RESUMEN TRABAJO DE GRADO

AUTOR(ES): NOMBRES Y APELLIDOS COMPLETOS

NOMBRE(S): LIZETH APELLIDOS: RÍOS EPALZA

FACULTAD: INGENIERÍA

PLAN DE ESTUDIOS: INGENIERÍA DE SISTEMAS

DIRECTOR:

NOMBRE(S): JOSÉ MARTIN APELLIDOS: CALIXTO CELY

TÍTULO DEL TRABAJO (TESIS): IMPLANTACIÓN DE UN SISTEMA DE MONITOREO PARA LA INFRAESTRUCTURA DE RED DE DATOS DE LA UFPS SEDE CÚCUTA Y CAMPOS ELÍSEOS.

El presente proyecto de grado en la modalidad trabajo dirigido, se realizó con el objetivo de implantar un sistema de monitoreo de red que permitiera establecer la línea base del funcionamiento óptimo y conocer el estado de los dispositivos, enlaces, recursos y servicios que conforman la infraestructura de red de datos de la UFPS sede Cúcuta y Campos Elíseos. El desarrollo del proyecto inició con el levantamiento de información de la infraestructura de red de datos, lo cual permitió definir las necesidades y requisitos que debía cumplir la herramienta de monitoreo. Posteriormente, se determinó la herramienta más adecuada y se diseñó e implantó el sistema de monitoreo. Finalmente, se realizaron las pruebas y ajustes para la validación y verificación de la solución implantada y se elaboraron los manuales de instalación, configuración y administración del sistema de monitoreo para dar una guía a la dependencia CSI en todos los procedimientos. Estas actividades se desarrollaron bajo la metodología PPDIOO (Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar), propuesta por la compañía Cisco.

PALABRAS CLAVE: Red de datos, monitoreo de red, SNMP, open source, Zabbix.

CARACTERÍSTICAS:

PÁGINAS: 130 PLANOS: ___ ILUSTRACIONES: 77 CD ROOM: ___

IMPLANTACIÓN DE UN SISTEMA DE MONITOREO PARA LA INFRAESTRUCTURA DE RED DE DATOS DE LA UFPS SEDE CÚCUTA Y CAMPOS ELÍSEOS

LIZETH RÍOS EPALZA

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

SAN JOSÉ DE CÚCUTA

2020

IMPLANTACIÓN DE UN SISTEMA DE MONITOREO PARA LA INFRAESTRUCTURA DE RED DE DATOS DE LA UFPS SEDE CÚCUTA Y CAMPOS ELÍSEOS

LIZETH RÍOS EPALZA

Proyecto de grado presentado como requisito para optar al título de

Ingeniero de Sistemas

Modalidad: Trabajo Dirigido

Director

JOSÉ MARTIN CALIXTO CELY

Ingeniero de Sistemas

Codirector

CARLOS EDUARDO PARDO GARCÍA

Ingeniero de Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

SAN JOSÉ DE CÚCUTA

2020

35003.01.13-3741

ACTA DE SUSTENTACIÓN DE TRABAJO DE GRADO

FECHA: *Junio 26 de 2020* *HORA:* 2:30 pm
PLAN DE ESTUDIOS: *INGENIERÍA DE SISTEMAS*

TITULO DEL TRABAJO DE GRADO: "IMPLANTACIÓN DE UN SISTEMA DE MONITOREO PARA LA INFRAESTRUCTURA DE RED DE DATOS DE LA UFPS SEDE CÚCUTA Y CAMPOS ELÍSEOS"

JURADOS:
Mgs. I.S. JEAN POLO CERQUERA O
Esp. I.S EUSEN ENRIQUE PEÑARANDA CARRILLO
MS. I.S. MARCO ANTONIO ADARME JAIMES

DIRECTOR: *MG. I.S* . JOSE MARTIN CALIXTO C
CODIRECTOR: Pd.D I.S CARLOS EDUARDO PARDO GARCIA

NOMBRE DEL ESTUDIANTE	***CÓDIGO***	***CALIFICACIÓN NÚMERO LETRA***
LIZETH RÍOS EPALZA	1151177	4,3 (CUATRO TRES)

APROBADA

FIRMA DE LOS JURADOS

JEAN P. CEQUEDA O.

MgS JEAN POLO CERQUERA O Esp. EUSEN PEÑARANDA CARRILLO

MSc. MARCO ANTONIO ADARME JAIME

Ph.D. JUDITH DEL PILAR RODRÍGUEZ TENJO
Coordinadora Comité Curricular

Vigilada Mineducación	**GESTIÓN DE SERVICIOS ACADÉMICOS Y BIBLIOTECARIOS**	

CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL Y LA PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO

Cúcuta,

Señores
BIBLIOTECA EDUARDO COTE LAMUS
Ciudad

Cordial saludo:

Lizeth Rios Epalza, identificado(s) con la C.C. Nº 1.093.783.415, autor(es) de la tesis y/o trabajo de grado titulado Implantación de un sistema de monitoreo para la infraestructura de red de datos de la UFPS sede Cúcuta y Campos Elíseos presentado y aprobado en el año 2020 como requisito para optar al título de Ingeniero de Sistemas; autorizo(amos) a la biblioteca de la Universidad Francisco de Paula Santander, Eduardo Cote Lamus, para que con fines académicos, muestre a la comunidad en general a la producción intelectual de esta institución educativa, a través de la visibilidad de su contenido de la siguiente manera:

- los usuarios pueden consultar el contenido de este trabajo de grado en la página web de la Biblioteca Eduardo Cote Lamus y en las redes de información del país y el exterior, con las cuales tenga convenio la Universidad Francisco de Paula Santander.

- Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato CD-ROM o digital desde Internet, Intranet etc.; y en general para cualquier formato conocido o por conocer.

Lo anterior, de conformidad con lo establecido en el artículo 30 de la ley 1982 y el artículo 11 de la decisión andina 351 de 1993, que establece que "**los derechos morales del trabajo son propiedad de los autores"**, los cuales son irrenunciables, imprescriptibles, inembargables e inalienables.

1.093.783.415
FIRMA Y CEDULA

Dedicatoria

A Dios, por absolutamente todo.

A mis padres, Miriam Epalza y Ramón Ríos por su amor, sacrificio y apoyo incondicional a lo largo de mi vida y por ser mi mayor motivación para culminar mis estudios profesionales.

A mis hermanos, Yorgi y Julieth por creer en mí y cada día motivarme a seguir adelante.

A mi sobrina, Thaliana por ser una de las personas más importantes en mi vida.

Agradecimientos

A Dios, por darme la oportunidad de culminar mis estudios profesionales.

A mis padres, hermanos y sobrina por su apoyo incondicional a lo largo de mi carrera.

A mis amigos y compañeros de la Universidad, por su cariño, compañía y apoyo brindado durante mi formación académica.

A mi director, Ing. José Calixto y codirector, Ing. Carlos Pardo por su tiempo y orientación durante la elaboración de este proyecto.

A mis jurados, por sus valiosos aportes, comentarios y sugerencias al proyecto para que este lograra mejorar su calidad.

A las personas que integran el Centro de Servicios de Información, en especial al Ing. Eusen Peñaranda por su colaboración durante la ejecución de este proyecto.

Tabla de Contenido

Índice de Tablas

Índice de Figuras

Índice de Anexos

Resumen

El presente proyecto de grado en la modalidad trabajo dirigido, se realizó con el objetivo de implantar un sistema de monitoreo de red que permita establecer la línea base del funcionamiento óptimo y conocer el estado de los dispositivos, enlaces, recursos y servicios que conforman la infraestructura de red de datos de la UFPS sede Cúcuta y Campos Elíseos. El desarrollo del proyecto inició con el levantamiento de información de la infraestructura de red de datos, lo cual permitió definir las necesidades y requisitos que debía cumplir la herramienta de monitoreo. Seguidamente, se determinó la herramienta más adecuada para la infraestructura de red de datos, la cual fue Zabbix versión 4.0; se diseñó e implantó el sistema de monitoreo, mismo que se instaló sobre la plataforma GNU/Linux CentOS 7. Posteriormente, se realizaron las pruebas y ajustes para la validación y verificación de la solución implantada y se elaboraron los manuales de instalación, configuración y administración para dar una guía a la dependencia CSI en todos los procedimientos ejecutados. Finalmente, se llevó a cabo una capacitación con el personal administrativo de CSI sobre el manejo del sistema de monitoreo de red. Estas actividades se desarrollaron bajo la metodología PPDIOO (Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar), propuesta por la compañía Cisco. La implantación del sistema de monitoreo permite que los componentes y servicios que conforman la infraestructura de red de datos sean monitoreados permanentemente mediante el protocolo SNMP; garantizando la disponibilidad de la red de datos, ya que, al alertar y notificar de manera inmediata al administrador de la red, este actúa rápidamente ante los eventos que se presentan.

Palabras clave: Red de datos, UFPS, monitoreo de red, SNMP, open source, Zabbix.

Abstract

The present project of degree in the modality of directed work, was carried out with the aim of implementing a network monitoring system that allows to establish the baseline of the optimal operation and know the status of the devices, links, resources and services that make up the data network infrastructure of the UFPS headquarters Cucuta and Elysées Champs. The development of the project began with the information survey of the data network infrastructure, which allowed to define the needs and requirements that the monitoring tool had to meet. The most appropriate tool for the data network infrastructure was then determined, which was Zabbix version 4.0; the monitoring system, which was installed on the GNU/Linux CentOS 7 platform, was designed and implemented. Subsequently, tests and adjustments were made for the validation and verification of the implanted solution and the installation, configuration and administration manuals were developed to guide the CSI dependency in all executed procedures. Finally, training was conducted with CSI's administrative staff on the management of the network monitoring system. These activities were developed under the PPDIOO methodology (Prepare, Plan, Design, Implement, Operate and Optimize), proposed by Cisco. The implementation of the monitoring system allows the components and services that make up the data network infrastructure to be monitored permanently using the SNMP protocol; ensuring the availability of the data network, because by immediately alerting and notifying the network administrator, the network administrator acts quickly in the face of the events that occur.

Keywords: Data Network, UFPS, Network Monitoring, SNMP, Open Source, Zabbix.

Introducción

En las organizaciones de hoy en día las redes de comunicación se han convertido en un elemento indispensable, ya que además de proporcionar la conectividad a nivel intranet, extranet e Internet, también proporcionan servicios de red. De esto se deriva la importancia de contar con un sistema de monitoreo que permita conocer el estado general de la infraestructura de red de datos y que notifique los eventos que se presentan.

Por esta razón, nace la propuesta de implantar un sistema de monitoreo que permita establecer la línea base del funcionamiento óptimo y conocer el estado de los dispositivos, enlaces, recursos y servicios que conforman la infraestructura de red de datos.

El proyecto presentado en este documento contiene la información correspondiente a la implantación de un sistema de monitoreo para la infraestructura de red de datos de la UFPS sede Cúcuta y Campos Elíseos. El documento incluye la descripción del problema, el marco referencial, la metodología, el desarrollo de los objetivos propuestos, las conclusiones y recomendaciones que se obtuvieron a lo largo del desarrollo del proyecto y los anexos que aportan contenido adicional al proyecto.

El Problema

1.1. Título

Implantación de un sistema de monitoreo para la infraestructura de red de datos de la UFPS sede Cúcuta y sede Campos Elíseos.

1.2. Planteamiento del Problema

Una de las funciones del Centro de Servicios de Información (CSI), dependencia perteneciente al Departamento de Sistemas e Informática de la Universidad Francisco de Paula Santander (UFPS), es mantener en correcto funcionamiento la red de datos en la UFPS sede Cúcuta y sede Campos Elíseos. El CSI se encarga de garantizar la disponibilidad de los servicios (DHCP, DNS, acceso remoto y transferencia de archivos) y sistemas de seguridad (firewalls); y del acceso a los recursos (servidores, sistemas de información y aplicaciones) y redes externas, tanto para los usuarios finales como para el administrador de la red.

Debido al crecimiento de usuarios y estaciones de trabajo en la UFPS la calidad del servicio se ha visto afectado, estos problemas requieren en gran medida aumentar el canal principal de acceso a Internet y ampliar la infraestructura de red de datos.

A causa de esto, la red de datos es cada vez más compleja, haciendo más difícil llevar a cabo tareas de administración y monitorización. Estas limitantes traen como resultado el no poder detectar de manera oportuna los problemas que se presentan en la red de datos, lo cual hace imposible garantizar el correcto funcionamiento de la misma.

Para llevar a cabo una administración eficiente de la red de datos, es indispensable contar con herramientas que permitan monitorear en tiempo real los componentes y servicios que conforman la infraestructura de red de datos.

1.3. Formulación del Problema

¿Qué herramientas existen en el mercado para el proceso de administración y monitorización de infraestructura de red?

1.4. Justificación

La UFPS sede Cúcuta, localizada en el barrio Colsag, cuenta con un backbone en fibra óptica con topología estrella extendida, que interconecta el centro de cableado principal con los demás edificios localmente dispersos; permitiendo así, la interconexión de 18 subredes. Dentro de cada uno de los edificios que cuentan con una subred, se pueden encontrar otros centros de cableado interconectados.

Por su parte, la sede Campos Elíseos del municipio de Los Patios se interconecta con la sede Cúcuta a través de una infraestructura proporcionada por el proveedor de servicios de Internet (ISP). En su totalidad, la infraestructura de red de datos está conformada por 53 centros de cableado ubicados en 36 edificios de la UFPS sede Cúcuta y Campos Elíseos (ver Anexo 1).

Esta infraestructura presta servicios de red a más de 3500 equipos de escritorio, portátiles, tabletas y teléfonos inteligentes; beneficiando así a una población universitaria de más de 18.206 personas entre administrativos, docentes, estudiantes de pregrado, postgrado y a distancia, según el boletín estadístico realizado por la Unidad de Información y Estadística de la Oficina de Planeación (Unidad de Información Estadística, 2019).

El tamaño de la red, su complejidad y el aumento de los usuarios conectados, incrementa el riesgo de sufrir un mal funcionamiento. Esto no solo provoca poca satisfacción de los usuarios, también perjudica los procesos de la organización, generando pérdidas de tiempo y dinero (Sosa Sosa, s. f.). Para reducir estos riesgos y actuar rápidamente ante los eventos que se puedan presentar, existen sistemas de monitoreo de red que permiten conocer el estado general

de los dispositivos de red activos, servidores, impresoras y estaciones de trabajo, mediante el protocolo simple de administración de red o SNMP (del inglés Simple Network Management Protocol).

Otra medida indispensable para garantizar la continuidad y pronta respuesta ante una falla es contar con un plan de contingencia, en el cual una de las actividades primordiales son las copias de seguridad. De acuerdo con el Modelo de Seguridad y Privacidad de la Información publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, 2016) “se debe contar con un proceso periódico de respaldo de la configuración de sus Servicios Tecnológicos, así como de la información almacenada en la infraestructura tecnológica”.

Con el desarrollo del presente proyecto, se contribuirá a mejorar la disponibilidad de la red de datos en la UFPS sede Cúcuta y Campos Elíseos y a optimizar el trabajo de la dependencia CSI. Siendo este uno de los beneficiarios directos, ya que se facilitará el proceso de monitoreo al ejecutarse de manera automática. Otros beneficiarios directos son los empleados, estudiantes y visitantes que tienen acceso a la red de datos.

De no llevarse a cabo este proyecto para CSI, se afectaría directamente al administrador de la red que seguiría llevando el monitoreo de la red de forma manual (esperando el reporte de un evento que anuncia una falla, lo cual se monitorea a través de comandos manuales como el ping o telnet; o en casos específicos realizando visitas a los diferentes centros de cableado para verificar el estado de los dispositivos y posteriormente identificar de donde proviene la falla), lo que genera tiempos de respuesta muy largos en la resolución de los eventos.

1.5. Objetivos

1.5.1. Objetivo General

Implantar un sistema de monitoreo de red que permita establecer la línea base del funcionamiento óptimo y conocer el estado de los dispositivos, enlaces, recursos y servicios que conforman la infraestructura de red de datos de la UFPS sede Cúcuta y Campos Elíseos.

1.5.2. Objetivos Específicos

- Determinar las herramientas que se ajustan a las necesidades de monitoreo de los dispositivos, enlaces, recursos y servicios que conforman la infraestructura de red de datos de la UFPS sede Cúcuta y Campos Elíseos.
- Realizar el proceso de implantación del sistema de monitoreo de red con las herramientas seleccionadas.
- Realizar pruebas y ajustes para la validación y verificación del sistema de monitoreo de red.
- Elaborar los manuales de instalación, configuración y administración del sistema de monitoreo de red para brindar una guía de los diferentes procesos.

1.6. Alcances y Limitaciones

1.6.1. Alcances

- Determinar las herramientas que se ajustan a las necesidades de monitoreo de la infraestructura de red de datos.
- Implantar en la infraestructura de red de datos la solución diseñada, para lo cual es necesario instalar y configurar el servidor principal y las herramientas seleccionadas.
- Activar el protocolo SNMPv3 en los dispositivos con IOS compatibles.

- Poner en operación el sistema de monitoreo de red. En un inicio solo se agregarán los dispositivos de red activos.
- Validar y verificar el correcto funcionamiento del sistema de monitoreo de red implantado, para lo cual es necesario realizar y ejecutar un plan de pruebas.
- Elaborar los manuales de instalación, configuración y administración del sistema de monitoreo de red para brindar una guía de los diferentes procesos.

1.6.2. Limitaciones

- El proyecto será implementado para el uso exclusivo de la dependencia CSI.
- Las herramientas deben estar baja una licencia open source o estar a disposición de la UFPS.
- En un inicio, la herramienta solo va a monitorear dispositivos de red activos

1.7. Delimitaciones

1.7.1. Delimitación Espacial

Como se observa en las figuras 1 y 2, el proyecto se llevará a cabo en las instalaciones de la UFPS sede Cúcuta y en la sede Campos Elíseos de municipio de Los Patios.

Figura 1. Ubicación satelital de la UFPS sede Cúcuta.
Fuente: (UFPS, s. f.). [Map]. https://satellites.pro/mapa_de_Colombia#7.898830,-72.488254,17.

Figura 2. Ubicación satelital de la UFPS sede Campos Elíseos.
Fuente: (Campos Elíseos, s. f.). [Map]. https://satellites.pro/mapa_de_Colombia#7.854715,-72.501258,17

1.7.2. Delimitación Temporal

Para la realización del proyecto se presupone un período de 4 meses, a partir de la aprobación del anteproyecto.

Marco Referencial

2.1. Antecedentes

A continuación, se presentan los antecedentes de investigaciones a nivel internacional, nacional y regional relacionados al tema que se viene abordando, con los cuales se aportará una mayor comprensión en lo que respecta a los sistemas de monitoreo de red y protocolos.

2.1.1. Antecedentes Internacionales

(Bustincio & Watson, 2018) , en Puno - Perú. Realizo una tesis titulada: “Implementación de un sistema de monitoreo y control de red, para un canal de televisión, basado en herramientas open source y software libre, Lima - 2017”, cuyo propósito fue monitorear los equipos y tráfico de red para ayudar a detectar de forma inmediata el momento en el que ocurre un problema o antes de que los usuarios finales noten las fallas. Se realizó una investigación de tipo descriptiva, bajo un diseño cuasi experimental, cuya muestra estuvo constituida por 36 usuarios del total del canal de televisión. La técnica utilizada para la recolección de datos fue la observación, mediante entrevista y encuesta. Con la implementación del sistema de monitoreo y control de red mediante el uso de la herramienta NAGIOS se logró una comprobación efectiva y constante de los servicios y dispositivos (host, procesador, memoria RAM, Router, Fibra Óptica, Access Point, servidor) del canal de televisión; asegurando una reacción oportuna para solucionar los fallos que se presenten en estos, los cuales proporciona mejora en la administración de los servicios y dispositivos de la red, para el personal.

Este antecedente de investigación presenta relación con el presente proyecto, en el sentido que proporciona una amplia información referente a los sistemas de gestión y monitoreo de redes, por lo cual guiara en la elaboración del marco teórico.

(Velasco Briones & Cagua Ordoñez, 2017), en Guayaquil. Realizo un proyecto titulado: “Implementación de un sistema de monitoreo de redes utilizando herramientas open source y proveer servicios de directorio a través de active directory en la Facultad de Filosofía, Letras y Ciencias de la Educación de la Universidad de Guayaquil”, el cual se desarrolló bajo una metodología PPDIOO (Preparar, Planificar, Diseñar, Implementar y Operar), propuesta por la compañía Cisco. La técnica utilizada fue la entrevista y el instrumento empleado, el cuestionario. Con la implementación del directorio activo y la herramienta de monitoreo Nagios se logró una mejor administración de los recursos de la red desde un solo servidor.

Este antecedente de investigación presenta relación con el presente proyecto, en el sentido de que orienta toda la metodología de trabajo asimismo proporciona una amplia información referente a las herramientas de monitoreo de redes para la elaboración del marco teórico.

(Villagómez & Israel, 2015) en Ambato – Ecuador. Realizo un proyecto titulado: “Servidor de control de dispositivos y servicios mediante el protocolo SNMP para la red de datos en CELEC E.P. unidad de negocio hidroagoyan.”. Se realizó una investigación de tipo aplicada y de campo. La técnica utilizada para la recolección de datos fue la observación, mediante tablas comparativas, entrevista y ficha de observación. Con la implementación del servidor de control Nagios Core como herramienta principal se permitió cubrir todas las necesidades y requerimientos planteados por la empresa, así también se abaratar costos de implementación del sistema de monitoreo con software libre.

Este antecedente de investigación presenta relación con el presente proyecto, en el sentido de que proporciona una amplia información referente al protocolo SNMP para la elaboración del marco teórico, asimismo se asemeja el tipo de investigación que se aborda.

2.1.2. Antecedentes Nacionales

(Gallego Adames & Lozano Garzón, 2015), en Bogotá. Realizo un proyecto titulado: "Rediseño e implementación de un sistema de monitoreo de la red de telecomunicaciones de distribuidora Nissan S.A", el cual se desarrolló adoptando un hibrido entre dos metodologías; la metodología SCRUM y la metodología de desarrollo de software en cascada. El desarrollo del sistema de monitoreo permitió centralizar la información para que su acceso y administración fuera más ágil y mucho más flexible, además se optimizaron los tiempos de respuesta frente a una caída del canal o falla del mismo. En cuanto al diseño de la herramienta se permite agregar más módulos si así se requiriere, ya que cuenta con una estructura muy dinámica y fácil de comprender.

Este antecedente de investigación presenta relación con el presente proyecto, en el sentido de que proporciona información referente a la importancia del monitoreo, por lo tanto, guiara en el planteamiento del problema.

(Ávila & Rafael, 2014), en Bogotá. Realizo una monografía titulada: "Diseño e implementación de un sistema de monitoreo basado en SNMP para la red nacional academia de tecnología avanzada", el objetivo general fue implementar un sistema de monitoreo de red, que permita observar el comportamiento de la infraestructura de comunicaciones de RENATA, garantizando la detección inmediata de incidentes con el fin de mantener la conectividad de las instituciones que cuentan con el servicio. Para tal propósito se diseñó la solución de monitoreo teniendo en cuenta los elementos y equipos de red, se determinó mediante una tabla comparativa cual era el software adecuado y se realizó la respectiva instalación de este. Con la implementación del sistema de monitoreo PRTG NETWORK MONITOR se logró mejorar las actividades del área técnica y en general de todo RENATA incluyendo las labores propias de la

operación, cumplimiento de ANS y obtención de las pruebas de cumplimiento a fin de resolver inconvenientes de facturación.

Este antecedente de investigación presenta relación con el presente proyecto, en el sentido de que proporciona una amplia información referente al protocolo SNMP y las herramientas de monitoreo de redes más utilizadas en el mercado, por lo tanto guiara en la elaboración del marco teórico.

2.1.3. Antecedentes Regionales

A nivel regional no se encontraron proyectos relacionados al tema de sistemas para el monitoreo de red.

2.2. Marco Teórico

Hoy en día, las redes de datos se han convertido en un elemento indispensable dentro de las organizaciones, no solo por permitir la conectividad a nivel Intranet y Extranet, también proporcionan servicios de red.

2.2.1. Gestión de Red

Según Martí (citado por Morelo, 2010) la gestión de red extiende sus bases sobre la planificación, organización y el control de los elementos comunicacionales para garantizar una adecuada calidad de servicio sobre un determinado costo; éste busca mejorar la disponibilidad, rendimiento y efectividad de los sistemas. Por lo que, la gestión de red se puede entender como un conjunto de procedimientos interesados en mantener la red en óptimo funcionamiento.

La información obtenida a través de los elementos y/o aplicaciones de la red pretende establecer dos procesos clave: el monitoreo y el control de red, ambos procesos se retroalimentan entre sí. Mientras que el monitoreo busca mantener información del comportamiento de todos los

entornos dispuestos sobre la red, el control busca mejorar el desempeño de los servicios que se dan lugar en una red (Morelo, 2010).

2.2.2. Monitoreo de Red

El monitoreo de red o la monitorización se define como la acción que permite verificar sistemáticamente el desempeño y la disponibilidad de los dispositivos críticos dentro de la red, a través de la identificación y detección de posibles problemas (Delgadillo Rivera & García Ronquillo, 2010).

2.2.2.1. Importancia del Monitoreo de Red. Según el sitio web tecnozero («Monitorizar nuestra red», 2014) las razones por las cuales es importante el proceso de monitoreo de red es:

- **Incremento de la eficiencia.** Los sistemas de monitoreo alertan y notifican en caso de presentarse una falla, por lo que no se requiere estar supervisando constantemente los componentes de la red y se puede dedicar el tiempo en otras actividades.
- **Planeación de recursos.** Permite la planificación de los recursos, mediante el conocimiento del uso de los recursos (CPU, espacio de disco, memoria, disco duro) de hardware, software y ancho de banda.
- **Optimización de la red.** El desempeño de la red puede ser optimizado a través del uso adecuado de los recursos de la infraestructura TI.
- **Mayor satisfacción para los usuarios.** Se consigue mejorar la experiencia del usuario asegurando la disponibilidad y la calidad de los servicios.
- **Verificación del cumplimiento de SLA.** Se puede garantizar los acuerdos a nivel de servicio (SLA), sobre todo para incidencias críticas.

- **Reducción de costos.** Por medio de los avisos, se asegura la identificación y resolución de problemas de forma más rápida.
- **Actualización.** Con la información suministrada por el proceso de monitoreo, se tiene un respaldo para tomar acciones; cambio o adición de proveedor, aumento de ancho de banda, cambio de equipos por fallas constantes, etc.

2.2.2.2. Tipos de Monitoreo. Según (Junco Romero & Rabelo Padua, 2018) existen al menos, dos puntos de vista para abordar el proceso de monitoreo de red: el enfoque activo y el enfoque pasivo. Aunque son diferentes ambos se complementan.

- **Enfoque activo.** Este tipo de monitoreo se realiza introduciendo paquetes de prueba en la red, o enviando paquetes a determinadas aplicaciones midiendo sus tiempos de respuesta. Este enfoque tiene la característica de agregar tráfico en la red y es utilizado para medir el rendimiento de la misma.
- **Enfoque pasivo.** Este enfoque se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por la red. Este enfoque no agrega tráfico en la red como lo hace el activo. Es utilizado para caracterizar el tráfico en la red y es utilizado para caracterizar el tráfico en la red y para contabilizar su uso.

