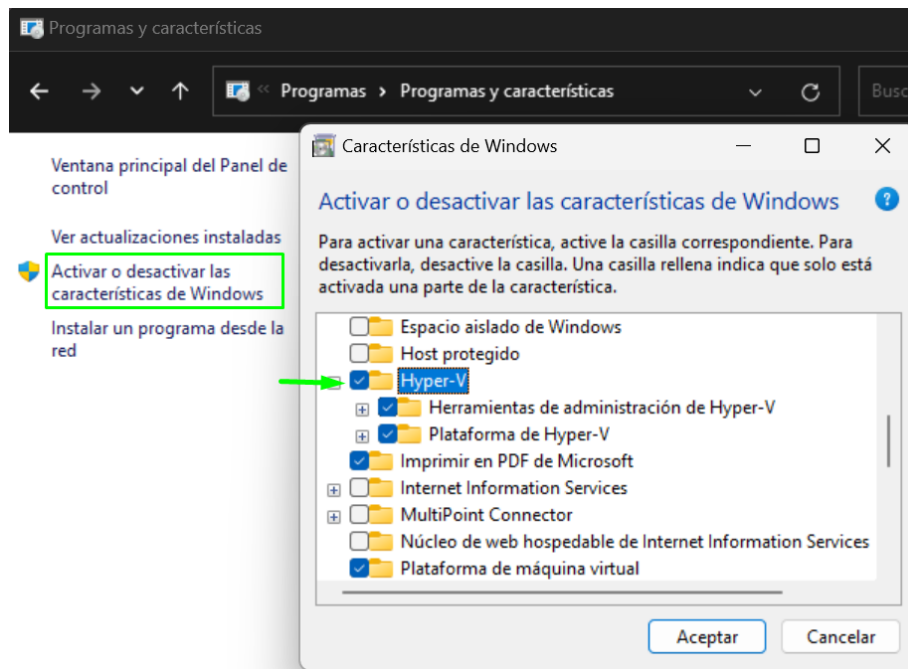


Fig. 12 Configuración Hyper-V Cliente

A continuación, se inicia la aplicación Hyper-V y se conecta el servidor al ordenador encargado de la gestión remota, tal como se muestra en la fig 13.

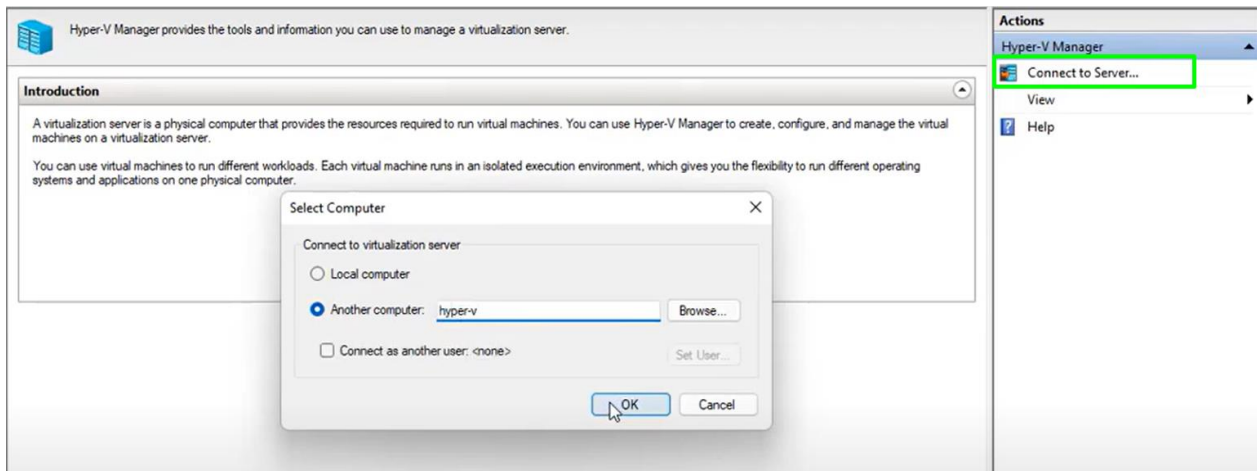


Fig. 13 Conexión remota al servidor

## **2. IMPLEMENTACIÓN DEL SISTEMA DE MONITOREO**

Para llevar a cabo este proyecto, se realizó una investigación exhaustiva sobre el software Zabbix, explorando sus funcionalidades y ventajas con el fin de maximizar su uso. Se planteó el montaje de Zabbix en una máquina virtual experimental antes de implementarlo en el servidor. Esto permitió realizar un análisis previo de los conceptos, recursos y configuraciones necesarias para el monitoreo continuo de las interfaces.

El proyecto está diseñado para facilitar la toma de decisiones del equipo de operaciones, basándose en datos de monitoreo, portabilidad y gráficos que muestren en tiempo real las variaciones de las variables en la interfaz del router.

En la primera fase del proyecto, Zabbix nos proporciona una herramienta esencial para el monitoreo de parámetros clave, tales como el OSNR, ancho de banda, temperatura, Pre-FEC, tiempo de actividad (uptime), tiempo de inactividad (downtime), potencia de salida y potencia de entrada. Estos indicadores son fundamentales para el éxito del proyecto. Tras adquirir un conocimiento sólido sobre el protocolo SNMP y realizar prácticas de configuración de Zabbix en una máquina virtual, procedemos a su implementación en el servidor local de la empresa.

En esta fase, se detallará el proceso de instalación de Zabbix, la creación del host (Router), la configuración de las variables de monitoreo, así como la generación de informes. Además, se incluirá la integración de Grafana, lo que permitirá una presentación más amigable y accesible de los datos monitoreados.

### **2.1. Instalación del servidor Zabbix 7.0 LTS**

Padtec S.A.S proporciona un espacio en el servidor local donde hemos instalado, en una máquina virtual, el sistema operativo Ubuntu server versión 24.04. Esta distribución de Linux es gratuita y de código abierto, lo que la hace ideal para nuestros propósitos.

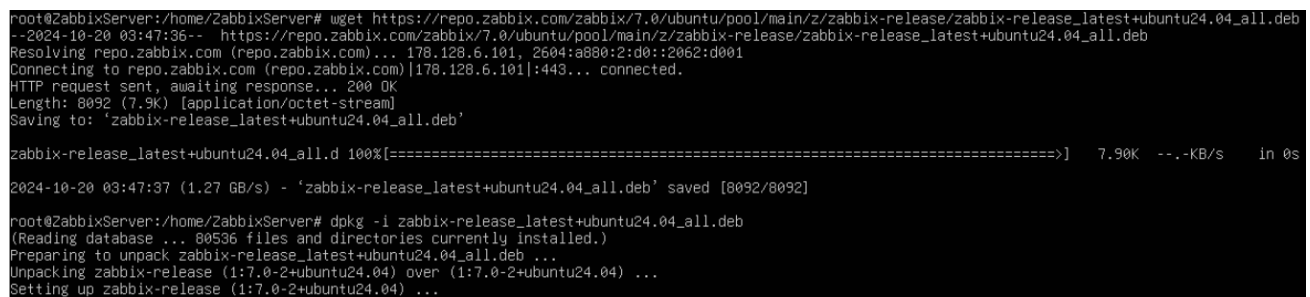
Para un funcionamiento óptimo, Zabbix necesita tanto memoria física como espacio en disco. La cantidad de espacio en disco requerido varía según el número de equipos o host y los parámetros que se vayan a monitorear. Se recomienda un mínimo de 8Gb de espacio en disco y al menos 2 núcleos de CPU.

Una vez cumplidos estos requisitos, el siguiente paso es seleccionar la versión de Zabbix en la página oficial. En la sección de descargas, se debe seleccionar la versión del sistema operativo Ubuntu 24.04.

### 2.1.1. Instalación del repositorio de Zabbix

Lo primero que se debe hacer es la instalación del repositorio oficial de Zabbix (ver fig 14), lo cual es necesario ejecutar los siguientes comandos:

```
# wget https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-
release/zabbix-release_latest+ubuntu24.04_all.deb
# dpkg -i zabbix-release_latest+ubuntu24.04_all.deb
# apt update
```



```
root@ZabbixServer:/home/ZabbixServer# wget https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest+ubuntu24.04_all.deb
--2024-10-20 03:47:36-- https://repo.zabbix.com/zabbix/7.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest+ubuntu24.04_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Connecting to repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8092 (7.9K) [application/octet-stream]
Saving to: 'zabbix-release_latest+ubuntu24.04_all.deb'

zabbix-release_latest+ubuntu24.04_all.d 100%[=====] 7.90K --.-KB/s in 0s
2024-10-20 03:47:37 (1.27 GB/s) - 'zabbix-release_latest+ubuntu24.04_all.deb' saved [8092/8092]

root@ZabbixServer:/home/ZabbixServer# dpkg -i zabbix-release_latest+ubuntu24.04_all.deb
(Reading database ... 80536 files and directories currently installed.)
Preparing to unpack zabbix-release_latest+ubuntu24.04_all.deb ...
Unpacking zabbix-release (1:7.0-2+ubuntu24.04) over (1:7.0-2+ubuntu24.04) ...
Setting up zabbix-release (1:7.0-2+ubuntu24.04) ...
```

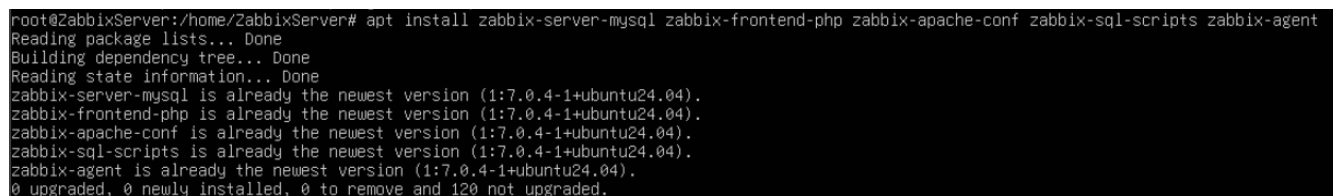
**Fig. 14** Instalación del repositorio de la página oficial

### 2.1.2. Instalación del servidor, la interfaz y el agente de Zabbix

En esta parte de la integración del servidor de Zabbix, se procede a instalar el servidor, la interfaz y el agente de Zabbix, donde el agente Zabbix permitirá recopilar los datos sobre el estado del servidor (ver fig 15).

El comando correspondiente es:

```
# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf
zabbix-sql-scripts zabbix-agent
```



```
root@ZabbixServer:/home/ZabbixServer# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
zabbix-server-mysql is already the newest version (1:7.0.4-1+ubuntu24.04).
zabbix-frontend-php is already the newest version (1:7.0.4-1+ubuntu24.04).
zabbix-apache-conf is already the newest version (1:7.0.4-1+ubuntu24.04).
zabbix-sql-scripts is already the newest version (1:7.0.4-1+ubuntu24.04).
zabbix-agent is already the newest version (1:7.0.4-1+ubuntu24.04).
0 upgraded, 0 newly installed, 0 to remove and 120 not upgraded.
```

**Fig. 15** Instalación de Zabbix server, la interfaz y el agente Zabbix

### 2.1.3. Creación de la base de datos inicial

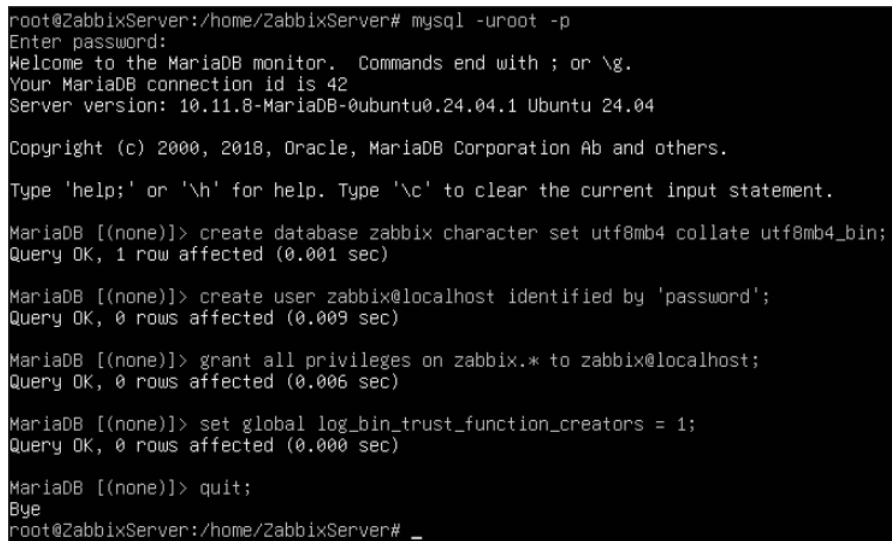
En esta etapa, es importante instalar la base de datos MySQL para utilizar Zabbix (ver fig 16). Esto permitirá recopilar y almacenar todos los datos de los agentes o equipos que se van a monitorear.

Se debe preparar la base de datos, para lo cual nos conectamos a la base de datos con el siguiente comando:

```
# mysql -uroot -p
```

Se crea la base de datos, el usuario, la contraseña y se da permisos de acceso al usuario creado con los siguientes comandos:

```
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by 'password';
mysql> grant all privileges on zabbix.* to zabbix@localhost;
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;
```



```
root@ZabbixServer:/home/ZabbixServer# mysql -uroot -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 42
Server version: 10.11.8-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> create user zabbix@localhost identified by 'password';
Query OK, 0 rows affected (0.009 sec)

MariaDB [(none)]> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0.006 sec)

MariaDB [(none)]> set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> quit;
Bye
root@ZabbixServer:/home/ZabbixServer# _
```

**Fig. 16** Creación de la base de datos inicial MySQL

#### 2.1.4. Importación del esquema y los datos iniciales

En el servidor Zabbix, es necesario importar el esquema y los datos iniciales a la base de datos, este paso nos pedirá ingresar la contraseña que recién se creó, el comando para realizar este paso es el siguiente:

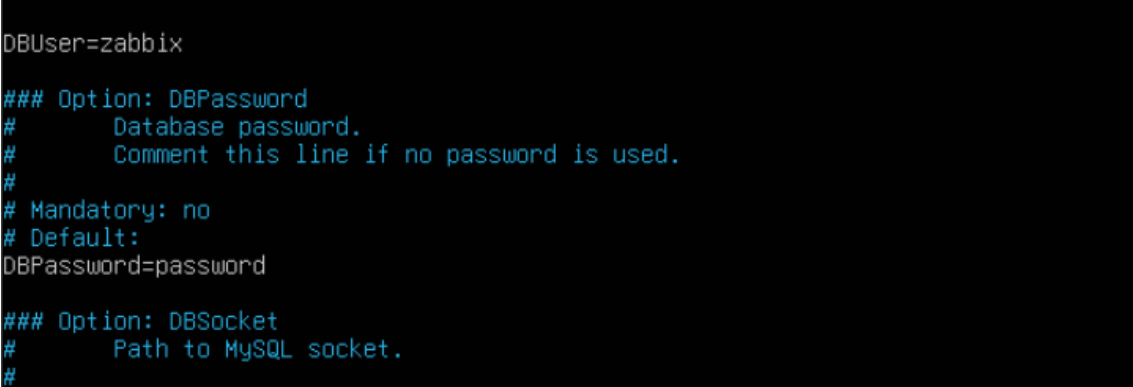
```
# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --
default-character-set=utf8mb4 -uzabbix -p zabbix
```

#### 2.1.5. Configuración de la base de datos para el servidor Zabbix

Para hacer uso de la base de datos del servidor se debe establecer una contraseña a la base de datos (ver fig 17) con el siguiente comando:

```
# sudo nano /etc/zabbix/zabbix_server.conf
```

Luego de estar dentro del archivo de configuración, buscamos el parámetro DBPassword=password, y guardamos luego de realizar el cambio, adicionalmente se debe eliminar el carácter “#”.



```
DBUser=zabbix
### Option: DBPassword
# Database password.
# Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=password
### Option: DBSocket
# Path to MySQL socket.
#
```

