Proyecto Final. MONITOREO DE INFRAESTRUCTURA DE RED CON NAGIOS (Mayo de 2023)

Zúñiga Pino Daniela, 2200625
Reina Sánchez Roxana, 2205049
Sandoval Delgado Juan José, 2190730
Casalins Orejuela Juan Sebastián 2201246

Departamento de Ingeniería
Universidad Autónoma de Occidente
Santiago de Cali, Valle

daniela.zuniga_pino@uao.edu.co
roxana.reina@uao.edu.co
juan_josn.sandoval@uao.edu.co
juan.casalins@uao.edu.co

Resumen – Este informe describe la implementación de un proyecto de monitoreo de infraestructura utilizando la herramienta Nagios en una red montada. Para ello, se utilizó Vagrant y VirtualBox para crear y gestionar máquinas virtuales, y se implementó Nagios para monitorear la disponibilidad y el rendimiento de la infraestructura de red. Se realizaron pruebas para verificar el monitoreo de equipos a través del dashboard de Nagios y la verificación de cambios en tiempo real del estado mostrado de los equipos. Los resultados principales muestran una mejora en la capacidad de monitorear y analizar la infraestructura de TI, lo que puede llevar a una mejor resolución de problemas y una mayor eficiencia en el mantenimiento y gestión de la red.

Palabras clave - Infraestructura de red, Monitoreo, Nagios, Virtualización.

Abstract – This report describes the implementation of an infrastructure monitoring project using the Nagios tool on a mounted network. To do this, Vagrant and VirtualBox were used to create and manage virtual machines, and Nagios was implemented to monitor the availability and performance of the network infrastructure. Tests were carried out to verify the monitoring of equipment through the Nagios dashboard and the verification of changes in real time of the displayed status of the equipment. The main results show an improvement in the ability to monitor and analyze the IT infrastructure, which can lead to better troubleshooting and greater efficiency in network maintenance and management.

Keywords - Network infrastructure, Monitoring, Nagios, Virtualization.

I. INTRODUCCIÓN

La infraestructura de red es fundamental en cualquier organización, y su disponibilidad y rendimiento son esenciales para garantizar una operación fluida de los servicios y aplicaciones de TI. En este contexto, el monitoreo de infraestructura se convierte en una actividad clave para mantener la disponibilidad y el rendimiento óptimo de la red. En este informe se describe la implementación de un proyecto utilizando la herramienta Nagios. Se montó una red real utilizando Vagrant y VirtualBox, y se utilizó Nagios para monitorear la disponibilidad y el rendimiento de los equipos en la red. Además, se realizaron pruebas para verificar el monitoreo de equipos a través del dashboard de Nagios y la verificación de cambios en tiempo real del estado mostrado de los equipos. Los resultados muestran la eficacia de Nagios como herramienta de monitoreo de infraestructura y su capacidad para mejorar la eficiencia y la resolución de problemas en la gestión de la red.

II. PROBLEMÁTICA

En el contexto de una infraestructura, es común encontrar una serie de desafíos que afectan la visibilidad y el control sobre el estado y rendimiento de los sistemas, dispositivos y servicios críticos. Algunos de estos desafíos incluyen:

A. *Fallos y tiempos de inactividad*

La falta de visibilidad adecuada puede dificultar la detección temprana de fallos en los sistemas y dispositivos críticos. Esto puede llevar a tiempos de inactividad no planificados que afectan la disponibilidad de los servicios y pueden ocasionar interrupciones en las operaciones. Es esencial contar con herramientas de monitoreo proactivas que permitan identificar rápidamente cualquier anomalía o tendencia que pueda indicar un posible fallo, de modo que se puedan tomar medidas preventivas o correctivas de manera oportuna.

B. *Degradación del rendimiento*

Sin una visibilidad adecuada, es difícil identificar y abordar problemas relacionados con la degradación del rendimiento en tiempo real. Los sistemas críticos pueden experimentar una disminución en su capacidad de respuesta, lo que afecta directamente la productividad y la experiencia del usuario final. Mediante el monitoreo constante del rendimiento de los sistemas y servicios, se pueden detectar cuellos de botella, identificar áreas de mejora y optimizar el rendimiento de manera proactiva para garantizar un funcionamiento fluido y eficiente.