2.2.3. SNMP (Simple Network Management Protocol)

Es un protocolo que forma parte de la capa de aplicación del modelo OSI, está diseñado para facilitar el intercambio de información entre los equipos de la red y su administrador, a fin de que este pueda supervisar su funcionamiento y sea posible tomar acciones en caso de fallas (Doctors & Vecchiotti, 2012).

2.2.3.1. Versiones Existentes de SNMP. Actualmente, existen tres versiones del protocolo que son: SNMPv1, SNMPv2c Y SNMPv3 (Delgadillo Rivera & García Ronquillo, 2010).

- **SNMPv1.** La primera versión protocolo SNMP, descrita en el RFC 1155 y 1157. La seguridad de esta versión está basada en comunidades con contraseñas simples sobre texto plano, que permiten a cualquier aplicación basada en SNMP tener acceso a la información con tan sólo poseer la cadena.
- **SNMPv2.** Tiene características en común con la versión 1 pero ofrece mejoras como, por ejemplo, operaciones adicionales. Utiliza el mismo modelo administrativo que la primera versión del protocolo SNMP, y como tal no incluye mecanismos de seguridad. Se describe en el RFC 1901, RFC 1905, RFC 1906, RFC 2578.
- **SNMPv3.** Es la actual y se define como la versión segura de SNMP, está agrega soporte para una autenticación fuerte y comunicación privada entre entidades administradas. Es un protocolo de manejo de red interoperable, que proporciona seguridad de acceso a los dispositivos por medio de una combinación de autenticación y cifrado de paquetes que trafican por la red. Se describe en el RFC 1905, RFC 1906, RFC 3411, RFC 3412, RFC 3414, RFC 3415.

2.2.3.2. Componentes Básicos de SNMP. Como se muestra en la figura 3, una red administrada a través del protocolo SNMP tiene tres componentes básicos. Según (Doctors & Vecchiotti, 2012) estos componentes son: NMS, agentes, y MIB.

- **NMS (Network Management System).** Son las interfaces entre el operador humano (administrador de red) y el sistema de gestión de la red, cuenta con una base de datos

que contiene toda la información necesaria para la gestión y que se obtiene de todas las bases de datos de las entidades a gestionar.

- **Agente**. Es un software que reside en un dispositivo administrado (dispositivos de red activos, computadores, impresora, etc.). Su trabajo consiste en responder las solicitudes que recibe, dependiendo del tipo de solicitud, debe devolver un valor o modificarlo (en el dispositivo sobre el que actúa).
- **MIB (Management Information Base).** Es una base de datos local de información de administración, en la que están contenidos todos los objetos que se van a administrar en la red junto con sus características. La información se almacena en forma de árbol, de manera jerárquica.

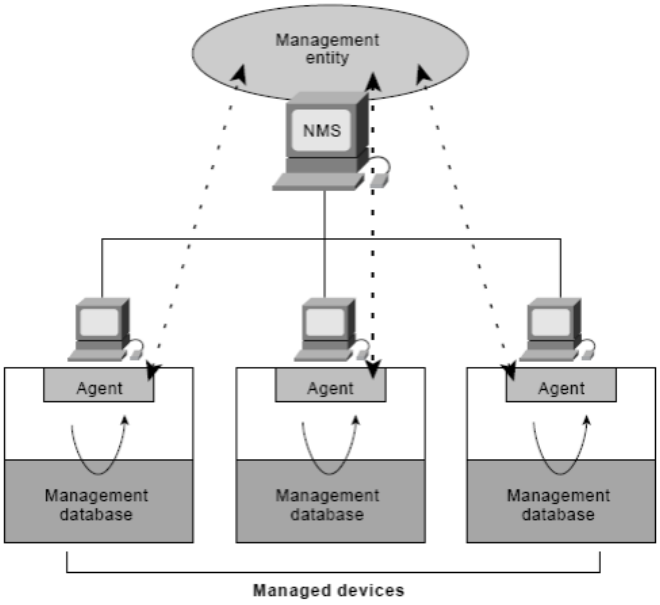


Figura 3. Componentes de SNMP**.**
Fuente: Jairo. (2012 , noviembre 12). SNMP Protocol. Docsity. https://www.docsity.com/pt/snmp-protocol/481541/.

2.2.3.3. Operaciones Básicas de SNMP. Según (Jardinez, 2009) los dispositivos administrados son supervisados y controlados usando cuatro operaciones SNMP básicas:

- **Operación de lectura.** Es usada por un NMS para supervisar elementos de red. El NMS examina diferentes variables que son mantenidas por los dispositivos administrados.
- **Operación de escritura.** Es usada por un NMS para controlar elementos de red. El NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados.
- **Operación de notificación.** Son usadas por los dispositivos administrados para reportar eventos en forma asíncrona a un NMS. Cuando cierto tipo de evento ocurre, un dispositivo administrado envía una notificación al NMS.
- **Operaciones transversales.** Son usadas por el NMS para determinar qué variables soporta un dispositivo administrado y para recoger secuencialmente información en tablas de variables como, por ejemplo, una tabla de rutas.

2.2.3.4. Mensajes SNMP. Los mensajes utilizados en SNMP son (ver Figura 4):

- **Get Request.** A través de este mensaje el NMS solicita al agente retornar el valor de un objeto de interés.

  Get Next Request. Es usado para recorrer una tabla de objetos. Una vez que se ha usado un mensaje GetRequest para recoger el valor de un objeto puede ser utilizado el mensaje GetNextRequest para repetir la operación con el siguiente objeto de la tabla.
- **Set Request.** Este tipo de mensaje es utilizado por el NMS para solicitar a un agente modificar valores de objetos.

- **Get Response.** Es usado por el agente para responder un mensaje GetRequest, GetNextRequest, o SetRequest.
- **Trap.** Permite a un agente notificar ciertas condiciones y cambios de estado a un proceso de administración.
- **Get Bulk Request**. Es usado por un NMS que utiliza la versión 2 o 3 del protocolo SNMP típicamente cuando es requerida una larga transmisión de datos, tal como la recuperación de largas tablas. En este sentido, es similar al mensaje GetNextRequest usado en la versión 1.
- **Inform Request.** Un NMS que utiliza la versión 2 o 3 del protocolo SNMP transmite un mensaje de este tipo a otro NMS con las mismas características, para notificar información sobre objetos administrados.

Los puertos comúnmente utilizados por el protocolo SNMP son el puerto 161, el cual escucha las peticiones GetRequest, GetNextRequest y SetRequest; y el puerto 162 que escucha los traps de los dispositivos. La figura 4 muestra un ejemplo de la utilización de los puertos UDP por SNMP para los gestores y agentes.

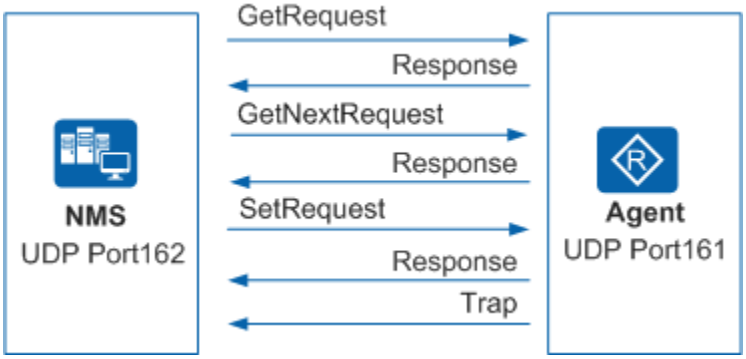


Figura 4. Mecanismos de trabajo de SNMP.
Fuente: (Working Mechanisms of SNMPv1/SNMPv2c, s. f.). Huawei. https://support.huawei.com/enterprise/en/doc/EDOC1100034234/73e6152/snmpv1-snmpv2c.

2.2.4. Herramientas de Monitoreo de Red

El proceso de gestión y monitoreo de redes se ha automatizado gracias al protocolo SNMP, que en resumen ha logrado mejorar la eficacia en general del proceso de administración de redes mediante el uso de herramientas de software (Ávila & Rafael, 2014).

En la actualidad existe un gran número de herramientas que permiten conocer el comportamiento general de la infraestructura para actuar rápidamente ante los incidentes. Estas herramientas se dan a conocer porque cuentan con un gran número de funcionalidades como monitorización remota, autodescubrimiento, monitoreo con o sin agentes, sistema de gestión de alertas, alto grado de documentación de los procesos de instalación y configuración, aplicación web, etc.

A continuación, se mencionan algunas de las herramientas más utilizadas en el mercado:

2.2.4.1. Cacti. Es una interfaz completa de RRDTool, almacena toda la información necesaria para crear gráficos y llenarlos con datos en una base de datos MySQL. La interfaz está completamente en PHP. Además de ser capaz de mantener los gráficos, fuentes de datos y de archivos Round Robin en una base de datos. También cuenta con soporte SNMP para la creación de gráficos de tráfico con MRTG. Esta herramienta cuenta con las siguientes funciones:

- **Fuentes de datos.** Para manejar la recolección de datos, se puede alimentar a Cacti con las rutas de acceso a cualquier script o comando externo, junto con todos los datos que el usuario necesitará para almacenar la base de datos MySQL. Las fuentes de datos también se pueden crear para que correspondan con los datos reales en las gráficas.
- **Gráficas.** Una vez que una o más fuentes de datos se definen, se puede crear un gráfico RRDTool utilizando los datos. Cacti permite crear casi cualquier gráfico

RRDTool utilizando todos los tipos estándar de gráficos y funciones de consolidación.

- **Gestión de usuarios.** Debido a las muchas funciones de Cacti, se incorpora una herramienta de gestión basada en el usuario para que se puede agregar usuarios y darles derechos a ciertas áreas.
- **Plantillas.** Cacti es capaz de escalar a un gran número de fuentes de datos y gráficos mediante el uso de plantillas. Esto permite la creación de un único gráfico o plantilla de fuente de datos que define cualquier gráfico o fuente de datos asociada con él. Las plantillas de host permiten definir las capacidades de un host para los cactus pueden sondear para información sobre la adición de un nuevo host (*Cacti - The Complete RRDTool-based Graphing Solution,* s. f.)

2.2.4.2. Nagios. Es un potente sistema de monitoreo que permite a las organizaciones identificar y resolver problemas de infraestructura de TI antes de que se afecten los procesos. Diseñado teniendo en cuenta los conceptos de escalabilidad y flexibilidad, Nagios da la tranquilidad de saber que los procesos de negocio de la organización no se verán afectados por las fallas en los servicios. Nagios permite detectar, reparar problemas y mitigar incidentes futuros antes de que afecten a los usuarios y clientes finales. Este sistema cuenta con las siguientes funciones:

- **Monitorear.** El personal de TI configura Nagios para supervisar componentes de la infraestructura de TI críticos, incluyendo las medidas del sistema, protocolos de red, aplicaciones, servicios, servidores y la infraestructura de red.
- **Alertar.** Nagios envía alertas cuando los componentes de infraestructura críticos fallan y se recuperan, proporcionando a los administradores la notificación de los

eventos importantes. Las alertas pueden ser entregadas a través de correo electrónico, mensaje de texto, o un script personalizado.

- **Responder.** El personal de TI puede reconocer alertas y comenzar a resolver las fallas e investigar las alertas de seguridad de inmediato.
- **Informar.** Los informes proporcionan un registro histórico de los incidentes, eventos, notificaciones, y la respuesta de la alerta para su posterior revisión. Los informes de disponibilidad ayudan a asegurar el cumplimiento de las SLAs.
- **Mantenimiento.** El tiempo de inactividad programado evita alertas durante los mantenimientos y actualizaciones programadas.
- **Planear.** Mostrar tendencias, gráficos e informes de planificación de capacidad para permitir identificar mejoras de infraestructura necesarias antes de que ocurran fallas (*Nagios Overview*, s. f.)

2.2.4.3. Zabbix. Es un software de código abierto que permite monitorear numerosos parámetros de una red, así como la salud e integridad de los distintos servicios o dispositivos. Zabbix utiliza distintos mecanismos de notificaciones, como SMS y correos electrónicos.

Zabbix ofrece:

- Detección automática de servidores y dispositivos de red.
- Descubrimiento de bajo nivel.
- Monitoreo distribuido con web de administración centralizada.
- Software de servidor para Linux, Solaris, HP-UX, AIX, BSD libres.
- Agentes de alto rendimiento (software de cliente para Linux, Solaris, HP-UX, AIX, BSD libres, BSD Open, OS X, Tru64/OSF1, Windows NT 4.0, Windows 2000, Windows 2003, Windows XP, Windows Vista).

- Monitoreo sin agentes.
- Autenticación de usuario segura.
- Permisos de usuario flexibles.
- Interfaz basada en web.
- Notificación flexible de correo electrónico de eventos predefinidos.
- Alto nivel (de negocios) vista de los recursos controlados.
- Registro de logs (*Zabbix Overview*, s. f.)

2.2.5. Sistema de Almacenamiento Remoto

Según el Instituto Nacional de Ciberseguridad (INCIBE, 2016) la creciente dependencia de las organizaciones de sus sistemas de información pone de manifiesto la necesidad de contar con medios y técnicas que permitan almacenar la información de la manera más adecuada. Una correcta gestión de este proceso permite mantener en todo momento la integridad, confidencialidad y disponibilidad de la información.

2.2.5.1. Tipos de Almacenamiento. A continuación, se describen los tipos de almacenamiento existentes:

- **Almacenamiento local.** La información se genera en equipos informáticos y desde ellos se modifica y transmite. Cada uno de estos equipos dispone de un sistema de almacenamiento local, normalmente discos duros donde se guarda la información. También es almacenamiento local el utilizado en tabletas y dispositivos móviles interno o en tarjetas de memoria (micro SD).
- **Servidores de almacenamiento en red.** Para poder disponer de un lugar común de trabajo donde almacenar el resultado de los trabajos individuales y poder compartir

información entre los diferentes usuarios de la empresa se dispone de servidores de almacenamiento en red.

- **Dispositivos externos.** Adicionalmente se puede disponer de sistemas externos que, conectados directamente a los equipos, permiten un almacenamiento extra de la información, evitando que se ocupe este espacio en el equipo. Estos pueden ser cintas magnéticas, discos duros externos, CD o DVD o pendrives conectados a través de distintos interfaces físicos.
- **Sistema de copias de seguridad.** Es muy recomendable establecer un procedimiento para sistematizar la realización de copias de respaldo de la información generada en la empresa, en soportes externos o en otra ubicación.
- **Servicios de almacenamiento en la nube.** Es posible utilizar servicios de almacenamiento en la nube como medio de almacenamiento externo, para compartir la información generada o para realizar copias de seguridad.

2.2.5.2. ¿Por qué Almacenar en la Nube?. Según el sitio web suempresa.com (*Todo lo que debes saber sobre el Almacenamiento en la Nube*, 2017) una de las principales ventajas que ofrece es que se cuenta con almacenamiento infinito y seguro, a un precio bajo o incluso gratuito.

Otras razones para almacenar la información en la nube son:

- **Personal más eficiente.** Un escenario donde la nube permite eliminar procesos repetitivos al automatizarlos. Esto brinda eficiencia y productividad.
- **Ahorro y sustentabilidad.** Desde el momento en que los servidores son virtualizados, es decir, mediante la adopción de la nube como forma de trabajo, se comenzará a ahorrar, al tener un menor uso de espacio físico, menos equipo y por ende, se reducirán los gastos.

- **Confiabilidad.** La nube funciona mediante plataformas que están altamente disponibles y gestionadas por expertos calificados, lo cual garantiza que, en caso de presentarse una falla en un servidor físico, el entorno virtual no resultará dañado. Asimismo, la privacidad es un asunto primordial, puesto que sólo tendrá acceso a las aplicaciones y datos gestionados por la nube el personal habilitado. Por esta razón, se acabarán las preocupaciones de perder información por accidente o intrusiones no permitidas.

2.3. Marco Conceptual

- **Monitorización:** es la acción y efecto de monitorizar que, según el Diccionario de la Lengua Española, significa observar, mediante aparatos especiales, el curso de uno o varios parámetros fisiológicos o de otra naturaleza, para detectar posibles anomalías. Por lo que, la monitorización de red es la acción que nos permite verificar sistemáticamente el desempeño y la disponibilidad de los dispositivos críticos dentro de la red, a través de la identificación y detección de posibles problemas (Delgadillo Rivera & García Ronquillo, 2010).
- **SNMP (Simple Network Management Protocol):** es un protocolo de capa de aplicación definido en el RFC 1157 para intercambiar información de administración entre dispositivos de red. Forma parte del conjunto de protocolos TCP/IP (*¿Qué es SNMP?*, s. f.).
- **Software Libre:** es un software que respeta las 4 libertades que la FSF (Free Software Foundation) establece:
    - Libertad de usar el programa, con cualquier propósito

  - Libertad de estudiar cómo funciona y modificarlo, adaptándolo a las necesidades.
  - Libertad de distribuir copias del programa
  - Libertad de mejorar el programa y hacer públicas esas mejoras

- **Open Source:** es la expresión con la que se conoce al software distribuido y desarrollado libremente. Su punto de vista se orienta en compartir el código, para que el software resultante sea de calidad superior al del propietario (Andrearrs, 2014). Es importante distinguir entre open source, que se caracteriza por presentar su código fuente y el software libre que es una cuestión de libertad, no de precio.
- **Almacenamiento remoto:** es un servicio de administración de datos utilizado para migrar archivos que se encuentran almacenados localmente a una ubicación de almacenamiento remota (*Almacenamiento remoto*, s. f.).

2.4. Marco Legal

- **SNMPv1** se define en RFC 1157.
- **SNMPv2** se define en las RFC 1441 a 1452.
- **SNMPv2c** se define en las RFC 1901 a 1908.
- **SNMPv2u** se define en las RFC 1909 a 1910.
- **SNMPv3** se define en las RFC 3411 a 3418 (*RFC Index*, s. f.).
- **Decreto 2573 de 2014** por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente las Leyes 1341 de 2009, y se dictan otras disposiciones.
- **Gobierno en Línea (GEL)** es una estrategia definida por el Gobierno Nacional, que pretende lograr un salto en la inclusión social y en la competitividad del país a través

de la apropiación y el uso adecuado de las Tecnologías de la Información y las Comunicaciones (T.I.C).

La directriz pertinente para esta investigación es la: gestión de la calidad y de seguridad de los servicios tecnológicos, que busca aplicar mecanismos adecuados de aseguramiento, control, inspección y mejoramiento de la calidad de los servicios tecnológicos, la cual hace parte del eje de TIC para la gestión.

- **Decreto 1078 de 2015** por medio del cual se expide el decreto único reglamentario del sector de tecnologías de la información y las comunicaciones (*MinTic*, s. f.)
- **ISO/IEC 27001** es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan (*ISO 27001*, s. f.).

2.5. Metodología

Este proyecto ha sido desarrollado bajo la metodología PPDIOO (Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar), la cual establece 6 fases ejecutadas secuencialmente:

- **Fase I: Preparar.** En esta fase se realizó el levantamiento de información de la infraestructura de red de datos y se evidenciaron los componentes y servicios a ser supervisados mediante el sistema de monitoreo de red.
- **Fase II: Planificar.** Dentro de esta fase se efectuó el levantamiento de información de las necesidades y requisitos de la infraestructura de red de datos.
- **Fase III: Diseñar.** En esta fase se realizó la determinación de la herramienta más adecuada para la infraestructura de red de datos, mediante la comparación y evaluación de las herramientas de monitoreo open source más destacadas en la actualidad; además de tener en cuenta la opinión del personal administrativo de CSI

sobre los resultados obtenidos. Así mismo, se realizó el diseño de la arquitectura lógica y física del sistema de monitoreo, basándose en los requisitos obtenidos durante la fase de planeación.

- **Fase IV: Implementar.** Dentro de esta fase se llevaron a cabo los procedimientos de instalación, configuración y monitorización de los componentes que conforman el sistema de monitoreo diseñado. Así mismo, se realizaron las pruebas para verificar el funcionamiento correcto de la solución implantada y validar el cumplimiento de los requisitos definidos por el personal administrativo de CSI y se creó el plan de continencia que permite recuperar la disponibilidad del sistema de monitoreo ante una falla.
- **Fase V: Operar.** En esta fase se puso en marcha el sistema de monitoreo con el fin de verificar su rendimiento y así poder realizar futuras optimizaciones.
- **Fase VI: Optimizar.** Dentro de esta fase se propusieron cambios en el sistema de monitoreo para mejorar el rendimiento de el mismo.

Finalmente, se elaboraron los manuales de instalación, configuración y administración del sistema de monitoreo de red y se realizó la capacitación sobre el manejo optimo del sistema de monitoreo de red con el personal administrativo de CSI.

Como se muestra en la figura 5, se establecieron una serie de actividades para cada fase con el fin de cumplir los objetivos establecidos.

	Nombre	Duracion
1	PROYECTO "SISTEMA DE MONITOREO PARA LA INFRAESTRUCTURA DE I	76 days?
2	Objetivo 1	21 days?
3	Preparar	7 days
4	Diseño y validación de instrumentos	2 days
5	Reunion con los administrativos de CSI	1 day
6	Revisión de documentación proporcionada por CSI acerca de la infraestructu	2 days
7	Visita de los centros de cableados que hacen parte de la infraestructura de	2 days
8	Planificar	3 days
9	Reunion con los administrativos de CSI	1 day
10	Definición de requisitos	2 days
11	Diseñar	11 days?
12	Búsqueda, consulta y análisis documental de las diferentes herramientas de	3 days
13	Análisis de herramientas de monitoreo	7 days
14	Diseño de la arquitectura fisica y logica	1 day?
15	Objetivo 2	26 days
16	Implementar	26 days
17	Preparación del entorno de despliegue para la herramienta de monitoreo	5 days
18	Despliegue de la herramienta de monitoreo	7 days
19	Búsqueda y consulta referente al proceso de activación del protocolo SNMP	2 days
20	Activación del protocolo SNMP en los dispositivos de red activos a monitorea	7 days
21	Ingreso de los dispositivos de red activos al sistema de monitoreo	5 days
22	Objetivo 3	17 days?
23	Diseño de pruebas de funcionamiento del sistema de monitoreo de red	3 days
24	Aplicación de pruebas de funcionamiento del sistema de monitoreo de red	7 days
25	Diseño del plan de contingencia	2 days?
26	Operar	1 day?
27	Puesta en marcha del sistema de monitoreo	1 day?
28	Optimizar	5 days
29	Ajustes pertinentes al sistema de monitoreo de red	5 days
30	Objetivo 4	13 days
31	Cierre	13 days
32	Recopilación del contenido de los manuales	2 days
33	Diseño del formato para los manuales	3 days
34	Creación de los respectivos manuales	7 days
35	Socialización del funcionamiento del sistema de monitoreo de red	1 day

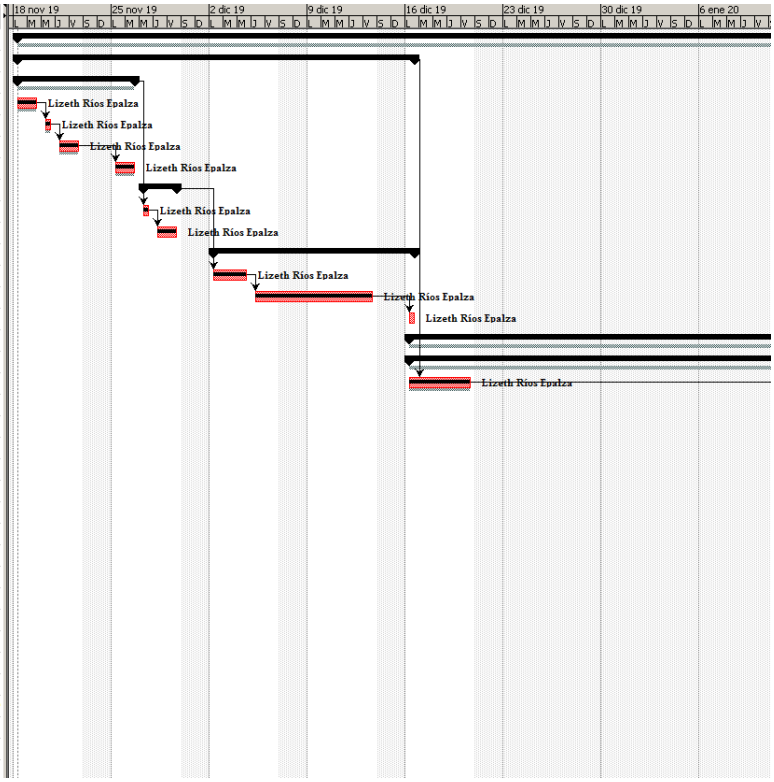


Figura 5. Actividades y diagrama de Gantt

Desarrollo del Proyecto

3.1. Fase I: Preparación

3.1.1. Centros de Cableado

La UFPS sede Cúcuta cuenta con varios centros de cableado ubicados en diferentes zonas geográficas, en cuya área, se extiende un backbone de fibra óptica con topología estrella extendida que interconecta el centro de cableado principal ubicado en el edificio Aula Sur con los demás edificios localmente dispersos mediante switches Gigabit Ethernet.

Por su parte, la sede Campos Elíseos se interconecta con la sede Cúcuta a través de una infraestructura proporcionada por el ISP. En su totalidad, la infraestructura de red de datos está conformada por 53 centros de cableado como se detallan en la tabla 1.

Tabla 1

Listado de centros de cableado de la UFPS

Sede	Edificio	Abreviatura	Cantidad
Cúcuta	Aula Sur	SA	3
	Aula Sur C	SC	1
	Aula Sur D	SD	1
	Aula Sur E	SE	1
	Aula Sur F	SF	2
	Aulas Norte	NA	1
	Biblioteca	BL	1
	Casona	CS	1
	CREAD	CR	3
	División de Sistemas	DS	2
	Fundadores	FU	4
	Fac. Ciencia de la Salud	FS	4
	Lab. Generales	LG	4
	Lab. Empresarial	LM	2

	Posgrados	PG	1
	Semipesados	SP	1
	Térreos	TE	1
	Torre Administrativa A	TA	2
	Torre Administrativa B	TB	1
	Investigación	IN	1
	Lab. Diseño Mecánico	DM	1
	Lab. Estructuras Civiles	EC	1
	Entrada Peatonal	EP	1
	Entrada Vehicular	EV	1
	Lab. Básicos	LB	1
	Aulas Generales	AG	1
	Comunicación Social	SG	1
Campos Elíseos	Sala de Profesores	SP	1
	Lab. Operaciones Unitarias	OU	1
	Lab. Anatomía Animal	AA	1
	Lab. Sanidad Vegetal	SV	1
	Lab. Cepas, Aguas y Nutrición	LC	1
	Lab. Biotecnológica Vegetal	BV	1
	Lab. Agroindustrial	AG	1
	Lab. Suelos	LS	1
	Lab. Calidad Ambiental	CA	1

En la figura 5 se muestran algunas fotografías que permiten observar parte de la infraestructura de red de datos.

