USO DE LA HERRAMIENTA NAGIOS PARA EL MONITOREO DE UNA RED

Onofre Ruiz Eric [1*,] *Del Río Cobos Oscar A.* [2,] *Castro Valdivia Ricardo* [3]
[1,2,3] Universidad Tecnológica del Centro de Veracruz
eric.onofre@utcv.edu.mx

Contexto

Las redes dentro de una organización juegan un papel muy importante que se centra en mantener la comunicación entre las diferentes computadoras y dispositivos de comunicación que pertenecen a esta. Los requerimientos de comunicación de una empresa son cada día más demandantes por lo que se necesita aplicar escalabilidad en la red, es decir, agregar más componentes a través de la adquisición de equipo de cómputo o dispositivos intermediarios que conforman a esta tales como, routers o switches, aumento de sucursales, contratación de personal de TI (Tecnologías de la Información), así como la adición de interfaces de red. Por lo anterior, la red necesita crecer también para brindar servicios a los nuevos dispositivos que la integran y entre más dispositivos la conformen, la complejidad de su administración aumenta.

La administración de una red no es una tarea fácil porque cuando se presenta una falla puede resultar complicado encontrar la causa raíz que lo genera, por lo que es importante darle soporte, así como monitorear su funcionamiento. El monitoreo en términos de redes es un acto de supervisión, de recuperación de información y verificación de la operatividad de los recursos que componen a una red. Este permite la identificación y resolución de problemas en términos de disponibilidad, capacidad, latencia de comunicación, utilización de recursos para cada aplicación, detección de fallas, cuellos de botella, y en algunos casos la resolución automática. Los aspectos anteriormente descritos, permiten que el administrador de red tome decisiones informadas sobre la utilización de los recursos de la red para justificar la adquisición de nueva infraestructura o mejoras en esta para eliminar cuellos de botella o problemas constantes que la red esté presentado.

Generalmente, las herramientas de monitoreo de red muestran la información y el estatus de los componentes de esta a través de interfaces gráficas que permiten al administrador identificar rápidamente la salud de la red; también suelen enviar alertas y notificaciones cuando un incidente se presenta. Si estas se implementan adecuadamente pueden ayudar al administrador de la red a decidir si la infraestructura es la adecuada o se deben hacer cambios, así como si se necesita adquirir equipo nuevo porque el anterior ocasiona que el servicio brindado a sus usuarios se vea degradado en términos de calidad. Aunque existen diferentes herramientas que pueden ayudar al administrador con diversas tareas de administración y monitoreo, éste debe conocer las características de cada una, analizar sus ventajas y desventajas, y con base en la identificación de los problemas que se presentan en la red y en sus necesidades, seleccionar la herramienta más idónea.

En este sentido, una herramienta para monitoreo de red se vuelve un recurso muy importante si se requiere tener un control adecuado de las métricas de la red, el nivel de servicio, la disponibilidad de esta, entre otras. Esta puede ser definida como una combinación basada en hardware y software que supervisa su funcionamiento de extremo a extremo recopilando datos sobre una amplia gama de métricas de su rendimiento, tales como, el ancho de banda, la latencia, la capacidad de respuesta y el uso del CPU de los dispositivos que la conforman.

La elección de la herramienta adecuada para monitoreo de la red, puede ser una decisión complicada si no se conocen a fondo las necesidades de la red o no se tiene una idea clara sobre la utilidad de esta. Por ello, los administradores de red deben mantener una visión amplia y detallada de sus componentes o servicios de red en una interfaz intuitiva y amigable que genere una variedad de reportes y que pueda ser personalizable.

Las opciones existentes con respecto a herramientas para monitorear una red son diversas, pasando por las comerciales y las de código abierto. Estas últimas llaman la atención de muchos administradores por sus características, las ventajas que ofrecen, su adaptabilidad y porque no representan un costo elevado en términos económicos, pero si en términos intelectuales porque muchas de estas herramientas funcionan bien cuando son instaladas en sistemas operativos de la misma categoría, lo cual resulta un poco más difícil para el administrador si no tiene conocimientos suficientes en ello. Por otro lado, las comerciales también ofrecen diversas ventajas con respecto a su facilidad de uso e implementación, sin embargo, estas representan un obstáculo para el administrador por su costo, soporte o gastos extras que estas representan. Los costos se han convertido en un factor importante porque los departamentos de TI buscan agilizar los presupuestos operativos.

