Sandbox Technology – Network Infrastructure Monitoring

Sotelo Mendez Fabio Maximiliano, Titonel Lucas Marcos, Peralta Nahuel Maximiliano, Ramos Milagros Ariadna

Facultad de Ciencias Exactas, Naturales y Agrimensura. Universidad Nacional del Nordeste. Corrientes, Argentina.

fabiomaxsotelo@gmail.com, mili.ariadna.13@gmail.com, lucas.t777@gmail.com, nahuelperaltagomez@gmail.com.

Abstract

Current network infrastructures require monitoring mechanisms capable of detecting failures, anticipating service degradation, and sustaining operational continuity. However, the direct application of new configurations, agents, or artifacts in production environments introduces risks that traditional monitoring does not solve by itself. This paper proposes an integrated approach to network infrastructure monitoring, complemented by a sandbox environment for the prior validation of configurations and the isolated analysis of potentially risky artifacts. The implementation was carried out in a virtualized laboratory, with one machine assigned to the monitoring server and another used as an isolated environment and monitored host, where load, failure, and unavailability scenarios were simulated. The results obtained show improvements in infrastructure visibility, early alert generation, and operational risk reduction by validating changes before their application in production. It is concluded that the integration between monitoring and sandboxing strengthens preventive network management, contributes to reducing detection and recovery times during incidents, and provides a more robust strategy for the secure operation of critical infrastructures.

Keywords

Network monitoring; Network Management System; sandbox environment; Zabbix; incident detection.

Tecnología Sandbox – Monitoreo de Infraestructura de Red

Resumen

Las infraestructuras de red actuales requieren mecanismos de monitoreo que permitan detectar fallas, anticipar degradaciones de servicio y sostener la continuidad operativa. Sin embargo, la aplicación directa de nuevas configuraciones, agentes o artefactos sobre entornos productivos introduce riesgos que el monitoreo tradicional no resuelve por sí solo. En este trabajo se propone un enfoque integrado de monitoreo de infraestructura de red, complementado con un entorno sandbox para la validación previa de configuraciones y el análisis aislado de artefactos potencialmente riesgosos. La implementación se llevó a cabo en un laboratorio virtualizado, con una máquina destinada al servidor de monitoreo y otra utilizada como entorno aislado y host monitoreado, sobre la cual se simularon escenarios de carga, fallas e indisponibilidad. Los resultados obtenidos evidencian mejoras en la visibilidad de la infraestructura, en la generación temprana de alertas y en la reducción del riesgo operativo al validar previamente cambios antes de su aplicación en producción. Se concluye que la integración entre monitoreo y Sandbox fortalece la gestión preventiva de redes, contribuyendo a disminuir los tiempos de detección y recuperación ante incidentes, y ofreciendo una estrategia más robusta para la operación segura de infraestructuras críticas.

Palabras clave

monitoreo de red; sistema NMS; entorno sandbox; Zabbix; detección de incidentes.

1. Introducción

Las redes de datos constituyen un componente crítico dentro de las organizaciones, ya que sostienen servicios esenciales para la comunicación, la operación diaria y la continuidad de los procesos tecnológicos. La disponibilidad y estabilidad de estos servicios impactan directamente en el funcionamiento institucional, por lo que resulta necesario contar con mecanismos que permitan supervisar el estado de la infraestructura y anticipar posibles fallas antes de que afecten a los usuarios finales.

A medida que las infraestructuras de red crecen en complejidad, incorporando servidores, equipos distribuidos, usuarios remotos, enlaces de comunicación y múltiples servicios simultáneos, la administración reactiva resulta insuficiente. En

este contexto, los sistemas de monitorización permiten observar la disponibilidad, el rendimiento y el comportamiento de los recursos tecnológicos, facilitando la detección temprana de incidentes, el análisis de tendencias y la toma de decisiones técnicas basadas en información operativa (Quintero Martínez y Tovar Balderas, 2021).

El monitoreo de infraestructura mediante un sistema NMS, o *Network Management System*, permite centralizar la recolección de métricas, visualizar el estado de los dispositivos, definir umbrales de alerta y generar notificaciones ante eventos anómalos. Herramientas de código abierto como Zabbix ofrecen capacidades para supervisar equipos, servicios y recursos mediante agentes, protocolos como SNMP y paneles de visualización configurables, lo que las convierte en una alternativa viable para entornos que requieren control operativo y reducción de costos (Zabbix, s. f.; Zhuma Mera et al., 2025).