Figura 6. Fotografías de algunos centros de cableado

3.1.2. Enlaces de Comunicación

Actualmente, la infraestructura de red de datos tiene dos enlaces de comunicación; estos son claves para la comunicación entre las sedes y el ISP. En la tabla 2 se detallan los enlaces de comunicación existentes.

Tabla 2

Enlaces de comunicación

Enlace	Tipo	Capacidad
UFPS Canal de datos principal	Fibra óptica	350 Mbps
UFPS Canal Campos Elíseos	Fibra óptica	200 Mbps

3.1.3. Equipos

En las tablas 3 y 4 se detallan los dispositivos de red activos y los recursos y servicios que hacen parte de la infraestructura de red de datos.

Tabla 3

Dispositivos de red activos

Sede	Dispositivo	Marca	Cantidad
Cúcuta	Switch	Cisco	93
		3Com	22
	Access Point	Cisco	180
Campos Elíseos	Switch	Cisco	10
	Access Point	Cisco	13

Tabla 4

Recursos y servicios de red

Tipo	Descripción	Cantidad
Recurso	Servidores	9
Servicio	DHCP	2
	DNS	5
	Firewall	6

Esta información se obtuvo mediante la realización de entrevistas al personal administrativo de CSI, la revisión documental de la red de datos y la visita a los centros de cableado. El formato de la entrevista aplicada se puede observar en el Anexo 2 del documento.

3.2. Fase II: Planificación

3.2.1. Necesidades para cada equipo

Ya que la infraestructura de red de datos está conformada por equipos de diferentes marcas y con diferentes funciones, se definieron los parámetros a monitorear para cada equipo: Esta información se obtuvo mediante la realización de entrevistas al personal administrativo de CSI, el formato de la entrevista aplicada se puede observar en el Anexo 3 del documento.

3.2.1.1. Switch.

- **CPU:**
    - Carga del procesador
- **General:**
    - Nombre del dispositivo
    - Descripción del dispositivo
    - Contacto del dispositivo
    - Ubicación del dispositivo
- **Interfaces:**
    - Descripción de la interfaz
    - Alias de la interfaz
    - Estado administrativo de la interfaz
    - Estado operativo de la interfaz
    - Ancho de banda
    - Bytes recibidos en la interfaz
    - Bytes transmitidos en la interfaz
- **Memoria:**
    - Espacio libre de la memoria
    - Carga de la memoria
    - Espacio usado de la memoria
- **Estado:**
    - Tiempo que lleva en funcionamiento el dispositivo
    - Estado de conexión del dispositivo (ping)

- **Temperatura:**
    - Temperatura

3.2.1.2. Servidor.

- **CPU:**
    - Uso del procesador
    - Numero de procesadores
- **Almacenamiento:**
    - Espacio libre de la partición
    - Espacio total de la partición
    - Espacio usado de la partición
- **General:**
    - Nombre del equipo
    - Estado del servidor
    - Tiempo que lleva en funcionamiento el servidor
- **Memoria:**
    - Espacio libre de la memoria
    - Carga de la memoria
    - Espacio usado de la memoria
- **Red:**
    - Bytes recibidos en la interfaz de red
    - Bytes transmitidos en la interfaz de red

3.2.2. Requisitos

Para obtener los requisitos se aplicó una entrevista al personal administrativo de CSI. El formato de la entrevista aplicada se puede observar en el más adelante del documento.

3.2.2.1. Requisitos Funcionales. Los requisitos funcionales son declaraciones de los servicios o funciones que debe proporcionar el sistema. En la tabla 5 se detallan los requisitos funcionales que se tuvieron en cuenta para el diseño del sistema de monitoreo.

Tabla 5

Requisitos funcionales

Id	Nombre del Requisito	Descripción	Prioridad
RF01	Equipos a monitorear	La herramienta de monitoreo permitirá monitorear cualquier equipo que se identifique con una dirección IP.	Alta
RF02	Parámetros a monitorear	La herramienta de monitoreo permitirá monitorear parámetros relacionados al almacenamiento, memoria, CPU, temperatura e interfaces de Red.	Alta
RF03	Gestión de equipos	La herramienta de monitoreo permitirá gestionar (añadir, editar o eliminar) los equipos y parámetros a monitorear.	Alta
RF04	Soporte SNMP	La herramienta de monitoreo contará con soporte para el protocolo SNMP.	Alta
RF05	Agentes	La herramienta de monitoreo contará con agentes para el monitorear de equipos sin protocolo SNMP.	Alta
RF06	Gestión de alertas	La herramienta de monitoreo permitirá gestionar alertas a través de las cuales se notifique el estado de los equipos.	Alta
RF07	Niveles de alerta	La herramienta de monitoreo permitirá definir	Alta

		diferentes niveles en función de la severidad del evento.	
RF08	Graficas	La herramienta de monitoreo permitirá obtener gráficas de los parámetros monitoreados.	Alta
RF09	Notificaciones	La herramienta de monitoreo permitirá notificar la existencia de un evento.	Alta
RF10	Reportes	La herramienta de monitoreo permitirá presentar reportes de distintos tipos.	Alta

3.2.2.2. Requisitos no Funcionales. Los requisitos no funcionales son restricciones de las funciones ofrecidas por el sistema. En la Tabla 6 se detallan los requisitos no funcionales que se tuvieron en cuenta para el diseño del sistema de monitoreo.

Tabla 6

Requisitos no funcionales

Id	Nombre del Requisito	Descripción	Prioridad
RNF01	Disponibilidad	La herramienta de monitoreo deberá estar disponible el 99,99% de las veces en que el usuario intente acceder.	Alta
RNF02	Entorno	La herramienta de monitoreo deberá ser compatible con los recursos de hardware del servidor disponible (ver Tabla 7).	Alta
RNF03	Interfaz	La herramienta de monitoreo deberá disponer de una interfaz web que permita observar el comportamiento de los equipos en tiempo real.	Alta
RNF04	Seguridad	El acceso a la interfaz web de la herramienta de monitoreo deberá estar restringido bajo un usuario y contraseña definidos.	Alta
RNF05	Seguridad	El usuario administrador designado es el	Alta

		único con permisos para acceder a la interfaz web y hacer cualquier tipo de modificación.	
RNF06	Implantación	La herramienta deberá ser open source o estar a disposición de la UFPS.	Alta

Tabla 7

Entorno disponible

Sistema Operativo	CPU	Disco Duro	RAM
CentOS 7	2 GHz	200 GB	4 GB

3.3. Fase III: Diseño

3.3.1. Determinación de la herramienta de monitoreo

En el mercado existe una gran variedad de herramientas open source para el proceso de monitorización de infraestructuras de red. Razón por la cual, se decidió realizar una tabla comparativa de las herramientas de monitoreo de red más destacadas en la actualidad.

3.3.1.1. Comparación. A continuación, se definen los parámetros que se tuvieron en cuenta para la realización de la tabla comparativa. Estos parámetros se basaron en los requisitos definidos en la fase de planeación y en algunas características que dan un valor agregado:

- **Licencia.** Tipo de licencia
- **Sistema operativo.** Sistemas operativos compatibles
- **Almacenamiento.** Sistemas de gestión de bases de datos compatibles
- **Aplicación web.** Permite el acceso desde cualquier dispositivo conectado a Internet
- **SNMP.** Soporte del protocolo de intercambio de información entre los equipos de la red y su administrador.

- **Agentes**. Permite recopilar y reportar una variedad de datos, incluyendo métricas de rendimiento, registros de eventos e información de seguimiento.
- **Graficas.** Permite que el monitoreo en tiempo real sea visual
- **Alertas.** Envía notificaciones vía correo o SMS en caso de presentarse un evento
- **Eventos.** Permite visualizar algún comportamiento atípico e informar
- **Predicción Estadística.** Permite predecir eventos antes de que sucedan
- **Reportes.** Permite mostrar un conjunto de parámetros o datos recopilados
- **Autodescubrimiento**. Permite analizar segmentos de red definidos para reconocer automáticamente los equipos.
- **Monitoreo distribuido**. Permite entregar múltiples sistemas recolectores de información y centralizar la información en un solo servidor.
- **Mapa de red.** Permite esquematizar la red de manera gráfica.

Tabla 8

Comparación de herramientas de monitoreo de red open source

Nombre	Licencia	Sistema Operativo	Almacenamiento	Aplicación Web	SNMP	Agentes	Graficas	Plantillas	Alertas	Eventos	Predicción Estadística	Reportes	Autodescubrimiento	Monitoreo Distribuido	Mapa de Red
Cacti	GNU GPL	Linux, Unix, Windows.	RRDtool, MySQL.	✓	✓	X	✓	✓	*	✓	X	*	*	X	✓
Nagios Core	GPLv2	Linux, Unix, Windows.	MySQL (opcional)	✓	*	✓	✓	✓	✓	✓	X	✓	X	✓	✓
Pandora FMS Community	GPLv2	Linux, FreeBSD, Windows.	MySQL, Oracle	✓	✓	✓	✓	✓	✓	✓	X	✓	X	X	✓
Zabbix	GPLv2	Linux, FreeBSD, Mac OS, Windows.	MySQL, PostgreSQL, Oracle	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Zenoss Core	GPLv2	RebHat, CentOS.	RRDtool, MySQL.	✓	✓	X	✓	✓	✓	✓	✓	✓	✓	✓	✓

Nota. El símbolo asterisco (*****) significa que se necesita instalar un plug-in para utilizar la funcionalidad. Fuente: Autoría propia.

Una vez se analizó la tabla comparativa, se consideraron dos alternativas de solución Nagios Core y Zabbix, por lo cual, se decidió realizar una instalación piloto para evaluar a fondo cada herramienta.

3.3.1.2. Instalación piloto. Con la finalidad de determinar la herramienta a implantar, se creó un entorno de despliegue. Para facilitar el proceso de creación se utilizó el software VirtualBox, el cual permite crear máquinas virtuales y realizar copias de instancias.

Para la evaluación de las herramientas de monitoreo preseleccionadas se tomaron varios de los parámetros mencionados anteriormente y se les asigno un porcentaje de relevancia. En la tabla 9 se detallan los porcentajes de evaluación y en la tabla 10 se detalla la escala de calificación que va desde 1 hasta el 5.

Tabla 9

Porcentajes de evaluación

Parámetro	**Porcentaje**
Aplicación web	10%
SNMP	10%
Agentes	10%
Graficas	10%
Plantillas	10%
Alertas	10%
Eventos	10%
Predicción estadística	5%
Reportes	10%
Autodescubrimiento	5%
Monitoreo distribuido	5%
Mapa de Red	5%
Total	**100%**

Tabla 10

Escalas de equivalencias

Cuantitativa	1	2	3	4	5
Cualitativa	Insuficiente	Regular	Bueno	Muy bueno	Excelente

3.3.1.2.1. Nagios Core. A continuación, se muestran algunas pantallas de la herramienta de monitoreo Nagios Core:

Figura 7. Pantalla de inicio de Nagios Core

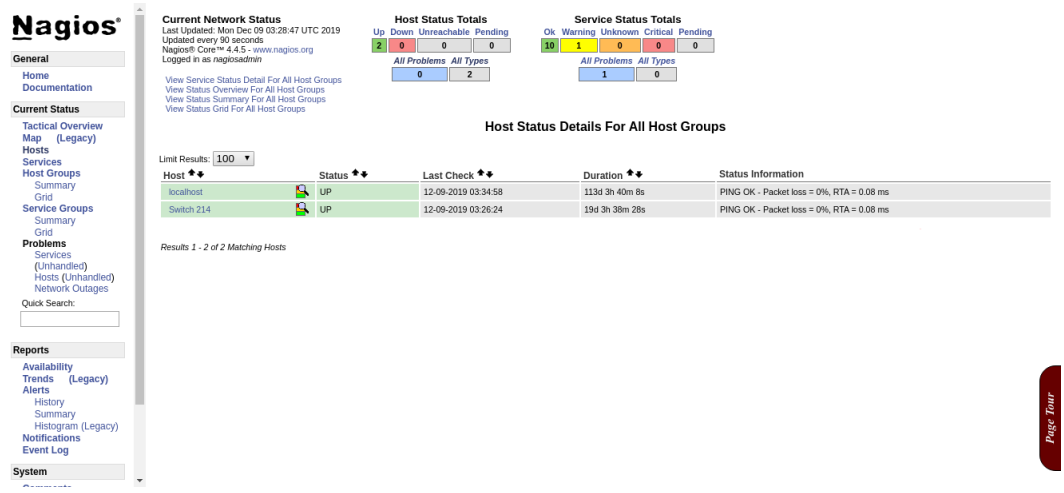


Figura 8. Pantalla de host de Nagios Core

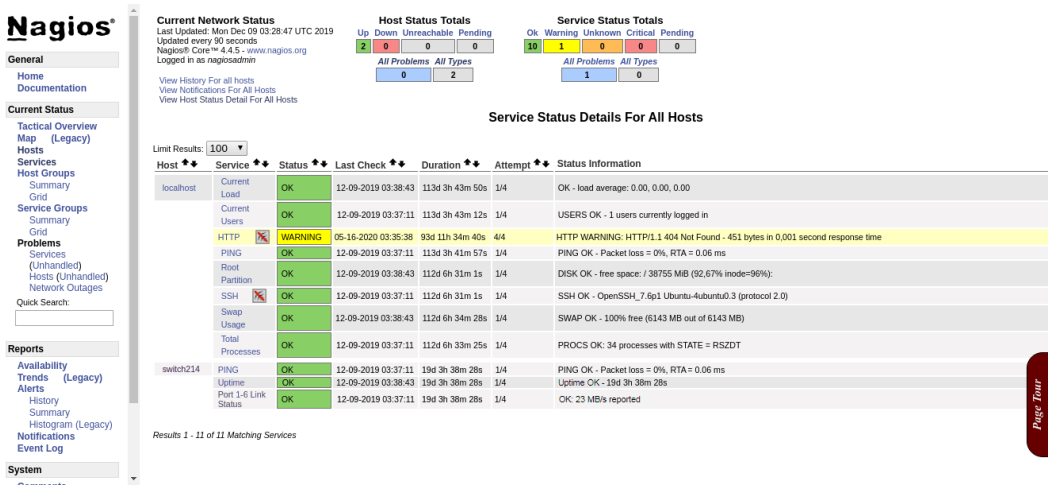


Figura 9. Pantalla de servicios de Nagios Core

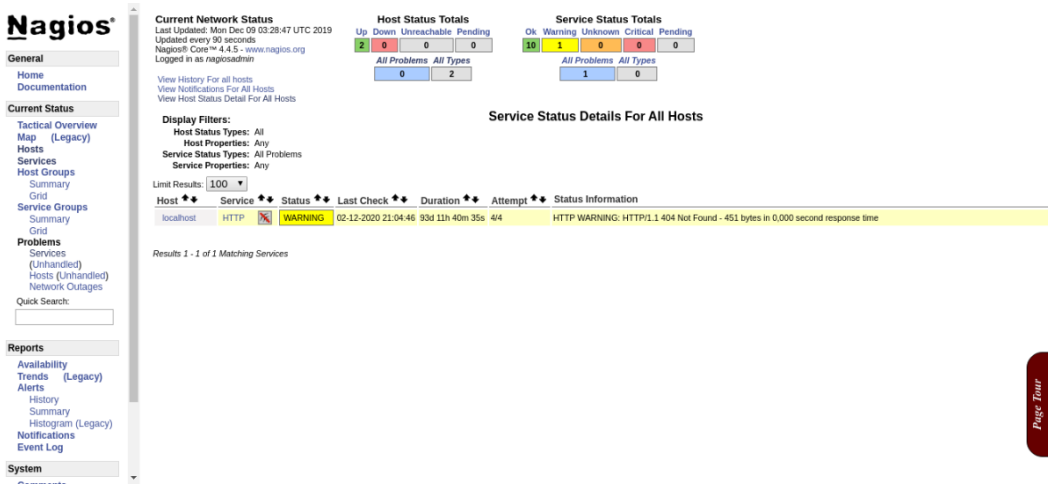


Figura 10. Pantalla de problemas de Nagios Core

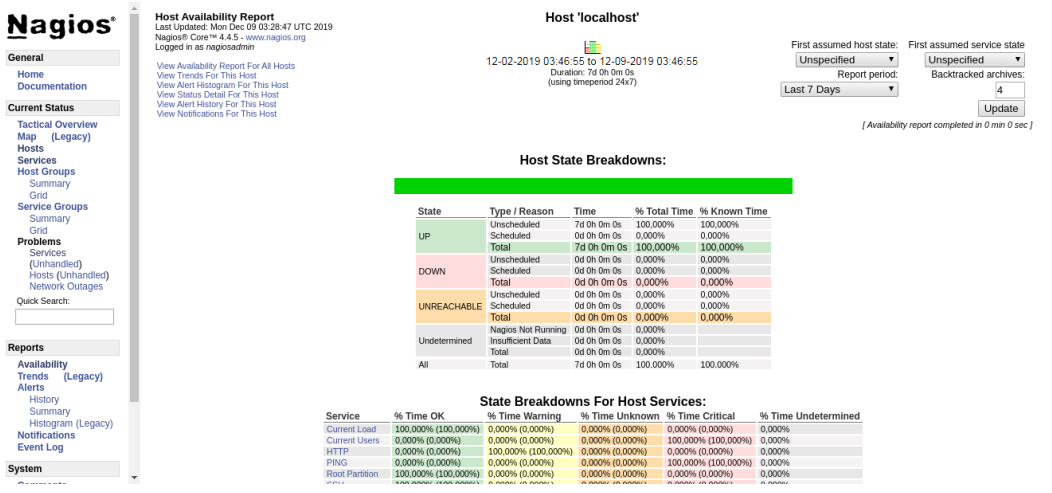


Figura 11. Pantalla de reportes de Nagios Core

3.3.1.2.2. Zabbix. A continuación, se muestran algunas pantallas de la herramienta de monitoreo Zabbix:

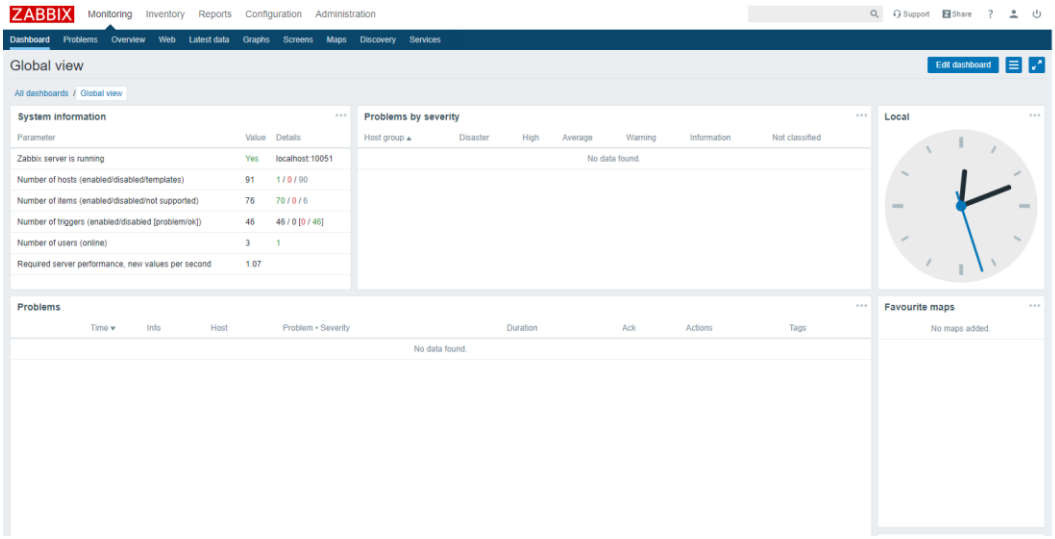


Figura 12. Pantalla de inicio de Zabbix

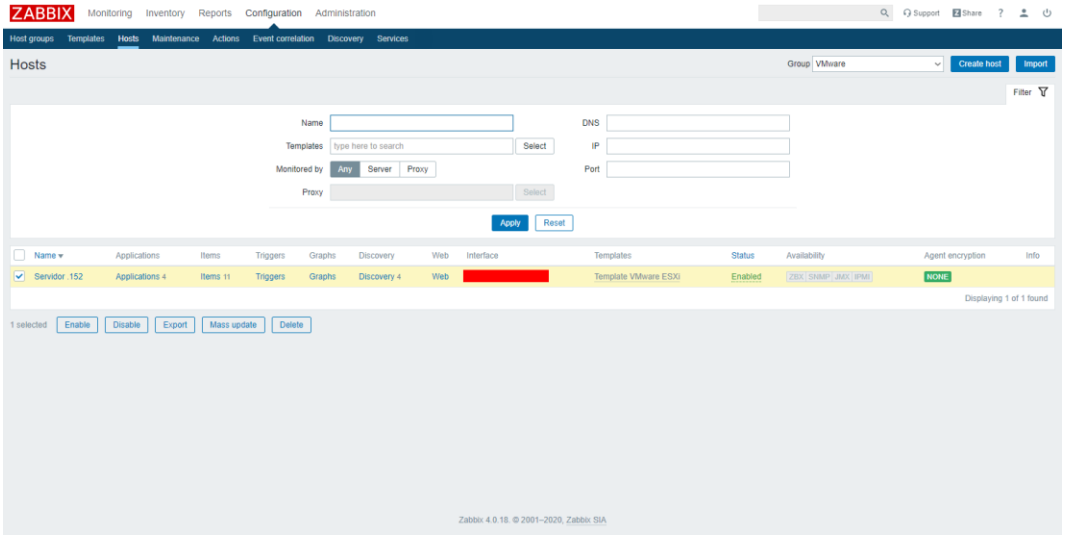


Figura 13. Pantalla de host de Zabbix

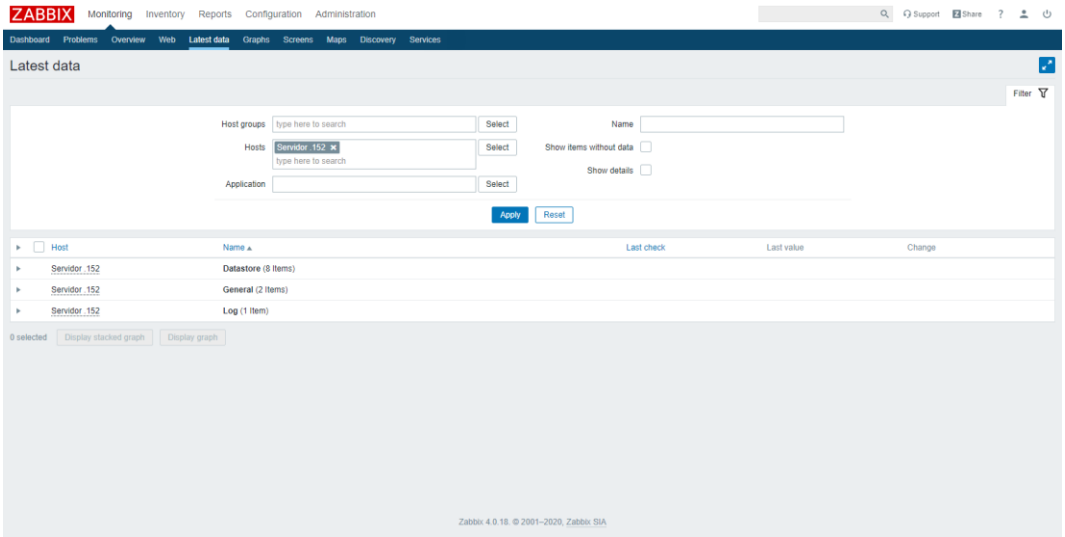


Figura 14. Pantalla de parámetros monitoreados de Zabbix

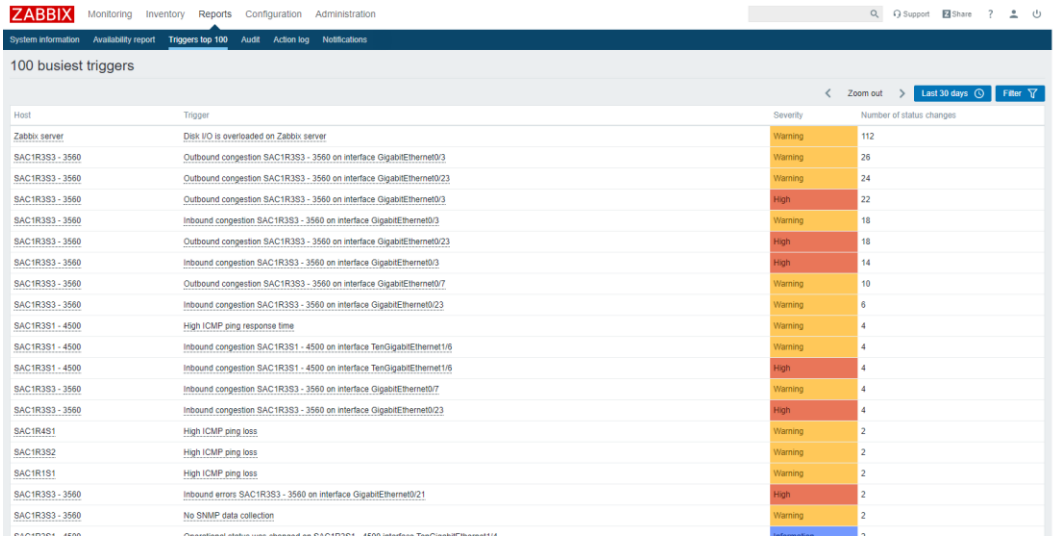


Figura 15. Pantalla de problemas de Zabbix

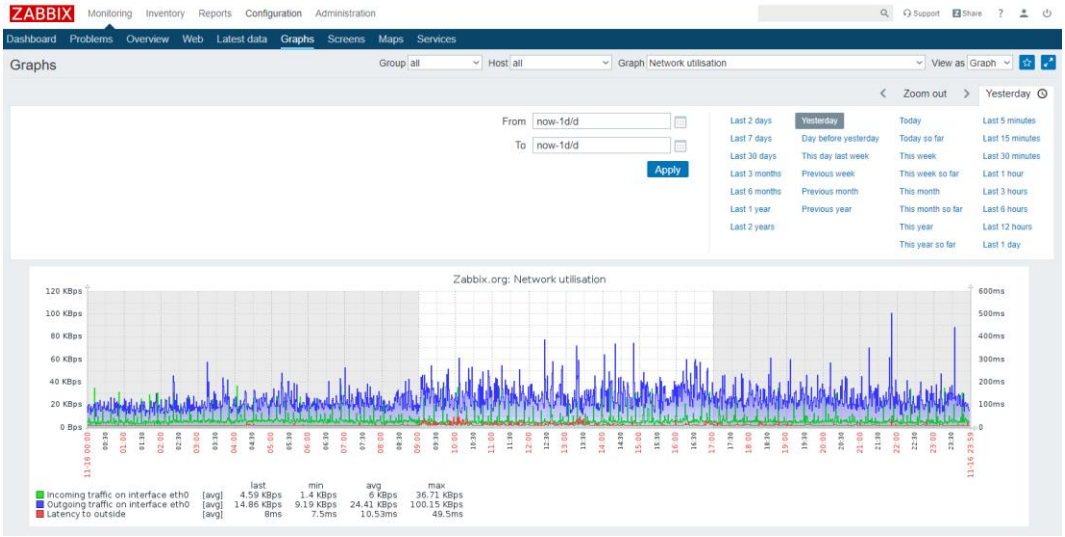


Figura 16. Pantalla de graficas de Zabbix

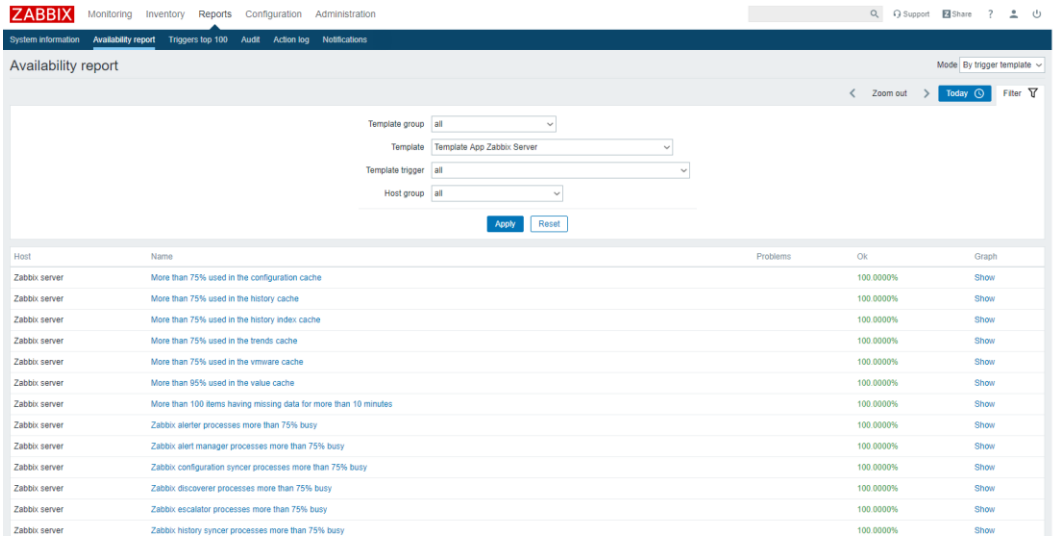


Figura 17. Pantalla de reportes de Zabbix

3.3.1.2.3. Resultados. El resultado de la evaluación de las herramientas de monitoreo preseleccionadas se resume en dos tablas de valoración y en una tabla de aspectos relevantes que se pudieron apreciar durante la evaluación de las herramientas de monitoreo.