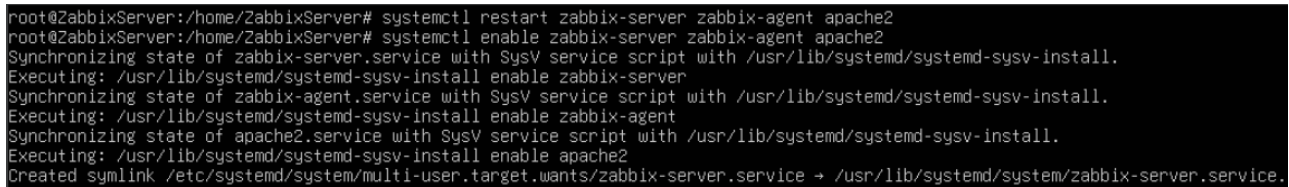
Fig. 17 Configuración de la base de datos



### 2.1.6. *Iniciación de los procesos del agente y del servidor Zabbix*

Para iniciar el servicio, es necesario reiniciar el servidor de Zabbix y los procesos del agente (ver figura 18). Además, se debe habilitar el servidor para que se reinicie automáticamente en caso de un corte de energía u otras interrupciones. Para ello, utilizamos los siguientes comandos:

```
# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2
```



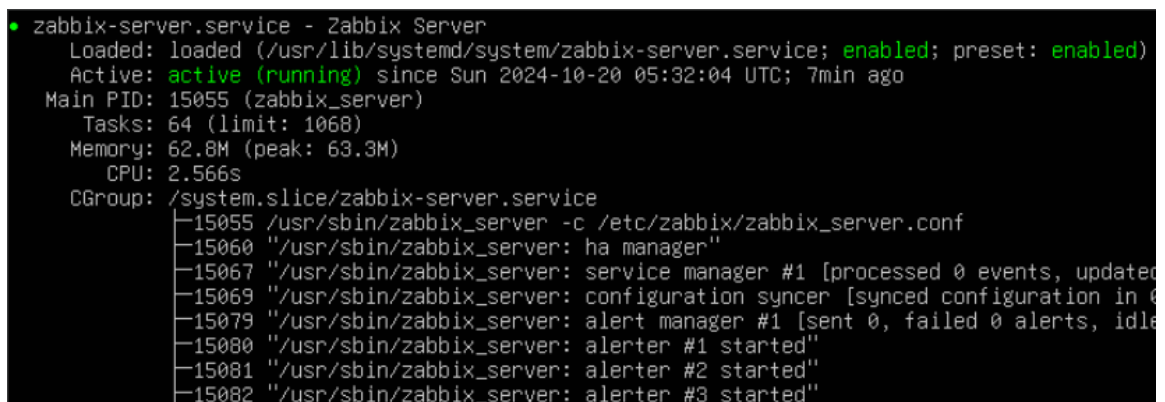
```
root@ZabbixServer:/home/ZabbixServer# systemctl restart zabbix-server zabbix-agent apache2
root@ZabbixServer:/home/ZabbixServer# systemctl enable zabbix-server zabbix-agent apache2
Synchronizing state of zabbix-server.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable zabbix-server
Synchronizing state of zabbix-agent.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable zabbix-agent
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-server.service → /usr/lib/systemd/system/zabbix-server.service.
```

**Fig. 18** Inicio de los procesos del agente y del servidor Zabbix

### 2.1.7. *Verificación del estado del servidor Zabbix*

Una vez se haya completado estos pasos, es importante verificar el estado tanto del del servidor (ver figura 19) como del agente (ver figura 20). Esto nos permitirá confirmar que ambos estén activos y que podamos acceder al servidor sin inconveniente. Si alguno de ellos no está en funcionamiento, es posible que se haya producido un error en la configuración.

```
# systemctl status zabbix-server
# systemctl status zabbix-agent
```



```
• zabbix-server.service - Zabbix Server
   Loaded: loaded (/usr/lib/systemd/system/zabbix-server.service; enabled; preset: enabled)
   Active: active (running) since Sun 2024-10-20 05:32:04 UTC; 7min ago
   Main PID: 15055 (zabbix_server)
     Tasks: 64 (limit: 1068)
    Memory: 62.8M (peak: 63.3M)
       CPU: 2.566s
    CGroup: /system.slice/zabbix-server.service
           └─15055 /usr/sbin/zabbix_server -c /etc/zabbix/zabbix_server.conf
             └─15060 "/usr/sbin/zabbix_server: ha manager"
               └─15067 "/usr/sbin/zabbix_server: service manager #1 [processed 0 events, updated
                 └─15069 "/usr/sbin/zabbix_server: configuration syncer [synced configuration in 0
                   └─15079 "/usr/sbin/zabbix_server: alert manager #1 [sent 0, failed 0 alerts, idle
                     └─15080 "/usr/sbin/zabbix_server: alerter #1 started"
                       └─15081 "/usr/sbin/zabbix_server: alerter #2 started"
                         └─15082 "/usr/sbin/zabbix_server: alerter #3 started"
```

**Fig. 19** Estado del servidor Zabbix

```

root@ZabbixServer:/home/ZabbixServer# systemctl status zabbix-agent
● zabbix-agent.service - Zabbix Agent
   Loaded: loaded (/usr/lib/systemd/system/zabbix-agent.service; enabled; preset: enabled)
   Active: active (running) since Sun 2024-10-20 05:32:04 UTC; 8min ago
   Main PID: 15041 (zabbix_agentd)
     Tasks: 13 (limit: 1068)
    Memory: 9.3M (peak: 10.3M)
       CPU: 815ms
    CGroup: /system.slice/zabbix-agent.service
           └─15041 /usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf
             └─15042 "/usr/sbin/zabbix_agentd: collector [idle 1 sec]"
               └─15043 "/usr/sbin/zabbix_agentd: listener #1 [waiting for connection]"
                 └─15044 "/usr/sbin/zabbix_agentd: listener #2 [waiting for connection]"
                   └─15045 "/usr/sbin/zabbix_agentd: listener #3 [waiting for connection]"

```

Fig. 20 Estado del agente Zabbix

### 2.1.8. Configuración de la interfaz web

Ahora que hemos confirmado que todos los servicios están activos, podemos acceder a la interfaz de Zabbix ingresando la URL con la dirección IP del servidor (ver figura 21). En este caso, sería de la siguiente manera: <http://192.168.1.20/zabbix>. Este acceso se puede realizar desde cualquier navegador.

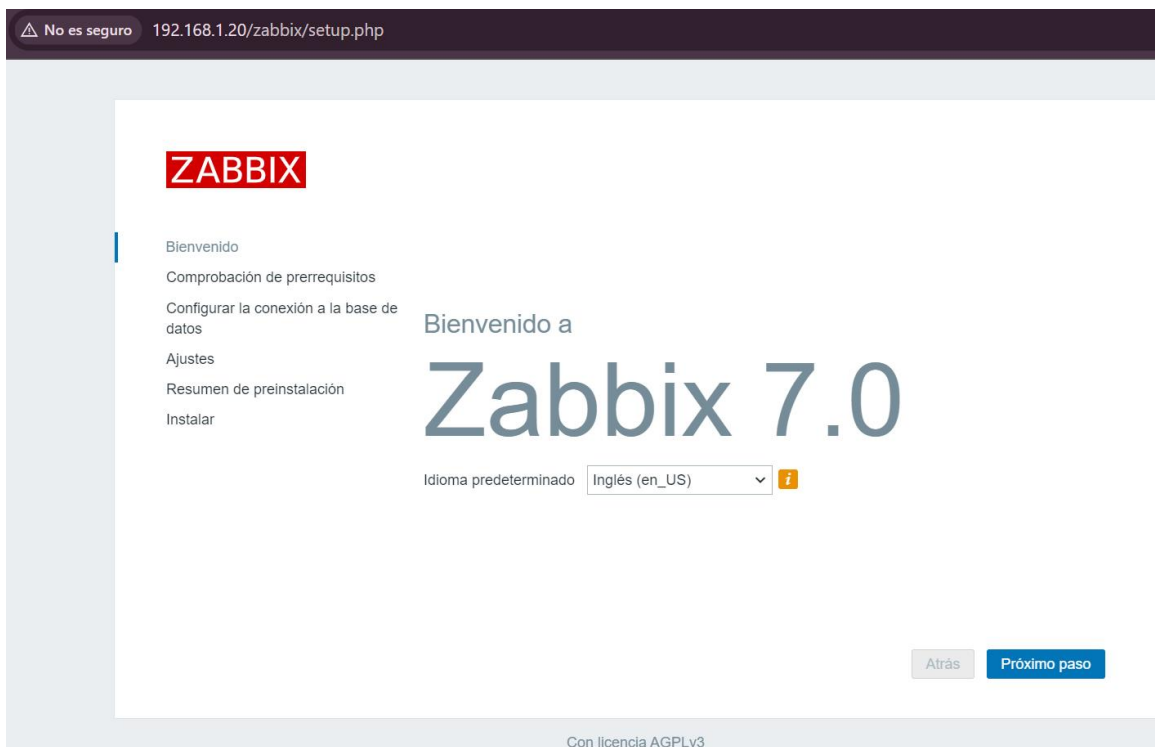


Fig. 21 Interfaz de bienvenida

### 2.1.9. Comprobación de prerequisites

Una vez que continuamos en la interfaz, debemos verificar los requisitos previos del servidor. Todos estos componentes deben estar en estado “OK” para poder avanzar con el proceso de instalación (ver figura 22).

The screenshot shows the Zabbix web interface at the URL 192.168.1.20/zabbix/setup.php. The main heading is 'Check of pre-requisites'. A table lists various system requirements with their current values and required values, all marked as 'OK'. The table is as follows:

	Current value	Required	
PHP version	8.3.6	8.0.0	OK
PHP option "memory_limit"	128M	128M	OK
PHP option "post_max_size"	16M	16M	OK
PHP option "upload_max_filesize"	2M	2M	OK
PHP option "max_execution_time"	300	300	OK
PHP option "max_input_time"	300	300	OK
PHP databases support	MySQL		OK
PHP bcmath	on		OK
PHP mbstring	on		OK
PHP option "mbstring.func_overload"	off	off	OK

At the bottom right of the table area, there are two buttons: 'Back' and 'Next step'. Below the table area, a footer indicates 'Licensed under AGPLv3'.

**Fig. 22** Verificación de prerequisites en la interfaz web

### 2.1.10. Configuración de la conexión a la base de datos

Una vez que avancemos, es necesario configurar la conexión a la base de datos, como se observa en la figura 23. Para ello, es importante tener en cuenta las configuraciones que realizamos anteriormente al instalar la base de datos.

192.168.1.20/zabbix/setup.php

**ZABBIX**

### Configurar la conexión a la base de datos

Cree la base de datos manualmente y configure los parámetros para conectarse a ella. Presione el botón "Siguiente paso" cuando haya terminado.

Bienvenido  
 Comprobación de prerequisites  
 Configurar la conexión a la base de datos  
 Ajustes  
 Resumen de preinstalación  
 Instalar

Tipo de base de datos:

Host de base de datos:

Puerto de base de datos:  0 - utilizar puerto predeterminado

Nombre de la base de datos:

Almacenar credenciales en:  Texto simple  Bóveda de HashiCorp  Bóveda de CyberArk

Usuario:

Contraseña:

Cifrado TLS de la base de datos: *La conexión no se cifrará porque utiliza un archivo de socket (en Unix) o memoria compartida (Windows).*

Con licencia [AGPLv3](#)

**Fig. 23** Configuración de la conexión a la base de datos

### 2.1.11. Ajustes adicionales

Como ajustes adicionales, es necesario asignar un nombre al servidor o, alternativamente, dejar los valores predeterminados, como se observa en la figura 24. Esto facilita la distinción entre varios servidores. En este caso, se utilizará el nombre “Padtec”. También se deberá seleccionar la zona horaria y el tema de la interfaz gráfica.

**ZABBIX**

### Settings

Zabbix server name:

Default time zone:

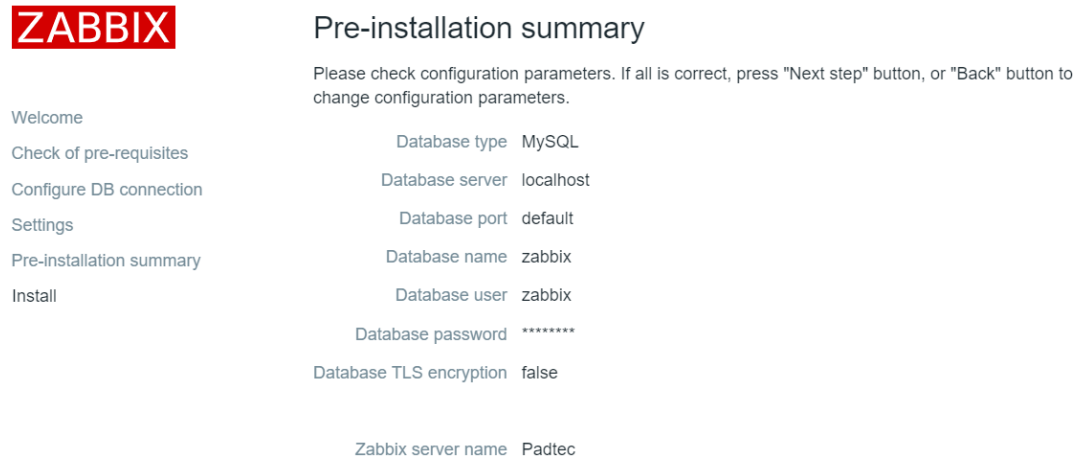
Default theme:

Welcome  
 Check of pre-requisites  
 Configure DB connection  
 Settings  
 Pre-installation summary  
 Install

**Fig. 24** Ajustes adicionales del servidor

### 2.1.12. Resumen de preinstalación

Luego de continuar, se mostrará un resumen de la preinstalación que se va a llevar a cabo (ver figura 25). Se verifican todos los parámetros que configuramos anteriormente, como el nombre de la base de datos, la contraseña y el usuario, para poder continuar con la instalación. Es importante tener en cuenta que, en este punto, pueden aparecer errores relacionados con la instalación que debemos corregir.



**ZABBIX**

Pre-installation summary

Please check configuration parameters. If all is correct, press "Next step" button, or "Back" button to change configuration parameters.

Welcome

Check of pre-requisites

Configure DB connection

Settings

Pre-installation summary

Install

Database type MySQL

Database server localhost

Database port default

Database name zabbix

Database user zabbix

Database password \*\*\*\*\*

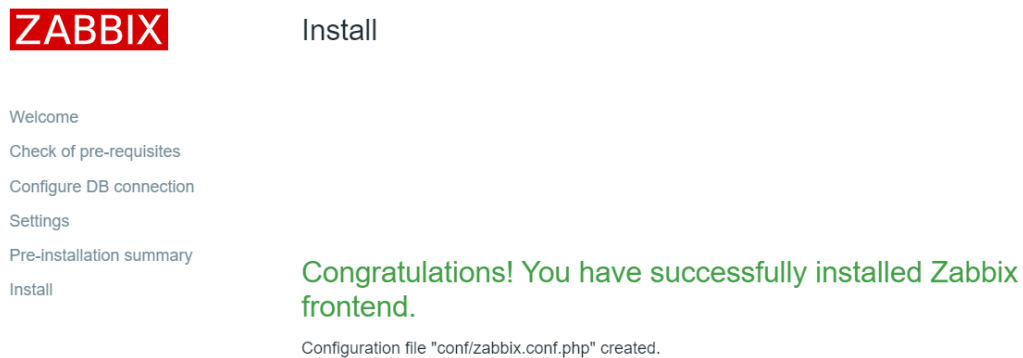
Database TLS encryption false

Zabbix server name Padtec

**Fig. 25** Resumen de la preinstalación

### 2.1.13. Instalación de Zabbix

Como configuración final de la instalación, después de seguir todos los pasos, se debería ver un mensaje que indique que la instalación ha sido exitosa, similar al de la figura 26. En este caso, proceda a hacer clic en “Finalizar”.