Sin embargo, el monitoreo por sí solo no elimina los riesgos asociados a la aplicación de cambios en una infraestructura real. La modificación de plantillas, agentes, reglas de alerta o configuraciones de red puede producir errores operativos si no se valida previamente en un entorno seguro. Por este motivo, se incorpora el concepto de sandbox como un espacio aislado de pruebas, orientado a validar configuraciones, agentes y escenarios de falla antes de trasladarlos a un entorno productivo. Este enfoque permite reducir riesgos, mejorar la confiabilidad del despliegue y fortalecer la continuidad operativa.

En este trabajo se propone la implementación de un entorno de monitoreo de infraestructura de red mediante un sistema NMS, complementado con un sandbox de validación. Para ello, se utiliza Zabbix como plataforma central de monitoreo y un laboratorio virtualizado como entorno aislado para realizar pruebas controladas. La propuesta busca mejorar la visibilidad de la infraestructura, favorecer la detección temprana de incidentes y disminuir los riesgos asociados a configuraciones no verificadas previamente.

1.2 Definiciones

- Monitoreo de infraestructura (NMS): plataforma que descubre, sondea y recolecta métricas/estados de equipos de red y servidores para visualizar, alertar y reportar.
- SNMP (v2c/v3): protocolo de gestión que consulta OIDs de una MIB (Get/Walk), recibe traps/inform y permite cambios controlados (Set).
- ICMP / Ping: prueba de alcance y latencia básica entre nodos.

- Syslog: envío centralizado de logs por UDP/TCP; base para alertas y auditoría.
- Agente de monitoreo: software local que expone métricas del host (CPU, RAM, disco, servicios) o ejecuta chequeos activos.
- SIEM: motor que correlaciona logs/alertas de múltiples fuentes (NMS, firewall, IDS/IPS, hosts) y prioriza eventos; genera paneles y tickets.
- IDS/IPS: inspección de tráfico (firmas y anomalías); IDS alerta, IPS puede bloquear en línea.
- ACL/Firewall: controles de política de red (permitir/denegar) con registro; base de segmentación y reducción de superficie de ataque.
- Sandbox: entorno aislado (VM/contendor/microVM) para detonar artefactos (archivos, URLs, flujos) y observar conducta sin impacto en producción.
- Análisis dinámico (sandbox): ejecución real para capturar procesos, cambios de archivos/registro y tráfico de red.
- Telemetría: datos de medición (métricas, logs, flujos, IoCs) enviados al NMS/SIEM para observabilidad y respuesta.}

1.3. Planteamiento del problema

La disponibilidad y estabilidad de las redes de computadoras son factores críticos para garantizar la continuidad de los servicios tecnológicos dentro de una organización. Sin embargo, en muchas infraestructuras, la detección de fallas sigue realizándose de manera reactiva, es decir, cuando el problema ya afectó al usuario final o interrumpió un servicio. Esta situación dificulta la toma de decisiones oportunas y puede aumentar los tiempos de detección y recuperación ante incidentes.

A esta problemática se suma el riesgo operativo asociado a la aplicación directa de configuraciones sobre entornos reales. La instalación de agentes, definición de triggers o cambios en reglas de monitoreo pueden generar errores si no son validados previamente. En consecuencia, resulta necesario contar con un entorno controlado que permita probar configuraciones, simular escenarios de falla y verificar el comportamiento del sistema de monitoreo antes de su implementación definitiva.

1.4. Objetivo general

Implementar y evaluar un entorno de monitoreo de infraestructura de red mediante un sistema NMS, complementado con un sandbox de validación, con el fin de mejorar la observabilidad de la infraestructura, detectar incidentes de forma temprana y reducir los riesgos asociados a la aplicación de configuraciones no verificadas en entornos productivos.

