Proyecto final
Telecomunicaciones 3
(10 de noviembre de 2021)

Iván C. Holguín, Miguel S. Rondón, Kevin A. Trujillo y Julián A. Vega

Facultad de ingeniería, Universidad Autónoma de Occidente
Cali, Colombia

ivan.holguin@uao.edu.co
miguel.rondon@uao.edu.co
kevin.trujillo@uao.edu.co
julian.vega@uao.edu.co

Abstract - A theoretical investigation was carried out on network monitoring systems focused on the detection of client computers and provision of services, in an internal network. After that, the solution to a theoretical problem was carried out where a Nagios service and two services were implemented.

Keywords - FTP, HTTP, SMP Nagios, Zabbix, Prometheus.

Resumen - Se realizó una investigación teórica sobre los sistemas de monitoreo de redes enfocados a la detección de equipos cliente y provisión de servicios, en una red interna. Posterior a ello se realizó la solución a un problema teórico donde se implementó un servicio Nagios y dos servicios.

***Índice de Términos* - FTP, HTTP, SMP Nagios, Zabbix, Prometheus.**

I. INTRODUCCIÓN

La compañía Realtek S.A. prestadora de servicios WEB y de transferencia de archivos, cuenta con una cantidad considerable de suscriptores que consumen sus servicios para usos y aplicaciones en su intranet; entre ellos la empresa fabricante de electrodomésticos ElectroVTRH S.A donde se cuenta con múltiples departamentos que requieren el uso de la página web de la compañía donde los clientes pueden realizar consultas y compras de los productos ofertados. Debido a la alta demanda de electrodomésticos en el segundo trimestre del año 2021, ElectroVTRH presentó problemas en su canal de información y ventas ya que la obtención de archivos y acceso mediante su página web no estuvo disponible durante horas críticas y sus servidores presentaron recalentamiento, generando grandes pérdidas económicas. La compañía presentó una queja formal a su proveedor de servicios. Realtek S.A. entonces, requiere un equipo de ingenieros que ayude a identificar las causas del problema, realizar un monitoreo de sus servicios y alertas para evitar futuras fallas.

II. MARCO TEÓRICO

A. FTP

Es un protocolo que permite la transferencia de archivos mediante una red TCP, la cual funciona entre computadoras conectadas a dicha red, en dónde su objetivo es el envío y recepción de datos, normalmente por los puertos 20 y 21. Este protocolo tiene como finalidad la transferencia de archivos a máxima velocidad de conexión, sin embargo no está sujeta a un buen complemento de seguridad de transmisión o de protección de datos ya que la información no está cifrada pero si cuenta con usuario y contraseña.[1]

B. HTTP

Es un protocolo que permite la solicitud de recursos, conocido por ser la base de la interacción de datos en el web conformado por una estructura cliente-servidor, es decir, los datos que sean solicitados van a llegar al destino de la instrucción inicial desde un navegador web, éstos pueden ser documentos HTML o la unión de documentos que especifiquen ya sea un texto, imágenes, videos, entre otros.[2]

C. SMTP

Es un protocolo simple de transferencia de correos electrónicos que es utilizado para la recepción y envío de correos electrónicos mediante protocolo TCP/IP, en el que normalmente se utiliza en conjunto con el protocolo de acceso a mensajes desde internet IMAP, el cual puede usarse para guardar posibles mensajes en un buzón del servidor para luego ser descargados y visualizados por el usuario. [3]

D. MONITOR DE RED

Un sistema monitor de red se apoya en los recursos de hardware y software que permiten hacer un análisis continuo de características internas del equipo, tal como el uso de ancho de banda, tráfico de datos, tiempo de actividad, entre otros. Los sistemas también tienen la capacidad de detectar dispositivos que se añaden a la red cómo también los qué influyen potencialmente en el uso de datos de esta, con la finalidad de interceptar fallas en la conexión que sean debido a sobre paso

en el límite de datos y qué afecten directamente al tráfico de estos. [4]