**ZABBIX**

Install

Welcome

Check of pre-requisites

Configure DB connection

Settings

Pre-installation summary

Install

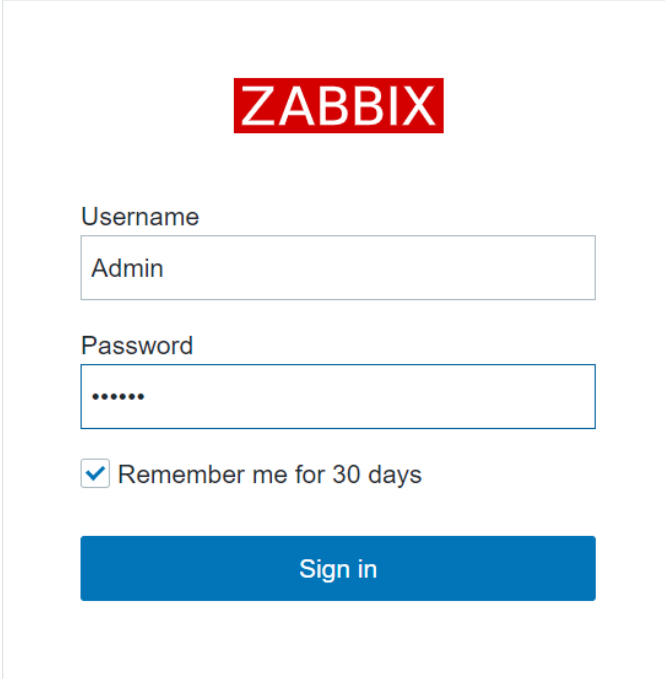
**Congratulations! You have successfully installed Zabbix frontend.**

Configuration file "conf/zabbix.conf.php" created.

**Fig. 26** Instalación exitosa de la interfaz web

#### 2.1.14. Inicio de sesión al servidor

Una vez finalizada la instalación, la interfaz nos llevará a ingresar el usuario y la contraseña para acceder. Se abrirá automáticamente la página de inicio de sesión, donde se podrá acceder al servidor utilizando el nombre de usuario “Admin” y la contraseña predeterminada “zabbix”, según se muestra en la figura 27.

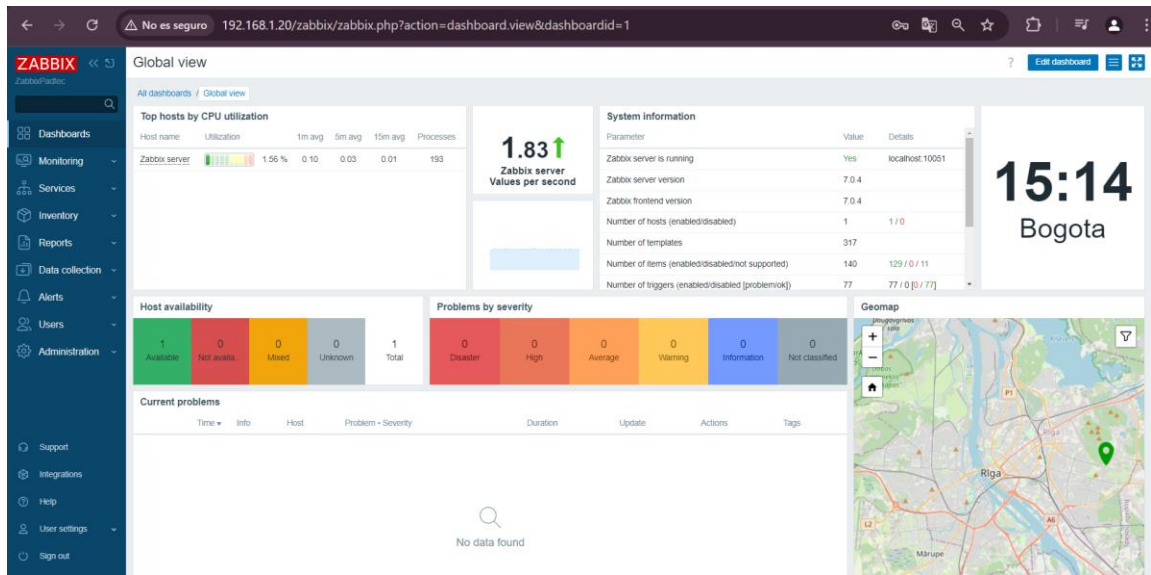


The image shows the Zabbix login interface. At the top, the word "ZABBIX" is displayed in white text on a red rectangular background. Below this, the form contains the following elements: a "Username" label above a text input field containing "Admin"; a "Password" label above a password input field containing six dots; a checked checkbox with the text "Remember me for 30 days"; and a blue rectangular button with the text "Sign in" in white.

**Fig. 27** Inicio de sesión Zabbix

#### 2.1.15. Interfaz web de Zabbix

Una vez que iniciemos sesión, se mostrará la página principal de Zabbix. En esta página, veremos varios parámetros, como el estado del sistema, que indicará si el Zabbix Server está funcionando correctamente (yes) junto con el puerto de conexión (10051). También se mostrará información sobre los hosts activos, los problemas detectados y un panel de control que presenta los componentes para el monitoreo de red (ver figura 28).



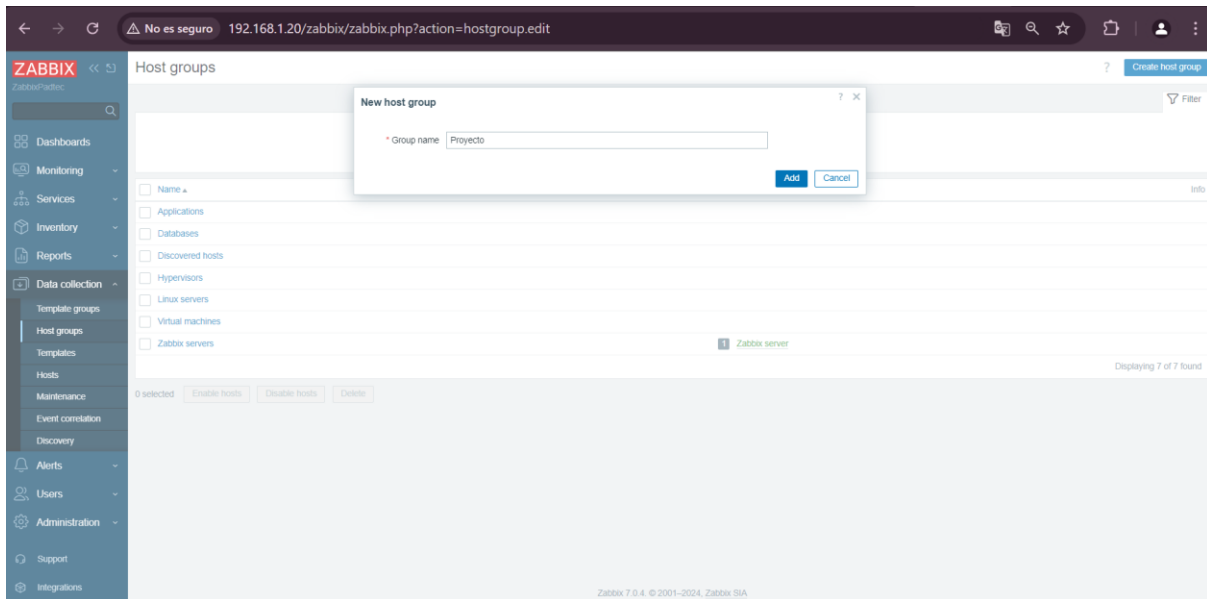
**Fig. 28** Panel de control del servidor

## 2.2. Creación de grupos de Host y de un Host

La configuración de grupos de Host permitirá la organización y el almacenamiento de múltiples host en Zabbix, sirviendo como un distintivo para todos los dispositivos que pertenezcan a este grupo. La creación de un host permitirá integrar un equipo en Zabbix para su posterior monitorización.

### 2.2.1. Configuración grupo de Host

Para configurar un grupo de Hosts, primero dirigirse al panel de control de Zabbix y seleccionar la opción “Recopilación de Datos”. Luego, accede a “Host Groups”. En la parte superior derecha de la pantalla, se encontrará la opción “Create Groups”. Haga clic en ella, y se abrirá una interfaz donde se ingresará el nombre distintivo para el grupo. En este caso, se nombrará “Proyecto” para incluir en este grupo los routers UfiSpace corporativos (ver figura 29). Es fundamental crear un grupo de hosts para facilitar la administración y la búsqueda de dispositivos específicos.



**Fig. 29** Creación del grupo de host “Proyecto”

### 2.2.2. Configuración del Host

Para la configuración de un Host, nos dirigimos de nuevo a la parte de “Recopilación de Datos”, donde escogemos la opción de Host. Luego, nos llevará a una interfaz donde se van a encontrar todos los Host creados, en la parte superior derecha de la pantalla, elegimos la opción “Create host”.

En la configuración del nuevo host se deberá llenar los parámetros solicitados de la siguiente manera (ver interfaz en la figura 30):

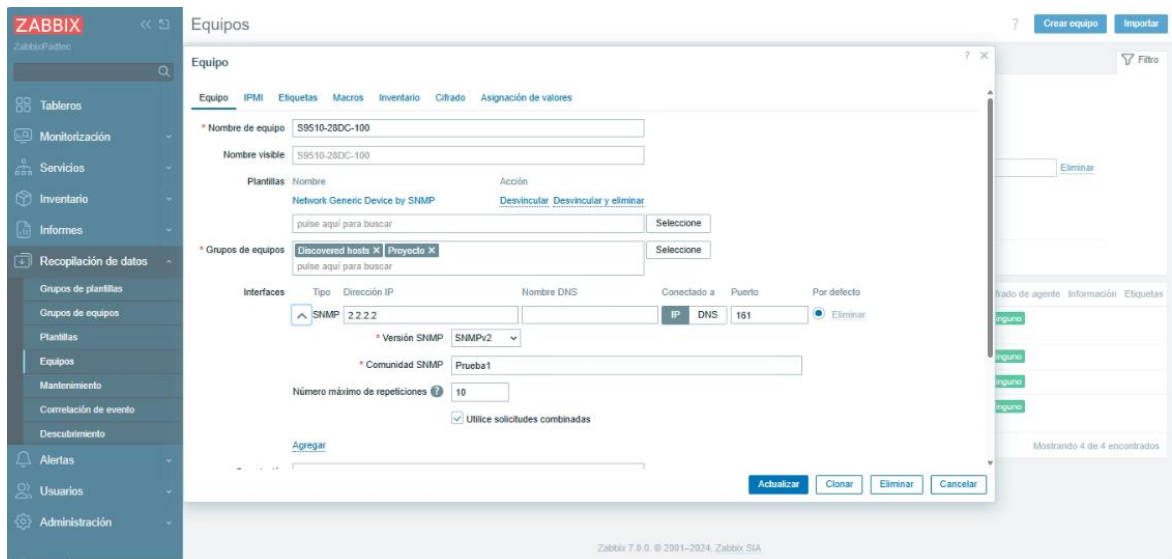
**Host name:** S9510-28DC-100; el nombre del primer router que se va a monitorear.

**Templates:** Network Generic Device by SNMP; se hará uso de una plantilla estándar para todos los router.

**Host groups:** Proyecto; grupo de host donde se van a encontrar los dispositivos respectivos a este proyecto.

**Interfaces:** En esta sección, se debe ingresar la dirección IP que identifica la interfaz OpenZR+, en este caso, se utilizará la dirección de loopback 2.2.2.2. El puerto predeterminado para el protocolo SNMP es el 161, y se optará por la versión SNMPv2. Finalmente, se ingresará la comunidad SNMP con el valor “prueba1”.





**Fig. 30** Configuración del host

### 2.2.3. Configuración del protocolo SNMP en los Routers

Para establecer una comunicación adecuadamente entre los router y el servidor de Zabbix, es necesario realizar las configuraciones SNMP adecuadas, que permiten responder a las solicitudes a través de los OID.

Primero, es fundamental asegurar un correcto direccionamiento de las interfaces, garantizando que tenga una dirección IP dentro de la misma red que el servidor, lo que facilitará una conectividad exitosa. En nuestro caso, utilizamos la interface loopback, enrutada por medio del protocolo OSPF, lo que asegura la comunicación entre el servidor Zabbix y el router.

Una vez lograda la conectividad entre los dispositivos, se procede a configurar el protocolo SNMP en el router. Para ello, tenemos en cuenta los siguientes comandos:

```
# enable
# configure terminal
# snmp-server view all .1 included
# snmp-server community Prueba1 group network-admin
# snmp-server enable snmp
# end
```

```
# copy running-config startup-config
```

### 2.2.4. Verificación de la configuración SNMP

Para verificar que la configuración se realizó con éxito, debemos dirigirnos a la sección donde se encuentran los hosts. Allí, habrá un recuadro marcado con las letras “SNMP” que debe aparecer en color verde como se observa en la figura 31. Este cambio de color indica que el sistema está siendo monitoreado correctamente.

The screenshot shows the Zabbix web interface for managing devices. The left sidebar contains navigation options like 'Equipos', 'Plantillas', and 'Alertas'. The main content area is titled 'Equipos' and includes a form to add a new device with fields for 'Nombre', 'DNS', 'IP', and 'Puerto'. Below the form is a table of existing devices. The table has columns for 'Nombre', 'Monitores', 'Iniciadores', 'Gráficos', 'Descubrimiento', 'Web', 'Interfaz', 'Proxy', 'Plantillas', 'Estado', 'Disponibilidad', and 'Cifrado de agente'. The 'Estado' column shows 'Activado' for all devices, and the 'Disponibilidad' column shows 'SNMP' in green for all devices, indicating successful configuration.

Nombre	Monitores	Iniciadores	Gráficos	Descubrimiento	Web	Interfaz	Proxy	Plantillas	Estado	Disponibilidad	Cifrado de agente	Información
DM4370	13	8		2	192.168.21.2	161		Template SNMP trap, Template SNMP trap fallback	Activado	SNMP	Ninguno	
S9510-28DC-100	334	146	41	3	2.2.2.2	161		Network Generic Device by SNMP	Activado	SNMP	Ninguno	
S9510-28DC-101	416	182	46	2	1.1.1.1	161		Network Generic Device by SNMP	Activado	SNMP	Ninguno	
Zabbix server	142	78	27	5	127.0.0.1	10050		Linux by Zabbix agent, Zabbix server health	Activado	ZBX	Ninguno	

Fig. 31 Dispositivos enlazados con SNMP

### 2.2.5. Parámetros a monitorear

Una vez que hemos configurado adecuadamente los hosts y verificado que los equipos enlazan correctamente con el servidor de Zabbix a través de SNMP, procedemos a identificar las variables que se van a monitorear.

El monitoreo de estos parámetros depende en gran medida de la plantilla seleccionada al crear el host, en este caso, “Network Generic Device by SNMP”. Esta plantilla utiliza los OID (Object Identifiers) para extraer una serie de parámetros importantes para la supervisión del dispositivo.

Primero, la plantilla verifica la conectividad con el dispositivo a través de un ping. Luego, realiza un escaneo de todo el equipo, identificando y describiendo cada una de sus interfaces y su nomenclatura. Durante este proceso de descubrimiento, se asocian diversos parámetros clave a cada interfaz, tales como los bits recibidos, bits enviados, paquetes descartados, paquetes con errores, tipo de interfaz, estado operacional, velocidad, entre otros, como se muestra en la figura 32.

Nombre	Monitor	Intervalo	Histórico	Tendencias	Tipo	Crear habilitado	Descubrir	Etiquetas
Network Generic Device by SNMP: Interface {#IFNAME} {#IFALIAS}: Bits received	net.if.in[ifName]{#SNMPINDEX}	1m	7d	365d	Agente SNMP	Si	Si	component: network interface: {#IFNAME} description: {#IFALIAS}
Network Generic Device by SNMP: Interface {#IFNAME} {#IFALIAS}: Bits sent	net.if.out[ifName]{#SNMPINDEX}	1m	7d	365d	Agente SNMP	Si	Si	component: network interface: {#IFNAME} description: {#IFALIAS}
Network Generic Device by SNMP: Interface {#IFNAME} {#IFALIAS}: Inbound packets discarded	net.if.in.discards[ifName]{#SNMPINDEX}	3m	7d	365d	Agente SNMP	Si	Si	component: network interface: {#IFNAME} description: {#IFALIAS}
Network Generic Device by SNMP: Interface {#IFNAME} {#IFALIAS}: Inbound packets with errors	net.if.in.errors[ifName]{#SNMPINDEX}	3m	7d	365d	Agente SNMP	Si	Si	component: network interface: {#IFNAME} description: {#IFALIAS}
Network Generic Device by SNMP: Interface {#IFNAME} {#IFALIAS}: Interface type	net.if.type[ifName]{#SNMPINDEX}	1h	7d	0	Agente SNMP	Si	Si	component: network interface: {#IFNAME} description: {#IFALIAS}
Network Generic Device by SNMP: Interface {#IFNAME} {#IFALIAS}: Operational status	net.if.status[ifName]{#SNMPINDEX}	1m	7d	0	Agente SNMP	Si	Si	component: network interface: {#IFNAME} description: {#IFALIAS}
Network Generic Device by SNMP: Interface {#IFNAME} {#IFALIAS}: Outbound packets discarded	net.if.out.discards[ifName]{#SNMPINDEX}	3m	7d	365d	Agente SNMP	Si	Si	component: network interface: {#IFNAME} description: {#IFALIAS}
Network Generic Device by SNMP: Interface {#IFNAME} {#IFALIAS}: Outbound packets with errors	net.if.out.errors[ifName]{#SNMPINDEX}	3m	7d	365d	Agente SNMP	Si	Si	component: network interface: {#IFNAME} description: {#IFALIAS}
Network Generic Device by SNMP: Interface {#IFNAME} {#IFALIAS}: Speed	net.if.speed[ifName]{#SNMPINDEX}	5m	7d	0	Agente SNMP	Si	Si	component: network interface: {#IFNAME} description: {#IFALIAS}

Fig. 32 Parámetros determinados por la plantilla

### 2.2.6. Creación de nuevos parámetros

Para identificar nuevos parámetros de monitoreo, procedemos a crear nuevos monitores específicos en cada uno de los dispositivos. Esto nos permitirá obtener datos adicionales que proporcionen información crítica para la toma de decisiones por parte del equipo de operaciones.