1.5. Objetivos específicos

- Analizar el uso de sistemas NMS como herramienta para la supervisión de disponibilidad, rendimiento y estado de dispositivos de red.
- Implementar el sistema NMS Zabbix como plataforma central para la recolección de métricas, visualización de dashboards y generación de alertas basadas en umbrales.
- Evaluar el comportamiento del sistema ante eventos simulados, como aumento de uso de CPU, consumo de memoria, pérdida de disponibilidad o caída de servicios.
- Implementar un entorno Sandbox para la ejecución y evaluación de configuraciones y simulación de escenarios.
- Determinar si la integración entre monitoreo NMS y validación en sandbox contribuye a una gestión más segura y proactiva de la infraestructura de red.

1.6. Fundamentación

La realización de este proyecto se fundamenta en la necesidad de mejorar la supervisión y disponibilidad de las infraestructuras de red, ya que los servicios tecnológicos dependen cada vez más de servidores, dispositivos y aplicaciones que deben mantenerse operativos. Frente a fallas o degradaciones del servicio, un sistema NMS permite recolectar métricas, visualizar el estado de la red y generar alertas tempranas, favoreciendo una gestión más preventiva y menos reactiva.

Además, el proyecto incorpora un entorno sandbox de validación para reducir los riesgos asociados a aplicar configuraciones directamente sobre una infraestructura real.

1.7. Hipótesis o supuesto de trabajo

La implementación de un sistema NMS basado en Zabbix, complementado con un entorno sandbox de validación, permite mejorar la visibilidad operativa de la infraestructura de red, favorecer la detección temprana de incidentes y reducir los riesgos derivados de aplicar configuraciones no probadas directamente sobre entornos productivos.

2. Marco Teórico

El monitoreo de infraestructura de red es una práctica orientada a observar de manera continua la disponibilidad, el rendimiento y el estado de los recursos tecnológicos que componen una organización, tales como servidores, enlaces, routers, switches, aplicaciones y servicios. Su importancia radica en que permite detectar fallas, degradaciones o comportamientos anómalos antes de que impacten directamente en los usuarios finales, favoreciendo la continuidad operativa y la atención temprana de incidentes (Quintero Martínez y Tovar Balderas, 2021).

Dentro de este enfoque se ubican los sistemas NMS, o Network Management System, los cuales permiten centralizar la supervisión de dispositivos y servicios de red. Un NMS recolecta métricas, registra eventos, visualiza el estado de la infraestructura y genera alertas ante condiciones definidas por el administrador. De esta manera, transforma datos técnicos, como uso de CPU, memoria, ancho de banda, latencia o disponibilidad, en información útil para diagnosticar problemas, analizar tendencias y tomar decisiones operativas.

Diversos trabajos destacan que las herramientas de monitoreo de código abierto constituyen una alternativa viable para la gestión de redes, ya que permiten supervisar recursos tecnológicos, detectar fallas y apoyar la administración técnica de la infraestructura sin depender necesariamente de soluciones comerciales. En este sentido, Velasco Briones (2017) desarrolla una implementación basada en Nagios para monitorear redes, evidenciando la utilidad de este tipo de herramientas para controlar recursos, identificar incidencias y mejorar los tiempos de respuesta. De forma complementaria, Intriago-Cedeño et al. (2022) señalan que la evaluación de herramientas de monitoreo permite seleccionar soluciones adecuadas según criterios de funcionalidad, seguridad, adaptabilidad y capacidad de supervisión.

Las funciones principales de un NMS incluyen el descubrimiento e inventario de dispositivos, la recolección de métricas de rendimiento, la generación de dashboards, el almacenamiento de históricos y la configuración de alertas basadas en umbrales. En redes tipo campus, se ha demostrado que el uso de herramientas de código abierto como Zabbix y Syslog-ng permite centralizar eventos, visualizar métricas clave y generar notificaciones automáticas en tiempo real, mejorando la detección de incidencias y la respuesta técnica ante eventos críticos (Zhuma Mera et al., 2025).

La adquisición de datos puede realizarse mediante distintos mecanismos. El sondeo activo, o modelo pull, ocurre cuando el NMS consulta periódicamente a los dispositivos mediante protocolos como ICMP o SNMP. La recolección pasiva, o modelo push, se produce cuando los dispositivos envían eventos al sistema mediante Syslog o traps SNMP.

Las métricas obtenidas por el NMS se almacenan como históricos o series temporales, lo que permite observar tendencias, reconocer comportamientos recurrentes y planificar capacidad. Por ello, el monitoreo de red no solo cumple una función reactiva ante fallas, sino que también actúa como una estrategia preventiva para mejorar la estabilidad, la seguridad operativa y la gestión de la infraestructura tecnológica.