Tabla 11

Resultado de la evaluación por rango de dígitos

Parámetro	**Nagios Core**	**Zabbix**
Aplicación web	2	5
SNMP	4	5
Agentes	5	5
Graficas	4	5
Plantillas	4	5
Alertas	5	5
Eventos	5	4
Predicción estadística	1	5
Reportes	2	3
Autodescubrimiento	1	5
Monitoreo distribuido	5	4
Mapa de Red	3	4
Total	**41**	**55**

Tabla 12

Resultado de la evaluación en porcentaje

Parámetro	**Nagios Core**	**Zabbix**
Aplicación web	0,2	0,5
SNMP	0,4	0,5
Agentes	0,5	0,5
Graficas	0,4	0,5
Plantillas	0,4	0,5
Alertas	0,5	0,5
Eventos	0,5	0,4

Predicción estadística	0,05	0,25
Reportes	0,2	0,3
Autodescubrimiento	0,05	0,25
Monitoreo distribuido	0,25	0,2
Mapa de Red	0,15	0,2
Total	**3,6**	**4,6**

Tabla 13

Aspectos relevantes en la evaluación de las herramientas de monitoreo

Aspecto	**Nagios Core**	**Zabbix**
Instalación y configuración inicial	La instalación y configuración inicial de Nagios Core no es complicada si se sigue la documentación oficial.	La instalación y configuración inicial para Zabbix es un poco más complicada, requiere una mayor cantidad de pasos y una base de datos para operar.
Configuración	La configuración de Nagios Core se realiza editando archivos de texto y siguiendo una determinada sintaxis.	La configuración de Zabbix se realiza a través de una interfaz basada en la web.
Aplicación web	La aplicación web de Nagios Core es bastante limitada, solo permite visualizar el estado de la red e informes.	La aplicación web de Zabbix (frontend) permite tener el control total (visualizar, gestionar y configurar) del sistema de monitoreo.
Soporte de protocolos	Las herramientas soportan los mismos protocolos de monitoreo. Por defecto Nagios Core no tiene el protocolo SNMP, para tener esta funcionalidad se requiere instalar un plug-in.	Las herramientas soportan los mismos protocolos de monitoreo
Graficas	Por defecto Nagios Core no tiene gráficas, para tener esta funcionalidad se requiere instalar un	Zabbix por su parte tiene sus propias gráficas.

	plug-in.	
Alertas y notificaciones	Nagios Core cuenta con dos tipos de alerta, warning y critical. Las notificaciones se pueden enviar por correo electrónico y SMS.	Zabbix cuenta con múltiples niveles de alerta. Las notificaciones se pueden enviar por correo electrónico, Jabber y SMS.
Plantillas	Nagios Core posee plantillas que permiten la herencia de parámetros entre host.	Zabbix posee plantillas que permiten la herencia de parámetros, disparadores, gráficas y reglas de descubrimiento. Además estas plantillas son compatibles con muchos fabricantes.
Reportes	Nagios Core permite visualizar reportes básicos.	Zabbix tiene una variedad de reportes.
Comunidad	Nagios Core cuenta con la mayor comunidad en el área de monitoreo de red.	La comunidad de Zabbix no es tan amplia como la de Nagios Core pero los miembros de Zabbix son más activos.
Precio	Nagios Core está disponible de forma gratuita, sin embargo, para acceder a más características se debe adquirir Nagios XI.	Zabbix está disponible de forma gratuita.

Como se puede observar en las tablas 11 y 12 la herramienta de monitoreo Zabbix obtuvo un mayor puntaje durante la evaluación. Asimismo, en la tabla 13 se aprecia que Zabbix cuenta con una mayor cantidad de puntos a favor, haciéndola la herramienta más completa. Aunque Nagios Core cuenta con las funcionalidades básicas para un monitoreo de red efectivo, su versión gratuita no está al nivel de Zabbix.

Una de las características más destacadas de Zabbix es que proporciona una interfaz web desde la cual es posible configurar casi todo el sistema de monitoreo (excepto los archivos del

agente de monitoreo y del servidor). Por su parte, la configuración de Nagios Core se realiza editando archivos de texto y siguiendo una determinada sintaxis, lo cual además de engorroso, puede generar errores de configuración.

Otra característica para destacar de Zabbix es la posibilidad de crear gráficas, ya que en muchos casos se hace más comprensible la información a través de gráficas que por medio de datos numéricos. Nagios no es especialmente conocido por la creación de gráficos, ya que por defecto no tiene gráficas, para tener esta funcionalidad se requiere instalar un plug-in.

3.3.1.3. Selección. En concordancia con los requisitos definidos para la implantación del sistema de monitoreo y de acuerdo a los resultados de la evaluación realizada, se tomó la decisión en conjunto con el personal administrativo de CSI de elegir a Zabbix como la herramienta más adecuada para la infraestructura de la red de datos de la UFPS, sede Cúcuta y Campos Elíseos.

3.3.2. Diseño

Una vez determinada la herramienta a implantar se diseñó la arquitectura y el escenario de implantación.

3.3.2.1. Arquitectura. Como se observa en la figura 18, Zabbix cuenta con cuatro componentes principales Zabbix Server, Zabbix Frontend, la base de datos, y los agentes de monitoreo. Zabbix Server es el componente central al que los agentes y procesos informan todos los datos recopilados. Toda la información de configuración y datos recopilados se almacenan en la base de datos, con la que tanto Zabbix Server como Zabbix Frontend interactúan. Los agentes Zabbix son compatibles con plataformas como Linux, UNIX y Windows; para los equipos sin un agente disponible, se utiliza el protocolo SNMP.

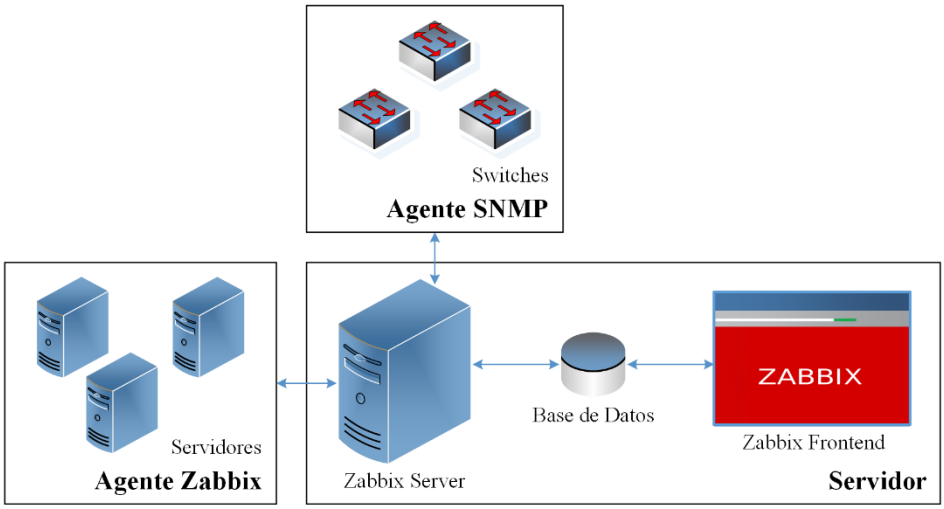


Figura 18. Arquitectura del sistema de monitoreo

3.3.2.2. Escenario de implantación. Las características externas del servidor se basaron en el entorno disponible para el despliegue del sistema de monitoreo (ver Tabla 7). Sin embargo, el espacio en disco duro se calculó para verificar que se contara con la cantidad adecuada, ya que este varía en forma directamente proporcional al tamaño de la Base de datos. El tamaño de la base de datos depende de variables como la cantidad de equipos, los parámetros, el historial de valores, los datos de tendencia y los eventos.

Para calcular el espacio total requerido, se utilizó la siguiente formula:

$$configuración + historial + tendencia + eventos = espacio\ total$$

Los datos de configuración de zabbix requieren un tamaño fijo, normalmente **10 MB**.

Se presupuso que la cantidad de equipos a monitorear son:

- 115 switch.
- 40 servidores.

Cada switch crea aproximadamente 200 parámetros, en total son $115 * 200 = 23000$ valores monitoreados. Por su parte, un servidor crea aproximadamente 40 parámetros, en total son $40 * 40 = 1600$ valores monitoreados.

Teniendo un total de 24600 valores monitoreados con una frecuencia de actualización de 60 segundos y una intención de conservar el historial de valores durante 30 días, la cantidad de valores será de $(24600/60) * 30 * 24 * 3600 = 1.062.720.000$. Dependiendo del sistema de gestión de base de datos utilizado y del tipo de valor (string, entero, flotante, log, etc.), el espacio requerido para cada valor es de aproximadamente 90 bytes. Esto significa que se requiere de $1.062.720.000 * 90 = \mathbf{95.65}\ \boldsymbol{GB}$ para almacenar el historial.

Teniendo un total de 24600 valores monitoreados con una frecuencia de actualización de 3600 segundos y una intención de conservar los datos de tendencia durante 365 días, la cantidad de valores será de $(24600/3600) * 365 * 24 * 3600 = 215.496.000$. Dependiendo del sistema de gestión de base de datos utilizado y del tipo de valor, el espacio requerido para cada valor es de aproximadamente 128 bytes. Esto significa que se requiere de $215.496.000 * 128 = \mathbf{27.58}\ \boldsymbol{GB}$ para almacenar los datos de tendencia.

El espacio requerido para cada evento generado por Zabbix es de aproximadamente 430 bytes. En el peor de los casos, Zabbix generará un evento por segundo, por lo cual, si se tiene una intención de conservar los datos de eventos durante un año, el espacio requiere es de $1 * 365 * 24 * 3600 * 430 = \mathbf{13.56}\ \boldsymbol{GB}$ para almacenar los datos de eventos.

Sumando el resultado de cada valor se obtuvo un total de **136.80 GB** de espacio mínimo en disco duro para ejecutar el sistema de monitoreo.

Como se detalla en la tabla 11 además del sistema operativo, Zabbix requiere de software extra para ejecutarse.

Tabla 14

Requisitos de software

Software	Plataforma	Versión
Base de Datos	MySQL	5.0.3 – 8.0.x
	Oracle	10 o posterior
	PostgreSQL	8.3 o posterior
	IBM DB2	9.7 o posterior
Apache	-	1.3.12 o posterior
PHP	-	5.4.0 o posterior

Como sistema de gestión de base de datos se eligió MariaDB, el cual es un derivado de MySQL con licencia GPL.

3.3.2.3. Grupos. Un grupo permiten clasificar equipos que comparten las mismas características. Para el sistema de monitoreo se diseñaron dos grupos descritos a continuación:

- **Switch.** Incluye todos los dispositivos de red activos que hacen parte de la infraestructura de red de datos.
- **Servidor.** Incluye todos los servidores administrados por CSI

3.3.2.4. Plantillas. Una plantilla permite asignar un conjunto de parámetros a equipos que comparten las mismas características. Para el sistema de monitoreo se diseñaron tres plantillas descritas a continuación:

- **Template Network Device SNMPv2.** Permite el monitoreo de dispositivos de red activos con protocolo SNMPv2.

- **Template Network Device SNMPv3 AuthPriv.** Permite el monitoreo de dispositivos de red activos con protocolo SNMPv3. Esta versión refuerza la prestación de seguridad (privacidad y control de acceso) en el intercambio de la información.
- **Template VMware ESXi.** Permite el monitoreo de servidores virtualizados en la plataforma VMware ESXi.

3.4. Fase IV: Implementación

3.4.1. Servidor

El sistema de monitoreo de red se desplego sobre la plataforma Linux, distribución CentOS 7. La instalación y configuración del servidor se encuentra detallado en el Anexo 4. **Instalación y Configuración del Servidor**del documento.

3.4.2. Herramienta

Antes de comenzar la instalación de Zabbix, versión 4.0, instale los paquetes requeridos para su despliegue (ver Tabla 14

Requisitos de software).

3.4.2.1. Paquetes.

3.4.2.1.1. Apache. Ingrese el siguiente comando para instalar el servidor web Apache:

```
[root@localhost ~]# yum -y install httpd
```

Inicie, verifique y habilite Apache:

```
[root@localhost ~]# systemctl start httpd.service
[root@localhost ~]# systemctl status httpd.service
[root@localhost ~]# systemctl enable httpd.service
```

Si Firewalld se está ejecutando, permita el acceso de Apache:

```
[root@localhost ~]# firewall-cmd --add-service=http --permanent
```

```
[root@localhost ~]# firewall-cmd --add-service=https --permanent
[root@localhost ~]# firewall-cmd --reload
```

3.4.2.1.2. PHP. Ingrese el siguiente comando para instalar PHP y los paquetes requeridos para Zabbix Frontend:

```
[root@localhost ~]# yum -y install php php-bcmath php-cli php-cgi php-common php-ctype php-devel php-gd php-gettext php-ldap php-mbstring php-mysql php-net-socket php-pear php-session php-snmp php-xml php-xmlwriter
```

Reinicie Apache:

```
[root@localhost ~]# systemctl restart httpd.service
```

3.4.2.1.3. MariaDB. Para instalar MariaDB 10.4, añada el repositorio a CentOS. Ingrese el siguiente comando para crear el archivo:

```
[root@localhost ~]# nano /etc/yum.repos.d/MariaDB.repo
```

Añada las siguientes líneas:

```
[mariadb]
name = MariaDB
baseurl = http://yum.mariadb.org/10.4/centos7-amd64
gpgkey=https://yum.mariadb.org/RPM-GPG-KEY-MariaDB
gpgcheck=1
```

Limpie la caché de índice:

```
[root@localhost ~]# yum makecache fast
```

Ingrese el siguiente comando para instalar MariaDB:

```
[root@localhost ~]# yum -y install MariaDB-server
```

Inicie, verifique y habilite MariaDB:

```
[root@localhost ~]# systemctl start mariadb.service
[root@localhost ~]# systemctl status mariadb.service
[root@localhost ~]# systemctl enable mariadb.service
```

Si Firewalld se está ejecutando, permita el acceso de MariaDB:

```
[root@localhost ~]# firewall-cmd --add-service=mysql --permanent
[root@localhost ~]# firewall-cmd --reload
```

Ingrese el siguiente comando para realizar las configuraciones iniciales de MariaDB:

```
[root@localhost ~]# mysql_secure_installation
```

Presione la tecla Enter para continuar.

Ingrese Y para actualizar la contraseña de MariaDB:

Ingrese la nueva contraseña, después, ingrese nuevamente la contraseña para confirmar:

Ingrese Y para remover los usuarios anónimos.

Ingrese Y para deshabilitar el acceso remoto del usuario root.

Ingrese Y para remover la base de datos de prueba.

Ingrese Y para recargar las tablas de privilegios.

3.4.2.2. Zabbix. Para uso en producción, se recomienda instalar desde paquetes de distribución.

Ingrese los siguientes comandos para añadir el repositorio a CentOS:

```
[root@localhost ~]# rpm -Uvh
https://repo.zabbix.com/zabbix/4.0/rhel/7/x86_64/zabbix-release-4.0-
2.el7.noarch.rpm
[root@localhost ~]# yum clean all
```

Ingrese el siguiente comando para instalar agente, get, zabbix server y frontend con soporte MySQL:

```
[root@localhost ~]# yum -y install zabbix-agent zabbix-get zabbix-
server-mysql zabbix-web-mysql
```

3.4.2.2.1. Creación de base de datos. Ingrese el siguiente comando para abrir la consola de MariaDB:

```
[root@localhost ~]# mysql -u root -p
```

Ingrese la contraseña de MariaDB.

Ingrese el siguiente comando para deshabilitar innodb_strict_mode:

```
MariaDB [(none)]> set global innodb_strict_mode='OFF';
```

Ingrese los siguientes comandos para crear la base de datos de Zabbix:

```
MariaDB [(none)]> create database zabbix character set utf8 collate utf8_bin;
MariaDB [(none)]> grant all privileges on zabbix.* to zabbix@localhost identified by 'contraseña MariaDB';
MariaDB [(none)]> flush privileges;
MariaDB [(none)]> quit;
```

Importe el esquema inicial:

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

3.4.2.2.2. Configuración de Zabbix Server. Ingrese el siguiente comando para abrir el archivo de configuración:

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

Línea 92: añada host de la base de datos.

```
DBHost=localhost
```

Línea 128: añada contraseña de la base de datos.

```
DBPassword=password
```

Inicie, verifique y habilite zabbix-server y zabbix-agent:

```
[root@localhost ~]# systemctl start zabbix-server zabbix-agent
[root@localhost ~]# systemctl status zabbix-server zabbix-agent
```

```
[root@localhost ~]# systemctl enable zabbix-server zabbix-agent
```

Si Firewalld se está ejecutando, permita el acceso de puertos a Zabbix:

```
[root@localhost ~]# firewall-cmd --add-port={10051/tcp,10050/tcp} --
permanent
[root@localhost ~]# firewall-cmd --reload
```

Ingrese el siguiente comando para abrir el archivo de configuración de Apache:

```
[root@localhost ~]# nano /etc/httpd/conf.d/zabbix.conf
```

Línea 20: elimine comentario y cambie la zona horaria de preferencia.

```
php_value date.timezone America/Bogota
```

Para aplicar cambios, reinicie Apache:

```
[root@localhost ~]# systemctl restart httpd.service
```

3.4.2.2.3. Configuración de Zabbix Frontend. Acceda a la URL: http://IP_servidor/zabbix desde un navegador web.

En la primera pantalla se muestra la página de bienvenida. Haga clic en el botón [Next step] para continuar.

Figura 19. Pantalla de bienvenida de Zabbix Frontend

Verifique que se cumplan todos los requisitos de software. Haga clic en el botón [Next step] para continuar.

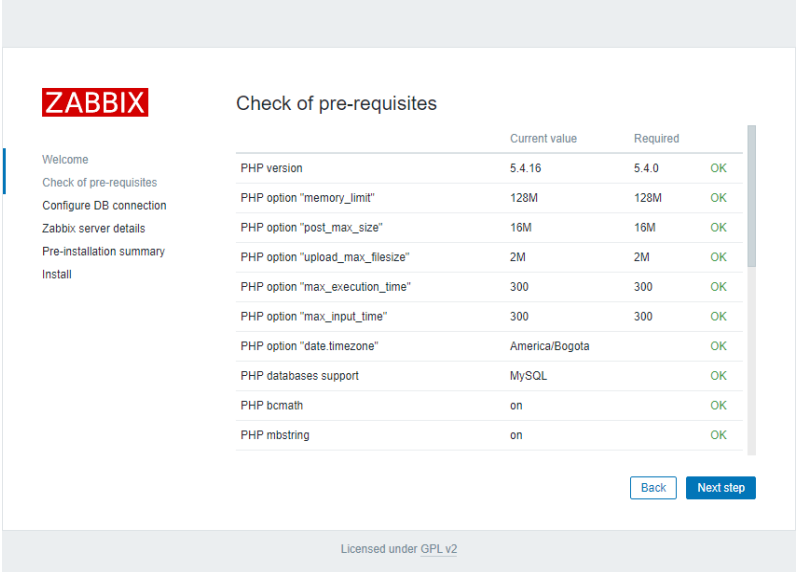


Figura 20. Pantalla de requisitos de Zabbix Frontend

Ingrese los datos correspondientes para la conexión con la base de datos. Haga clic en el botón Next step para continuar.

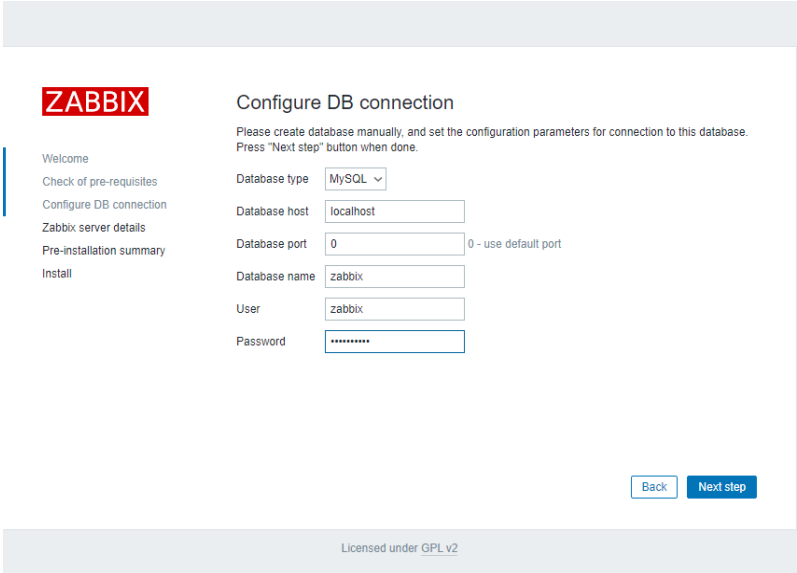


Figura 21. Pantalla de configuración de la base de datos

Ingrese los datos del servidor. Haga clic en el botón [Next step] para continuar.

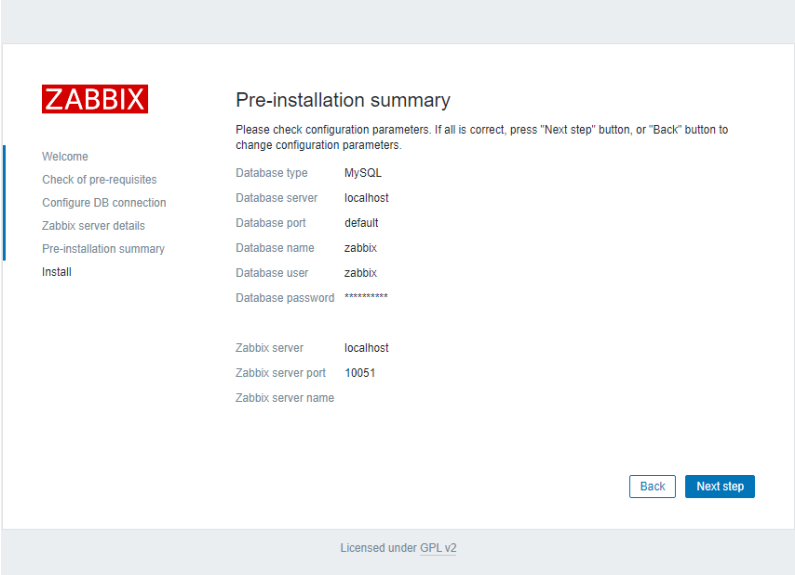


Figura 22. Pantalla de configuración del servidor

Verifique el resumen de la configuración. Haga clic en el botón [Next step] para continuar.

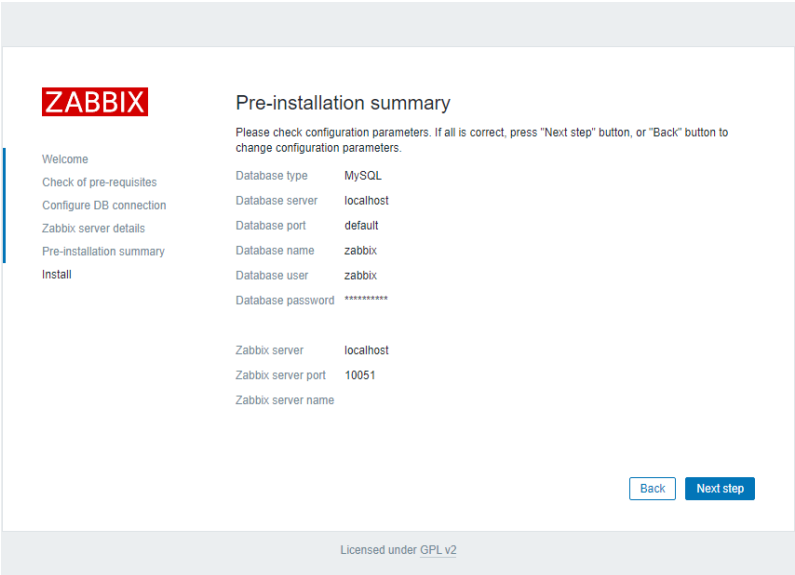


Figura 23. Pantalla de resumen de la instalación de Zabbix Frontend

Haga clic en el botón [Finish] para completar la instalación.

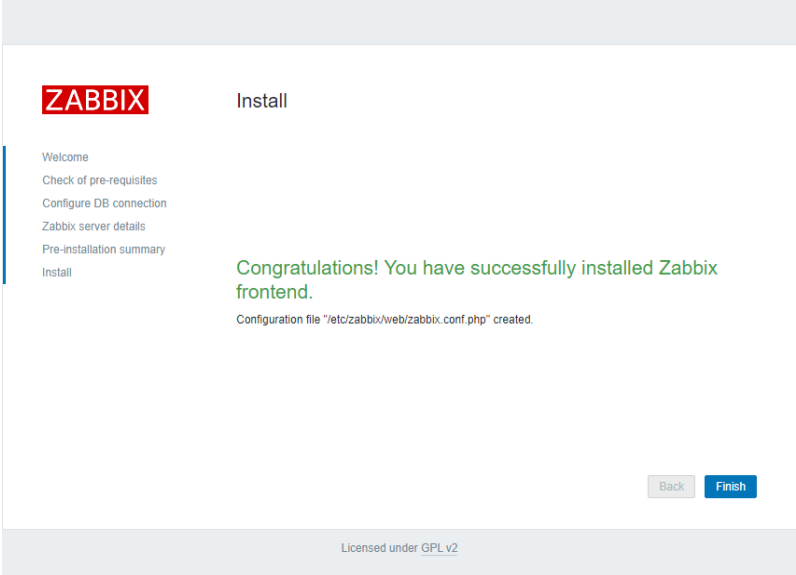


Figura 24. Pantalla de finalización de Instalación de Zabbix Frontend

Una vez finalice la instalación, se puede acceder a Zabbix Frontend. El nombre de usuario predeterminado es Admin y la contraseña es zabbix.