C. *Gestión de capacidades*

La falta de visibilidad sobre las capacidades y recursos disponibles en una infraestructura puede llevar a un uso ineficiente de los mismos. Puede resultar complicado realizar una planificación adecuada y tomar decisiones informadas sobre la asignación de recursos. Con una mayor visibilidad, es posible monitorear y analizar los recursos disponibles, como el uso de la CPU, la memoria y el almacenamiento, lo que permite una gestión más efectiva de las capacidades. Esto incluye la identificación de posibles cuellos de botella, la optimización del uso de recursos y la planificación de futuras necesidades de escalabilidad.

III. OBJETIVOS

El objetivo principal de este proyecto es implementar un sistema de monitoreo de infraestructura de red utilizando la herramienta Nagios y las herramientas de virtualización Vagrant y VirtualBox.

El objetivo final es tener una herramienta que permita monitorear de manera efectiva la infraestructura de red y detectar y resolver problemas de manera proactiva antes de que afecten a los usuarios finales.

IV. REQUERIMIENTOS

La implementación del proyecto se divide en tres requerimientos principales: montar una red de equipos virtuales, utilizar un sistema para el monitoreo de la infraestructura de red, y mostrar los resultados de monitoreo a través de los dashboards que proveen herramientas como Nagios. Además, se realizan pruebas para verificar el monitoreo de equipos a través del dashboard de Nagios y la verificación de cambios en tiempo real del estado mostrado de los equipos.Para ello, se necesita una herramienta de virtualización como Vagrant y VirtualBox para crear el entorno de prueba.

V. PRUEBAS MÍNIMAS ESPERADAS

Para este proyecto de monitoreo de infraestructura, se han establecido al menos dos pruebas mínimas esperadas que deben realizarse para validar su correcto funcionamiento:

1) Verificación de monitoreo de equipos a través del dashboard que provee la herramienta seleccionada. Esta prueba debe demostrar que el sistema de monitoreo está funcionando correctamente y que se están recibiendo datos de los equipos monitoreados.

2) Verificación de cambios en tiempo real del estado mostrado de los equipos de acuerdo a cambios en su estado. Esta prueba debe demostrar que el sistema de monitoreo es capaz de detectar y notificar cambios en tiempo real en los equipos monitoreados, permitiendo una rápida identificación y solución de problemas.

VI. ALTERNATIVAS DE SOLUCIÓN

Nagios es una solución de código abierto de monitoreo de sistemas y redes que se ha utilizado ampliamente durante muchos años. Es conocido por ser confiable y escalable, y tiene una gran comunidad de usuarios y desarrolladores detrás de él. Nagios permite monitorear una amplia gama de recursos, incluidos servidores, dispositivos de red, aplicaciones y servicios, y puede generar alertas en tiempo real cuando se detectan problemas. Además, Nagios ofrece una gran cantidad de plugins y complementos que permiten una mayor personalización y extensibilidad

DataDog es una plataforma de monitoreo y análisis de logs en la nube que puede utilizarse para monitorear la infraestructura, las aplicaciones y los registros en tiempo real. DataDog ofrece una amplia gama de capacidades, como monitoreo de la infraestructura, monitoreo de la aplicación, análisis de registros y análisis de seguridad. Al igual que Nagios, DataDog tiene una amplia gama de plugins para monitorear diferentes tipos de servicios y aplicaciones, pero también puede monitorear los sistemas en la nube, como AWS y Google Cloud Platform.

Además, DataDog proporciona visualizaciones y alertas en tiempo real, así como integraciones con otras herramientas y servicios de terceros.

Zabbix es otra alternativa popular a Nagios, que se enfoca en el monitoreo de redes, servidores y aplicaciones. Zabbix utiliza una arquitectura cliente-servidor y cuenta con una amplia gama de características, incluyendo la detección de problemas, alertas en tiempo real, la capacidad de monitorear múltiples tipos de dispositivos y la capacidad de generar informes personalizados. Zabbix también proporciona la capacidad de monitorear sistemas operativos y servicios en la nube, como AWS y Azure.