2.1. Arquitectura NMS y su relación con el monitoreo

La arquitectura de un Sistema de Gestión de Red, o NMS, puede organizarse en capas que permiten recolectar datos desde la infraestructura, procesarlos y presentarlos como información útil para la operación técnica. De este modo, métricas como disponibilidad, tráfico, uso de CPU, memoria o latencia dejan de ser datos aislados y se convierten en indicadores para detectar fallas, analizar tendencias y apoyar la toma de decisiones (Quintero Martínez y Tovar Balderas, 2021).

En este sentido, la integración de un entorno sandbox permite fortalecer el proceso de monitoreo, ya que ofrece un espacio controlado para validar configuraciones, plantillas, agentes y reglas de alerta antes de aplicarlas sobre un entorno productivo.

2.1.1. Capa de adquisición

La capa de adquisición interactúa con dispositivos de red, servidores y servicios monitoreados para recolectar datos de disponibilidad, rendimiento y estado operativo. Esta recolección puede realizarse mediante un modelo activo o pull, donde el NMS consulta periódicamente a los dispositivos mediante ICMP o SNMP, y mediante un modelo pasivo o push, donde los equipos envían eventos al sistema a través de Syslog o traps SNMP. El protocolo SNMP permite obtener información de gestión desde objetos definidos en la MIB, como estado de interfaces, tráfico, uso de memoria o CPU (Harrington et al., 2002).

2.1.2. Capa de procesamiento y almacenamiento

La capa de procesamiento y almacenamiento transforma la telemetría recolectada en información operativa. En esta etapa, los datos se almacenan como históricos o series temporales, se comparan con umbrales definidos y se procesan mediante reglas de alerta para identificar condiciones anómalas, como uso elevado de CPU, consumo excesivo de memoria, pérdida de conectividad o caída de servicios. Herramientas como Zabbix permiten configurar triggers, plantillas y reglas de notificación para automatizar la detección de eventos relevantes (Zabbix, s. f.-b). En redes tipo campus, el uso de Zabbix junto con herramientas de gestión de registros ha permitido centralizar eventos, clasificar alertas por criticidad y mejorar la respuesta técnica ante incidentes (Zhuma Mera et al., 2025).

2.1.3. Capa de operación y visualización

La capa de operación y visualización presenta la información procesada de forma comprensible para los administradores de red mediante dashboards, gráficos históricos, mapas topológicos, listados de problemas y reportes de capacidad. Su finalidad es facilitar la interpretación del estado de la infraestructura, permitiendo identificar el recurso afectado, la criticidad del evento y las acciones necesarias. Una implementación adecuada evita generar alertas sin contexto y prioriza información útil para diagnosticar, actuar y verificar.

2.2. Tecnología sandbox

Mientras que el NMS se orienta a la observabilidad de la infraestructura mediante métricas, alertas y dashboards, la tecnología sandbox complementa este enfoque al proporcionar un entorno aislado para realizar pruebas sin afectar sistemas productivos. En términos generales, un sandbox es un espacio controlado donde es posible ejecutar procesos, validar configuraciones o analizar comportamientos sin comprometer el entorno principal (Fortinet, s. f.; IBM Security, s. f.).

En este trabajo, el sandbox se aborda principalmente como un entorno de validación para el monitoreo de infraestructura de red. Su finalidad consiste en probar agentes, plantillas, triggers, umbrales y escenarios de falla antes de trasladarlos a una infraestructura real. Esta práctica permite reducir riesgos operativos, evitar configuraciones defectuosas y comprobar que el sistema NMS responda adecuadamente ante eventos simulados, como sobrecarga de CPU, consumo elevado de memoria, pérdida de conectividad o caída de servicios.

En escenarios de seguridad más avanzados, el sandbox también puede utilizarse para analizar artefactos sospechosos, como archivos o direcciones URL, observando su comportamiento dentro de una máquina virtual o entorno aislado. Sin embargo, en la presente propuesta este uso se considera una posible extensión futura, ya que el enfoque principal se centra en la validación operativa del monitoreo mediante NMS.