Es importante que no se confundan los términos código abierto, software libre y software gratuito. El primer término, se refiere a un software con código fuente que está disponible públicamente bajo una licencia que otorga a los usuarios el derecho de estudiar, cambiar y distribuir el software como lo deseen. El segundo, se refiere al software que respeta la libertad de los usuarios y la comunidad, es decir, que los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Finalmente, el tercero es un software que está disponible sin costo alguno; a diferencia del software libre y del software de código abierto, el software gratuito no hace referencia ni enfatiza la libertad de ninguna manera.

La cantidad de herramientas disponibles es abundante, sin embargo, en el presente trabajo se describirá la herramienta de código abierto “Nagios”, la cual es reconocida por su rendimiento y flexibilidad.

Notas

En el presente artículo se dará a conocer la herramienta “Nagios” para monitorear una red y optimizar su funcionamiento. La importancia de la utilización de esta herramienta radica en que los administradores de red pueden identificar problemas y puntos críticos porque ofrece complementos que ayudan a supervisar el funcionamiento de los dispositivos intermediarios y finales de la red tales como, routers, swtiches, puntos de acceso, servidores, protocolos de red y la mayoría de los componentes de la infraestructura. También, mediante el uso de un mapa de la red a través de vistas multiusuario y de usuarios específicos en una interfaz web, el administrador puede verificar la eficiencia de esta y consultar información detallada.

Uno de los servicios más sobresalientes que brinda esta herramienta es el envío de alertas cuando uno de los componentes de la infraestructura de red falla, es decir, este notifica y genera información del error para que el administrador conozca la falla, la verifique y pueda dar solución. Las alertas se pueden presentar en tres colores: rojo, amarillo y verde. Cuando la alerta presentada es de color rojo con la descripción “Critical”, significa que el dispositivo debe ser atendido de inmediato porque el fallo está ocasionando pérdidas de conexión en la red, así como la red se encuentra vulnerable a ataques. Si la alerta es de color amarillo con la descripción “Warning”, significa que se están presentando retardos en la red, y si no se presenta problema alguno, el color de la alerta será verde, lo que significa que ese segmento de la red está funcionando correctamente.

Otro servicio que ofrece Nagios es la planificación de actualizaciones en la red antes de que fallen los componentes de esta. Este servicio genera una evaluación general de la infraestructura e identifica las posibles actualizaciones a realizar para brindar un servicio sin fallas o pérdidas en la conexión. Asimismo, esta herramienta puede solucionar algunos problemas de red por sí misma, es decir, que cuando Nagios detecta un problema en un dispositivo de la infraestructura lo reinicia automáticamente, y en caso de que se presente una nueva falla en ese dispositivo emite una alerta.

Para mejorar el funcionamiento de esta herramienta de monitoreo es necesaria la instalación de los denominados “Plugins”. Estos procesan argumentos de línea de comandos, así como supervisan los componentes de red devolviendo los resultados a Nagios Core; este determinará el estado del resultado generando la alerta correspondiente en caso de exista algún fallo o en caso contrario, no lo notificará.

Además, Nagios cuenta con algunos complementos cuya instalación es opcional. Cada uno de estos cumplen con una función diferente dentro del monitoreo de la infraestructura de TI. Por ejemplo, NagVis es uno de los complementos de Nagios más elegante que permite la visualización de los componentes de la red a través de la creación de mapas de esta, ayudando a identificarlos más rápidamente, y ofreciendo una organización personalizada de acuerdo con lo que los administradores de red deseen visualizar. Es un complemento que genera el número de mapas que el administrador de red necesite. NagVis cuenta con una interfaz web propia independiente a la de Nagios, pero este trabaja con la configuración realizada en la herramienta principal (Nagios), es decir, que los dispositivos registrados en esta herramienta estarán disponibles para la creación de mapas en NagVis.