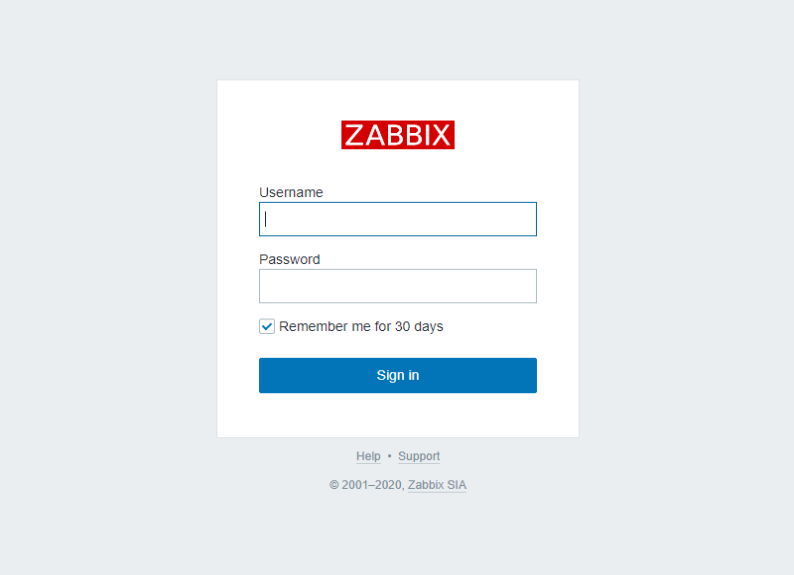


Figura 25. Pantalla de inicio de sesión de Zabbix

3.4.3. Monitoreo

Antes de iniciar con el proceso de monitoreo, se debe activar y configurar el agente en cada uno de los equipos a monitorear.

3.4.3.1. Agente Zabbix. Los agentes de monitoreo son compatibles con plataformas Linux, UNIX, Mac OS X y Windows. La instalación y configuración es muy similar en las diferentes plataformas.

Ingrese el siguiente comando para instalar el agente de monitoreo:

```
[root@localhost ~]# yum -y zabbix-agent
```

Inicie, verifique y habilite zabbix-agent:

```
[root@localhost ~]# systemctl start zabbix-agent
[root@localhost ~]# systemctl status zabbix-agent
[root@localhost ~]# systemctl enable zabbix-agent
```

Ingrese el siguiente comando para abrir el archivo de configuración:

```
[root@localhost ~]# nano /etc/zabbix/zabbix_agentd.conf
```

Línea 98: añada la dirección IP del servidor.

```
Server=Dirección IP
```

Línea 118: añada la dirección IP del equipo.

```
ListenIP=Dirección IP
```

Línea 141: añada la dirección IP del servidor activo.

```
ServerActive=Dirección IP
```

Línea 152: añada el nombre del equipo.

```
Hostname=Nombre del equipo
```

Para aplicar cambios, reinicie el equipo:

```
[root@localhost ~]# systemctl restart zabbix-agent
```

3.4.3.2. Agente SNMP. En los dispositivos de red con IOS compatibles, se configuro el protocolo SNMPv3. La versión 3 refuerza la prestación de seguridad (privacidad y control de acceso) en el intercambio de la información.

Conéctese al dispositivo e ingrese la contraseña para continuar.

Ingrese el siguiente comando. Después, ingrese la contraseña del dispositivo para acceder al modo privilegiado:

```
Switch> enable
```

Verifique la información del protocolo SNMP en el dispositivo:

```
Switch# show running-config
```

Si no hay información SNMP presente, continúe. Si hay algún comando SNMP registrado, se puede modificar o deshabilitar colocando no antes del comando.

Ingrese el siguiente comando para acceder al modo configuración:

```
Switch# configure terminal
```

Se requiere configurar las siguientes variables:

- **Grupo.** Especifica el nivel de seguridad que se va a utilizar.
- **Usuario.** Pertenece al grupo anterior.
- Apuntar el servidor al dispositivo, para habilitar las notificaciones.

3.4.3.2.1. Creación de grupo. `Switch (configure) # snmp-server group [nombre_grupo] [versión {v1 | v2c | v3}] [nivel {auth | noauth | priv}]`

3.4.3.2.2. Creación de usuario. `Switch (configure) # snmp-server user [nombre_usuario] [nombre_grupo] [versión {v1 | v2c | v3}] [autenticación {auth md5 | auth sha} [contraseña]] [privacidad {priv des | priv aes 128} [contraseña]]`

3.4.3.2.3. Notificaciones al servidor. `Switch (configure) # snmp-server host [IP_servidor] traps version 3 [nivel {auth | noauth | priv}] [nombre_usuario]`

```
Switch (configure) # snmp-server enable traps
```

Ingrese exit para salir del modo de configuración.

Ingrese el siguiente comando para guardar la configuración:

```
Switch# write memory
```

Verifique la activación del protocolo SNMPv3:

```
Switch# show snmp
```

3.4.3.3. Creación de grupo. Antes de crear un equipo en el sistema de monitoreo, se requieren dos elementos, grupo y plantilla.

Vaya al menú Configuration → Host groups y haga clic en el botón [Create host group].

Es necesario ingresar el campo Group name.

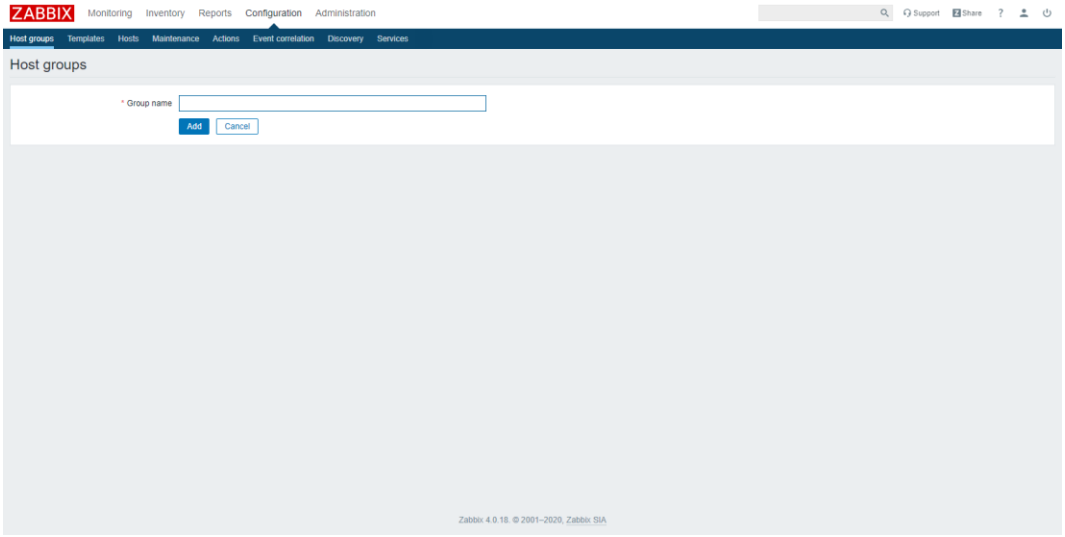


Figura 26. Pantalla de creación de grupo

Una vez ingresado el nombre del grupo, haga clic en el botón [Add].

3.4.3.4. Creación de plantilla. Vaya al menú Configuration → Templates y haga clic en el botón [Create template].

Es necesario ingresar los siguientes campos:

- **Template name.** Nombre de la plantilla.
- **Groups.** Grupo en el que se quiere clasificar la plantilla.

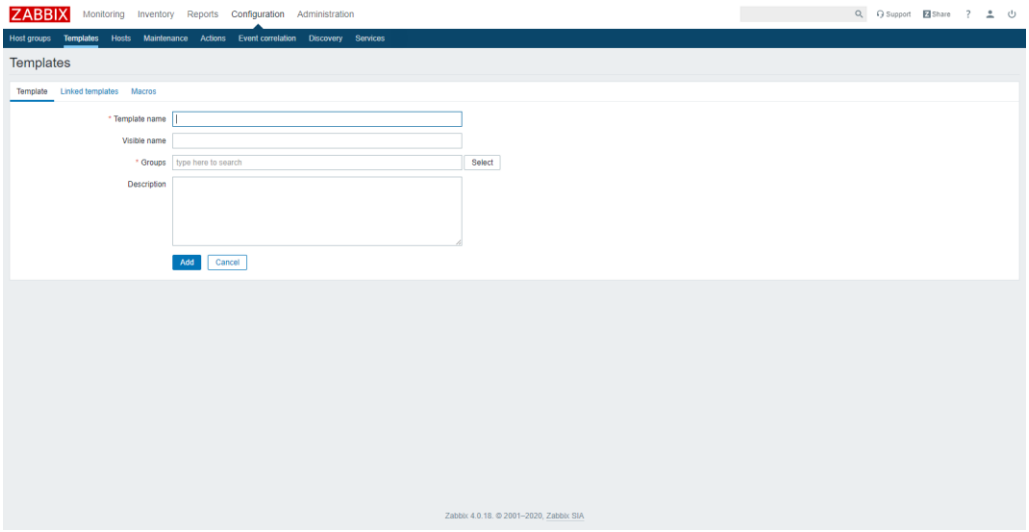


Figura 27. Pantalla de creación de plantilla

Una vez ingresados los datos, haga clic en el botón [Add].

3.4.3.4.1. Creación de parámetro Una vez creada la plantilla, se pueden configurar los datos a recopilar.

Vaya al menú Configuration → Templates y haga clic sobre la plantilla a editar. Después, vaya a la pestaña Items y haga clic en el botón [Create item].

Es necesario ingresar los siguientes campos:

- **Name.** Nombre del parámetro.
- **Type.** Tipo de monitoreo.
- **Key.** Nombre de la variable a solicitar.
- **Type of information.** Tipo de dato a solicitar.
- **Update.** Intervalo de actualización.

Dependiendo del tipo de monitoreo seleccionado, se piden más datos.

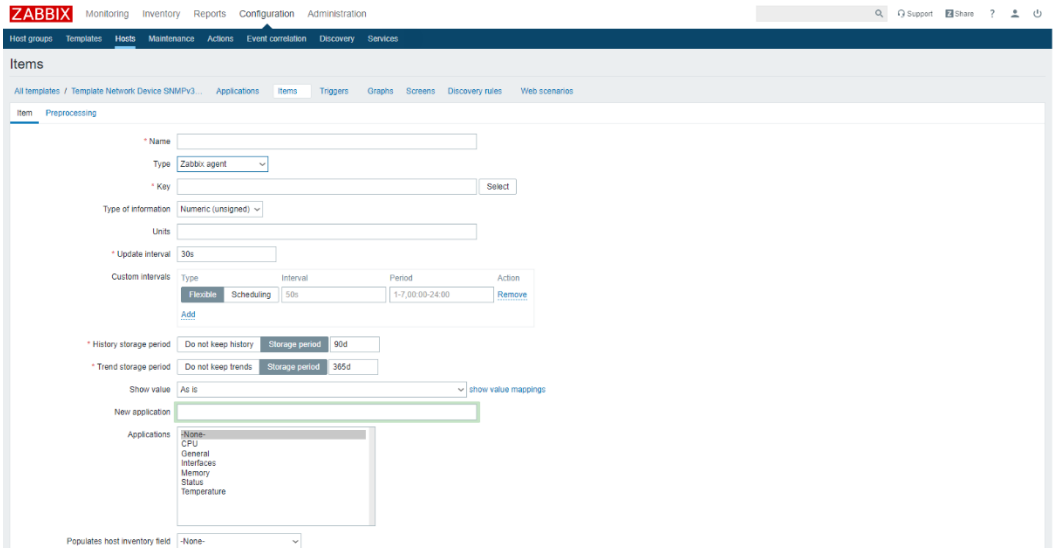


Figura 28. Pantalla de creación de parámetro

Una vez ingresados los datos, haga clic en el botón [Add].

3.4.3.4.2. Creación de alerta Vaya al menú Configuration → Templates y haga clic sobre la plantilla a editar. Después, vaya a la pestaña Triggers y haga clic en el botón [Create trigger].

Es necesario ingresar los siguientes campos:

- **Name.** Nombre de la alerta.
- **Severity.** Nivel de severidad de la alerta.
- **Expression.** Condición de la alerta.

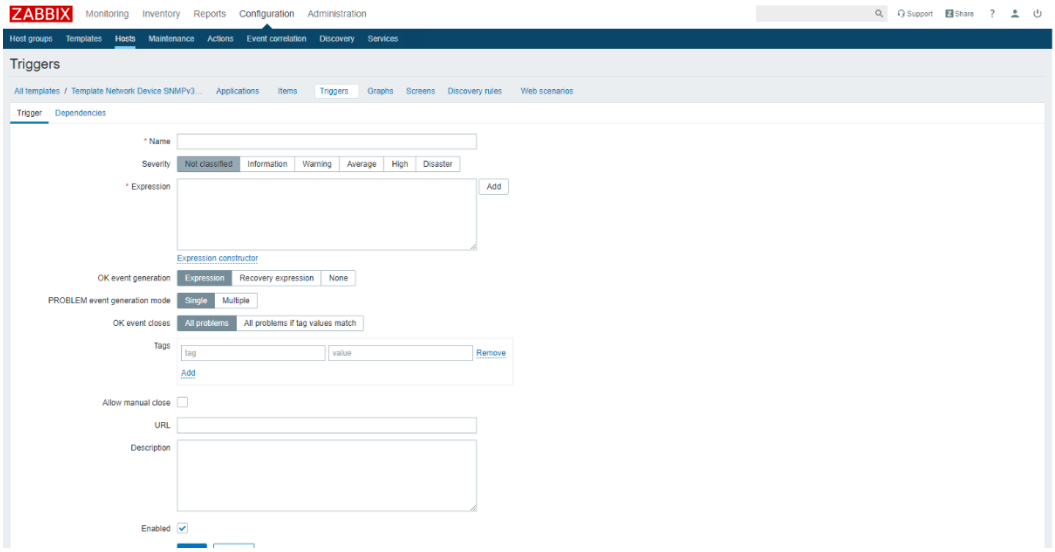


Figura 29. Pantalla de creación de alerta

Una vez ingresados los datos, haga clic en el botón [Add].

3.4.3.4.3. Creación de grafica Vaya al menú Configuration → Templates y haga clic sobre la plantilla a editar. Después, vaya a la pestaña Graphs y haga clic en el botón [Create graph].

Es necesario ingresar los siguientes campos:

- **Name.** Nombre de la gráfica.
- **Width.** Anchura de la gráfica.
- **Height.** Altura de la gráfica.

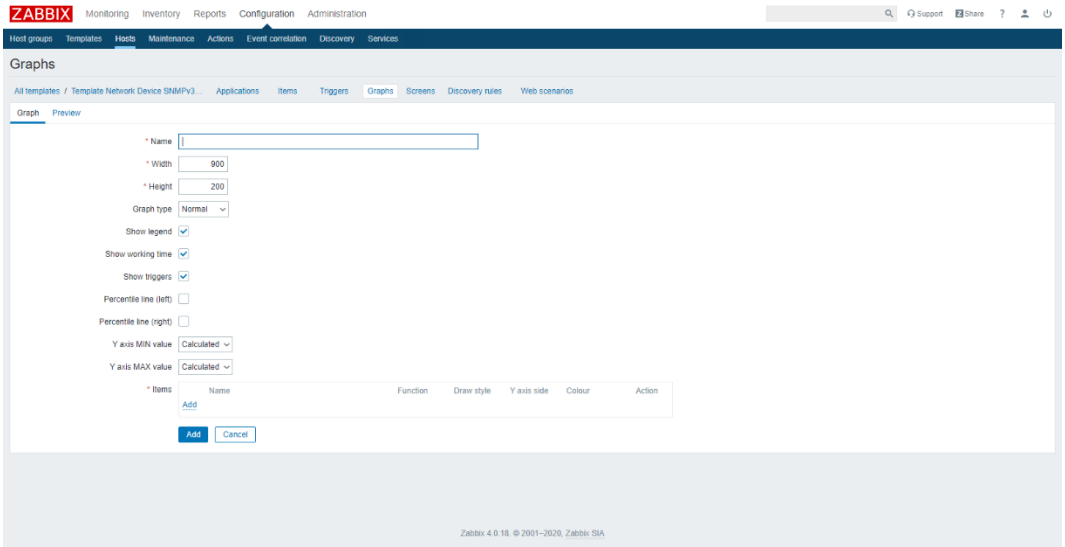


Figura 30. Pantalla de creación de grafica

Una vez ingresados los datos, haga clic en el botón [Add].

3.4.3.4.4. Creación de regla de descubrimiento. Vaya al menú Configuration → Templates y haga clic sobre la plantilla a editar. Después, vaya a la pestaña Discovery rules y haga clic en el botón [Create discovery rule].

Es necesario ingresar los siguientes campos:

- **Name.** Nombre de la regla de descubrimiento.
- **Type.** Tipo de monitoreo.
- **Key.** Nombre de la variable a solicitar.
- **Update.** Intervalo de actualización.

Dependiendo del tipo de monitoreo seleccionado, se piden más datos.

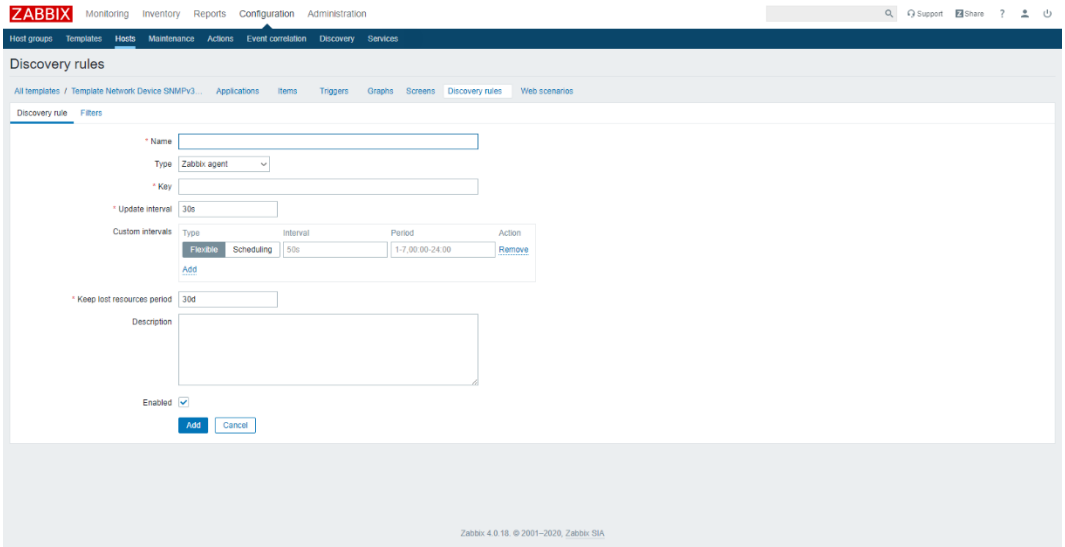


Figura 31. Pantalla de creación de regla de descubrimiento

Una vez ingresados los datos, haga clic en el botón [Add].

3.4.3.5. Creación de equipos en Zabbix. Vaya al menú Configuration → Hosts y haga clic en el botón [Create host].

Es necesario ingresar los siguientes campos:

- **Host name.** Nombre del equipo.
- **Groups.** Grupo en el que se quiere clasificar el equipo.
- **Agent interfaces.** Si se quiere monitorear el equipo mediante un agente Zabbix. Es necesario ingresar la dirección IP y el puerto de comunicación.
- **SNMP interfaces.** Si se quiere monitorear el equipo mediante el protocolo SNMP. Es necesario ingresar la dirección IP y el puerto de comunicación.

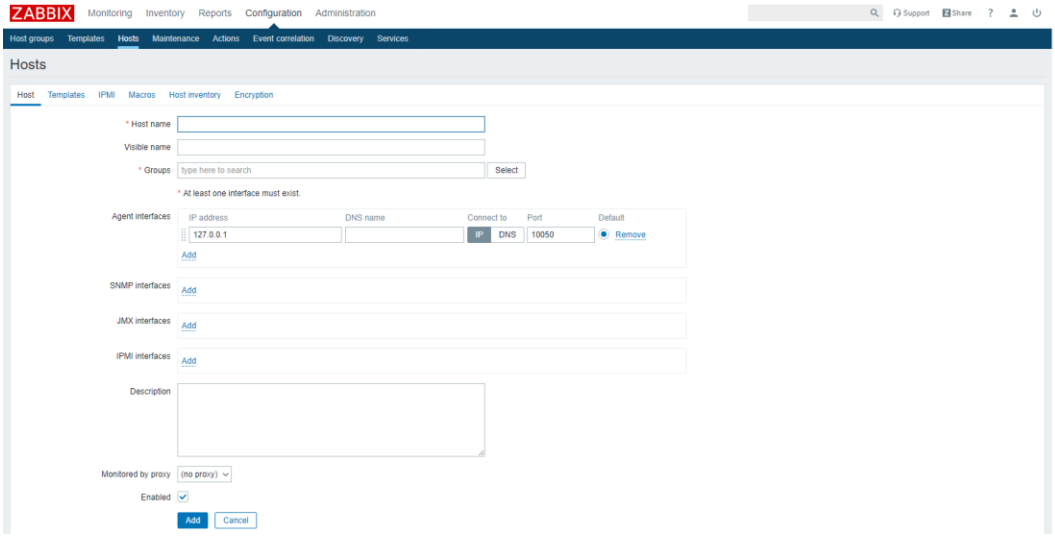


Figura 32. Pantalla de creación de equipos

Una vez ingresado los datos del host, haga clic en el botón [Add].

Para asociar la plantilla previamente creada, vaya a la pestaña Template.

Busque la plantilla y haga clic en el botón [Add], después haga clic en el botón [Update] para finalizar la creación del equipo.

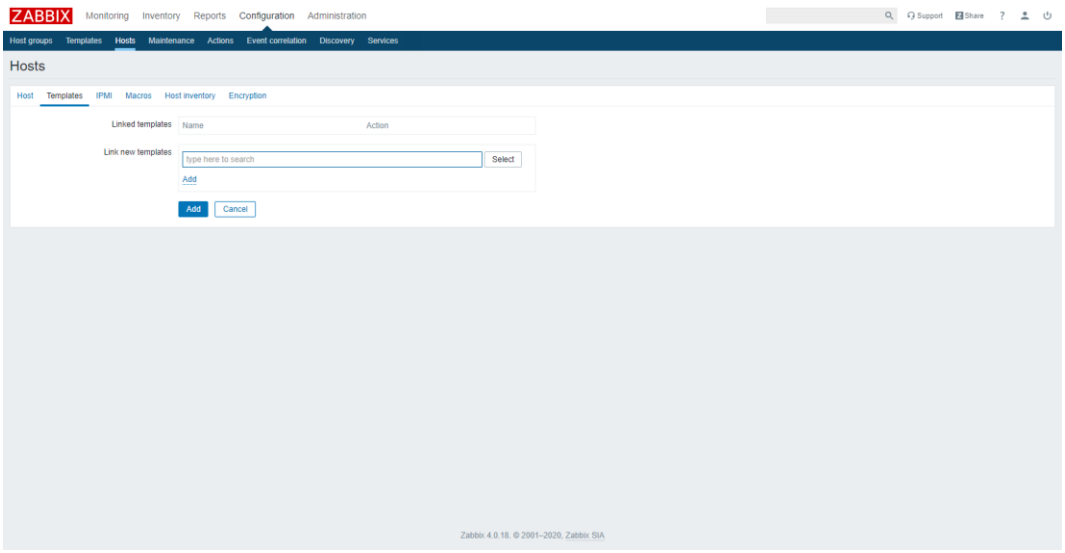


Figura 33. Pantalla de asociación de plantilla

Zabbix toma más o menos 1 hora para empezar a mostrar la información. Para ver la información recopilada, vaya al menú Monitoring → Latest data y seleccione el equipo a visualizar.

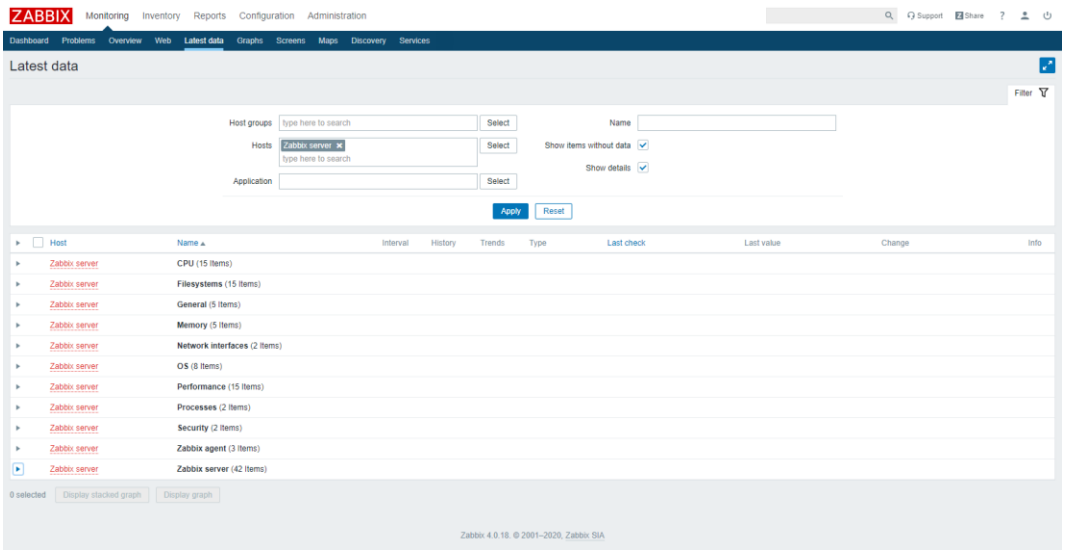


Figura 34. Pantalla de visualización de datos recopilados

3.4.4. Pruebas

Las pruebas comprendieron la verificación del funcionamiento correcto de la solución implantada y la validación del cumplimiento de los requisitos definidos por CSI. El plan de pruebas aplicado se puede observar en el Anexo 6.

Plan de Pruebasdel documento.

3.4.4.1. Pruebas Unitarias. Se realizaron con el fin de verificar que cada componente de la arquitectura del sistema de monitoreo funcionara correctamente de forma individual.