3. Instrumentación

Para llevar adelante la implementación del monitoreo y la validación mediante sandbox, se preparó un entorno de laboratorio controlado, compuesto por una máquina física y varias máquinas virtuales. La decisión de utilizar virtualización tuvo dos objetivos principales: aislar los componentes para evitar interferencias con otros sistemas y permitir la construcción de un entorno reproducible, similar al que se utilizaría en producción.

El hardware utilizado fue una computadora personal con procesador multinúcleo, 8 GB de memoria RAM y almacenamiento suficiente para alojar varias máquinas virtuales simultáneamente. Este equipo funcionó como host de virtualización, utilizando VirtualBox como plataforma para la creación y gestión de las máquinas virtuales.

Sobre el hipervisor se implementaron dos máquinas virtuales independientes:

3.1. Máquina virtual "Servidor Zabbix":

Esta VM fue configurada con el sistema operativo Ubuntu Server 20.04.3, debido a su estabilidad y soporte extenso en entornos de red. En esta máquina se instalaron los componentes indispensables para Zabbix Server: el servidor web (Apache), motor de bases de datos (MariaDB), PHP y finalmente el paquete de Zabbix Server + Frontend. Esta máquina actuó como núcleo del sistema de monitoreo, centralizando la recepción de métricas, el almacenamiento de históricos y la visualización gráfica mediante dashboards.

3.2. Máquina virtual "Sandbox" / host monitoreado:

La segunda VM se destinó a representar un equipo de la infraestructura a monitorear. Su finalidad fue simular un dispositivo real, instalar en ella el agente Zabbix y validar la comunicación con el servidor antes de aplicarlo a otros hosts. Esta instancia actuó como entorno de prueba, permitiendo verificar configuraciones sin afectar equipos o servicios reales. En este entorno se reprodujeron distintas situaciones controladas (carga de CPU artificial, agotamiento de memoria, caída de servicios) para observar el comportamiento del monitoreo.

Ambas máquinas virtuales se conectaron a la misma red virtual interna dentro del hipervisor, lo que garantizó comunicación directa mediante IP privada entre servidor Zabbix y agente, sin exposición a la red externa.

Antes de comenzar el monitoreo, se instalaron en la VM del sandbox los paquetes necesarios para que el agente Zabbix pudiera enviar métricas sobre recursos del sistema. Seguidamente, se configuró en el archivo zabbix_agentd.conf la dirección IP del servidor Zabbix, habilitando el flujo de comunicación. Una vez iniciado el agente, el servidor Zabbix detectó automáticamente el host y permitió asociarle plantillas de monitoreo.

La instrumentación también incluyó el armado de un entorno de pruebas sobre la continuidad del servicio, utilizando herramientas básicas de diagnóstico como ping, stress (para simular uso elevado de CPU o RAM), y comandos de verificación de estado del agente.

Como resultado de esta instrumentación, se obtuvo un entorno controlado, seguro y apto para validar tanto el monitoreo de infraestructura como el uso preventivo de sandbox antes de aplicar configuraciones definitivas en producción. Esto permitió simular escenarios de carga, error e indisponibilidad, evidenciando la capacidad de Zabbix para generar alertas, actualizar widgets en tiempo real y registrar históricos de métricas.

4. Implementación/Ejecución del programa

4.1. Zabbix como plataforma NMS del proyecto

Zabbix es una plataforma de monitoreo de infraestructura de red de tipo NMS, orientada a la supervisión de servidores, dispositivos de red, servicios, aplicaciones y recursos tecnológicos. Su funcionamiento permite recolectar métricas mediante agentes, protocolos como ICMP y SNMP, y mecanismos de alerta basados en condiciones definidas por el administrador. Además, ofrece dashboards personalizables, plantillas de monitoreo, triggers, notificaciones automáticas y almacenamiento de históricos para analizar tendencias y capacidad (Zabbix, s. f.-b).

En este proyecto se seleccionó Zabbix por tratarse de una herramienta de código abierto, escalable y adaptable a distintos entornos de infraestructura. Su capacidad para centralizar el monitoreo de múltiples hosts, trabajar con agentes propios y SNMP, generar alertas automáticas y representar métricas mediante widgets lo convierte en una alternativa adecuada para implementar una solución de monitoreo sin depender de licencias comerciales por dispositivo o sensor.