El primer paso en este proceso fue llevar a cabo una investigación exhaustiva sobre el árbol de MIB de los dispositivos, lo que nos permitió identificar los OID correspondientes a los parámetros adicionales que deseamos monitorear. Entre los OID más relevantes encontrados para la interfaz OpenZR+, se destacan los siguientes parámetros detallados en la Tabla 2:

**Tabla 2** OID que identifica los parámetros relevantes de monitoreo.

PARÁMETRO	OID
Power IN	.1.3.6.1.4.1.36673.100.1.20.1.6.1.2.1.1.0.67.1
Power Out	.1.3.6.1.4.1.36673.100.1.20.1.6.1.2.1.1.0.64.1
OSNR	.1.3.6.1.4.1.36673.100.1.20.1.6.1.2.1.1.0.29.1
ESNR	.1.3.6.1.4.1.36673.100.1.20.1.6.1.2.1.1.0.30.1
Pre-FEC BER Avg	.1.3.6.1.4.1.36673.100.1.20.1.6.1.2.1.1.0.11.1
Temperatura del modulo	.1.3.6.1.4.1.36673.100.1.20.1.4.1.2.1.1.0.2

### 2.2.7. Configuración de monitores

Para la configuración de un Monitor, nos dirigimos de nuevo a la parte de “Recopilación de Datos”, donde escogemos la opción de Equipos. Luego, nos llevará a una interfaz donde se van a encontrar todos los Equipos creados, seleccionamos el apartado “Monitores” del equipo al cual le vamos a crear el monitor y en la parte superior derecha de la pantalla, elegimos la opción “Crear monitor”.

En la configuración del nuevo monitor se deberá llenar los parámetros solicitados de la siguiente manera (ver figura 33):

**Nombre:** Interface cd0(cd0): Power OUT; el nombre de la variable que se va a monitorear.

**Tipo:** Agente SNMP; será el tipo de SNMP del dispositivo.

**Monitor:** net.if.pout

**Tipo de información:** Numérico (coma flotante); tipo del valor que se va a recopilar.

**Interfaz del equipo:** 2.2.2.2:161; Dirección IP y puerto al que está asociado la interfaz a monitorear.

**SNMP OID:** .1.3.6.1.4.1.36673.100.1.20.1.6.1.2.1.1.0.64.1; OID que identifica la potencia de salida.

**Unidad:** dBm; unidades en las que se encuentra el valor.

**Intervalo de actualización:** 1m; intervalo que se va a actualizar el valor, “m” referente a minuto.

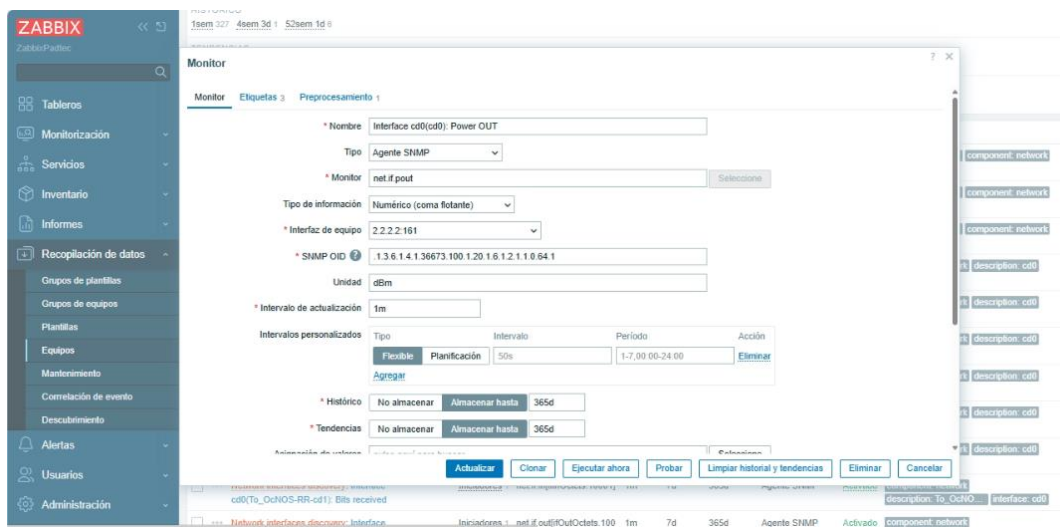


Fig. 33 Configuración del monitor

Los OID recopila estos valores en formato entero, por lo que es necesario realizar un procesamiento adicional para poder convertirlos a su unidad original. Para llevar a cabo esta conversión, en la sección superior seleccionamos la opción “Preprocesamiento”. A continuación, agregamos un nuevo preprocesamiento y elegimos la opción “Personalizar multiplicador”. En este caso, el parámetro que debemos establecer es “0.01”, como se presenta en la figura 34.



Fig. 34 Preprocesamiento de la variable

Para verificar que se está obteniendo el valor adecuado, seleccionamos el apartado en la parte inferior “Probar” en la figura 35. Luego, seleccionamos “Obtener valor y probar”.

En nuestro caso estamos saliendo con una potencia de 0 dBm desde la interfaz OpenZR+ (cd0).

Fig. 35 Verificación del valor recopilado

En el router podemos observar como el valor de la potencia de salida es similar al que nos muestra la plataforma Zabbix. Además, nos entrega: | potencia actual (-0.00) | potencia máxima genera alarma (6.00) | potencia máxima recomendada (4.00) | potencia mínima recomendada (-16.00) | potencia mínima genera alarma (-18.01) | unidades del valor (dBm)

```
S9510-28DC-100#show qsfp-dd 0 monitors media | include Tx Optical Power
Tx Optical Power      | 1 | -0.00 | 6.00 | 4.00
-16.00 | -18.01 | dBm |
S9510-28DC-100#
```

Fig. 36 Potencia de salida desde el router

### 2.2.8. Configuración de las gráficas

Para la configuración gráfica de los datos, debemos generar las gráficas específicas para cada monitor creado.

Primero, nos dirigimos de nuevo a la parte de “Recopilación de Datos”, donde escogemos la opción de Equipos. Luego, nos llevará a una interfaz donde se van a encontrar todos los

Equipos creados, seleccionamos el apartado “Gráficos” del equipo al cual le vamos a generar el gráfico y en la parte superior derecha de la pantalla, elegimos la opción “Crear gráficos”.

En el apartado “Monitores”, seleccionamos el monitor el cual queremos visualizar, como se ve en la figura 37.

**Fig. 37** Configuración de la gráfica

### 2.2.9. Verificación de las gráficas

Una vez que hemos creado las gráficas para cada uno de los monitores establecidos, procedemos a revisar las visualizaciones que Zabbix proporciona para el monitoreo de las interfaces OpenZR+. A continuación, examinaremos gráficamente los parámetros más relevantes.

Para ello, nos dirigimos a la sección de “Monitorización”, y luego accedemos a “Equipos”. En el apartado de “Gráficos” asociados al dispositivo que deseamos visualizar, encontraremos todas las gráficas generadas. Esto nos permitirá analizar de manera efectiva

al rendimiento de la interfaz OpenZR+ y tomar decisiones informadas basadas en los datos presentados.

### 3. RESULTADOS DE LAS GRÁFICAS DE LOS PARÁMETROS PRINCIPALES MONITOREADOS

#### 3.1. Monitoreo de potencia de entrada y salida en la interfaz OpenZR+

Estas gráficas nos muestran los valores históricos y en tiempo real de la potencia de entrada y de salida en la interfaz OpenZR+ del router UfiSpace. Estos datos se pueden observar en un periodo de tiempo de actualización cada 30 segundos aproximadamente, el históricos de estas gráficas se puede observar desde hace 5 minutos hasta 1 año atrás, según se requiera. En la grafica 37 se observa el comportamiento de las potencias de salida y entrada de la interfaz OpenZR+ del router UfiSpace.

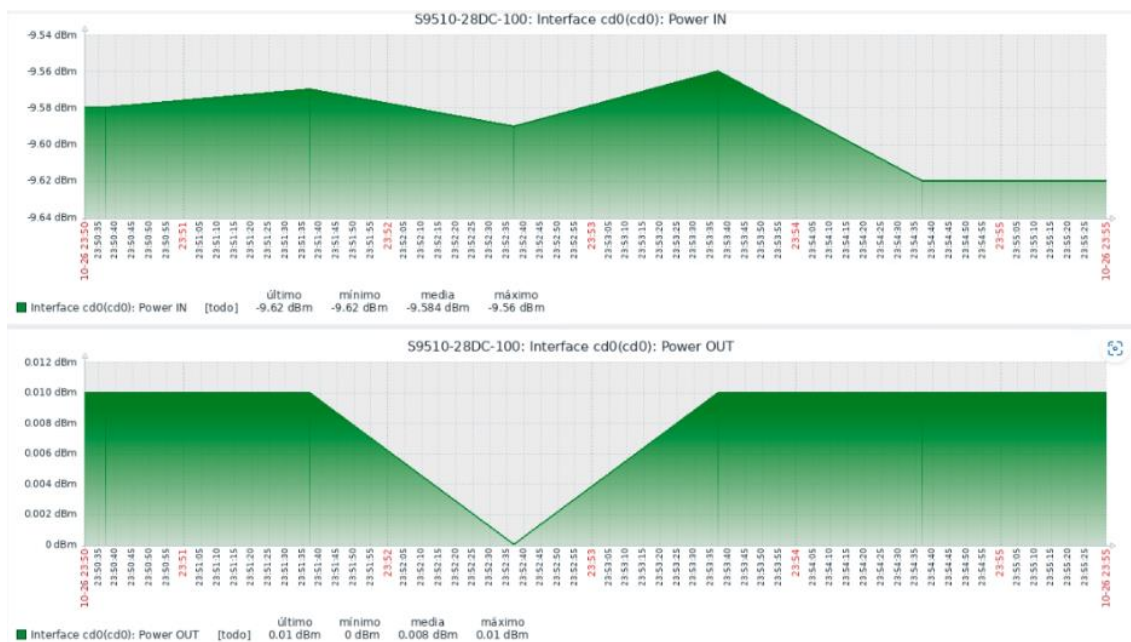


Fig. 38 Potencia de entrada y Potencia de salida de la interfaz OpenZR+ del router

#### 3.2. Monitoreo de OSNR en la interfaz OpenZR+ del router UfiSpace

Esta gráfica nos muestra los valores históricos y en tiempo real del OSNR en la interfaz OpenZR+ del router UfiSpace monitoreado y así poder obtener una medida determinada e



histórica del valor señal-ruido. Estos datos se pueden observar igual que los anteriores en un periodo de tiempo de actualización cada 30 segundos aproximadamente.

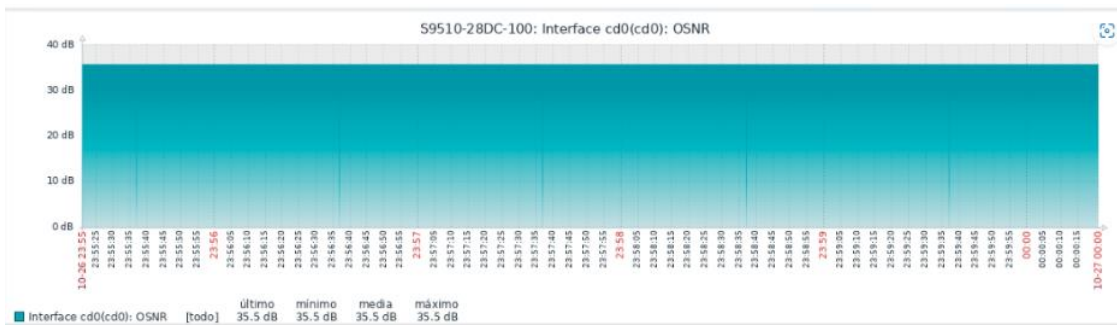


Fig. 39 OSNR de la interfaz OpenZR+ del router

### 3.3. Monitoreo PREFEC y TEMPERATURA del receptor en la interfaz OpenZR+

Para estas gráficas se determina el pre-FEC el cual nos indica el número de error de bits, adicionalmente se grafican los valores de la temperatura del módulo de la interfaz OpenZR+. Al igual que las anteriores gráficas, estos datos se pueden observar en un periodo de tiempo de actualización cada 30 segundos aproximadamente y determinar el tiempo histórico según sea la necesidad.

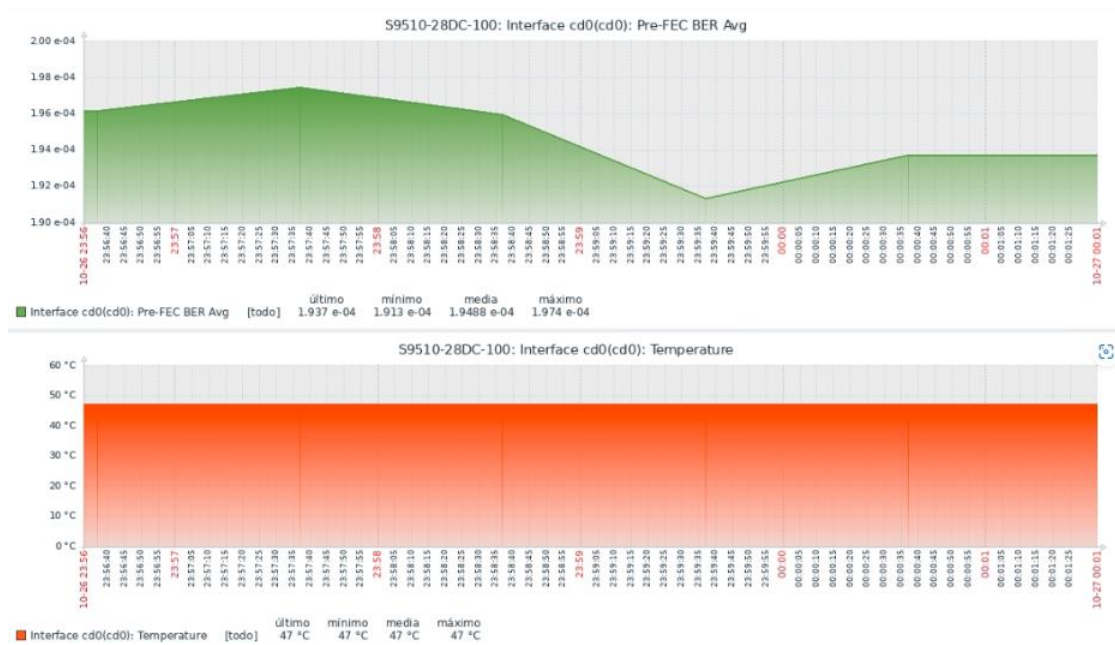


Fig. 40 Pre-FEC y Temperatura del módulo en la interfaz OpenZR+ del router

### 3.4. Monitoreo tráfico en la red.

En esta gráfica observamos todo el valor de tráfico en la interfaz OpenZR+ del router, el número de bits recibidos y enviados, paquetes con errores y descartados, estos valores son los medidos por la plantilla predefinida por Zabbix. Al igual que las anteriores gráficas estos datos se pueden observar en un periodo de tiempo de actualización cada 30 segundos aproximadamente y determinar el tiempo histórico según sea la necesidad.