Para verificar que Zabbix Server aceptaba conexiones en el puerto 10051, se ejecutó el comando *netstat*.

```
[root@zabbixcsi ~]# netstat -tulpn |grep 10051
tcp        0      0 0.0.0.0:10051           0.0.0.0:*               LISTEN
14064/zabbix_server
tcp6       0      0 :::10051                ::::*                   LISTEN
14064/zabbix_server
[root@zabbixcsi ~]#
```

Figura 35. Prueba Zabbix Server

Como se observa en la figura 35, el servidor acepta conexiones en el puerto 10051. Para comprobar Zabbix Frontend, se verifico el funcionamiento correcto del servidor Apache.

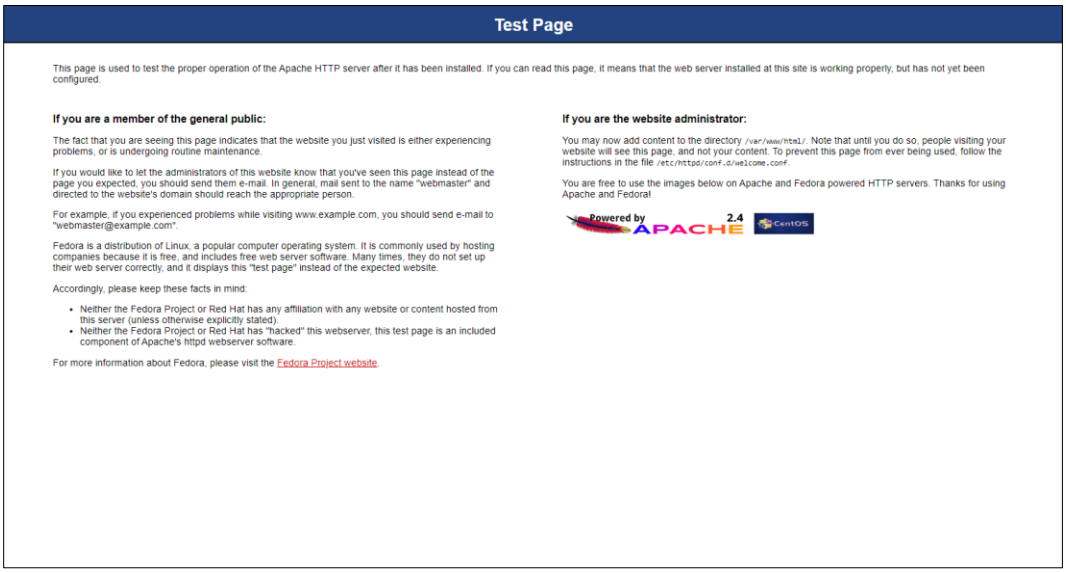


Figura 36. Prueba Zabbix Frontend

Como se observa en la figura 36, el servidor Apache funciona correctamente.

Una vez se verifico Zabbix Frontend, se accedió a la url del sistema de monitoreo para comprobar la conexión con la base de datos.

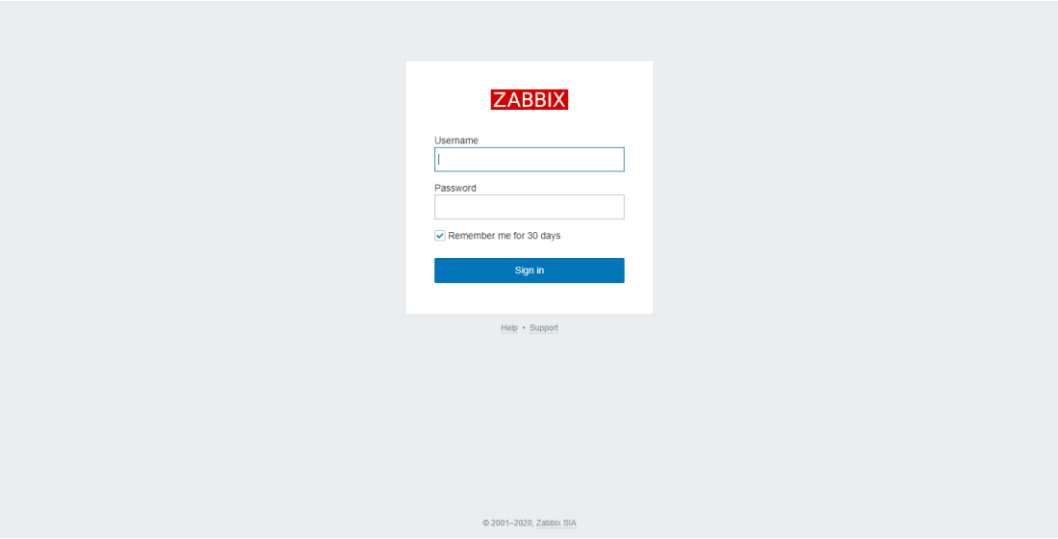


Figura 37. Pantalla de inicio de sesión

Como se observa en la figura 37, el sistema de monitoreo funciona correctamente.

En los equipos con agente zabbix, se comprobó la conexión en el puerto 10050.

```
[root@cinera ~]# netstat -tulpn |grep 10050
tcp        0      0 0.0.0.0:10050           0.0.0.0:*               LISTEN
1240/zabbix_agentd
tcp6       0      0 :::10050                :::*                    LISTEN
1240/zabbix_agentd
[root@cinera ~]#
```

Figura 38. Prueba agente zabbix

Como se observa en la figura 38, el servidor acepta conexiones en el puerto 10050.

Para verificar los agentes SNMP, se ejecutó el comando snmpwalk.

```
SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software, C3560E Software (C3560E-IPE
ASEK9-M), Version 15.0(2)SE11, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Sat 19-Aug-17 09:10 by prod_rel_team
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.1226
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (520139171) 60 days, 4:49:51.71
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: SAC1R1S2
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 6
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORID.1 = OID: SNMPv2-SMI::enterprises.9.7.129
SNMPv2-MIB::sysORID.2 = OID: SNMPv2-SMI::enterprises.9.7.115
SNMPv2-MIB::sysORID.3 = OID: SNMPv2-SMI::enterprises.9.7.265
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-SMI::enterprises.9.7.112
SNMPv2-MIB::sysORID.5 = OID: SNMPv2-SMI::enterprises.9.7.106
SNMPv2-MIB::sysORID.6 = OID: SNMPv2-SMI::enterprises.9.7.47
SNMPv2-MIB::sysORID.7 = OID: SNMPv2-SMI::enterprises.9.7.122
SNMPv2-MIB::sysORID.8 = OID: SNMPv2-SMI::enterprises.9.7.135
SNMPv2-MIB::sysORID.9 = OID: SNMPv2-SMI::enterprises.9.7.43
SNMPv2-MIB::sysORID.10 = OID: SNMPv2-SMI::enterprises.9.7.37
SNMPv2-MIB::sysORID.11 = OID: SNMPv2-SMI::enterprises.9.7.92
SNMPv2-MIB::sysORID.12 = OID: SNMPv2-SMI::enterprises.9.7.53
SNMPv2-MIB::sysORID.13 = OID: SNMPv2-SMI::enterprises.9.7.54
SNMPv2-MIB::sysORID.14 = OID: SNMPv2-SMI::enterprises.9.7.52
SNMPv2-MIB::sysORID.15 = OID: SNMPv2-SMI::enterprises.9.7.93
SNMPv2-MIB::sysORID.16 = OID: SNMPv2-SMI::enterprises.9.7.186
SNMPv2-MIB::sysORID.17 = OID: SNMPv2-SMI::enterprises.9.7.128
SNMPv2-MIB::sysORID.18 = OID: SNMPv2-SMI::enterprises.9.7.121
SNMPv2-MIB::sysORID.19 = OID: SNMPv2-SMI::enterprises.9.7.44
SNMPv2-MIB::sysORID.20 = OID: SNMPv2-SMI::enterprises.9.7.350
SNMPv2-MIB::sysORID.21 = OID: SNMPv2-SMI::enterprises.9.7.33
```

Figura 39. Prueba agente SNMP

Como se observa en la figura 39, este comando muestra la lista de IODs asociadas al equipo.

3.4.4.2. Pruebas de Integración. Las pruebas de integración tuvieron como objetivo verificar la comunicación entre el servidor Zabbix y los equipos que conforman la red de datos.

Para comprobar la comunicación, se agregaron los equipos en el sistema de monitoreo. Si el sistema de monitoreo se comunicaba correctamente con el agente, se activaba un icono de color verde correspondiente al tipo de agente como se observa en las figuras 40 y 41.

Figura 40. Prueba de comunicación entre Zabbix Server y el Agente Zabbix

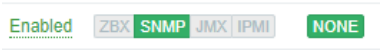


Figura 41. Prueba de comunicación entre Zabbix Server y Agente SNMP

3.4.4.3. Pruebas Funcionales. El propósito de estas pruebas fue validar que el sistema de monitoreo de red implantado satisfacía los requisitos definidos por CSI.

Para validar que el sistema de monitoreo permita monitorear equipos de red, se agregaron los equipo que conforma la red de datos. Las figuras 42 y 43 muestran un ejemplo de cada tipo de equipo que conforma la red de datos.

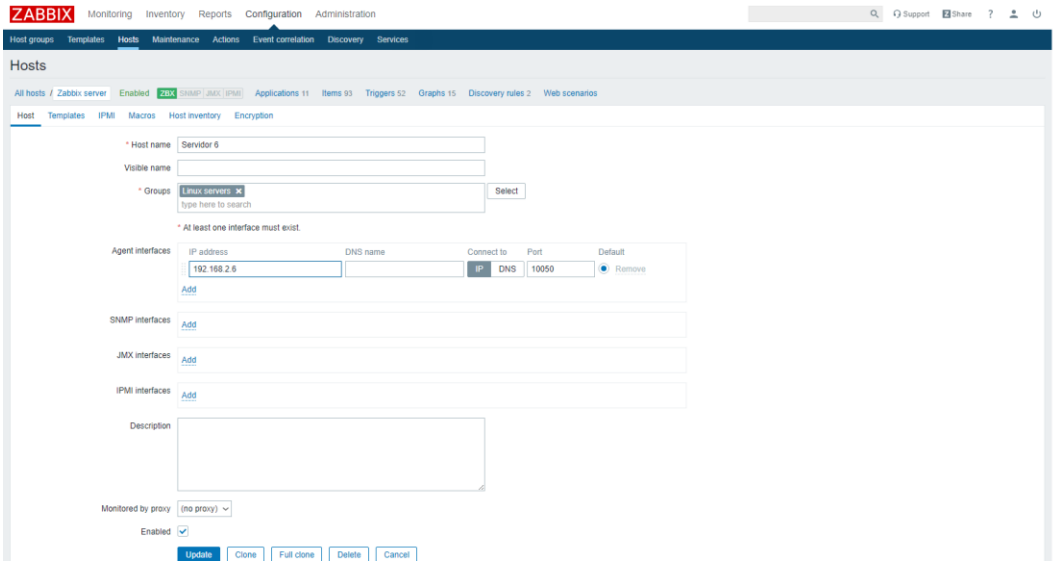


Figura 42. Prueba monitoreo de servidor

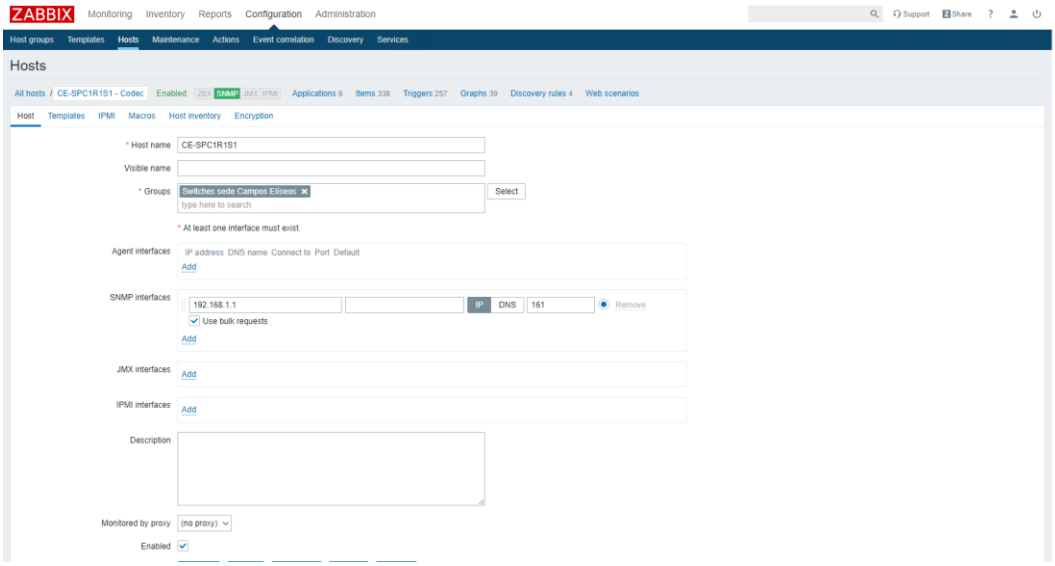


Figura 43. Prueba monitoreo de switch

Una vez agregado el equipo, se pueden observar los parámetros que fueron recopilados por el agente.

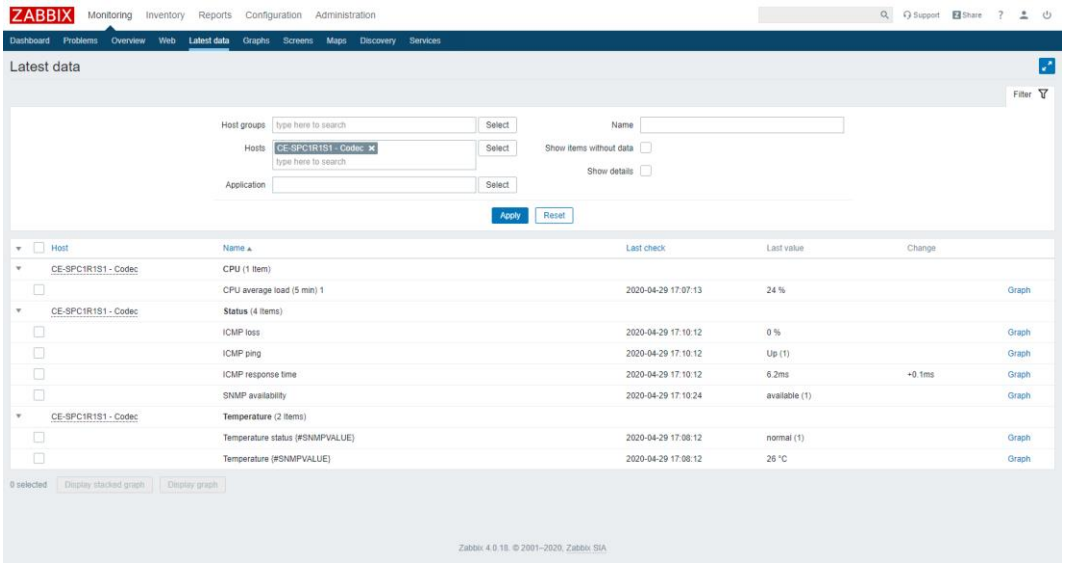


Figura 44. Prueba monitoreo de parámetros

Como se muestra en la figura 44, el sistema permite monitorear parámetros de red. La recopilación total de los datos puede tardar más o menos una hora.

Como se muestra en la figura 45, el sistema de monitoreo construye graficas del comportamiento de los parámetros.

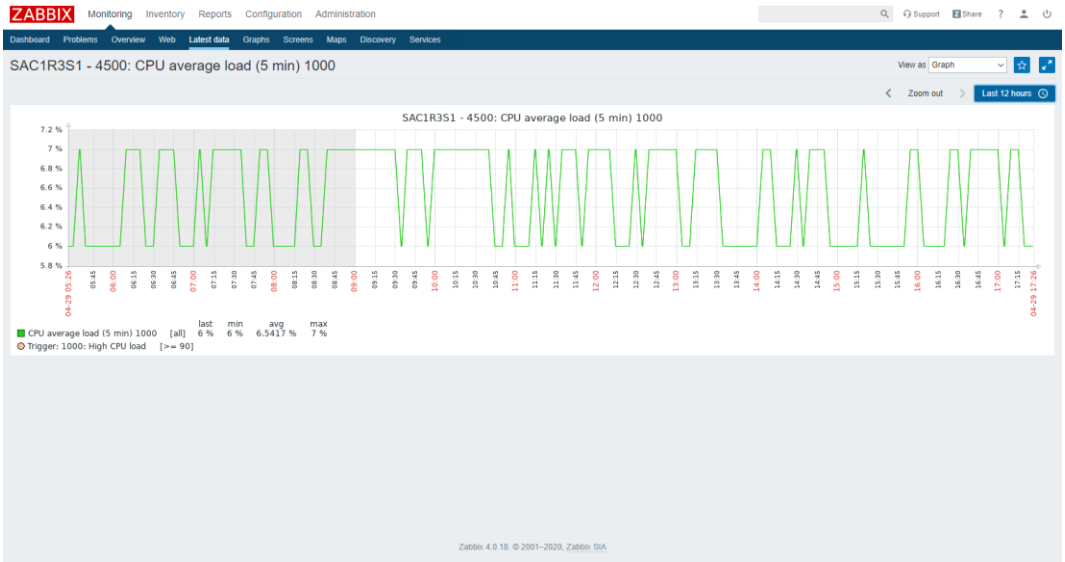


Figura 45. Prueba grafica

Para la notificación de un evento, las pruebas consistieron en provocar cambios en el equipo. Las figuras 46 y 47 muestran un ejemplo de notificación de correo.

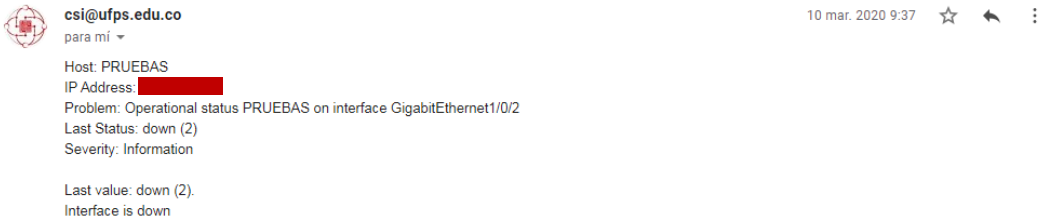


Figura 46. Prueba notificación

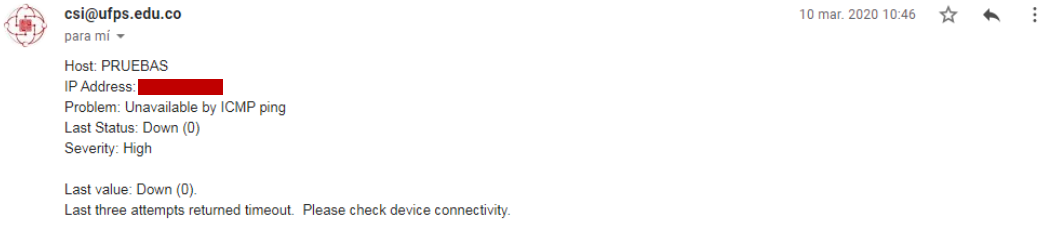


Figura 47. Prueba notificación2

Como se muestra en las figuras 48 y 49, el sistema de monitoreo cuenta con una variedad de reportes.

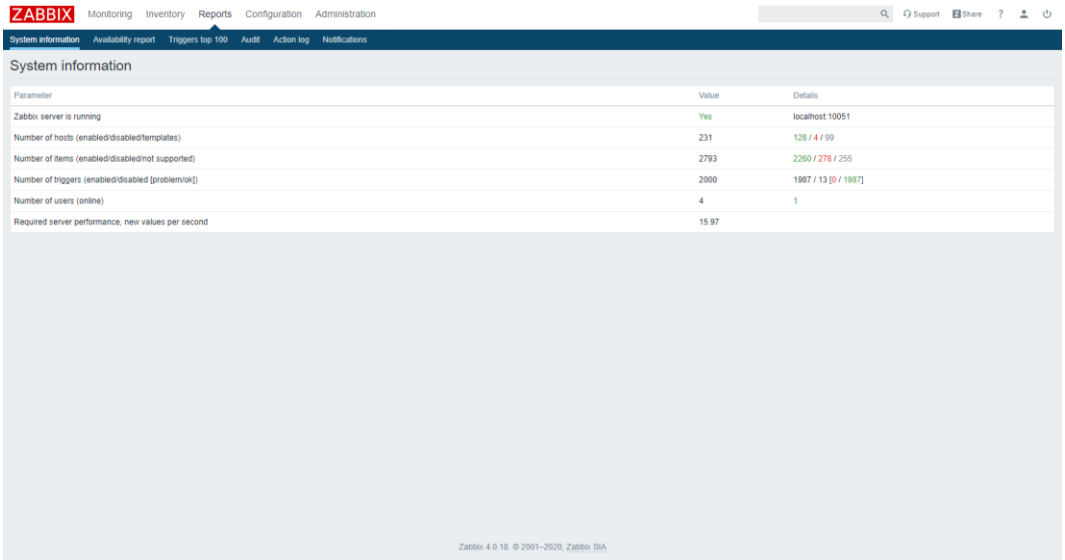


Figura 48. Prueba reporte

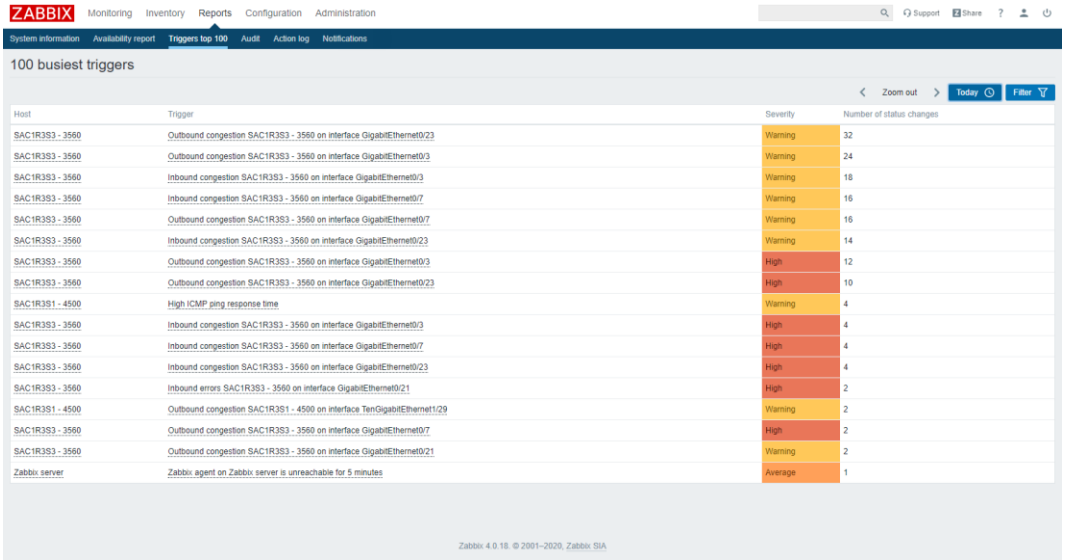


Figura 49. Prueba reporte2

3.4.5. Plan de Contingencia

Los planes de contingencia indican las acciones que se deben realizar para recuperar la disponibilidad de un sistema ante una falla.

Con el fin de garantizar la continuidad y pronta respuesta ante una falla en un elemento de la red, se establecen las estrategias de copias de seguridad, dependiendo de la función que realice cada uno de los elementos de la red.

3.4.5.1. Base de datos. La información de la configuración y los datos recopilados de Zabbix se almacenan en la base de datos, por lo cual, este es uno de los componentes del sistema de monitoreo que más cuidado requiere. Aunque existen diferentes métodos para la realización de copias de seguridad de bases de datos MariaDB, el más utilizado se basa en el uso de la herramienta mysqldump.

La estrategia para las copias de seguridad de la base de datos zabbix, consiste en ejecutar de forma automática el comando mysqldump. Para ello, se incluye en el archivo crontab del servidor “ZabbixCSI” una sentencia que invoca todos los días a las 1 de la mañana un script. El contenido del script se puede observar en el Anexo 5.

Script Base de Datosdel documento.

Ante una falla total o parcial de los datos almacenados, se procederá de la siguiente manera:

1. Descomprimir la última copia de seguridad realizada a la base de datos, almacenada en el servidor “ZabbixCSI”. En caso de una falla total o parcial del servidor, se contará con un respaldo en el servidor de almacenamiento remoto “Backup”.
2. . Restaurar la copia de seguridad en el gestor de base de datos.

3.4.5.2. Servidores. La estrategia para el respaldo de los servicios de red, consiste en copiar en el servidor de almacenamiento remoto “Backup” los archivos de configuración que se encuentran en los servidores que poseen los servicios.

Ante una falla total o parcial de un servidor, se procederá de la siguiente manera:

1. Desconectar totalmente el servidor de la red
2. Copiar el ultimo respaldo realizado
3. Restaurar el respaldo

4. Reiniciar los servicios afectados

3.4.5.3. Dispositivos de Red Activos. La información de la configuración y la imagen IOS de los dispositivos de red se almacena respectivamente en la memoria NVRAM (startup-config) y en la memoria flash. La estrategia para el respaldo de los dispositivos de red activos consiste en copiar el contenido de las memorias al servidor almacenamiento remoto “Backup”; este proceso se realiza manualmente con cada dispositivo.

Ante una falla total o parcial de los dispositivos de red activos, se procederá de la siguiente manera:

1. Desconectar totalmente el dispositivo de la red
2. Conectarse al dispositivo a través del puerto de consola
3. Copiar el último respaldo realizado

3.5. Fase V: Operación

Finalizada la implantación del sistema de monitoreo de red, se inició la fase de operación. Durante esta fase, Zabbix realizó un monitoreo constante de la infraestructura de red de datos y notifico los eventos presentados.

3.6. Fase VI: Optimización

A fin de mejorar el rendimiento de la base de datos, se ajustó la frecuencia de actualización en los parámetros que no sufrían cambios de forma frecuente. Asimismo, se cambió el tiempo de almacenamiento de los datos, ya que al pasar el tiempo las tablas crecen considerablemente.

3.7. Manuales

Los manuales de instalación, configuración y administración se realizaron con Docusaurus, una herramienta de Facebook que permite construir y mantener la documentación

de un proyecto. Esta herramienta utiliza el lenguaje Markdown para escribir la documentación y luego, generar las páginas en HTML. Los manuales del proyecto se basaron en la documentación oficial de los componentes del sistema de monitoreo y en la experiencia de la autora.