Dentro de la propuesta, Zabbix se utiliza junto con un entorno sandbox de validación. Este entorno permite probar previamente configuraciones del agente, plantillas, triggers y reglas de monitoreo antes de trasladarlas a un escenario productivo. De este modo, se busca reducir el riesgo de interrupciones, falsas alertas o errores de configuración durante la implementación definitiva.

4.2. Instalación del servidor Zabbix

La instalación se realizó en una máquina virtual con Ubuntu Server 20.04, configurada exclusivamente para actuar como servidor NMS.

Los pasos generales fueron:

1. Instalación de dependencias (Apache/Nginx, PHP y MariaDB).
2. Instalación del paquete de servidor Zabbix.
3. Creación de la base de datos para almacenar histórico de métricas.
4. Configuración del acceso web vía navegador.

Acceso a panel de administración mediante el navegador: http://192.168.x.x/zabbi, aclarando que la IP es local.

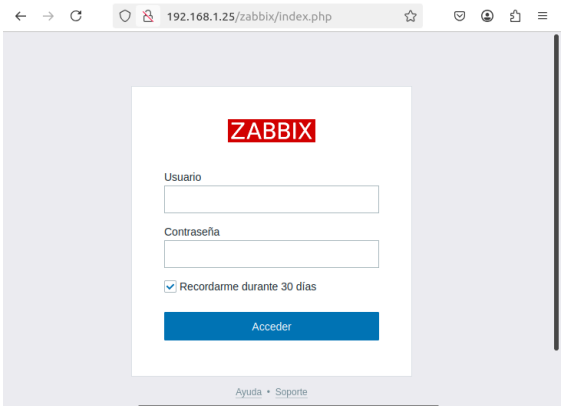

Figura 1 - Acceso al panel de Zabbix

Al ingresar, Zabbix presenta un *dashboard* inicial con estado general del sistema, número de hosts activos, problemas recientes y disponibilidad.

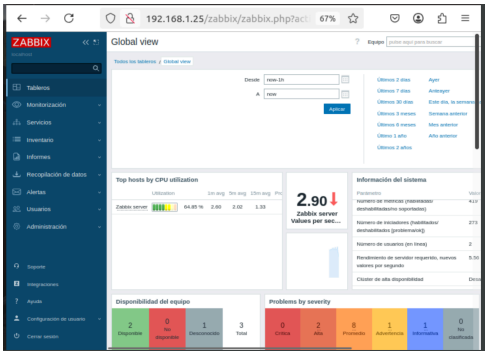

Figura 2 - Panel principal de Zabbix

4.3. Agregación de Hosts

Para comenzar el monitoreo se deben agregar hosts, que son los equipos o dispositivos que se desean supervisar (PC, router, servidor, switch, servicios, etc.).

Cada host puede ser monitoreado mediante:

- Agente Zabbix instalado localmente (mejor nivel de detalle).
- SNMP, para switches/routers.
- ICMP (ping), para disponibilidad básica.

Flujo para agregar un host:

1. Instalar el agente Zabbix en el equipo a monitorear.
2. Configurar en el archivo del agente la IP del servidor Zabbix.
3. En Zabbix Web → Configuration → Hosts → Create host.
4. Asignar una plantilla (template) según el tipo de host.

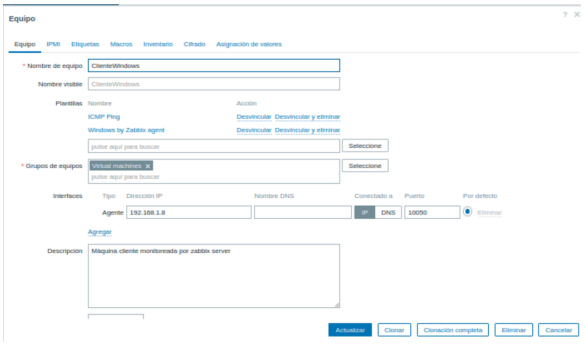

Figura 3 - Formulario para añadir un nuevo host/agente

Una vez agregado, el host comienza a enviar métricas y aparece en el dashboard.