Otra alternativa es Prometheus, una plataforma de monitoreo y alerta de código abierto que se enfoca en el monitoreo de servicios en contenedores. Prometheus proporciona una amplia gama de características, incluyendo el monitoreo de métricas, la alerta en tiempo real, la visualización de datos y la recuperación automática. A diferencia de Nagios, que utiliza plugins, Prometheus tiene una arquitectura basada en la exportación de métricas que puede ser utilizada para monitorear cualquier cosa que genere métrica

VII. NAGIOS

El sistema de monitoreo seleccionado fue Nagios, el cual es un sistema de monitoreo de código abierto que permite a los usuarios monitorear activamente sus sistemas y redes para detectar problemas y errores antes de que se conviertan en graves. Fue creado en 1999 por Ethan Galstad y ha sido una herramienta esencial para los administradores de sistemas durante más de 20 años [7]. Permite a los administradores de sistemas identificar y resolver problemas de rendimiento y disponibilidad antes de que afecten a los usuarios finales.

Puede monitorear cualquier cosa que tenga una dirección IP y utilice los protocolos de red habituales. Se utiliza comúnmente en entornos empresariales para monitorear redes complejas y garantizar la disponibilidad y el rendimiento de los servicios críticos para el negocio. Nagios se basa en plugins que se ejecutan en el servidor de Nagios o en los hosts que se están monitoreando y que proporcionan información sobre el estado de los servicios y recursos [10]. Nagios también tiene la capacidad de enviar alertas a través de una variedad de medios, como correo electrónico, mensajes de texto y llamadas telefónicas, en caso de que se produzcan problemas.

Ofrece una serie de ventajas para los usuarios que la utilizan. En primer lugar, Nagios es de código abierto, lo que significa que es gratuito y está disponible para que cualquier persona lo descargue y lo utilice. Esto hace que sea una opción atractiva para empresas y organizaciones que buscan una solución rentable para el monitoreo de sus sistemas y redes.

Además, Nagios es altamente personalizable y escalable, lo que significa que se puede adaptar a las necesidades específicas de cada usuario y que puede manejar grandes cantidades de datos sin problemas. Nagios también cuenta con una amplia comunidad de usuarios y desarrolladores que ofrecen soporte y actualizaciones regulares, lo que garantiza que la herramienta se mantenga actualizada y en constante evolución.

Otra ventaja de Nagios es su flexibilidad y compatibilidad con una amplia gama de sistemas operativos y herramientas de software, lo que permite su integración con otros sistemas de monitoreo y automatización. Nagios también ofrece una amplia gama de opciones de notificación y alerta, lo que garantiza que los usuarios puedan recibir alertas en tiempo real cuando se produce una falla en el sistema o la red.

VIII. HERRAMIENTAS A USAR

Para el proyecto de monitoreo de infraestructura, se utilizarán las siguientes herramientas:

1) Vagrant: Es una herramienta de código abierto para la creación y gestión de entornos de desarrollo virtualizados [2]. Permitirá crear una configuración de máquinas virtuales para simular una red de equipos.

2) VirtualBox: Es un software de virtualización de sistemas operativos de propósito general. Será utilizado para alojar las máquinas virtuales creadas por Vagrant.

3) Nagios: Es una herramienta de monitoreo de red que se utilizará para realizar el monitoreo de la infraestructura de red montada [1].

4) Apache: Es una herramienta poderosa y altamente configurable que permite alojar y entregar contenido web a través del protocolo HTTP.

2) PHP: Lenguaje de programación de código abierto diseñado especialmente para el desarrollo de aplicaciones web dinámicas. En este caso era un prerequisito de nagiost.

3) Vsftpds: Proporciona un servicio confiable y seguro para la transferencia de archivos entre sistemas, permitiendo a los usuarios acceder, cargar y descargar archivos a través del protocolo FTP. En este caso fue uno

de los servicios a monitorear de una de las maquinas cliente.