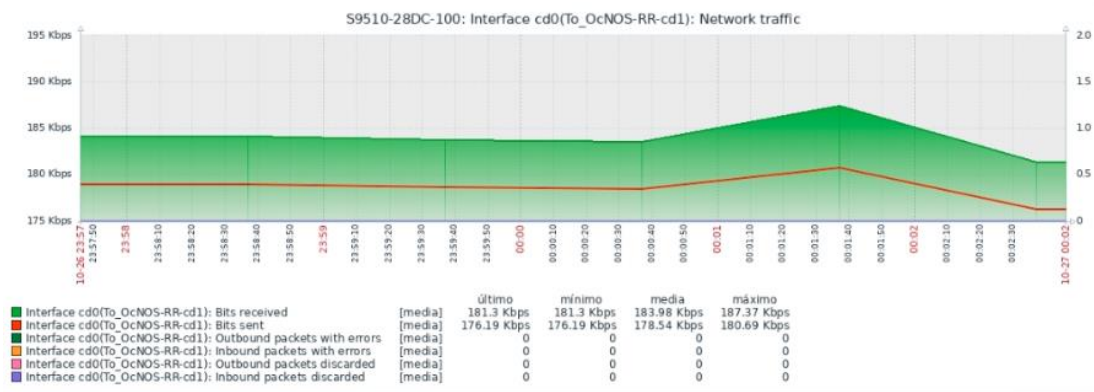


Fig. 41 Parámetros obtenidos por la plantilla predeterminada

Uno de los propósitos del monitoreo es determinar un ajuste óptimo de parámetros para asegurar que las redes IPoDWDM cumplan con los estándares de calidad del servicio y sirva para implementar alarmas. A continuación, se presenta la implementación de alarmas e informes periódicos de desempeño, como apoyo al equipo de gestión de la empresa.

### 3.5. Implementación de Informes y Alarmas

Para lograr un monitoreo más reactivo del equipo de operaciones ante las anomalías y eventos en la red, se integran los informes periódicos del dashboard creado en la interfaz web de Zabbix. Además, se activan las notificaciones de fallas y eventos, lo que permite una reacción más efectiva.

#### 3.5.1. Configuración de Informes programados en Zabbix

Para habilitar los informes programados en Zabbix, es necesario instalar el paquete adicional Zabbix-Web-Service. A continuación, se detallan los pasos a seguir:

En el servidor de Zabbix instalamos el paquete necesario.

```
# apt install Zabbix-web-service
# apt update
# apt upgrade
```

Una vez instalado el paquete, debemos configurar los parámetros necesarios en el archivo de configuración del servidor Zabbix. Esto incluye la limitación del número de reportes por día y la especificación de la URL del servicio web.

Para ello, accedemos a la carpeta de configuración del servidor Zabbix y editamos el archivo *zabbix\_server.conf*

```
# nano /etc/zabbix/zabbix_server.conf
```

Dentro de este archivo, buscamos las siguientes líneas y realizamos las configuraciones correspondientes:

**StartReporters:** Aquí se puede limitar el número de reportes que se generan por día. Por ejemplo, si se desea permitir 3 reportes diarios (como se señala en la figura 42), establece:

```
# StartReporters=3
```

**WebServiceURL:** Especifica la URL del servicio web. Si el servicio está instalado en la misma máquina virtual, la configuración será algo como esto señalado en la figura 42, incluyendo el puerto 10053:

```
# WebserviceURL=http://localhost:10053/report
```

Para finalizar se debe reiniciar el servicio de Zabbix.

```
### Option: StartReportWriters
#       Number of pre-forked report writer instances.
#
# Mandatory: no
# Range: 0-100
# Default:
StartReportWriters=3

### Option: WebserviceURL
#       URL to Zabbix web service, used to perform web related
WebserviceURL=http://192.168.1.20:10053/report
#
# Mandatory: no
# Default
```

Fig. 42 Configuración del Web Service

Para garantizar que el servicio web de Zabbix pueda aceptar conexiones desde las direcciones necesarias, es importante ajustar la configuración del archivo de webservice. Primero se debe editar el archivo de configuración del web service de Zabbix:

```
# nano /etc/zabbix/zabbix_web_service.conf
```

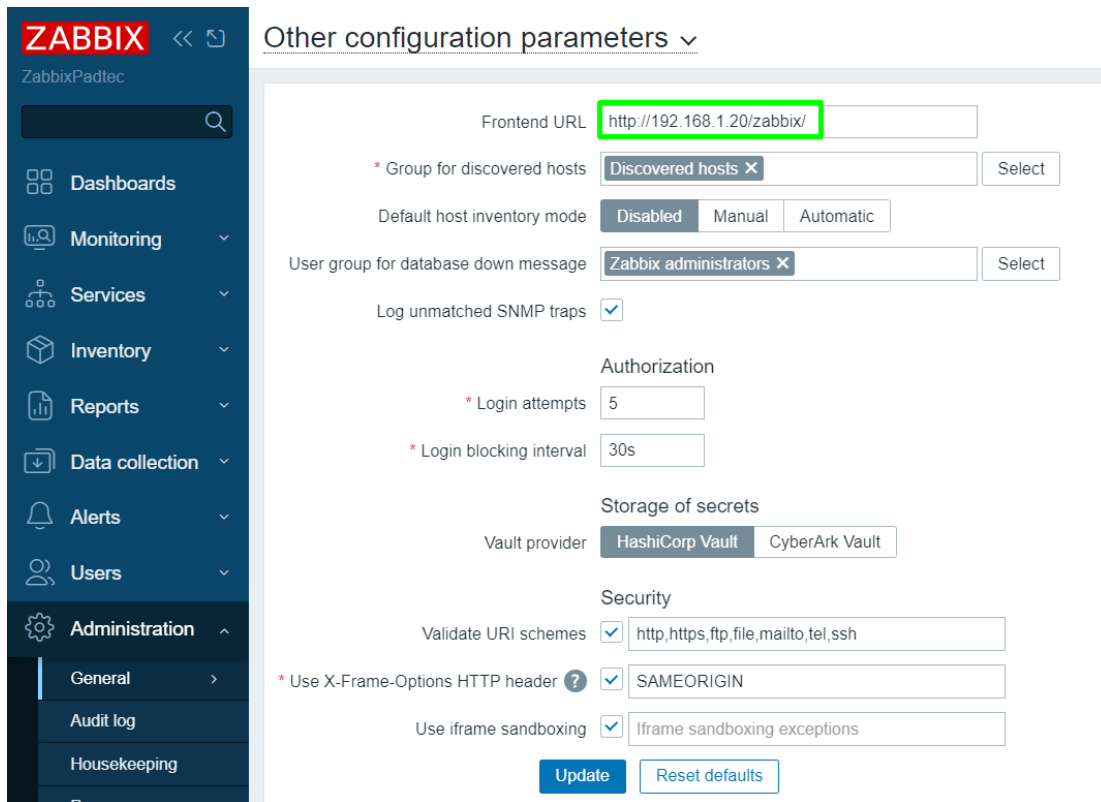
Buscamos la opción AllowedIP en el archivo. Esta configuración determina qué direcciones IP pueden acceder al servicio. Para permitir el acceso desde cualquier dirección IP, se puede configurar de la siguiente manera descrita en la figura 43. Además, de permitir conexiones IP, se debe asegurar que el servicio de correo esté debidamente configurado para interactuar con el web service.

```
### Option: AllowedIP
#       List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabbix servers and Zabbix proxies.
#       Incoming connections will be accepted only from the hosts listed here.
#       If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' are treated equally
#       and ':::0' will allow any IPv4 or IPv6 address.
#       '0.0.0.0/0' can be used to allow any IPv4 address.
#       Example: AllowedIP=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
#
# Mandatory: yes
# Default:
# AllowedIP=
AllowedIP=127.0.0.1,::1,0.0.0.0/0,zabbix, zabbix.example.com

### Option: ListenPort
#       Service will listen on this port for connections from the server.
#
# Mandatory: no
# Range: 1024-32767
# Default:
ListenPort=10053
```

Fig. 43 Configuración de los servicios

Para configurar la URL asociada a la instalación de Zabbix, se accede a la interfaz web. Ingresamos en la opción de *Administración -> General -> Otros*. Allí, buscamos el campo para ingresar la URL del servicio web y establece la dirección completa <http://192.168.1.20/zabbix/> (ver figura 44).



**Fig. 44** Configuración de la URL

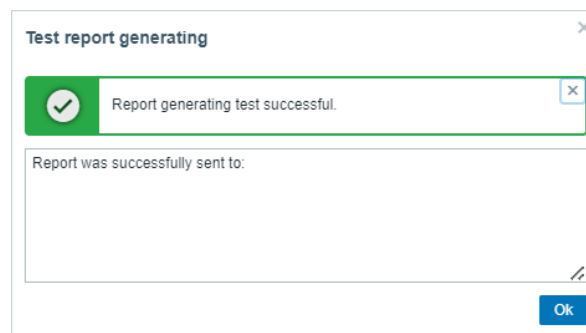
Para crear un reporte programado en Zabbix, nos dirigimos a la opción *reportes -> reportes programados* y seleccionamos crear reporte. En la configuración, se deben ajustar los parámetros según la necesidad, en nuestro caso decidimos que los reportes se generen cada semana, durante un mes empezando desde noviembre y terminando en diciembre. Además, se le asigna el dashboard creado que queremos enviar en el informe, un asunto y una descripción. Esta descripción se resume en la figura 45.

The screenshot shows the 'Scheduled reports' configuration interface in Zabbix. The left sidebar contains navigation options like Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Alerts, Users, Administration, Support, Integrations, Help, and User settings. The main area is titled 'Scheduled reports' and contains a form with the following fields and options:

- Owner:** Admin (Zabbix Administrator)
- Name:** Report
- Dashboard:** Global view
- Period:** Previous day, Previous week, Previous month, Previous year
- Cycle:** Daily, Weekly, Monthly, Yearly
- Start time:** 12 : 00
- Repeat on:** Monday, Tuesday, Wednesday, Thursday, Friday (checked), Saturday, Sunday
- Start date:** 2024-11-07
- End date:** 2024-12-28
- Subject:** Reporte de monitoreo
- Message:** Este es el reporte de monitoreo basado en la semana anterior.
- Subscriptions:** Recipient: Admin (Zabbix Administr...; Generate report by: Admin (Zabbix Admini...; Status: Include; Action: Remove
- Description:** (Empty text area)
- Enabled:**
- Buttons:** Update, Clone, Test (highlighted with a green arrow), Delete, Cancel

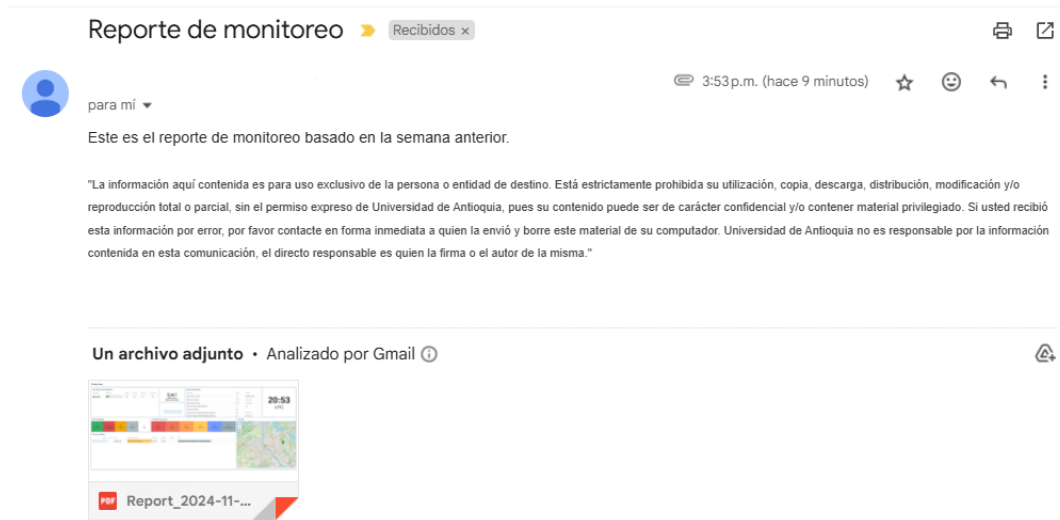
**Fig. 45** Configuración del reporte periódico

Como modo de prueba, generamos un reporte inmediato desde la opción Test, tal como se muestra en la figura 46. Al completar el proceso, aparecerá una pestaña confirmando que el reporte se ha enviado con éxito al correo asociado al perfil del usuario, similar al mostrado en la figura 46.



**Fig. 46** Envío del reporte

En el correo asociado, recibimos un archivo PDF que contiene el dashboard configurado y diseñado en Zabbix, lo que nos permite visualizar de manera clara y concisa la información relevante, como el indicado en la figura 47.



**Fig. 47** Correo recibido

#### 4. DESAGREGACIÓN DE LAS VARIABLES EN GRAFANA

Para optimizar el monitoreo y la presentación de resultados, así como para facilitar la toma de decisiones, se ha optado por el software de código abierto Grafana. Este servidor permite visualizar de manera más amigable y organizada los datos recopilados de las variables, ofreciendo gráficas más claras y diversas opciones de formato para ilustrar los resultados.

Grafana facilita la consulta, visualización, generación de alertas y exploración de los registros obtenidos en Zabbix. Además, proporciona herramientas para mostrar los datos en paneles en vivo, con gráficas y visualizaciones detalladas que mejoran la comprensión de la información. Cabe anotar que las variables se visualizan por canal óptico, es decir, por cada longitud de onda, dado que cada longitud de onda transporta información única sobre las características espectrales de los objetos o fenómenos observados.

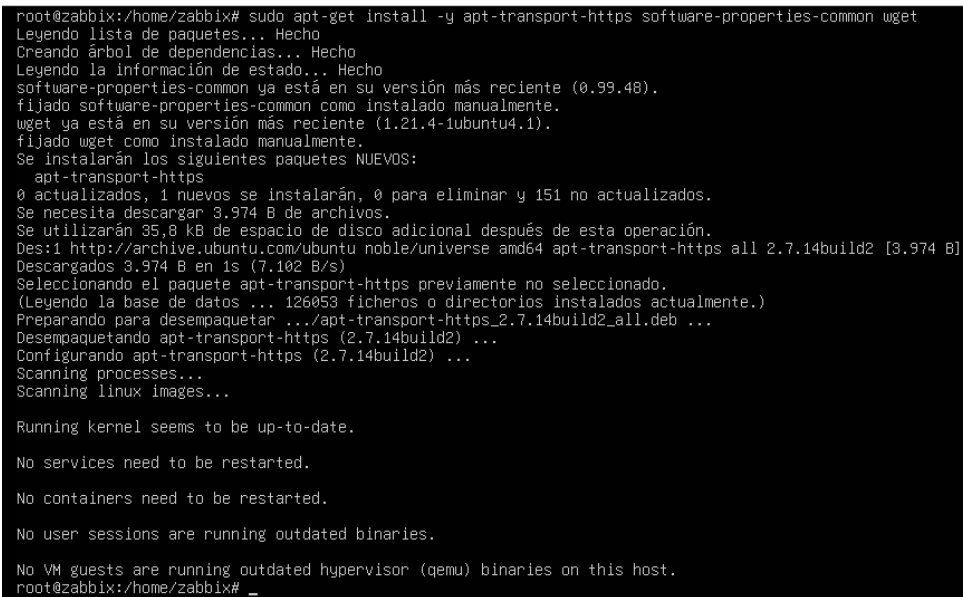
## 4.1. Instalación del servidor Grafana

En esta etapa del proyecto, procedemos a instalar el servidor Grafana. Antes de ello, es necesario instalar ciertos prerequisites. Esta instalación se llevará a cabo en la misma máquina virtual que hospeda el servidor Zabbix, ya que cuenta con el suficiente espacio y no consume muchos recursos de procesamiento.