4.4. Monitoreo mediante Widgets (Dashboards personalizados)

Los widgets que se utilizaron fueron disponibilidad de host, rendimiento de Ram y rendimiento de CPU:

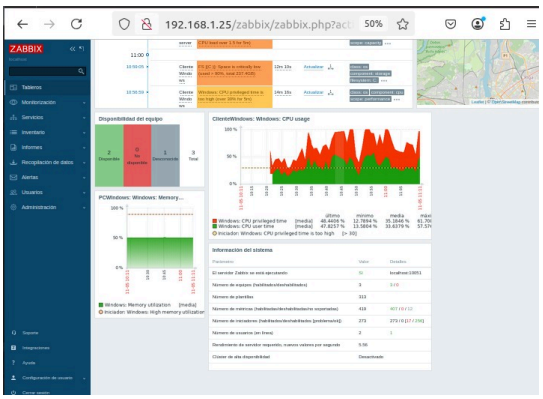

Figura 4 - Dashboards personalizado

4.5. Alertas y umbrales (Triggers)

Zabbix permite generar alertas en base a condiciones definidas.

Ejemplos configurados:

- CPU > 85% durante 3 minutos
- Latencia ICMP mayor a 100 ms
- Host sin respuesta durante 60 segundos

Cuando una condición se cumple, Zabbix genera un trigger de severidad:

- Information
- Warning
- High
- Critical

Además, envía notificaciones configuradas vía e-mail o mensajería (Gmail).

Figura 5 - Mensaje de alerta en Gmail

4.6. Uso del Sandbox dentro de la implementación

Antes de monitorear un nuevo host o aplicar una plantilla, se utilizó un entorno Sandbox (máquina virtual aislada) para:

- Instalar el agente y validar configuración.
- Probar templates sin impactar producción.
- Verificar compatibilidad de versiones.

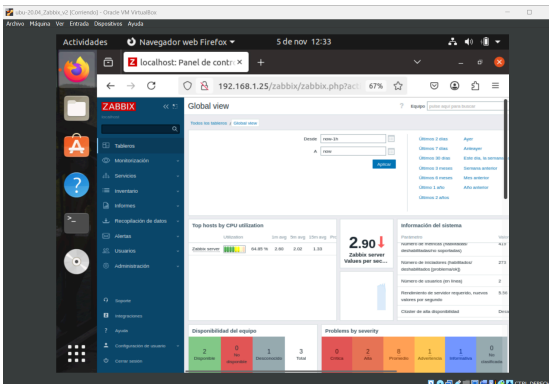

Figura 6 - Servidor en una máquina virtual "aislada"

Esto permitió detectar errores de configuración del agente sin afectar la infraestructura real, y aplicar en producción solo configuraciones validadas.

4.7. Resultados Obtenidos

Durante la implementación se logró configurar un servidor Zabbix y un host monitoreado dentro de un entorno virtualizado. El sistema permitió recolectar métricas de disponibilidad, uso de CPU, memoria y estado de servicios, representándolas mediante dashboards y gráficos históricos.

Las pruebas realizadas en el sandbox permitieron validar agentes, plantillas y triggers antes de su aplicación definitiva. Además, se simularon escenarios de falla, como sobrecarga de CPU, consumo elevado de memoria y pérdida de disponibilidad, verificando la generación de alertas ante condiciones anómalas.

Estos resultados muestran que la combinación entre un sistema NMS y un entorno sandbox de validación mejora la observabilidad de la infraestructura y reduce riesgos asociados a configuraciones no verificadas.

5. Conclusión y posibles mejoras

A partir de los resultados obtenidos, se concluye que la implementación de un sistema NMS basado en Zabbix, complementado con un entorno sandbox de validación, permite mejorar la observabilidad de la infraestructura de red y favorecer una gestión más preventiva de los incidentes. La propuesta permitió centralizar métricas, visualizar el estado de los recursos monitoreados y generar alertas ante condiciones anómalas, cumpliendo con el objetivo de disponer de una solución práctica para supervisar disponibilidad, rendimiento y estado operativo.

Asimismo, el uso del sandbox permitió validar agentes, plantillas, triggers y escenarios de falla antes de trasladarlos a un entorno productivo. Esto respalda el supuesto de trabajo planteado, ya que la validación previa contribuye a reducir riesgos asociados a configuraciones no verificadas, falsas alarmas o interrupciones no previstas. De esta manera, la combinación entre monitoreo NMS y sandbox fortalece el proceso de implementación y mejora la confiabilidad del sistema de monitoreo.