III. ANÁLISIS Y RESULTADOS

A. *Alternativas de solución*

1) *Nagios*

Es un software de código abierto cuya función es la de monitorizar redes incluyendo el estado físico de los equipos y los principales servicios que estos proveen. Entre sus características principales figura la monitorización de protocolos, HTTP, SNMP, SMTP, POP3, etc. Mientras que en los recursos de sistemas de hardware se tiene la carga del procesador, uso de los discos, memoria, estado de los puertos, etc. [5]

a) Ventajas

Puede escalar fuera del servidor, por lo que es más fácil de mantener. Por otro lado, es altamente personalizable e integrable con otros servicios. Es una plataforma muy poderosa para las redes de aplicaciones y la seguridad [8]. Tiene un sistema de detección automática para encontrar dispositivos conectados. Ofrece una gran cantidad de complementos adicionales y de creación propia. [9]

b) Desventajas

No tiene soporte en Windows ni MAC, Sus configuraciones deber hacerse en la maquina Nagios. No ofrece gráficos por defecto. Interfaz de configuración web desactualizada. [9]

2) *Zabbix*

Sistema de monitoreo enfocado a las capacidades de rendimiento y la capacidad de los servidores. Permite rastrear redes de equipos, aplicaciones y bases de datos. Diseñado por Alexei Vladishev, este sistema está diseñado con base a MySQL, PostgreSQL, SQLite, Oracle o IBM DB2 como base de datos. Mientras su backend está escrito en C y su front end está escrito en PHP, sus múltiples herramientas permiten monitorizar protocolos SNMP, TCP y ICMP, como también IPMI, JMX, SSH y telnet, usando parámetros de configuración personalizados. [6]

c) Ventajas

Tiene un tablero de instrumentos muy limpio y totalmente personalizable (mejor que Nagios) por lo que puede proporcionar información básica con mayor facilidad. Sus modificaciones pueden hacerse totalmente en línea. Posee una gran gama de gráficos asociados a los servicios listos para ser usados. Posee una interfaz web moderna. Ofrece soporte a una mayor cantidad de protocolos con respecto a Nagios. Posee un sistema de escalamiento en las notificaciones [9]

d) Desventajas

No se puede ejecutar la detección automática de forma predeterminada. No permite la integración de complementos personalizados. [9]

3) *Prometheus*

Es un sistema de monitorización de redes y de alertas. Con licencias de código libre lanzado en 2012 por la compañía SoundCloud posterior a ello se unió a Cloud Native Computing Foundation en el 2016. Este sistema en sus cuatro métricas implementa un contador direccionado a las solicitudes de tipo HTTP y HTTPS, mientras que su métrica de Calibre, puede establecer monitoreo a los estados físicos de los servidores como: disco duro y uso de memoria. Toda esta información se guarda en un Histograma cada 1ms, 10ms o 25ms. Finalmente, este tiene exportadores de datos compatibles con MySQL, Kafka, JMX, HAProxy y NGINX. [7]

a) Ventajas

Debido a su propia codificación es naturalmente integrable con casi todos los sistemas de la industria. Además de ser muy amigable visualmente y en su facilidad de uso. Es útil para monitorear la funcionalidad de la aplicación y es compatible con los principales sistemas operativos de computador [8]

b) Desventajas

El escalado de aplicaciones (incluido su marco de monitoreo) afecta a los datos de series en tiempo real, por lo que resulta en un aumento en los esfuerzos de mantenimiento e incremento en los costos del servicio. [8]

B. *Implementación*

Se decidió implementar una máquina Nagios para dar solución al sistema de monitoreo debido a que esta posee por defecto un servicio de detección automática de equipos lo cual ahorrará tiempo a la hora de realizar el monitoreo a toda la red y recursos de CPU.

1) *Procedimiento*

Basados en la documentación de NAGIO XI [10] se decidió implementar una máquina virtual con las herramientas de ORACLE VM tomando la plantilla ".ova" que se provee en la documentación. Posterior a ello, se detectaron de manera automática todas las máquinas de la red local que sirvieron para enfocar dos máquinas al monitoreo de servicios con tipo de transferencia HTTP y FTP.

Con el fin de evaluar el monitoreo se subió una página WEB ligera y posterior a ello se cargó una página más robusta. Mientras que para el monitoreo del estado físico de los equipos se implementó una herramienta de estresante mediante el packete de desarrollo stress. En el caso de la CPU se estreso 2 núcleos virtuales y en el caso de la memoria se intentó saturar por completo la partición por 120 ms.