### 4.1.1. Configuración de los prerequisites

Para iniciar con la instalación de estos prerequisites, utilizaremos el repositorio oficial de Grafana [13]. A continuación, se presentan los comandos necesarios para instalar los requisitos previos, como se observa en la figura 48:

```
# sudo apt-get install -y apt-transport-https software-properties-common  
wget
```



```
root@zabbix:/home/zabbix# sudo apt-get install -y apt-transport-https software-properties-common wget  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
software-properties-common ya está en su versión más reciente (0.99.48).  
fijado software-properties-common como instalado manualmente.  
wget ya está en su versión más reciente (1.21.4-1ubuntu4.1).  
fijado wget como instalado manualmente.  
Se instalarán los siguientes paquetes NUEVOS:  
  apt-transport-https  
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 151 no actualizados.  
Se necesita descargar 3.974 B de archivos.  
Se utilizarán 35,8 kB de espacio de disco adicional después de esta operación.  
Des:1 http://archive.ubuntu.com/ubuntu noble/universe amd64 apt-transport-https all 2.7.14build2 [3.974 B]  
Descargados 3.974 B en 1s (7.102 B/s)  
Seleccionando el paquete apt-transport-https previamente no seleccionado.  
(Leyendo la base de datos ... 126053 ficheros o directorios instalados actualmente.)  
Preparando para desempaquetar .../apt-transport-https_2.7.14build2_all.deb ...  
Desempaquetando apt-transport-https (2.7.14build2) ...  
Configurando apt-transport-https (2.7.14build2) ...  
Scanning processes...  
Scanning linux images...  
  
Running kernel seems to be up-to-date.  
  
No services need to be restarted.  
  
No containers need to be restarted.  
  
No user sessions are running outdated binaries.  
  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
root@zabbix:/home/zabbix# _
```

**Fig. 48** Instalación de prerequisites servidor Grafana

Adicionalmente importamos los Key GPG, que son las claves criptográficas utilizadas en el contexto de la firma y cifrado de datos, como prerequisite con los siguientes comandos, como se muestra en la figura 49:



```
# sudo mkdir -p /etc/apt/keyrings/  
  
# wget -q -O - https://apt.grafana.com/gpg.key | gpg --dearmor | sudo tee  
/etc/apt/keyrings/grafana.gpg > /dev/null
```



```
root@zabbix:/home/zabbix# sudo mkdir -p /etc/apt/keyrings/  
root@zabbix:/home/zabbix# wget -q -O - https://apt.grafana.com/gpg.key | gpg --dearmor | sudo tee /etc/apt/keyrings/grafana.gpg  
> /dev/null  
root@zabbix:/home/zabbix# _
```

**Fig. 49** Configuración de los Key GPG

### 4.1.2. *Instalación del repositorio Grafana*

Los siguiente que se debe hacer es la instalación del repositorio oficial de Grafana, lo cual es necesario ejecutar los siguientes comandos, mostrados en la figura 50:

```
# echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg]  
https://apt.grafana.com stable main" | sudo tee -a  
/etc/apt/sources.list.d/grafana.list
```



```
root@zabbix:/home/zabbix# echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com stable main" | sudo tee -a  
/etc/apt/sources.list.d/grafana.list  
deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com stable main  
root@zabbix:/home/zabbix# _
```

**Fig. 50** Instalación del repositorio de la página oficial Grafana

### 4.1.3. *Instalación de Grafana*

Lo primero que se debe realizar es la actualización correspondiente de los paquetes, luego de esto, realizamos la instalación del software, como se ve en la figura 51.

```
# sudo apt-get update  
  
# sudo apt-get install grafana
```

```

Legendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Legendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  musl
Se instalarán los siguientes paquetes NUEVOS:
  grafana musl
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 151 no actualizados.
Se necesita descargar 123 MB de archivos.
Se utilizarán 464 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
Des:1 http://archive.ubuntu.com/ubuntu/noble/universe amd64 musl amd64 1.2.4-2 [416 kB]
Des:2 https://apt.grafana.com/stable/main amd64 grafana amd64 11.2.0 [123 MB]
Descargados 123 MB en 35s (3,548 kB/s)
Seleccionando el paquete musl:amd64 previamente no seleccionado.
(Leyendo la base de datos ... 126057 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../musl_1.2.4-2_amd64.deb ...
Desempaquetando musl:amd64 (1.2.4-2) ...
Seleccionando el paquete grafana previamente no seleccionado.
Preparando para desempaquetar .../grafana_11.2.0_amd64.deb ...
Desempaquetando grafana (11.2.0) ...
Configurando musl:amd64 (1.2.4-2) ...
Configurando grafana (11.2.0) ...
Info: Selecting UID from range 100 to 999 ...

Info: Adding system user `grafana' (UID 112) ...
Info: Adding new user `grafana' (UID 112) with group `grafana' ...
Info: Not creating home directory `/usr/share/grafana'.
### NOT starting on installation, please execute the following statements to configure grafana to start automatically using syst
emd
  sudo /bin/systemctl daemon-reload
  sudo /bin/systemctl enable grafana-server
### You can start grafana-server by executing
  sudo /bin/systemctl start grafana-server
Procesando disparadores para man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@zabbix:/home/zabbix#

```

Fig. 51 Instalación de Grafana

#### 4.1.4. Inicio de los procesos del servidor Grafana

Para iniciar el servicio, es necesario empezar con los procesos del servidor Grafana. Además, se debe habilitar el servidor para que se reinicie automáticamente en caso de un corte de energía u otras interrupciones que causen el reinicio del servidor. Para ello, utilizamos los siguientes comandos, igual detallados en la figura 52 y 53:

```
# sudo systemctl start grafana-server
# sudo systemctl enable grafana-server
```

```
root@zabbix:/home/zabbix# sudo systemctl start grafana-server
```

Fig. 52 Inicio de los procesos del servidor Grafana

```

root@zabbix:/home/zabbix# systemctl enable grafana-server
Synchronizing state of grafana-server.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable grafana-server
Created symlink /etc/systemd/system/multi-user.target.wants/grafana-server.service → /usr/lib/systemd/system/grafana-server.serv
ice.
root@zabbix:/home/zabbix#

```

Fig. 53 Habilitación del servidor

#### 4.1.5. Verificación del estado del servidor

Una vez se haya completado estos pasos, es importante verificar el estado del servidor. Esto nos permitirá confirmar que esté activo y que podamos acceder al servidor sin inconveniente, el código se muestra en la figura 54.

```
# sudo systemctl status grafana-server
```

```
root@zabbix:/home/zabbix# sudo systemctl status grafana-server
• grafana-server.service - Grafana instance
   Loaded: loaded (/usr/lib/systemd/system/grafana-server.service; enabled; preset: enabled)
   Active: active (running) since Tue 2024-09-24 19:41:17 UTC; 10min ago
     Docs: http://docs.grafana.org
   Main PID: 40990 (grafana)
    Tasks: 10 (limit: 9335)
   Memory: 42.7M (peak: 56.1M)
      CPU: 4.253s
   CGroup: /system.slice/grafana-server.service
           └─40990 /usr/share/grafana/bin/grafana server --config=/etc/grafana/grafana.ini --pidfile=/run/grafana/grafana-ser
sep 24 19:41:23 zabbix grafana[40990]: logger=provisioning.dashboard t=2024-09-24T19:41:23.842349167Z level=info msg="finished >
sep 24 19:41:24 zabbix grafana[40990]: logger=plugins.update.checker t=2024-09-24T19:41:24.139294337Z level=info msg="Update ch>
sep 24 19:41:24 zabbix grafana[40990]: logger=grafana.update.checker t=2024-09-24T19:41:24.193519497Z level=error msg="Update c>
sep 24 19:41:24 zabbix grafana[40990]: logger=plugin.angular detectorsprovider.dynamic t=2024-09-24T19:41:24.283128861Z level=er>
sep 24 19:41:24 zabbix grafana[40990]: logger=plugin.angular detectorsprovider.dynamic t=2024-09-24T19:41:24.283192958Z level=In>
sep 24 19:41:24 zabbix grafana[40990]: logger=grafana-apiserver t=2024-09-24T19:41:24.613878909Z level=info msg="Adding GroupVe>
sep 24 19:41:24 zabbix grafana[40990]: logger=grafana-apiserver t=2024-09-24T19:41:24.614752374Z level=info msg="Adding GroupVe>
sep 24 19:43:13 zabbix grafana[40990]: logger=infra.usagstats t=2024-09-24T19:43:13.834409378Z level=info msg="Usage stats are>
sep 24 19:51:23 zabbix grafana[40990]: logger=cleanup t=2024-09-24T19:51:23.814218069Z level=info msg="Completed cleanup jobs" >
sep 24 19:51:24 zabbix grafana[40990]: logger=plugins.update.checker t=2024-09-24T19:51:24.337177574Z level=info msg="Update ch>
root@zabbix:/home/zabbix#
```

Fig. 54 Verificación del estado del servidor

#### 4.1.6. Configuración de la interfaz web

Ahora que hemos confirmado que todos los servicios están activos, podemos acceder a la interfaz de Grafana ingresando la URL con la dirección IP del servidor adicionando el puerto específico 3000. En este caso, sería de la siguiente manera: `http://192.168.1.20:3000`. Este acceso se puede realizar desde cualquier navegador. Se abrirá automáticamente la página de inicio de sesión, donde se le pedirá cambiar la contraseña y el usuario predeterminado es "Admin", similar a lo que se muestra en la figura 55.

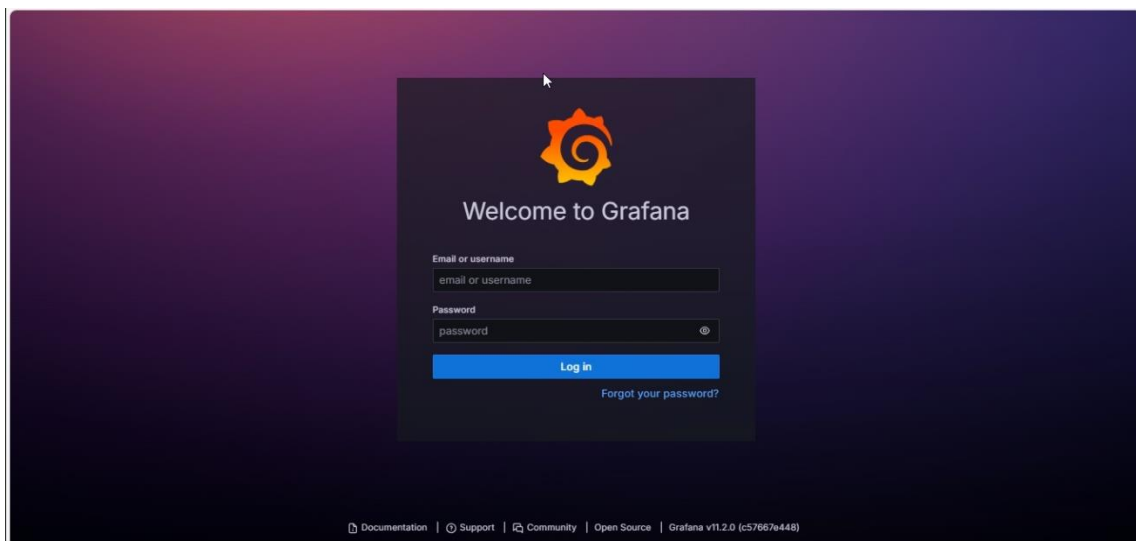


Fig. 55 Inicio de sesión de Grafana

#### 4.1.7. Interfaz web de Grafana

Una vez que iniciemos sesión, se mostrará la página principal de Grafana. En esta página, mostrada en la figura 56, veremos varios parámetros necesarios para la integración de Zabbix en Grafana.

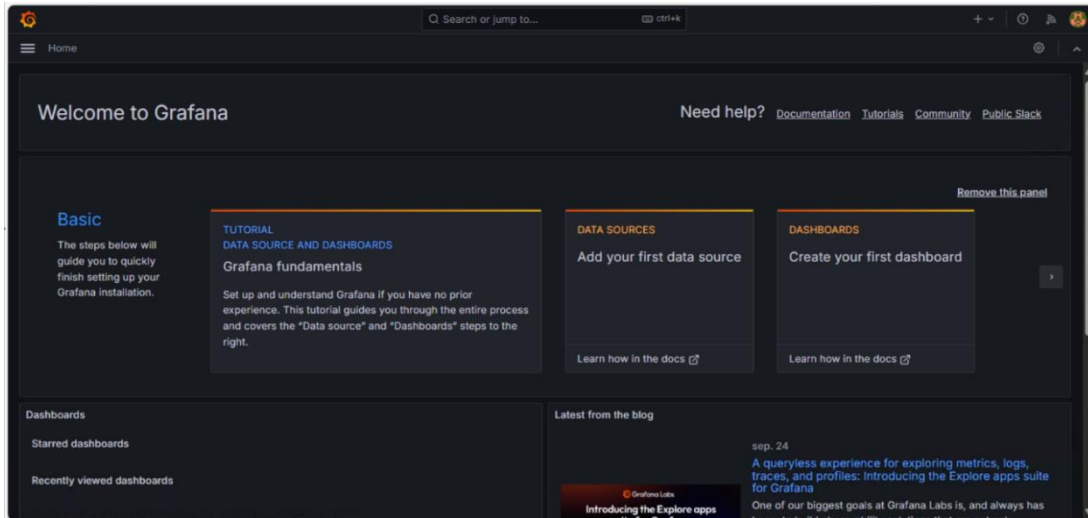


Fig. 56 Interfaz web de Grafana

#### 4.1.8. Instalación del plugin de Zabbix

Para la integración de Zabbix en Grafana, es necesario acceder a la base de datos de Zabbix, para ello, ingresamos el siguiente comando en el servidor (ver figura 57):

```
# grafana-cli plugins install alexanderzobnin-zabbix-app
```

```
root@zabbix:/home/zabbix# grafana-cli plugins install alexanderzobnin-zabbix-app
INFO [09-24|20:14:16] Starting Grafana logger=settings version= commit= branch= compiled=1970-01-01T00:00:00Z
INFO [09-24|20:14:16] Config loaded from logger=settings file=/usr/share/grafana/conf/defaults.ini
INFO [09-24|20:14:16] Config loaded from logger=settings file=/etc/grafana/grafana.ini
INFO [09-24|20:14:16] Config overridden from command line logger=settings arg="default.paths.data=/var/lib/grafana"
INFO [09-24|20:14:16] Config overridden from command line logger=settings arg="default.paths.logs=/var/log/grafana"
INFO [09-24|20:14:16] Config overridden from command line logger=settings arg="default.paths.plugins=/var/lib/grafana/plugins"
INFO [09-24|20:14:16] Config overridden from command line logger=settings arg="default.paths.provisioning=/etc/grafana/provisioning"
INFO [09-24|20:14:16] Target logger=settings target=[all]
INFO [09-24|20:14:16] Path Home logger=settings path=/usr/share/grafana
INFO [09-24|20:14:16] Path Data logger=settings path=/var/lib/grafana
INFO [09-24|20:14:16] Path Logs logger=settings path=/var/log/grafana
INFO [09-24|20:14:16] Path Plugins logger=settings path=/var/lib/grafana/plugins
INFO [09-24|20:14:16] Path Provisioning logger=settings path=/etc/grafana/provisioning
INFO [09-24|20:14:16] App mode production logger=settings
+ Downloaded and extracted alexanderzobnin-zabbix-app v4.5.4 zip successfully to /var/lib/grafana/plugins/alexanderzobnin-zabbix-app
Please restart Grafana after installing or removing plugins. Refer to Grafana documentation for instructions if necessary.
root@zabbix:/home/zabbix# _
```

Fig. 57 Instalación del plugin

Luego de la instalación del plugin, es necesario reiniciar el servidor, siguiendo el comando presentado en la figura 58.