A continuación, se muestran algunas imágenes del sitio de documentación:

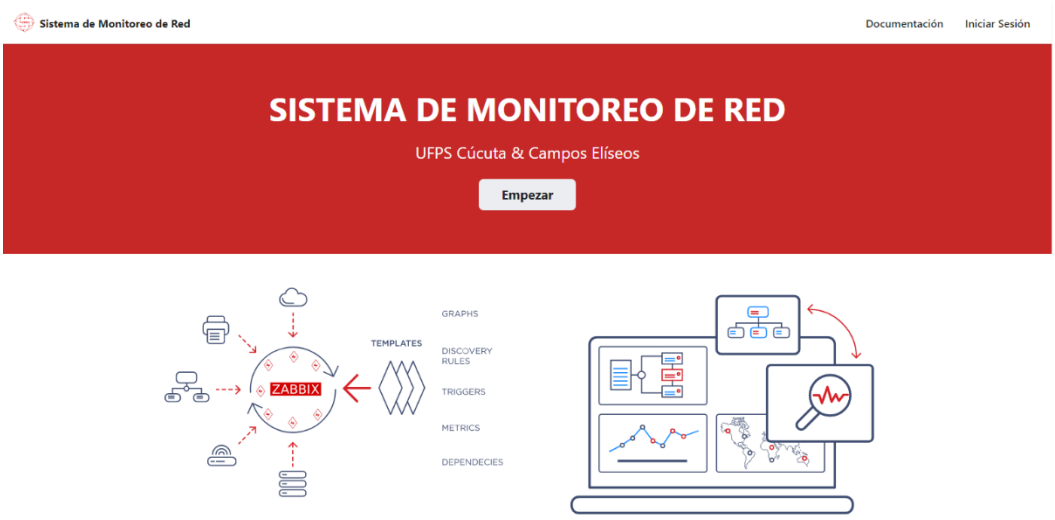


Figura 50. Pantalla de inicio del sistema de monitoreo

Figura 51. Pantalla de inicio de la documentación del sistema de monitoreo

Figura 52. Pantalla de introducción de la sección Servidor

Figura 53. Pantalla de introducción de la sección Zabbix

3.8. Capacitación

Para dar finalidad al proyecto, se llevó a cabo una capitación con el personal administrativo de CSI sobre el manejo del sistema de monitoreo de red. Los tema tratados en la capacitación fueron:

- Socialización del sitio de documentación.
- Ingreso al sistema de monitoreo.

- Administración del sistema de monitoreo a nivel básico.

A continuación, se muestran algunas imágenes del desarrollo de la capacitación:

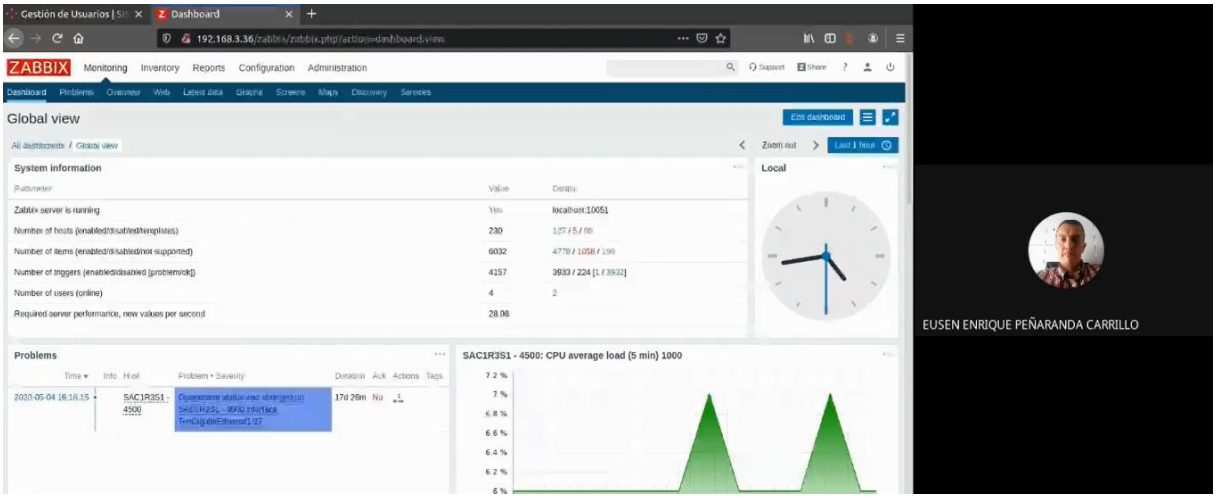


Figura 54. Desarrollo de la capacitación

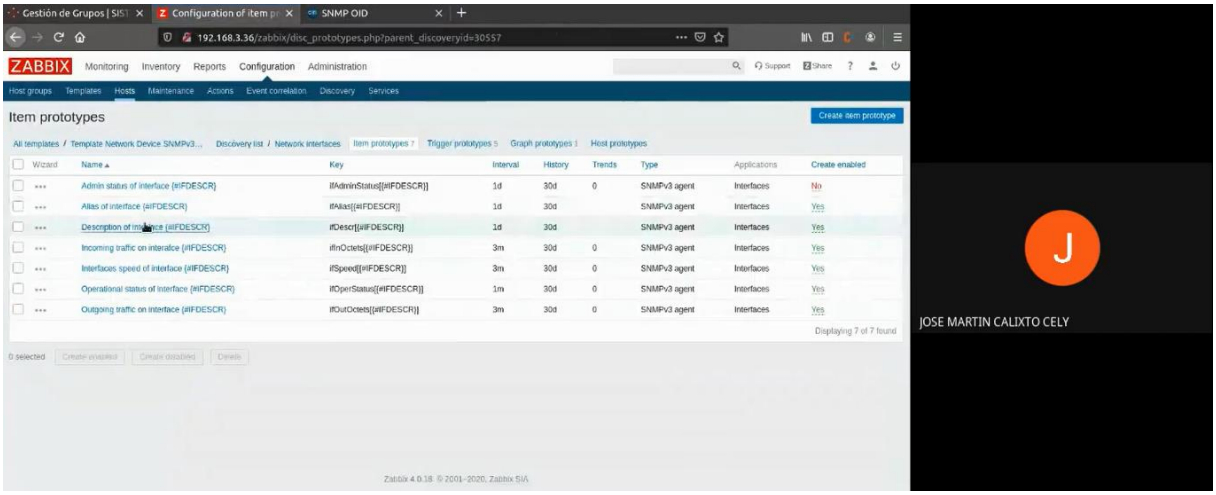


Figura 55. Desarrollo de la capacitación

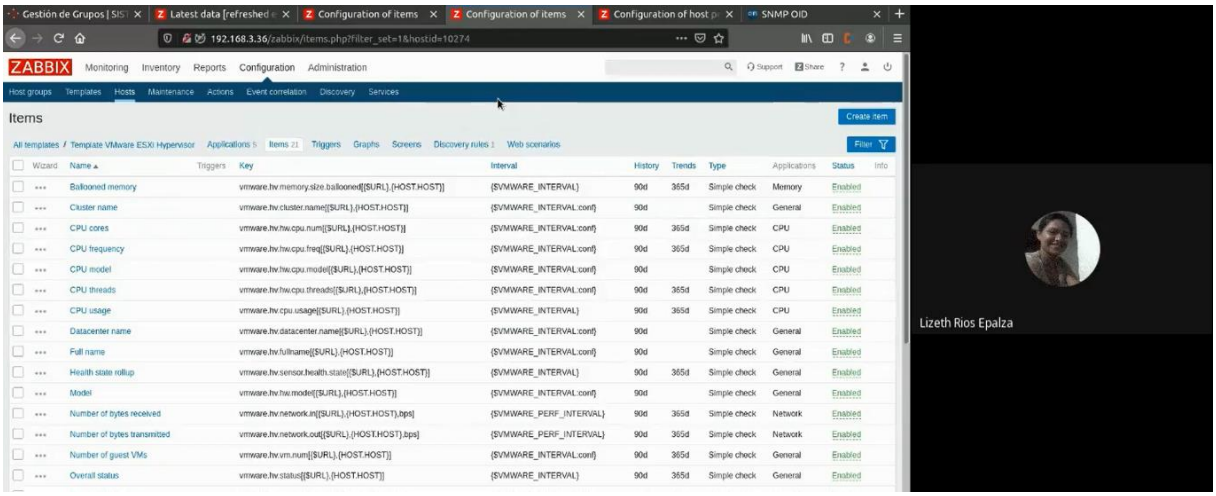


Figura 56. Desarrollo de la capacitación

En el Anexo 7.

Asistencia de la Capacitación del documento se puede observar la asistencia de la capacitación.

Conclusiones

De acuerdo a la comparación e instalación piloto de las herramientas de monitoreo open source más destacadas en la actualidad, se concluyó que la herramienta más adecuada para la infraestructura de red de datos es Zabbix, ya que cuenta con características y funcionalidades que hacen que sea una herramienta muy completa.

La implantación y puesta en marcha del sistema de monitoreo permite que los componentes y servicios que conforman la infraestructura de red de datos sean monitoreados permanentemente mediante el protocolo SNMP; garantizando la disponibilidad de la red de datos, ya que, al alertar y notificar de manera inmediata al administrador de la red, este actúa rápidamente ante los eventos que se presentan.

Se llevó a cabo con plena satisfacción la implantación del sistema de monitoreo en la infraestructura de red de datos UFPS sede Cúcuta y Campos Elíseos, donde se conoce el estado actual de cada equipo monitoreado.

Recomendaciones

Cuando pase la crisis mundial generada por la pandemia coronavirus y la red de datos se encuentre en su funcionamiento normal, se recomienda obtener a través del sistema de monitoreo la información respectiva para establecer la línea base del funcionamiento óptimo de la red de datos; esto con el fin de comparar el comportamiento de la red de datos en un determinado tiempo con el perfil óptimo de funcionamiento de red.

Ampliar el personal del CSI, que permita encargarse del monitoreo y la seguridad de la infraestructura de red de datos en la UFPS sede Cúcuta y Campos Elíseos.

Verificar e instalar nuevas actualizaciones de Zabbix y de los componentes del sistema de monitoreo, para resolver posibles inconvenientes que se presenten con las versiones actuales. Asimismo, se recomienda ser cuidadoso al momento de realizar este proceso, ya que existe una variedad de paquetes.

Revisar constantemente el estado de la memoria y del almacenamiento del servidor "ZabbixCSI", de esta manera se podrá seguir añadiendo más equipos al sistema de monitoreo.

A medida que se renueven los equipos o que la infraestructura de red de datos incremente se recomienda ir añadiéndolos al sistema de monitoreo; de esta forma se contara con la información completa de los elementos de la red.

Aunque se cuenta con la funcionalidad de autodescubrimiento, se recomienda adicionar solo los componentes críticos de la red de datos para no saturar el sistema de monitoreo.

Implantar un software que permita respaldar la información vital de los dispositivos y servicios de la red de forma automática; garantizando la continuidad y pronta respuesta ante una falla.

Referencias Bibliográficas

Almacenamiento remoto. (s. f.). EcuRed. https://www.ecured.cu/Almacenamiento_remoto

Andrearrs. (2014, mayo 7). Diferencias entre Software Libre y Open Source. *Hipertextual*. https://hipertextual.com/archivo/2014/05/diferencias-software-libre-y-open-source/

Ávila, G., & Rafael, V. (2014). *Diseño e implementacion de un sistema de monitoreo basado en SNMP para la Red Nacional Académica de Tecnología Avanzada* [Universidad Santo Tomas]. http://repository.usta.edu.co/handle/11634/766

Bustincio, Q., & Watson, J. (2018). *Implementación de un sistema de monitoreo y control de red, para un canal de televisión, basado en herramientas Open Source y Software Libre, Lima—2017* [Universidad Nacional del Altiplano]. http://repositorio.unap.edu.pe/handle/UNAP/9019

Cacti—The Complete RRDTool-based Graphing Solution. (s. f.). https://www.cacti.net/what_is_cacti.php

Campos Elíseos. (s. f.). [Map]. https://satellites.pro/mapa_de_Colombia#7.854715,-72.501258,17

Delgadillo Rivera, J. L., & García Ronquillo, L. D. (2010). *Monitorización de servicios de red y servidores* [Universidad Nacional Autónoma de México]. http://www.ptolomeo.unam.mx:8080/xmlui/handle/132.248.52.100/1027

Doctors, A., & Vecchiotti, R. (2012). *Sistema de gestión y monitorización de fallas para clientes de SANNET Soluciones C.A* [Universidad Católica Andrés Bello]. http://biblioteca2.ucab.edu.ve/anexos/biblioteca/marc/texto/AAS7463.pdf

Gallego Adames, M., & Lozano Garzón, C. A. (2015). *Rediseño e implementación del sistema de monitoreo de la red de telecomunicaciones de distribuidora Nissan S.A*. Universidad Católica de Colombia.

INCIBE. (2016, mayo 16). *Almacenamiento seguro de la información. Una guía de aproximación para el empresario*. Instituto Nacional de Ciberseguridad. https://www.incibe.es/protege-tu-empresa/guias/almacenamiento-seguro-informacion-guia-aproximacion-el-empresario

ISO 27001. (s. f.). ISOTools. https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Jairo. (2012, noviembre 12). *SNMP Protocol*. Docsity. https://www.docsity.com/pt/snmp-protocol/4814541/

Jardinez, R. T. (2009). *Propuesta de un Sistema de Monitoreo para la Red de ESIME Zacatenco utilizando el Protocolo SNMP y Software Libre* [Instituto Politécnico Nacional]. https://pdfs.semanticscholar.org/44cf/dc50054092b45c92fd1e78a88e92b2b3c75e.pdf

Junco Romero, G., & Rabelo Padua, S. (2018). Los recursos de red y su monitoreo. *Revista Cubana de Informática Médica*, *10*(1), 76-83.

MinTIC. (2016). *Modelo de seguridad y privacidad de la información*. 58.

MinTic Decretos. (s. f.). Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/portal/inicio/Normatividad/Decretos/

Monitorizar nuestra red. (2014, mayo 12). *tecnozero Soluciones Informaticas*. https://www.tecnozero.com/blog/por-que-es-importante-monitorizar-nuestra-red/

Morelo, L. (2010). Planificación y gestión de red. En *Los sistemas y la contabilidad* (p. 58). Universidad Dr. Rafael Belloso Chacín. https://www.calameo.com/read/0049907372ca704547380

Nagios Overview. (s. f.). Nagios. https://www.nagios.org/about/overview/

¿Qué es SNMP? (s. f.). ManageEngine. https://www.manageengine.com/es/network-monitoring/what-is-snmp.html

RFC Index. (s. f.). https://tools.ietf.org/rfc/index

Sosa Sosa, V. J. (s. f.). *Gestión de redes*. Maestria en Ciencias de la Computación, México, D.F. https://www.tamps.cinvestav.mx/~vjsosa/clases/redes/GestionRedes.pdf

Todo lo que debes saber sobre el Almacenamiento en la Nube. (2017). suempresa.com. https://www.suempresa.com/wp-content/uploads/2017/11/eBook_Julio_V2.pdf

UFPS. (s. f.). [Map]. https://satellites.pro/mapa_de_Colombia#7.898830,-72.488254,17

Unidad de Información Estadística. (2019). *Cifras UFPS* (p. 57). Universidad Francisco de Paula Santander. https://ww2.ufps.edu.co/public/archivos/pdf/e18461ba6ea2d49b7febada32487a46b.pdf

Velasco Briones, C. A., & Cagua Ordoñez, G. S. (2017). *Implementación de un sistema de monitoreo de redes utilizando herramientas open source y proveer servicios de directorio a través de active directory en la facultad de Filosofía y Ciencias de la educación de la universidad de Guayaquil.* [Universidad Politécnica Salesiana Sede Guayaquil]. http://dspace.ups.edu.ec/handle/123456789/13474

Villagómez, B., & Israel, J. (2015). *Servidor de control de dispositivos y servicios mediante el protocolo SNMP para la red de datos en la CELEC .E.P. Unidad de negocio Hidroagoyán* [Universidad Técnica de Ambato]. https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/13063

Working Mechanisms of SNMPv1/SNMPv2c. (s. f.). Huawei. https://support.huawei.com/enterprise/en/doc/EDOC1100034234/73e6152/snmpv1-snmpv2c

Zabbix Overview. (s. f.). Zabbix. https://www.zabbix.com/documentation/4.0/manual/introduction/about

Anexos

En esta sección se presentan los anexos que aportan información adicional al contenido del proyecto de grado.

El **Anexo 1 (Red Física de la UFPS)** observado en el anteproyecto, no se adjuntó en este documento para preservar la confidencialidad de la información proporcionada por la dependencia CSI.

Anexo 2.

Entrevista PR-01

Tabla 15

Entrevista PR-01

Objetivo:	Obtener información necesaria para identificar al personal encargado de administrar la red, la topología e infraestructura física y lógica, además de los problemas, necesidades y alcances del proyecto.
Entrevistado:	Coordinador de CSI, Administrador de la red
Preguntas	
1. ¿Quiénes conforman CSI? 2. ¿Cuáles son las funciones de CSI? 3. ¿Cuántas sedes tiene la UFPS, y en cuáles de estas CSI administra la red de datos? 4. ¿Cómo está estructurada la red de datos? 5. ¿Quiénes acceden a la red de datos? 6. ¿Cómo se lleva a cabo el proceso de monitoreo, y con qué herramientas se cuenta para ello? 7. ¿Qué necesidades se quieren cubrir con el proyecto?	

Anexo 3.

Entrevista PL-01

Tabla 16

Entrevista PL-01

Objetivo:	Obtener información necesaria para definir los requerimientos de la red de datos.
Entrevistado:	Coordinador de CSI, Administrador de la red
Preguntas	

1. ¿Cree que en la organización se debe implantar un sistema de monitoreo?
2. ¿Existe algún sistema de monitoreo en la red de datos?
3. ¿CSI cuenta con presupuesto para un sistema de monitoreo?
4. ¿Conoce o ha escuchado mencionar alguna de estas herramientas de monitoreo de red?
5. ¿Qué dispositivos, enlaces, recursos y servicios se requieren monitorear?
6. ¿Cuáles son las características de hardware a monitorear de los dispositivos?
7. A nivel de aplicación ¿Cuáles son los requerimientos que la herramienta de monitoreo debe poseer?

Anexo 4.

Instalación y Configuración del Servidor

Antes de comenzar la instalación, descargue el archivo ISO CentOS 7 desde la página oficial y asegúrese de que el servidor cumpla con los requisitos de hardware recomendados: (ver **¡Error! No se encuentra el origen de la referencia.**).

Instalación

Inicie el servidor y seleccione Install CentOS 7.

Figura 57. Tipo de instalación

Si el arranque es correcto, se inicia el asistente de instalación.

Seleccione el idioma que se desea utilizar durante la instalación y haga clic en el botón [Continuar].

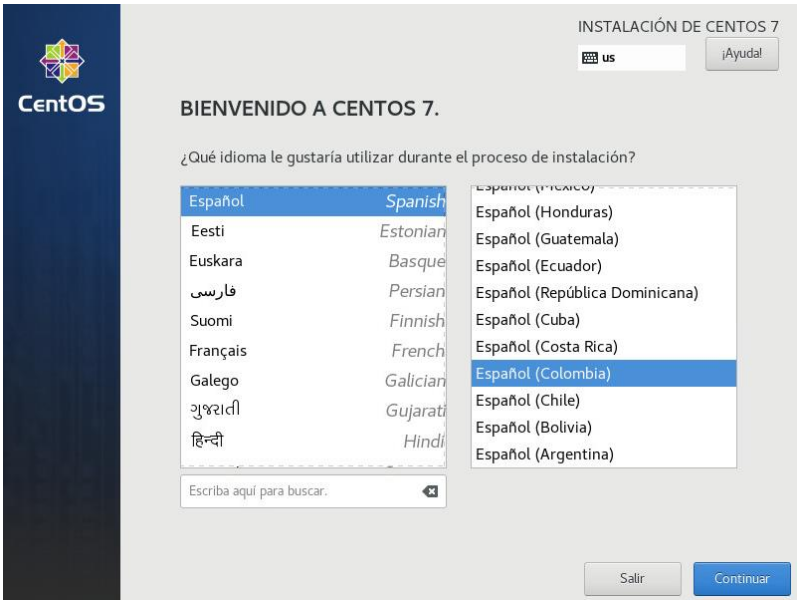


Figura 58. Selección de idioma

La siguiente pantalla muestra un grupo de categorías a configurar antes de empezar la instalación.

Figura 59. Resumen de instalación

Fecha y Hora

Seleccione la región y ciudad que desea establecer y haga clic en el botón [Listo].

Figura 60. Selección de Fecha y hora

Teclado

Seleccione el teclado y haga clic en el botón [Listo].

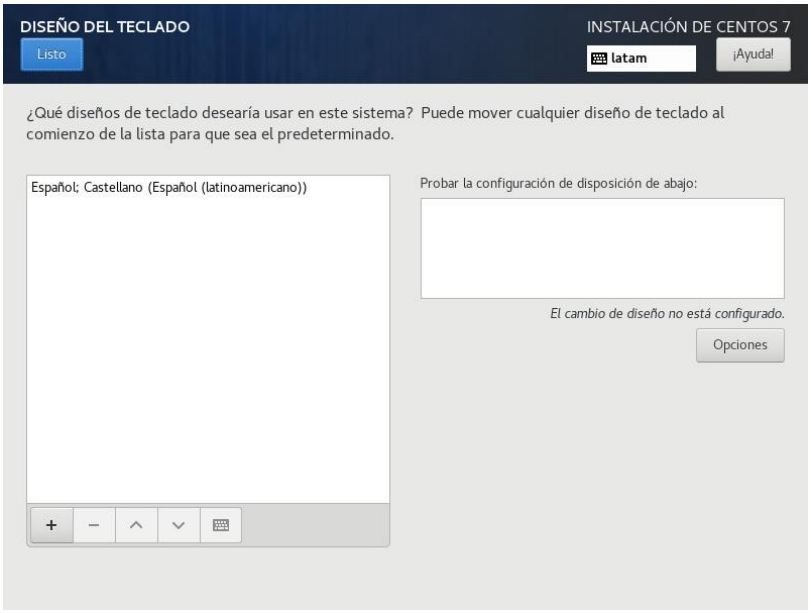


Figura 61. Selección de teclado

Soporte de Idioma

Seleccione el soporte de idioma y haga clic en el botón [Listo].

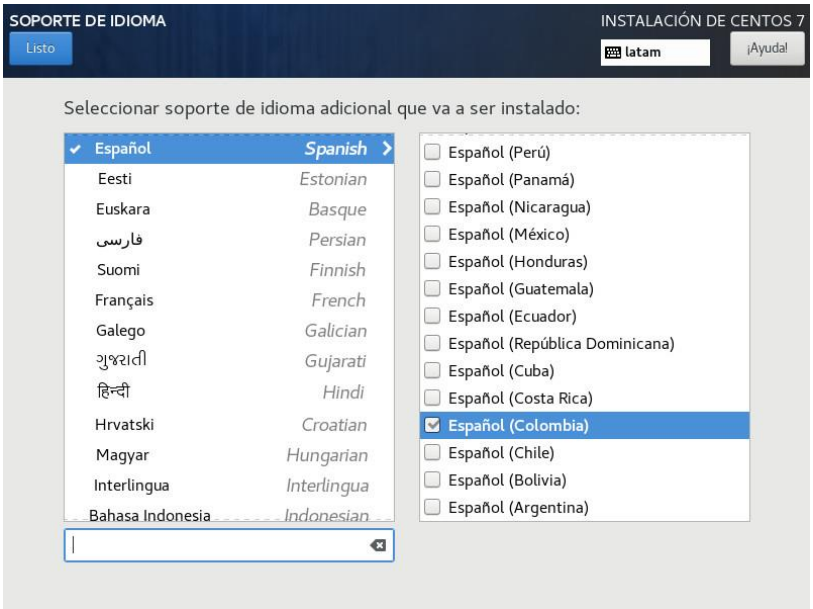


Figura 62. Selección de idioma

Origen de Instalación

Por defecto, el origen de la instalación es el medio de arranque. Seleccione la fuente de instalación y haga clic en el botón [Listo].

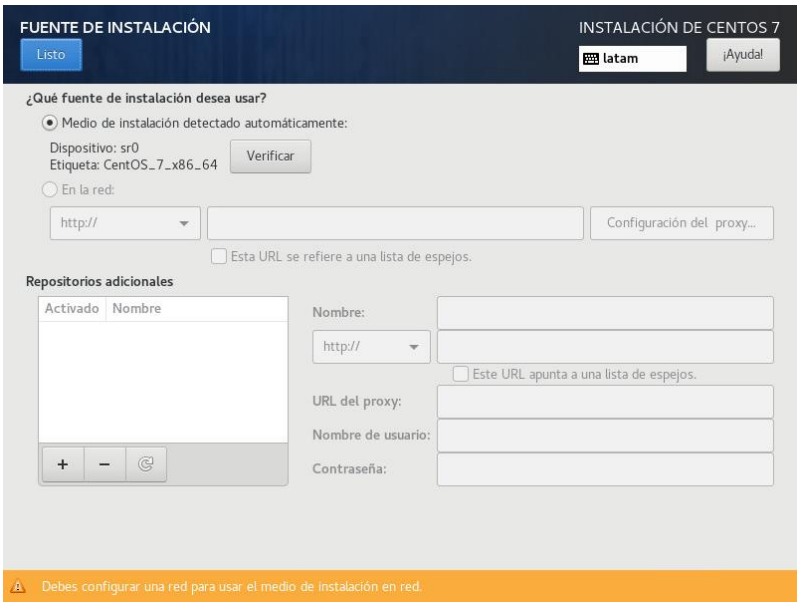


Figura 63. Selección de origen de instalación

Selección de Software

Seleccione Servidor de infraestructura y el paquete de administración remota para Linux y después, haga clic en el botón [Listo].

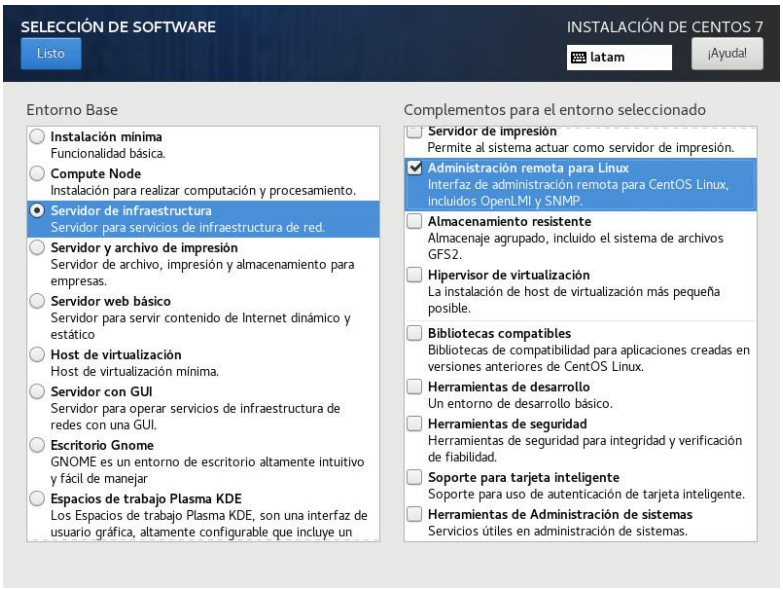


Figura 64. Selección de software

Destino de la Instalación

Seleccione el disco de instalación y haga clic en el botón [Listo].