Cada herramienta tendrá una función específica dentro del proyecto, Vagrant permitirá la creación de un entorno virtual para montar la red de equipos, VirtualBox aloja las máquinas virtuales creadas por Vagrant, y Nagios permitirá el monitoreo de la infraestructura de red montada

IX. ESTRUCTURA POR IMPLEMENTAR

Para la implementación del proyecto de monitoreo de redes se llevará a cabo un proceso de aprovisionamiento a través de la herramienta Vagrant, la cual nos permitirá la creación y configuración automática de tres máquinas virtuales. Estas máquinas virtuales están constantemente enviando información para observar cómo se congestiona y cómo se descongestiona la red

Una vez que las máquinas virtuales estén en funcionamiento, se implementará Nagios como herramienta de monitoreo para la detección de problemas en tiempo real siguiendo su manual de instalación [6],

En la implementación, se definirán los puntos de monitoreo en las máquinas virtuales y se llevarán a cabo pruebas de carga constante en el sistema para observar cómo se congestiona y cómo se descongestiona para asegurarse de que el sistema de monitoreo funciona correctamente y se medirá el rendimiento de la red y la respuesta del sistema ante diferentes cargas. Esto permitirá evaluar la capacidad del sistema y detectar posibles cuellos de botella o problemas en la infraestructura.

En resumen, la implementación del proyecto de monitoreo involucra la configuración y aprovisionamiento de tres máquinas virtuales, dos clientes (cliente 1 con http y cliente dos con ftp), un monitor (maquina nagios).

X. DESARROLLO

Utilizando VirtualBox y Vagrant, se realiza su configuración y aprovisionamiento. incluyendo la instalación y configuración del software adicional como apache[9], php, ncpa y ajustes de red junto con el agente de Nagios en cada máquina virtual para que reporte el estado de la máquina y sus servicios al servidor de Nagios.

A. Configuración de Nagios

Nagios como se ha mencionado previamente es de utilidad para monitorear los servicios y recursos críticos en las máquinas virtuales a las cuales se instala Apache y Nagios junto al plugin nrpe, habilitando el firewall a Nagios, se hace uso del repositorio EPEL, sin necesidad de compilar el código fuente. Utilizando una máquina como servidor Nagios para monitorear a sí misma y a otras máquinas remotas. El proceso de instalación incluye Nagios Core, los plugins de Nagios y el plugin NRPE. Para instalar los plugins de Nagios, se instala el repositorio EPEL y luego usa el comando yum para instalar el paquete nagios-plugins-all[5]. Los plugins se prueban en la consola usando sintaxis de Nagios y argumentos necesarios. Para instalar Nagios Core, se instala el paquete nagios y activa y arranca el servicio nagios utilizando los comandos systemctl.

B. Pruebas de carga y monitoreo

Una vez que se han configurado todas las herramientas, se realizan pruebas de carga en el sistema para observar cómo se congestiona y cómo se descongestiona la red. Durante estas pruebas, se monitorea el sistema utilizando Nagios y se toman medidas en respuesta a las alertas generadas por el sistema de monitoreo.

C. Evaluación del rendimiento

Después de realizar las pruebas de carga y monitoreo, se analizan los resultados para evaluar el rendimiento del sistema y detectar posibles cuellos de botella o problemas en la infraestructura.

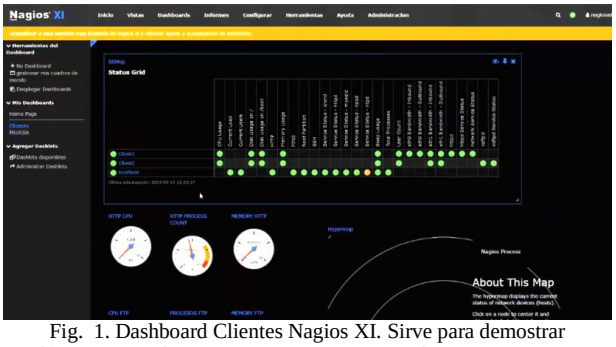

Fig. 1. Dashboard Clientes Nagios XI. Sirve para demostrar gráficamente y rápidamente el estatus de las máquinas a monitorear

XI. RESULTADOS DE PRUEBA

Una vez que se ha dado el vagrant up a las máquinas provisionadas y configurado nagios XI, se realizan pruebas de carga en el sistema para observar cómo se congestiona y cómo se descongestiona la red. En pocas palabras lo que se realizó para medir fue congestionar el servicio para así monitorearlo, Durante estas pruebas, se monitorea el sistema utilizando Nagios y se toman medidas en respuesta a las alertas generadas por el sistema de monitoreo como se muestra en la figura 2.