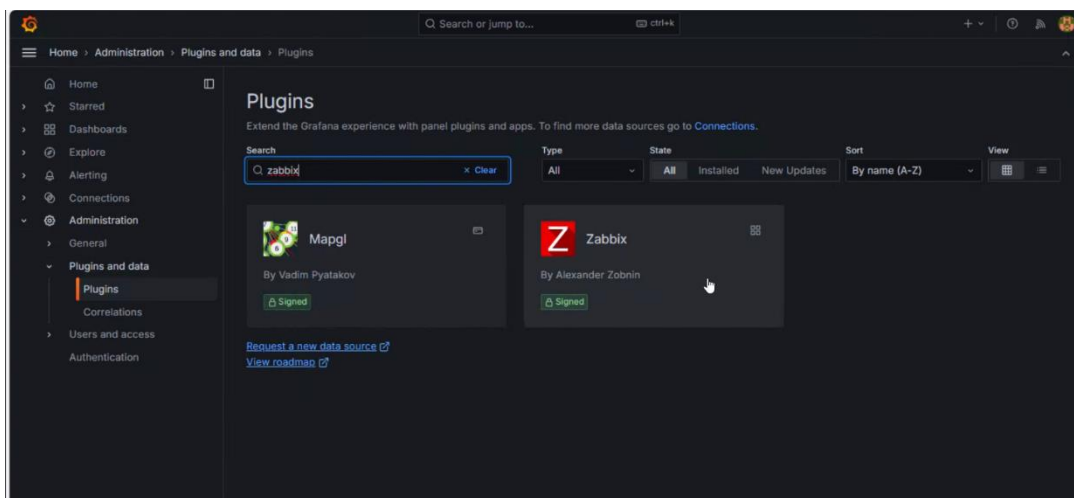
```
# sudo systemctl restart grafana-server
```

```
root@zabbix:/home/zabbix# sudo systemctl restart grafana-server
```

**Fig. 58** Reinicio del servidor

#### 4.1.9. *Habilitación del plugin de Zabbix en Grafana*

Luego de la instalación del plugin en el servidor es necesario habilitarlo en la interfaz web de Grafana (ver figura 59), para acceder a esto seguimos la siguiente ruta: *Home > Administrador > Plugins and Data > Plugins*.



**Fig. 59** Habilitación del Plugin en Grafana

## 4.2. Creación del Dashboard

En esta sección, tras completar la integración de la base de datos de Zabbix con Grafana, creamos el primer Dashboard para monitorear la interfaz OpenZR+ del router UfiSpace.

Para configurar el Dashboard, seguimos estos pasos: *Home > Dashboards > Create Dashboard > Add visualization > Zabbix*. Al ingresar, podremos observar la siguiente interfaz de la fig 60.

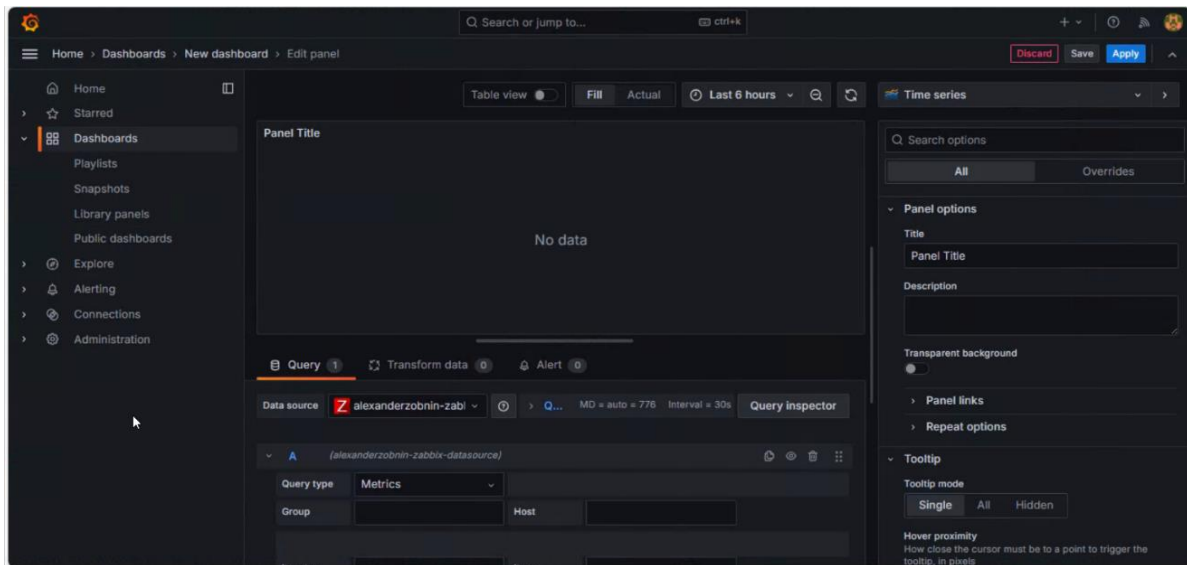


Fig. 60 Creación del Dashboard

#### 4.2.1. Configuración de los hosts en Grafana

En esta etapa, procederemos a integrar el equipo para visualizar los datos en la interfaz de Grafana.

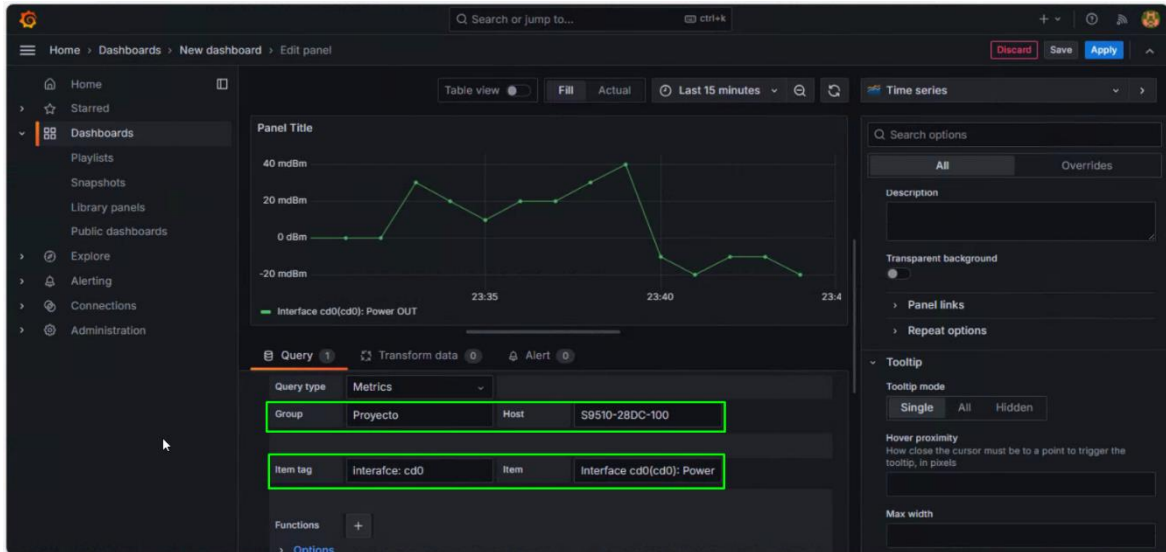
Primero, debemos seleccionar los parámetros que deseamos visualizar, los cuales se cargarán automáticamente desde la base de datos de Zabbix. Los parámetros en este caso son los siguientes (en la figura 61 se observa la interfaz):

**Group:** Proyecto; Grupo de host que se configuró en Zabbix

**Host:** S9510-28DC-100; Nombre del host en Zabbix

**Item tag:** interface: cd0; Interface OpenZR+ que estamos monitoreando

**Item:** Interface cd0(cd0): Power OUT; Variable que queremos visualizar



**Fig. 61** Configuración del host en Grafana

#### 4.2.2. *Dashboard de monitoreo*

Al concluir el proceso de definición de las variables más relevantes para el monitoreo de las interfaces OpenZR+, hemos desarrollado un Dashboard integral que incorpora todos estos indicadores clave. Esto permitirá al equipo de operaciones optimizar el rendimiento de las interfaces de manera más efectiva. La implementación del Dashboard en Grafana, una herramienta reconocida por su interfaz amigable y sus potentes capacidades de visualización, facilita un monitoreo más eficiente y en tiempo real de las métricas de OpenZR+. De este modo, no solo mejoramos la visibilidad de los datos, sino que también potenciamos la capacidad de respuesta del equipo ante cualquier eventualidad, asegurando un rendimiento adecuado de las interfaces.

## 5. RESULTADOS DEL MONITOREO EN EL DASHBOARD INTEGRADO

La capacidad de analizar los datos obtenidos a través de Zabbix y su desagregación en Grafana, permite identificar áreas de mejora en la infraestructura de red, lo que contribuye a aumentar la calidad de transmisión en los dispositivos ofrecidos por la empresa.

A continuación, se muestran las gráficas e información configuradas en el servidor de Grafana, para la interpretación más accesible de las variables en la interfaz OpenZR+ del router UfiSpace.

### 5.1. Estado operacional de la interfaz OpenZR+, potencia de entrada y salida

En esta primera parte del dashboard se observan las gráficas del estado operacional de la interfaz OpenZR+ del router donde se personaliza el valor recopilado para que nos muestre cuando esta UP la interfaz o DOWN, la potencia de salida y la potencia de entrada, según se ve en la figura 62.

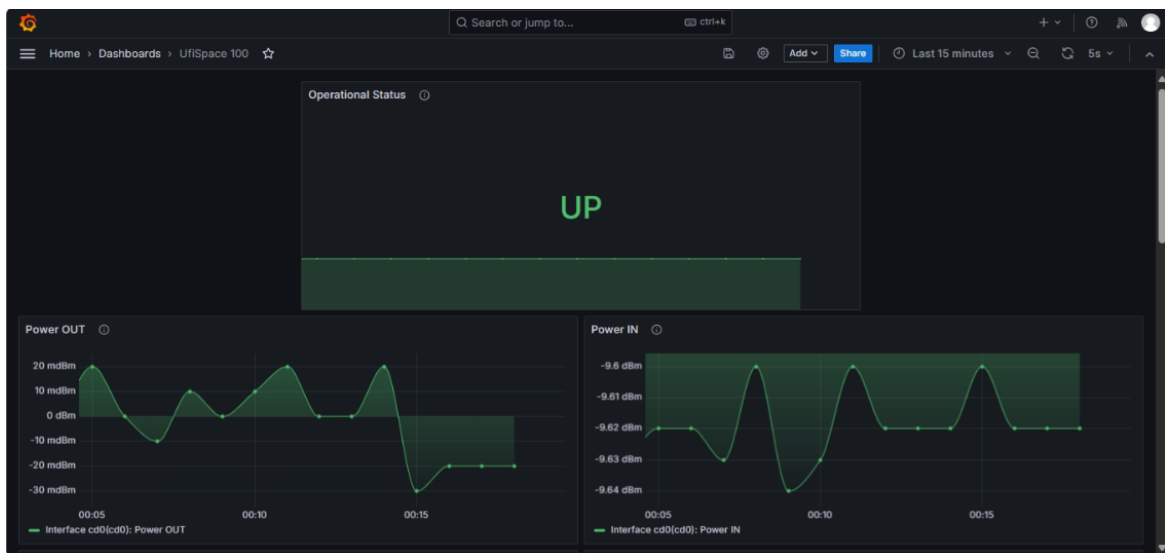


Fig. 62 Visualización de las variables en Grafana (1),

### 5.2. Tasa de transferencia, velocidad, paquetes enviados y recibidos

En esta segunda parte del dashboard se observan las gráficas de la tasa de transferencia donde nos indica la cantidad de tráfico que pasa por la interfaz OpenZR+ del router tanto transmitido como recibido, así mismo la velocidad, los paquetes con errores y descartados, que se envían y que se reciben en la interfaz OpenZR+, mostrados en la figura 63, así mismo poder identificar por el equipo de operaciones cuando tenemos errores en las tramas y poder corregirlo previamente.





**Fig. 63** Visualización de las variables en Grafana (2)

### 5.3. OSNR, TEMPERATURA Y PRE-FEC

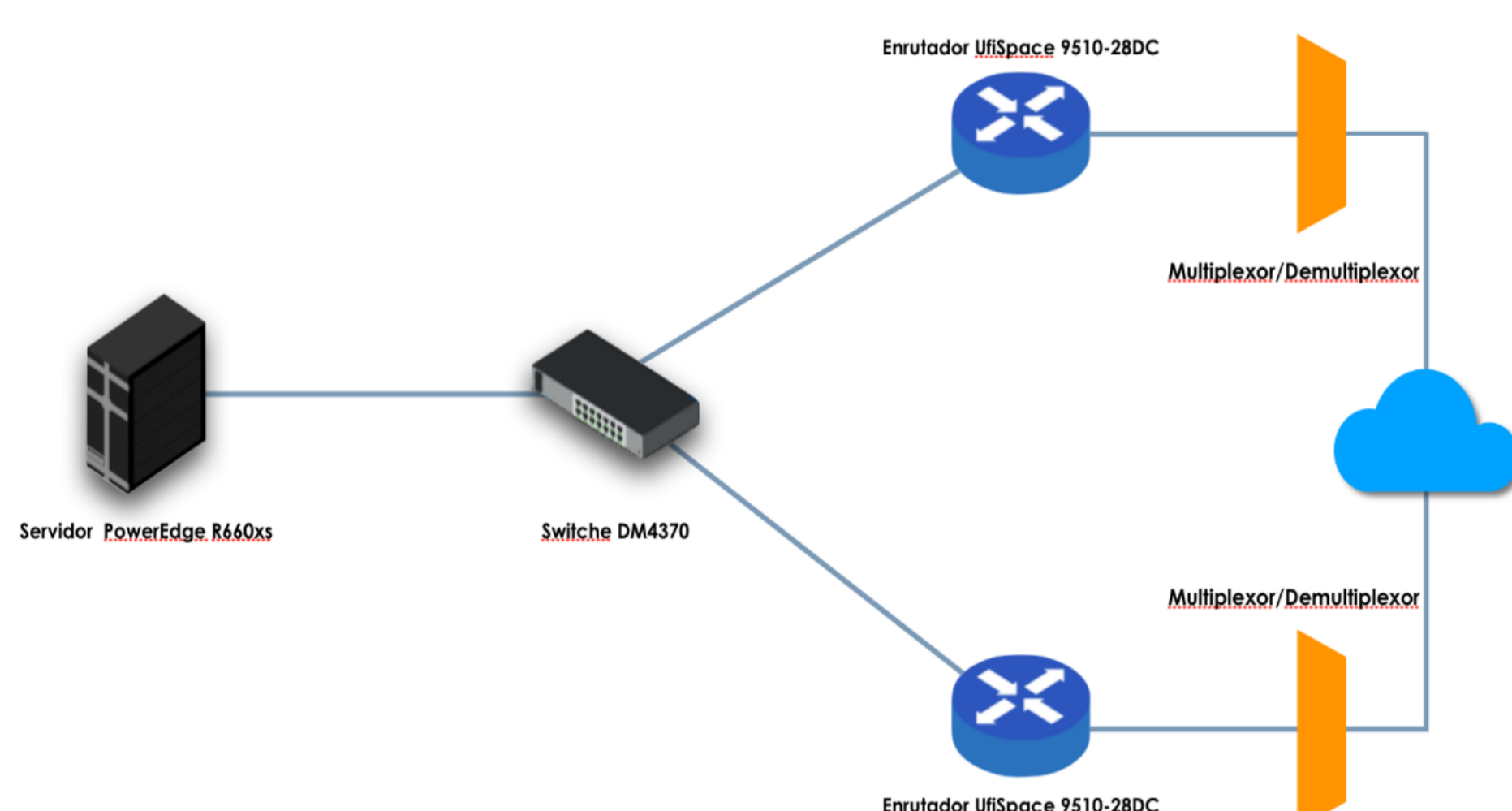
En esta tercera parte del dashboard se observan las gráficas del OSNR, así mismo la temperatura del módulo en la interfaz OpenZR+ y el pre-FEC, resumidas en la figura 64.