Si bien el proyecto fue desarrollado en un laboratorio controlado, los resultados permiten proyectar su aplicación en infraestructuras reales con mayor cantidad de dispositivos y servicios. Como mejoras futuras, se propone ampliar el número de hosts monitoreados, incorporar dispositivos de red mediante SNMP, integrar herramientas de gestión de logs o SIEM, automatizar respuestas ante eventos críticos y evaluar métricas cuantitativas como MTTD y MTTR en escenarios productivos.

6. Declaración sobre el uso de herramientas de inteligencia artificial

Durante la preparación de este trabajo, los autores utilizaron herramientas de inteligencia artificial generativa, específicamente ChatGPT y Gemini, con el fin de mejorar la redacción, organización, claridad del lenguaje y legibilidad del manuscrito. Asimismo, la herramienta fue utilizada como apoyo para la revisión de estilo, adecuación del formato académico, estructuración de secciones y mejora de la presentación general del contenido.

Tras utilizar esta herramienta, los autores revisaron, corrigieron y editaron el contenido generado según fuera necesario. En consecuencia, los autores asumen plena responsabilidad por el contenido final de la publicación, incluyendo sus objetivos, metodología, resultados, conclusiones y referencias bibliográficas.

7. Referencias

Fortinet. (s. f.). What is sandboxing? Sandbox security and environment. https://www.fortinet.com/resources/cyberglossary/what-is-sandboxing

Harrington, D., Presuhn, R., y Wijnen, B. (2002). An architecture for describing Simple Network Management Protocol (SNMP) management frameworks (RFC 3411). RFC Editor. https://www.rfc-editor.org/rfc/rfc3411

IBM Security. (s. f.). What is sandboxing? https://www.ibm.com/topics/sandboxing

Intriago-Cedeño, M. L., Carrera-Sánchez, F. A., Morejón-López, E., y Pita-Valencia, J. S. (2022). Evaluación de herramientas de monitoreo para mejorar la seguridad de la red de datos. CIENCIAMATRIA, 8(4), 1535-1553. https://doi.org/10.35381/cm.v8i4.1053

Levi, D., Meyer, P., y Stewart, B. (2002). Simple Network Management Protocol (SNMP) applications (RFC 3413). RFC Editor. https://www.rfc-editor.org/rfc/rfc3413

Panimalar, A., Tamilselvi, K., y Vani, K. (2018). Sandbox technology. International Research Journal of Engineering and Technology, 5(3). https://www.irjet.net/archives/V5/i3/IRJET-V5I3117.pdf

Quintero Martínez, M. I., y Tovar Balderas, S. A. (2021). Monitorización de infraestructura tecnológica como mejora en centros de datos. TIES, Revista de Tecnología e Innovación en Educación Superior, 3. https://doi.org/10.22201/dgtic.26832968e.2021.3.2

TechTarget. (2024, septiembre 30). The role of network sandboxing and testing. https://www.techtarget.com/searchnetworking/tip/The-role-of-network-sandboxing-and-testing

TestGrid. (s. f.). Sandbox environment for testing. https://testgrid.io/blog/sandbox-environment-for-testing

Velasco Briones, C. A. (2017). Implementación de un sistema de monitoreo de redes utilizando Nagios [Trabajo de titulación, Universidad Politécnica Salesiana]. Repositorio Institucional de la Universidad Politécnica Salesiana. https://dspace.ups.edu.ec/bitstream/123456789/13474/1/UPS-GT001824.pdf

Zabbix. (s. f.-a). Monitor a network switch or router with Zabbix. https://www.zabbix.com/documentation/current/en/manual/guides/monitor_switch

Zabbix. (s. f.-b). Network monitoring. https://www.zabbix.com/network_monitoring

Zhuma Mera, E., Oviedo-Armijos, O., Carreño-Sandoya, S., y Samaniego-Mena, E. (2025). Gestión y monitoreo con alertas en redes tipo campus usando software de código abierto. Ingeniería e Innovación, 13(2). https://doi.org/10.21897/rii.3999

Ziggaf Kanjaa, Z. (2018). *Diseño y despliegue de un sistema de monitorización de red para gestión de fallos y rendimiento* [Proyecto fin de grado, Universidad Politécnica de Madrid]. Archivo Digital UPM. https://oa.upm.es/53093/