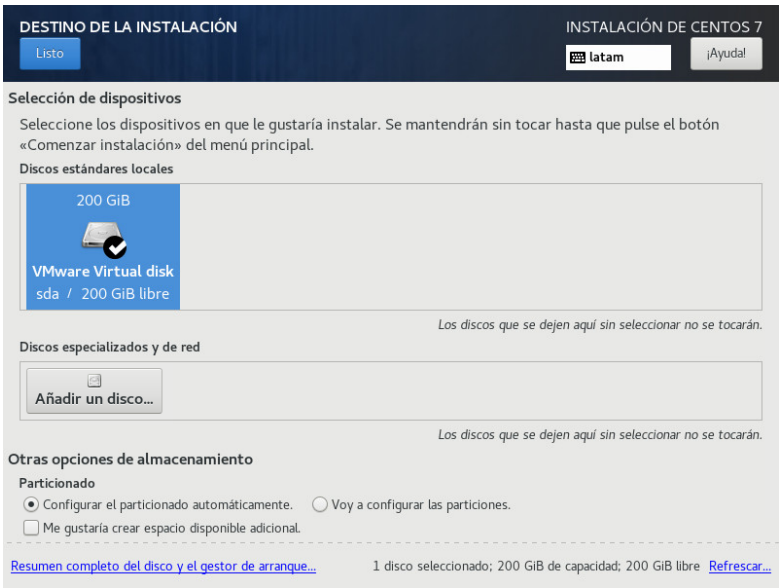


Figura 65. Selección de destino de instalación

Red y Nombre de Equipo

El asistente detecta y configura las interfaces. Haga clic en el botón [Listo].

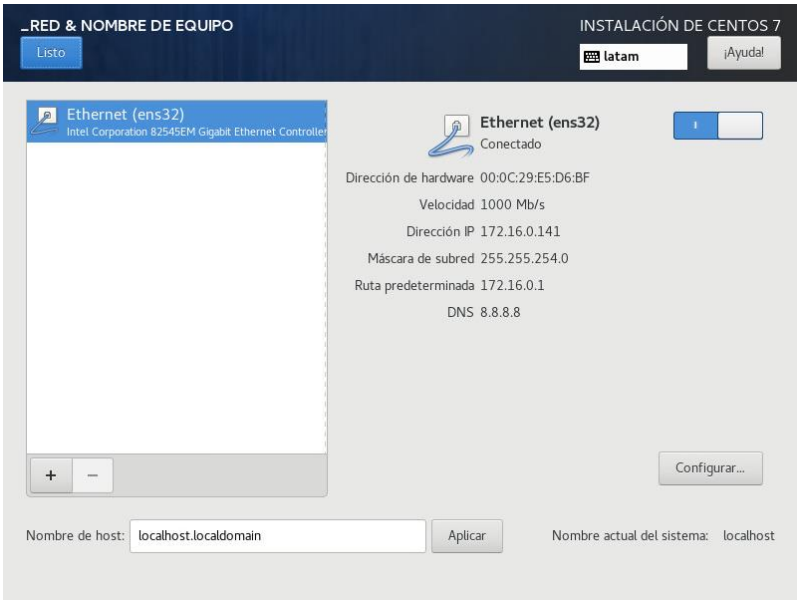


Figura 66. Selección de interfaces

Una vez finalice la configuración, haga clic en el botón [Empezar instalación].

Figura 67. Inicio de instalación

Configuración del Perfil

Configure la contraseña del usuario root y si lo desea, cree un usuario.

Figura 68. Configuración del perfil

Contraseña del Usuario Root

Ingrese la contraseña que desee para el usuario root y haga clic en el botón [Listo].

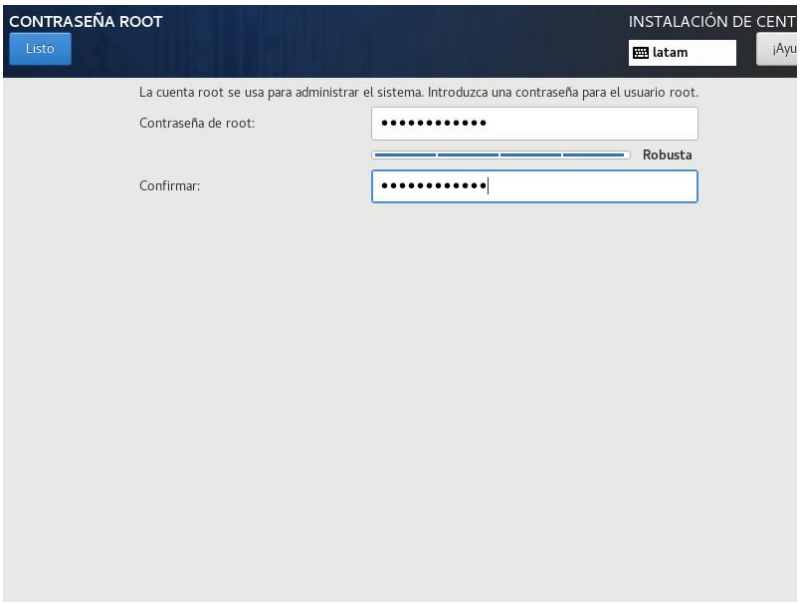


Figura 69. Contraseña de root

Pasos Finales

Una vez finalice la configuración e instalación de paquetes, haga clic en el botón [Reiniciar] para completar la instalación.

Figura 70. Reinicio

Después de reiniciar, el servidor se encuentra listo.

Figura 71. Inicio de sesión

Configuración

Configuración de Red en Modo GUI

Nmtui es una herramienta que interactúa con NetworkManager para configurar las interfaces de red en sistemas operativos Linux Red Hat y derivados.

Ingrese el siguiente comando y presione la tecla Enter para abrir la herramienta nmtui:

```
[root@localhost ~]# nmtui
```

Seleccione [Modificar una conexión] y presione la tecla Enter para continuar.

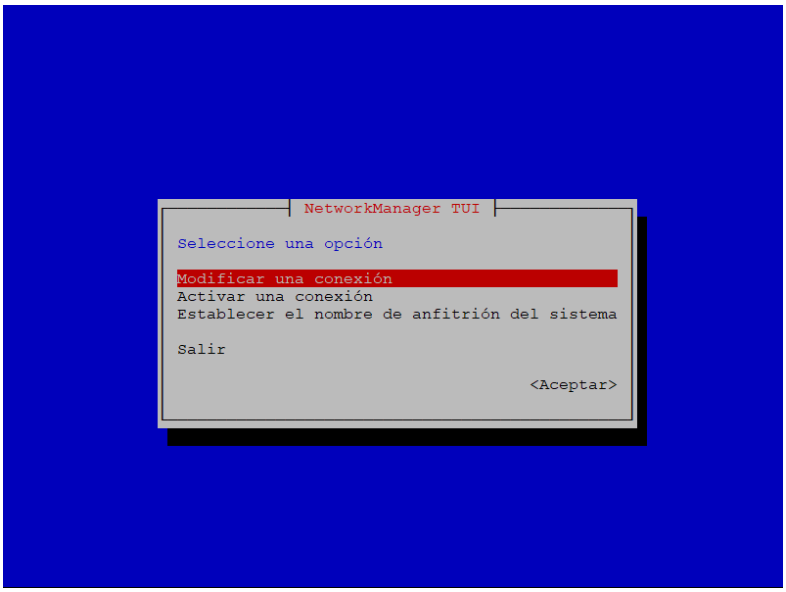


Figura 72. Modificación de conexión

Seleccione la interfaz a modificar. Después, seleccione [Editar...] y presione la tecla **Enter** para continuar.

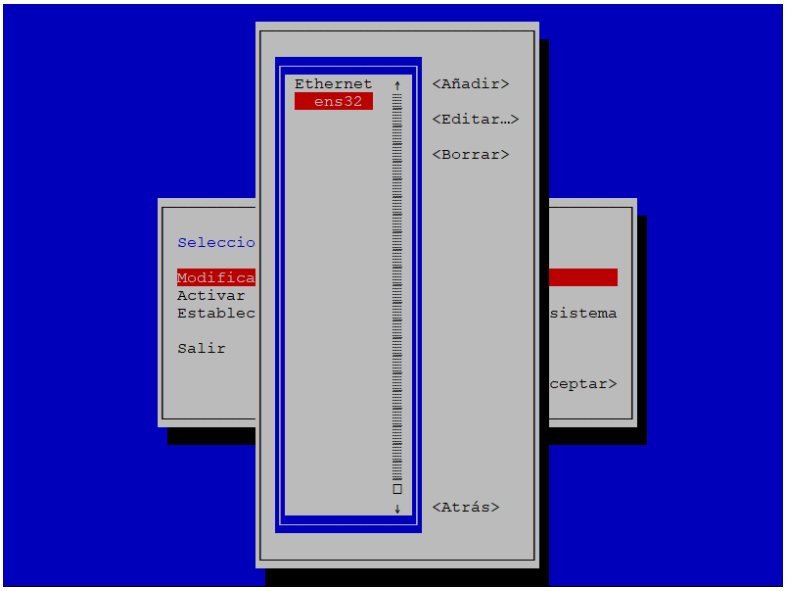


Figura 73. Selección de interfaz

Cambie de Automática a Manual y seleccione [Mostrar].

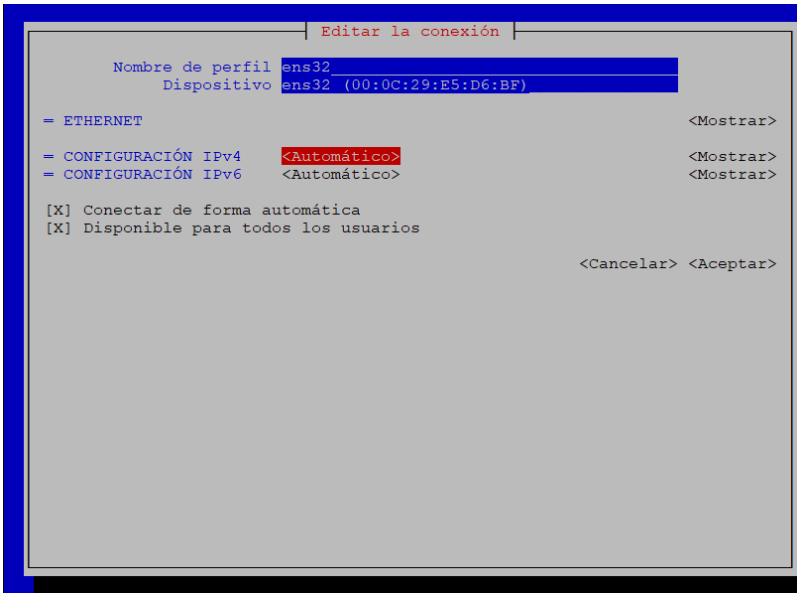


Figura 74. Cambio de IP

Ingrese los datos para configurar la interfaz. Seleccione [Aceptar] y presionar la tecla **Enter** para guardar.

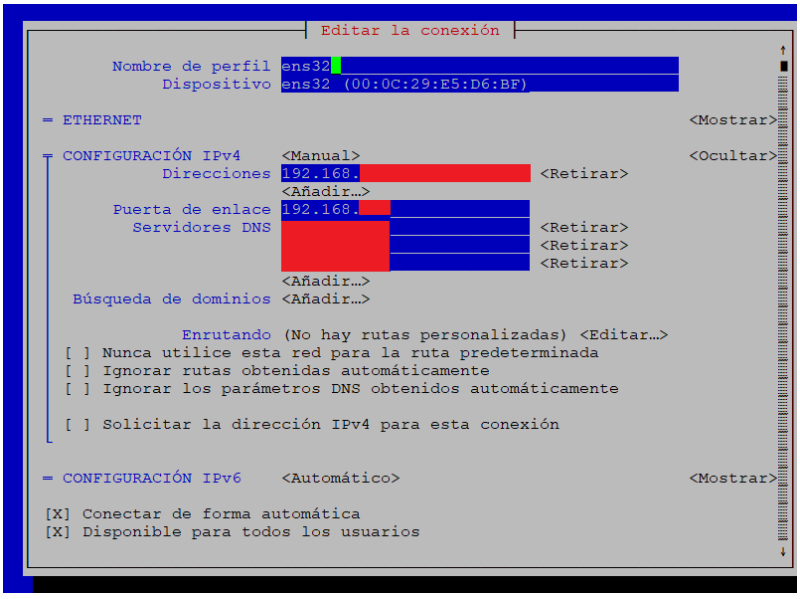


Figura 75. Cambio de IP

Seleccione [Atrás] y presionar la tecla Enter. Después, seleccione [Salir] o [Aceptar] y presionar la tecla **Enter** para terminar la configuración.

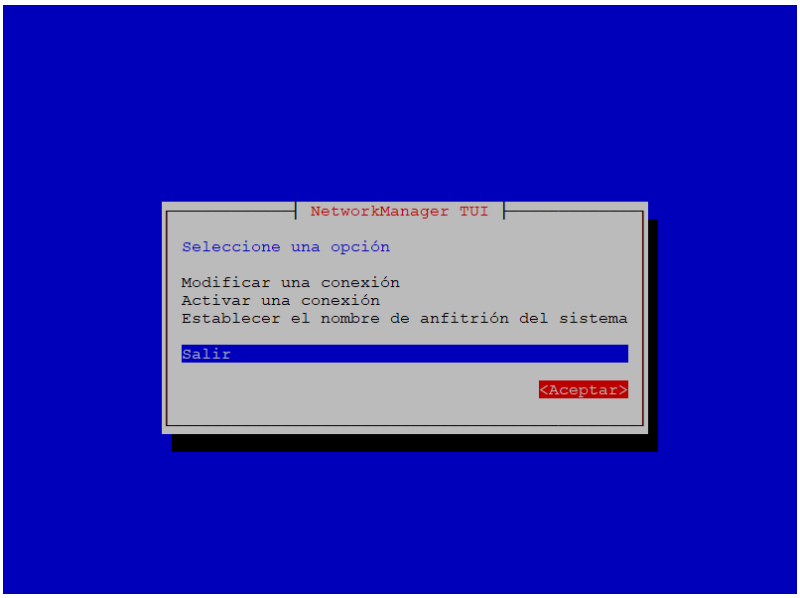


Figura 76. Salir

Para aplicar cambios, reinicie el servicio network. Ingrese el siguiente comando y presione la tecla Enter:

```
[root@localhost ~]# systemctl restart network.service
```

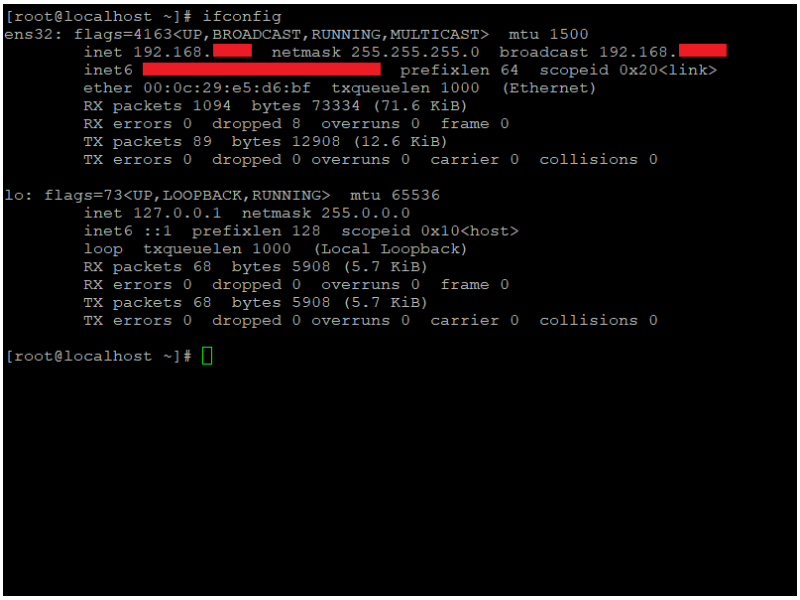


Figura 77. Verificación de IP

Anexo 5.

Script Base de Datos

```
#!/bin/bash

# fecha y hora
fecha=$(date +%Y%m%d-%H%M)
# ruta de la carpeta donde se guardan las copias de seguridad
directorio=/home/backups
# nombre del archivo
archivo=backupDB_$fecha.sql

#comando mysqldump
/usr/bin/mysqldump --defaults-extra-file=/root/mylogin.cnf --add-drop-table --add-locks --extended-insert --single-transaction --quick zabbix | bzip2 > $directorio/$archivo.bz2 && \echo "Respaldo realizado exitosamente" >> $directorio/bitacora_$fecha.txt

#Elimina los archivos con más de 7 días
find $directorio/* -mtime +7 -exec rm {} \;

#envía una copia del archivo al servidor de almacenamiento remoto “Backup”.
su -c "scp -rpq $directorio/$archivo.bz2 root@BACKUP:/home/backups" root \&& echo "Respaldo al servidor remoto realizado exitosamente" >> /home/backups/bitacora_$fecha.txt && $directorio/bitacora_$fecha.txt
```

A continuación, se detallan las opciones incluidas en el comando mysqldump para realizar copias de seguridad más rápidas y efectivas:

- **--add-drop-table:** añade un DROP TABLE antes de cada sentencia CREATE; lo que permite que a la hora de restaurar la base de datos, no haya que borrar previamente las tablas ya existentes de forma manual.
- **--add-locks:** añade bloqueos alrededor de las sentencias INSERT; lo que implica operaciones de inserción más rápidas cuando se restaure la base de datos.
- **--extended-insert:** proporciona sentencias de INSERT más compactas y rápidas.
- **--single-transaction:** Emite una única transacción para todo el proceso de creación de la copia de seguridad, con lo cual se garantiza un estado consistente sin necesidad de bloquear Zabbix.
- **--quick:** Recupera las filas de la base de datos una a la vez, por lo cual se acelera el proceso de creación.

Anexo 6.

Plan de Pruebas

El plan de pruebas incluye pruebas unitarias, de integración y funcionales. El formato de las pruebas se detalla a continuación:

Tabla 17

Formato de pruebas

Nombre de la prueba	Identificador
Descripción de la prueba:	
Pasos:	
Resultado esperado:	

Pruebas unitarias

En este caso, las pruebas unitarias tienen como objetivo verificar que cada componente de la arquitectura del sistema de monitoreo funcione correctamente de forma individual.

Tabla 18

PU-01

Zabbix Server	PU-01
Descripción de la prueba: Comprobar que Zabbix Server acepta conexiones en el puerto 10051	
Pasos: 1. Ingresar al servidor Zabbix 2. Ejecutar el comando *netstat -tulpn | grep 10051*	
Resultado esperado: Al ejecutar el comando, se mostrara que el puerto está aceptando la conexión	

Tabla 19

PU-02

Base de Datos	PU-02
Descripción de la prueba: Comprobar que la base de datos se está ejecutando correctamente	
Pasos: 1. Ingresar al servidor Zabbix 2. Ejecutar el comando *service mariadb status* 3. Ir a la url del sistema de monitoreo	
Resultado esperado: Al ir a la url del sistema de monitoreo no se mostrara ningún error con la conexión a la base de datos.	

Tabla 20

PU-03

Zabbix Frontend	PU-03
Descripción de la prueba: Comprobar que el servidor Apache funciona correctamente	
Pasos: 1. Ir a la url del servidor Zabbix	
Resultado esperado: Se mostrara la pantalla de inicio del sistema de monitoreo	

Tabla 21

PU-04

Agente Zabbix	PU-04
Descripción de la prueba: Comprobar que existe y se ejecuta el agente Zabbix en los servidores	
Pasos: 1. Ingresar al servidor 2. Ejecutar el comando *netstat -tulpn | grep 10050*	
Resultado esperado: Al ejecutar el comando, se mostrara que el puerto está aceptando la conexión	

Tabla 22

PU-05

Agente SNMP	PU-05
Descripción de la prueba: Comprobar que el protocolo SNMP este activo en los switches	
Pasos: 1. Ingresar al servidor Zabbix 2. Ejecutar el comando *snmpwalk*	
Resultado esperado: Al ejecutar el comando, se mostrara el listado de OIDs asociados al equipo	

Fuente: Autoría propia.

Pruebas de integración

En este caso, las pruebas de integración tienen como objetivo verificar la comunicación entre los componentes de la arquitectura del sistema de monitoreo.

Tabla 23

PI-01

Zabbix Server y Agente Zabbix	PI-01
Descripción de la prueba: Comprobar la comunicación entre el servidor del sistema de monitoreo de red y los servidores que hacen parte de la infraestructura de red de datos.	
Pasos: 1. Ir a la url del sistema de monitoreo 2. Iniciar sesión 3. Ir al menú Configuration → Hosts y hacer clic en el botón [Create host] 4. Ingresar los campos necesarios y hacer clic en el botón [Add].	
Resultado esperado: De no haber ningún problema, se observara que en los datos del host estará un icono indicativo de color verde con la palabra ZBX.	

Tabla 24

PI-02

Zabbix Server y Agente SNMP	PI-02
Descripción de la prueba: Comprobar la comunicación entre el servidor del sistema de monitoreo de red y los	

switches que hacen parte de la infraestructura de red de datos.
Pasos: 1. Ir a la url del sistema de monitoreo 2. Iniciar sesión 3. Ir al menú Configuration → Hosts y hacer clic en el botón [Create host] 4. Ingresar los campos necesarios y hacer clic en el botón [Add].
Resultado esperado: De no haber ningún problema, se observara que en los datos del host estará un icono indicativo de color verde con la palabra SNMP.

Pruebas Funcionales

En este caso, las pruebas funcionales tienen como objetivo validar que el sistema de monitoreo de red implantado cubra los requisitos definidos por CSI.

Tabla 25

PF-01

Monitoreo de Equipos	PF-01
Descripción de la prueba: Validar que el sistema de monitoreo permita monitorear cualquier equipo que se identifique con una dirección IP.	
Pasos: 1. Ir a la url del sistema de monitoreo 2. Iniciar sesión 3. Ir al menú Configuration → Hosts y hacer clic en el botón [Create host] 4. Ingresar los campos necesarios y hacer clic en el botón [Add]. 5. Repetir los pasos anteriores con cada tipo de equipo que conforma la red de datos.	
Resultado esperado: De no haber ningún problema, se observara que en los datos del host estará un icono indicativo de color verde con el tipo de monitoreo seleccionado.	

Tabla 26

PF-02

Monitoreo de Parámetros	PF-02
Descripción del caso: Validar que el sistema de monitoreo permita monitorear parámetros relacionados al almacenamiento, memoria, CPU, temperatura e interfaces de Red.	
Pasos:	

1. Ir a la url del sistema de monitoreo 2. Iniciar sesión 3. Ir al menú Configuration → Hosts y hacer clic sobre el nombre del equipo previamente creado. 4. Ir a la pestaña de Template y asociar la plantilla al host
Resultado esperado: Al ir al menú Monitiring → Latest data, se observara la información del equipo

Tabla 27

PF-03

Gestión de Equipos	PF-03
Descripción del caso: Validar que el sistema de monitoreo permita gestionar (añadir, editar o eliminar) los equipos a monitorear o monitoreados, y sus parámetros.	
Pasos: 1. Ir a la url del sistema de monitoreo 2. Iniciar sesión 3. Ir al menú Configuration → Hosts y hacer clic sobre el nombre del equipo 4. Hacer clic sobre la opción preferida (create host, update, clone, full clone, delete)	
Resultado esperado: El sistema de monitoreo permite añadir, editar y eliminar un equipo o parámetro	

Tabla 28

PF-04

Soporte de Protocolo	PF-04
Descripción del caso: Validar que el sistema de monitoreo permita monitorear equipos a través del protocolo SNMP.	
Pasos: 1. Ir a la url del sistema de monitoreo 2. Iniciar sesión 3. Ir al menú Configuration → Hosts y hacer clic en el botón [Create host] 4. Ingresar los campos necesarios y hacer clic en el botón [Add].	
Resultado esperado: De no haber ningún problema, se observara que en los datos del host estará un icono indicativo de color verde con la palabra SNMP.	

Tabla 29

PF-05

Agentes	PF-05
Descripción del caso: Validar que el sistema de monitoreo permita monitorear equipos a través de un agente	
Pasos: 1. Ir a la url del sistema de monitoreo 2. Iniciar sesión 3. Ir al menú Configuration → Hosts y hacer clic en el botón [Create host] 4. Ingresar los campos necesarios y hacer clic en el botón [Add].	
Resultado esperado: De no haber ningún problema, se observara que en los datos del host estará un icono indicativo de color verde con la palabra ZBX.	

Tabla 30

PF-06

Gestión de Alertas	PF-06
Descripción del caso: Validar que el sistema de monitoreo permita gestionar alertas a través de las cuales se notifique el estado de los equipos	
Pasos: 1. Ir a la url del sistema de monitoreo 2. Iniciar sesión 3. Ir al menú Configuration → Template y hacer clic sobre el nombre de la plantilla previamente creada. 4. Ir a la pestaña de Triggers y hacer clic sobre la opción preferida (create trigger, update, clone, delete)	
Resultado esperado: El sistema de monitoreo permite añadir, editar y eliminar una alerta	

Tabla 31

PF-07

Niveles de Alerta	PF-07
Descripción del caso: Validar que el sistema de monitoreo permita definir diferentes niveles en función de la severidad del evento.	
Pasos:	

1. Ir a la url del sistema de monitoreo 2. Iniciar sesión 3. Ir al menú Configuration → Template y hacer clic sobre el nombre de la plantilla previamente creada. 4. Ir a la pestaña de Triggers y hacer clic en el botón [Create trigger] 5. Ingresar los campos necesarios y hacer clic en el botón [Add].
Resultado esperado: El sistema de monitoreo cuenta con varios niveles de severidad para alertar la presencia de un evento.

Tabla 32

PF-08

Graficas	PF-08
Descripción del caso: Validar que el sistema de monitoreo permita obtener gráficas de los parámetros monitoreados.	
Pasos: 1. Ir a la url del sistema de monitoreo 2. Iniciar sesión 3. Ir al menú Monitiring → Latest data y hacer clic sobre el enlace Graph de un parámetro.	
Resultado esperado: Al hacer clic sobre el enlace, se mostrara la gráfica construida para el parámetro.	

Tabla 33

PF-09

Notificaciones	PF-09
Descripción del caso: Validar que el sistema de monitoreo permita notificar la existencia de un evento	
Pasos: 1. Apagar el equipo de pruebas	
Resultado esperado: El sistema de monitoreo enviara un correo electrónico al administrador de la red para notificar la presencia del evento.	

Tabla 34

PF-10

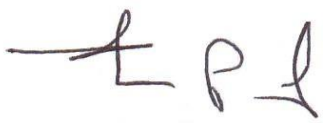
Reportes	PF-10
Descripción del caso: Validar que el sistema de monitoreo permita presentar reportes de distintos tipos	
Pasos: 1. Ir a la url del sistema de monitoreo 2. Iniciar sesión 3. Ir al menú Reports	
Resultado esperado: El sistema de monitoreo cuenta con diferentes tipos de reportes	

Anexo 7.

Asistencia de la Capacitación

Tabla 35

Asistencia de la capacitación virtual

IDENTIFICACIÓN DE LA CAPACITACIÓN		
Tema: Manejo del sistema de monitoreo de red		**Lugar:** Plataforma Meet
Fecha: 27/04/2020		**Duración:** Una hora y media
Hora de Inicio: 4:30 p.m.		**Hora de Finalización:** 06:00 p.m.
Capacitadora: Lizeth Ríos Epalza		**Capacitados:** Personal administrativo de CSI
LISTADO DE ASISTENCIA		
NOMBRE	ROL	FIRMA
Eusen Enrique Peñaranda Carrillo	Profesional Universitario	
José Martín Calixto Cely	Coordinador de CSI