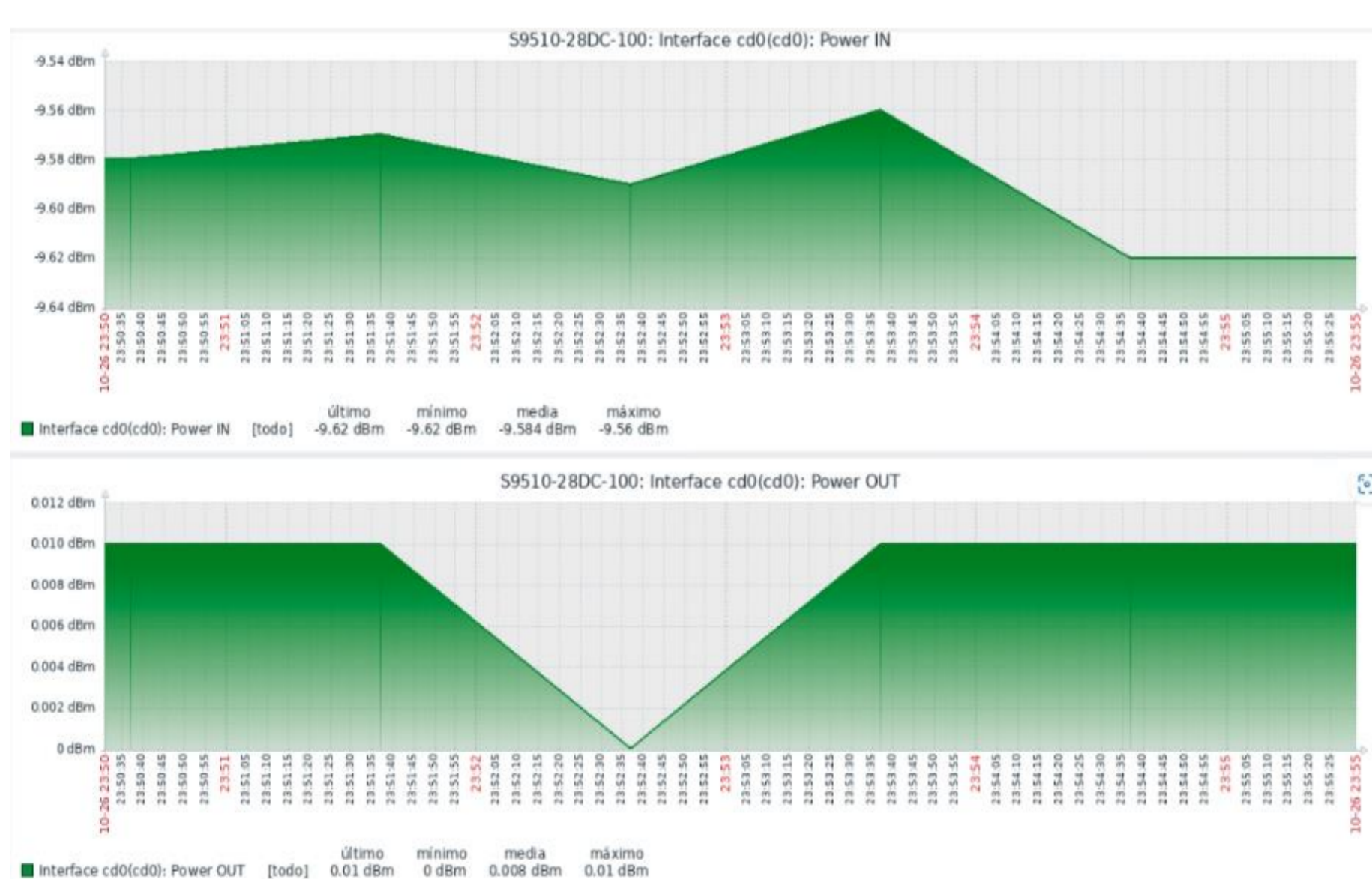
**Fig. 64** Visualización de las variables en Grafana (3)

## Introducción

Las telecomunicaciones han experimentado un avance tecnológico significativo, con un crecimiento anual en capacidades de transmisión que superan los 400G por hilo de fibra óptica. Este progreso requiere un monitoreo constante de parámetros importantes, especialmente en soluciones IPoDWDM. En el ámbito IP, el monitoreo sigue siendo predominante a través de líneas de comando, lo que limita la visibilidad de históricos y parámetros críticos para la resolución de eventos.



Este Proyecto tiene como objetivo implementar un sistema de monitoreo continuo de interfaces OpenZR+ mediante la plataforma Zabbix y el protocolo SNMP. La solución permite recopilar y almacenar datos fundamentales en un servidor, facilitando el acceso a históricos y proporcionando referencias valiosas para la resolución de problemas o la identificación de degradaciones en la red.



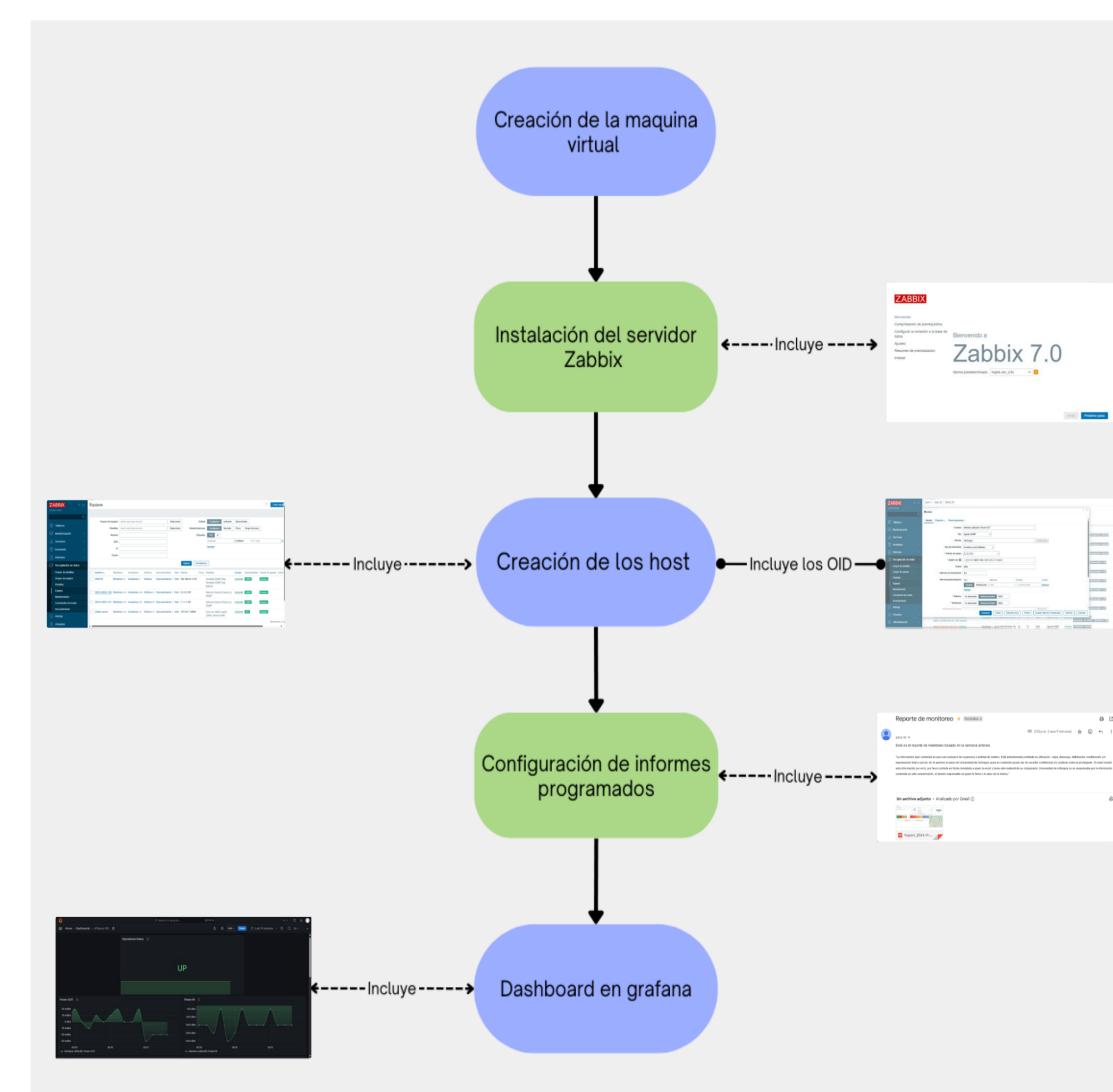
## Objetivos

- ✓ Configurar el servidor para la implementación de la plataforma Zabbix
- ✓ Implementar la plataforma Zabbix en la maquina virtual del servidor.
- ✓ Hacer pruebas de captura de datos de la plataforma Zabbix sobre un montaje de red IPoDWDM en los laboratorios.
- ✓ Analizar los datos recopilados por la plataforma de monitoreo para identificar puntos de mejora en el sistema que se esta monitoreando.
- ✓ Generar informes periódicos en Zabbix para la detección temprana de anomalías del desempeño de las redes IPoDWDM.

## Metodología

- ✓ Documentación para la configuración del servidor y la instalación de Zabbix en la maquina virtual
- ✓ Determinar una solución IPoDWDM en el laboratorio e Integrar los equipos UfiSpace a la plataforma Zabbix
- ✓ Identificar los parámetros arrojados por Zabbix y priorizar las variables que aporten mayor información a los operadores.
- ✓ Asegurar que las redes IPoDWDM cumplan con los estándares de calidad del servicio
- ✓ Definir con la empresa el dashboard y la plantilla de informes periódicos.

## Resultados



## Conclusiones

- ✓ Zabbix permite establecer un sistema de monitoreo efectivo y en tiempo real, lo cual nos permite visibilidad constante del desempeño de las interfaces OpenZR+.
- ✓ Por medio del árbol MIB de los equipos, se identifican los OID correspondiente a los parámetros mas relevantes de la interfaz y así personalizar el monitoreo.
- ✓ Los datos recopilados por la plataforma han demostrado ser muy importantes para realizar un diagnostico proactivo del estado de las interfaces.
- ✓ Zabbix permite la generación de informes periódicos que ayudan a la detección temprana de problemas y degradación de la red.

## VII. CONCLUSIONES

- La implementación de Zabbix ha permitido establecer un sistema de monitoreo efectivo y en tiempo real, que proporciona visibilidad constante sobre el desempeño de las interfaces OpenZR+. Esto ha facilitado la identificación inmediata de cualquier anomalía en la red.
- El uso de SNMP ha garantizado que las comunicaciones entre el servidor Zabbix y los dispositivos gestionados se realicen de manera segura, protegiendo la integridad de los datos, lo cual es fundamental en un entorno de red crítico.
- Los dispositivos UfiSpace nos proporcionan la herramienta del árbol MIB, lo que nos permite identificar los OID correspondientes a los parámetros relevantes que no son capturados por las plantillas predefinidas en Zabbix. Esta capacidad facilita la personalización del monitoreo, asegurando una recopilación de datos más completa.
- Los datos recopilados por la plataforma han demostrado ser muy importantes para realizar un diagnóstico proactivo del estado de equipos, enfocándose en métricas clave como el consumo de ancho de banda, paquetes con errores, relación señal-ruido, potencia de salida y, de entrada, tasa de transferencia, entre otros. Esto facilita la planificación de un mantenimiento preventivo más eficiente.
- Zabbix ha permitido la emisión de alertas oportunas sobre anomalías en la red, así como la generación de informes periódicos que ayudan en la detección temprana de problemas y en el seguimiento continuo del desempeño, mejorando la capacidad de respuesta ante incidentes.
- La capacidad de analizar los datos obtenidos a través de Zabbix y su desagregación en Grafana, permite identificar áreas de mejora en la infraestructura de red, lo que contribuye a aumentar la calidad de transmisión en los dispositivos ofrecidos por la empresa. Esto asegura una experiencia más satisfactoria para los clientes y un monitoreo más riguroso.

---

## VIII. REFERENCIAS

- [1] Sánchez Lucas, D. (2017). Redes ópticas de transmisión DWDM: diseño e implementación. Proyecto Fin de Carrera / Trabajo Fin de Grado, E.T.S.I. y Sistemas de Telecomunicación (UPM), Madrid.
- [2] Antil, R., Pinki, S. B., & Beniwal, S. (2012). An overview of DWDM technology & network. *Int. J. Sci. Technol. Res*, 1(11), 43-46.
- [3] Villagómez, E. G. G. (2014). Estudio de Factibilidad para la Implementación de una Red de Fibra Óptica entre Desaguadero y Moquegua. Pontificia Universidad Católica del Perú (Perú).
- [4] Peñarredonda, D. A. B., Silva, I. D. T., & Mateus, E. A. (2010). Redes ópticas DWDM: diseño e implementación. *Visión electrónica*, 4(1), 70-80.
- [5] López, J. F. R. (2022). Diseño de red SCM/DWDM con detección coherente para aplicaciones 5G en banda milimétrica (Master's thesis, Universidad Distrital Francisco José de Caldas (Colombia)).
- [6] ¿Qué es un router? [Página web]. [Consultada el 30, agosto, 2024]. Disponible en internet: <[https://www.cisco.com/c/es\\_mx/solutions/small-business/resource-center/networking/what-is-a-router.html](https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html)>.
- [7] UfiSpace. Productos de telecomunicaciones [Página web]. [Consultada el 29, junio, 2024]. Disponible en internet: <<https://www.ufispace.com/products/telco>>.
- [8] Ip Infusion. OcNOS Open Compute Network Operating System for Service Providers Version 6.4.2 [Página Web]. Disponible en internet: <[https://docs.ipinfusion.com/service-provider/#page/OcNOS-SP/SplashPage\\_SP.html](https://docs.ipinfusion.com/service-provider/#page/OcNOS-SP/SplashPage_SP.html)>.
- [9] Junco Romero, G., & Rabelo Padua, S. (2018). Los recursos de red y su monitoreo. *Revista Cubana de Informática Médica*, 10(1), 76-83.
- [10] Server Zeo. What is Zabbix [blog]. 2021. [Consultada: 30 junio 2024]. Disponible en: <<https://www.zabbix.com/documentation/current/en/manual/introduction/about>>
- [11] Benavides Sánchez, C. A. (2023). Implantación de la herramienta ZABBIX de monitoreo para el núcleo de red de la Empresa Airmaxtelecom Soluciones Tecnológicas S.A. gratuita y de código abierto [Tesis de pregrado, Universidad Técnica del Norte].
- [12] SOLIS, M. A. U. (2014). IMPLEMENTACIÓN DE PLATAFORMA DE MONITOREO ZABBIX PARA SISTEMAS DE TELECOMUNICACIONES TELSUR (Doctoral dissertation, Universidad Austral de Chile).
- [13] Install Grafana on Debian or Ubuntu [blog]. 2024. [Consultada: 26 septiembre 2024]. Disponible en: <<https://grafana.com/docs/grafana/latest/setup-grafana/installation/debian/>>
- [14] DELL Technologies. Servidor de montaje en rack PowerEdge R660xs [Página web].

- [Consultada el 30, junio, 2024]. Disponible en internet: <<https://www.dell.com/es-es/shop/ipovw/poweredge-r660xs>>.
- [15] Cisco. QSFP-DD Optical Transceivers for High-Speed Connections [Página Web]. (February 8, 2023). Disponible en internet: <<https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/qsfp-dd-optical-trxs-high-speed-cxns-aag.html>>.
- [16] Ramaswami, R., Sivarajan, K., & Sasaki, G. (2009). Optical Networks: A Practical Perspective. Ed. Morgan Kaufmann. 3th edition. pp 928. ISBN 0080920721, 9780080920726

## IX. ANEXOS

### *ANEXO A: Características Equipo UfiSpace*

Procesador de 8 núcleos y 28 interfaces de alta velocidad, incluidos puertos 400G con funciones Flexible Ethernet (FlexE) y OpenZR+. También admite funciones de sincronización completa de IEEE 1588v2 y SyncE. La compatibilidad con la red sensible al tiempo (TSN) 802.1CM para fronthaul hace que el S9510-28DC sea la mejor opción para la aplicación xHual. Adecuado para implementaciones tanto en interiores como en exteriores, el S9510-28DC tiene componentes redundantes intercambiables en caliente, 1RU, 440 mm de ancho x 302 mm de profundidad x 43,5 mm de alto (17,32" x 11,89" x 1,71"), Peso: 4,9 kg (10,80 lb)



**ANEXO B:** *Características Switche Datacom*

Velocidad de cable con reenvío, filtrado y calidad de servicio (QoS) L2, L3 y MPLS basados en hardware, VLAN IEEE802.1Q con capacidades Q-in-Q y VLAN Translate, Agregación de enlaces y LACP, Soporte para aplicaciones Ring a través de protocolos EAPS o ERPS, STP/RSTP para protección de bucle, Túnel de protocolo lento L2 (L2CP), Hasta 8 colas de QoS por puerto, Enrutamiento estático y enrutamiento dinámico mediante protocolos OSPF y BGP, Redundancia de IP virtual a través del protocolo VRRP, Funcionamiento como enrutador de borde de etiqueta o enrutador de conmutación de etiqueta mediante encapsulación MPLS, LDP para distribución de etiquetas en infraestructura de red MPLS, Límite de velocidad de entrada y salida, Programación de paquetes mediante los modos SP y WFQ, Coincidencias de ACL por puerto, dirección MAC, IP, DSCP, TCP/UDP, Interfaz de administración CLI con Telnet/SSH  
Soporte TACACS y RADIUS para administración de políticas de acceso y gestión.