Otro complemento destacable es "PNP4Nagios". Este es mayormente es utilizado para generar estadísticas del rendimiento de los componentes de la infraestructura de red. La función de este complemento es graficar en tiempo real el rendimiento los componentes tomando en cuenta la configuración que se realizó en cada uno de ellos, siendo el más común el denominado "Ping". Este comando es necesario para la comunicación entre los componentes de red que ayuda a graficar el funcionamiento de esta analizando la transmisión de paquetes. Cuando un paquete es enviado por el emisor su integridad es del 100%, pero en el transcurso del envío, pueden existir pérdidas por distintos factores tales como, tráfico en la red, colisiones, entre otros. Si alguno de los factores anteriormente descritos se presenta, este complemento entra en función graficando la integridad de los paquetes en transcurso o su estabilidad. Lo anterior ayuda a que la calidad de servicio de la red mejore.

Finalmente, la organización, la eficiencia y eficacia, la detección de fallas, el aumento de seguridad y la mejora de la calidad de servicio de la red son factores importantes para una empresa. Mediante la utilización de esta herramienta de monitoreo y sus complementos se pueden alcanzar muchos objetivos en términos de operatividad en la red, así como se pueden solucionar diversos problemas que se presenten en su infraestructura. Esta tarea se hará más fácil si se realiza el etiquetado de los dispositivos para que se registren en Nagios y se puedan localizar por medio de su ubicación física y dirección lógica. Cabe hacer mención que tanto la herramienta Nagios como sus complementos son totalmente gratuitos.

Los resultados que se pueden obtener con la utilización de Nagios varían de acuerdo con las necesidades de cada empresa. Sin embargo, debido a que es esta herramienta tiene interfaces muy amigables que generan mapas de la red que pueden ser comprensibles para cualquier persona que no está familiarizada con el área, ayudarán a identificar problemas en esta de acuerdo con las alertas que emite. Además, esta permite que el administrador tome decisiones e implemente mecanismos de mantenimiento y seguridad que ayuden a que la red funcione correctamente disminuyendo su vulnerabilidad y pérdidas en el envío de paquetes.

Referencias

Foundation, F. S. (18 de Junio de 2017). *¿Qué es software libre?* Obtenido de https://gnu.org/philosophy/free-sw.es.html

Gartner. (2008). *Open Source Survey*. Obtenido de http://gartner.com/technology/home.jsp

Gómez, J., & Baños, R. (2006). *Seguridad en Sistemas Operativos Windows y Linux.* España: RA-MA.

Gómez, J., Padilla, N., & Gil, J. (2006). *Administración de Sistemas Operativos Windows y Linux: Un Enfoque Práctico.* Madrid, España: RA-MA.

Hernantes, J. (2015). *IT Infrastructure- Monitoring Tools. Computing in Science and Engineering.* IEEE Software.

Linge, J. (15 de Marzo de 2012). *PNP4Nagios*. Obtenido de http://docs.pnp4nagios.org/es/pnp-0.6/start

Nagios Enterprises. (2017). Obtenido de Nagios Core User Manual: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/toc.html

Nagios Enterprises. (2017). Obtenido de Monitoring Routers and Switches: https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/monitoring-routers.html

Nagios Enterprises. (2017). Obtenido de Nagios Network Analyzer: https://nagios.com/products/nagios-network-analyzer/

Nagios Plugins Documentation. (2013). *Nagios Plugins Documentation*. Obtenido de NagVis 1.8 Documentation: https://nagios-plugins.org/documentation/

NagVis Documentation. (04 de 03 de 2019). *NagVis*. Obtenido de http://docs.nagvis.org/1.8/en_US/index.html

Porter, P. G. (2013). *Monitoring Network Devices with Nagios*. Obtenido de https://paulgporter.net/2013/01/30/network-monitoring-nagios/

Stallings, W. (2004). *Comunicaciones y Redes de Computadoras.* Madrid: Pearson Education.