2) *Evidencias*

1. Visitar el repositorio de desarrollo Github [11].

IV. DISCUSIÓN

Dado que las anteriores pruebas fueron exitosas en los diferentes equipos, se procedió a instalar graficas enfocadas al monitoreo en tiempo real mediante el dashboard. Estas herramientas a futuro podrán evidenciar y alertar del funcionamiento critico o en operación de los servicios que fresca la empresa, así como también detectar errores a futuro o detectar requerimientos de máquina que no se tengan en cuenta.

Entre los inconvenientes que se evidenciaron en la implementación del servicio de monitoreo, cabe resaltar que no se pudo monitorear el flujo de datos debido a que es necesario tener acceso al router físico y las llaves de acceso lo cual sería muy necesario en caso de que las necesidades de la empresa a nivel de seguridad requirieran de la alerta de una transferencia de datos o conexión de usuarios específicos a un computador.

V. Conclusiones

A pesar de que existen diferentes plataformas que permiten el monitoreo de redes todas tienen un énfasis que las hace significativas para las diferentes aplicaciones. En el caso de nagios, se encontró que es una herramienta que permite la detección de equipos y servicios en tiempo real de manera simple ya que es muy intuitiva para el usuario. Para el caso de este proyecto, fue muy eficiente.

Al no contar con una herramienta en Nagios que nos permitiera conocer de manera explícita el número de transferencias (FTP) o de solicitudes get (HTTP), se consideró el monitoreo de otro tipo de parámetros como el uso de memoria y CPU

Es importante contar con una herramienta de monitoreo cuando se tienen redes grandes, debido a que permite identificar y alertar de forma oportuna sobre posibles fallas en la disponibilidad y calidad de los servicios que se prestan de acuerdo a parámetros configurables por el administrador de la red, brindando la posibilidad de solucionar los problemas detectados antes de que se presenten de forma crítica.

Para el monitoreo de la CPU y memoria de las máquinas asociadas a Nagios, fue indispensable tener un indicador que nos permitiera visualizar el estado de estas dos variables. Sin embargo fue necesario descargar un paquete en los dispositivos monitoreados que brindara la posibilidad de modificar el comportamientos de estos parámetros sin la necesidad de generar procesos manualmente

VI. Referencias

[1] FTP: qué es y cómo funciona (xataka.com) . Tomado de https://www.xataka.com/basics/ftp-que-como-funciona

[2] Generalidades del protocolo HTTP - HTTP | MDN (mozilla.org). Tomado de https://developer.mozilla.org/es/docs/Web/HTTP/Overview

[3] IBM Docs. Tomado de https://www.ibm.com/docs/es/i/7.3?topic=information-smtp

[4] ¿Qué es el monitoreo de red? - Cisco . Tomado de https://www.cisco.com/c/es_mx/solutions/automation/what-is-network-monitoring.html

[5] Monitorización en tiempo real con Nagios - LIDER IT Consulting. Tomado de https://www.liderit.es/monitorizacion-en-tiempo-real-con-nagios/ [Articulo web]

[6] ¿QUE ES ZABBIX? herramienta de monitoreo de redes (quasarbi.com). Tomado de https://quasarbi.com/ZABBIX.html [Articulo web]

[7] Grafana y Prometheus para monitoreo de contenedores | Aplyca. Tomado de https://www.aplyca.com/es/blog/grafana-y-prometheus-para-monitoreo-de-contenedores

[8] Prometeo vs. Nagios | MetricFire Blog. Tomado de https://www.metricfire.com/blog/prometheus-vs-nagios/#strongWhen-to-use-Hosted-Prometheus-by-MetricFirestrong

[9] Comparación de Nagios y Zabbix: ¿cuál es mejor para la supervisión de la red? (dementium2.com). Tomado de https://dementium2.com/administrador-neto/comparacion-de-nagios-y-zabbix-cual-es-mejor-para/

[10] Nagios XI Resources. Tomado de https://www.nagios.com/resources/nagios-xi/

[11] Telecomunicaciones 3 Proyecto Final Tomado de https://github.com/miguel-rondon/Telecomunicaciones-3-Proyecto-Final/blob/master/Guia.md

Apéndice

Reconocimiento