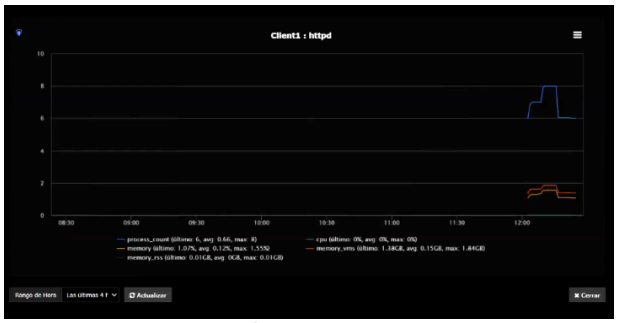

Fig. 2. Servicio http máquina cliente1. Sirve para demostrar gráficamente y rápidamente el estatus del servicio de una de las máquinas a monitorear

XII. CONCLUSIONES

En conclusión, la implementación del proyecto de monitoreo de red utilizando Vagrant, VirtualBox, y Nagios ha demostrado ser altamente efectiva para medir y monitorear el rendimiento de la red

Se pudo comprobar que el aprovisionamiento de las máquinas virtuales mediante Vagrant y VirtualBox fue una estrategia muy efectiva para la implementación del proyecto, ya que se logró implementar en poco tiempo y se pudieron replicar las configuraciones en diferentes entornos sin ningún problema.

La implementación de tres máquinas virtuales ha permitido realizar pruebas de congestión y de descongestión, lo que ha permitido analizar el comportamiento de la red en diferentes situaciones.

Nagios nos permitió monitorear la red en tiempo real y detectar posibles problemas de manera oportuna antes de que se convirtieran en fallas críticas.

En general, el proyecto de implementación y monitoreo de una red con Nagios fue una experiencia enriquecedora y exitosa que nos permitió obtener una comprensión más profunda de las redes, su rendimiento y los desafíos que se presentan al monitorearlas. Con las herramientas adecuadas y una estrategia efectiva, es posible implementar una red sólida y confiable y mantener un buen rendimiento.

XIII. REFERENCIAS

[1]. Nagios. (2021). Nagios Core documentation. [Online]. Disponible en: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/

[2]. HashiCorp. (2021). Vagrant documentation. [Online]. Disponible en: https://www.vagrantup.com/docs/

[3]. The CentOS Project. (2021). CentOS documentation. [Online]. Disponible en: https://www.centos.org/docs/

[4]. M. López. (2019). "Abrir puertos en CentOS 7". [Online]. Disponible en: https://ik4.es/abrir-puertos-en-centos-7/.

[5]. Nagios Enterprises. (2021). "Nagios Network Analyzer Manual Installation Instructions". [Online]. Disponible en: https://assets.nagios.com/downloads/nagios-network-analyzer/docs/Network_Analyzer_Manual_Installation_Instructions.pdf.

[6]. Cómo instalar. (2021). "Cómo instalar Nagios en CentOS 7" [Online]. Disponible en: https://comoinstalar.me/como-instalar-nagios-en-centos-7/.

[7]. North Networks. (2021). "¿Qué es Nagios?", North Networks. [Online]. Disponible en: https://www.north-networks.com/que-es-nagios/#:~:text=Nagios%20es%20un%20sistema%20de,mismos%20no%20sea%20el%20deseado.

[8]. Cómo instalar. (2021). "Cómo instalar PHP en CentOS 7". [Online]. Available: https://comoinstalar.me/como-instalar-php-en-centos-7/.

[9]. Cómo instalar. (2021). "Cómo instalar Apache en CentOS 7". [Online]. Available: https://comoinstalar.me/como-instalar-apache-en-centos-7/.

[10]. Nagios Enterprises. (2021). "About Nagios", Nagios. [Online]. Available: https://www.nagios.org/about/history/

[11]. Nagios Enterprises. (2021) "Configuring a Linux Server to Send Netflow Data to Network Analyzer", Nagios Network Analyzer Documentation. [Online]. Disponible en: https://assets.nagios.com/downloads/nagios-network-analyzer/docs/Configuring-A-Linux-Server-To-Send-Netflow-Data-To-Network-Analyzer.pdf.