TiES Revista de Tecnología e Innovación en Educación Superior

MONITORIZACIÓN DE INFRAESTRUCTURA TECNOLÓGICA COMO MEJORA EN CENTROS DE DATOS

Manuel Ignacio Quintero Martínez
Sergio Anduin Tovar Balderas

http://www.ties.unam.mx/

Fecha de recepción: septiembre 23 de 2019 • Fecha de publicación: abril de 2021

Abril 2021 • Volumen 2 • Número de revista 1 • ISSN en trámite

Abril 2021 • Volumen 2 • Número 1 • ISSN en trámite
http://www.ties.unam.mx/

MONITORIZACIÓN DE INFRAESTRUCTURA TECNOLÓGICA COMO MEJORA EN CENTROS DE DATOS

Resumen

La infraestructura tecnológica en los centros de datos es una parte vital y debe estar disponible la mayor parte del tiempo para sus usuarios. Para ello muchas actividades se involucran. Una de ellas es la monitorización, que se vuelve crítica tanto en la prevención como en la atención a incidencias de cómputo. En este artículo se presentan algunos elementos a considerar para la incorporación de sistemas de monitorización, así como una breve descripción de Nagios, una de las opciones de licencia libre más populares.

Palabras clave:
Monitorización, infraestructura tecnológica, disponibilidad, Nagios.

AVAILABILITY IMPROVEMENT IN DATA CENTERS USING TECHNOLOGICAL INFRASTRUCTURE MONITORING

Abstract

Technological infrastructure in data centers is a vital part and should be available most of the time for its users, and it involves many activities, one of them is monitoring, which becomes critical, both in prevention and in the attention to computer incidents. This article presents some elements to be considered to incorporate monitoring systems, as well as a brief description of Nagios and some of its capabilities, one of the most popular free license monitoring systems.

Keywords:
Monitoring, technological infrastructure, availability, Nagios.

TiES Revista de Tecnología e Innovación en Educación Superior

Monitorización de infraestructura tecnológica como mejora en centros de datos
Manuel Ignacio Quintero Martínez
Sergio Anduin Tovar Balderas
Abril 2021 • Volumen 2 • Número 1 • ISSN en trámite
http://www.ties.unam.mx/

MONITORIZACIÓN DE INFRAESTRUCTURA TECNOLÓGICA COMO MEJORA EN CENTROS DE DATOS

Introducción

La infraestructura tecnológica en un centro de datos involucra muchos elementos, como: sistemas (eléctrico, aire acondicionado), seguridad (física y lógica), equipos (servidores, telecomunicaciones) y su ubicación, estantes, organizadores, etcétera.

Uno de los objetivos de un centro de datos es ofrecer servicios con el empleo de infraestructura tecnológica. La disponibilidad de los servicios es uno de los principales requisitos y preocupaciones, ya que deben estar a la mano la mayor parte del tiempo o cuando son requeridos. Por ello es importante identificar cambios en los servicios que se ofrecen en el centro de datos y en la infraestructura tecnológica asociada a los mismos, para atender de una manera más precisa los eventos que puedan presentarse. Aquí toma relevancia la implementación de al menos un sistema de monitorización.

Un sistema de monitorización puede entenderse como uno o más sistemas que de manera conjunta, dentro de la infraestructura tecnológica, tienen la función de vigilar la presencia de fallas en otros sistemas [1].

Los sistemas de monitorización pueden ayudar a detectar y solucionar problemas en la infraestructura y los servicios que soportan, antes de que se produzca una crisis. Esto se logra cuando el sistema de monitorización envía una alerta de patrones establecidos, como posibles desencadenantes o causantes de problemas [1].

Así, se puede establecer que la monitorización de la infraestructura tecnológica busca, en forma general, tener un medio de vigilancia constante que indique la disponibilidad y la utilización de recursos, haciendo posible la identificación de variaciones no deseadas y posibles errores en el futuro, o bien, que podrían estar en proceso y requieren atención.

Sin embargo, esta no es la única función que cumplen los sistemas de monitorización. Entre sus bondades está la realización de análisis de datos históricos o mostrar tendencias de los elementos que se monitorizan. Es significa que cuando se presentan problemas a lo largo del tiempo, se emplean los datos recabados del equipo, servicio y recursos utilizados, para la proyección, la renovación o la actualización de la infraestructura en un futuro. Además, el análisis de problemas recurrentes permite encontrar su causa para resolverlos. Todo esto, en conjunto con planes de acción, permite mejorar los niveles de servicio de un centro de datos.

Desarrollo

Factores para la implementación de un sistema de monitorización

Los administradores de TI que cuentan con un sistema para monitorizar la infraestructura tecnológica en un centro de datos, tienen muchas ventajas: desde identifi-

car cuando un equipo pierde conectividad o un servicio se detiene, hasta tener datos sobre la utilización de recursos en una fecha y hora específicos. Todo dependerá de la granularidad con la que se estén revisando los equipos. En general, no existe una implementación estándar que solucione todas las necesidades en diversas organizaciones (por ejemplo, las instituciones de educación superior), esto debido a sus características particulares y la adecuación específica para cada una. Por tal motivo, a continuación se plantearán algunos elementos importantes para evaluar y diseñar su implementación.

Monitorización por orden de importancia

David Josephsen menciona que "sin un entendimiento claro de los sistemas considerados críticos, cualquier iniciativa de monitorización estará condenada al fracaso" [1]. Por ello se vuelve importante identificar cuáles son los activos que sería interesante monitorear antes de evaluar, instalar y configurar cualquier herramienta que ayude a revisar el estado de los equipos, debido a que no todos tienen la misma relevancia dentro de la organización. Por lo tanto, priorizar y ordenar los activos (equipos y servicios) es el primer paso. De esta manera se podrán establecer objetivos, debido a que es imposible vigilar todos los puntos de todos los recursos tecnológicos. Al menos en un principio, serán los de mayor criticidad los que deberían ser monitorizados constantemente.

Generación de información, no de datos

Se debe establecer una diferencia entre dos términos usados comúnmente: *datos e información*. Un *dato* es un valor que representa algo, mientras que *información* es un conjunto de datos que tienen un proceso y significado para su destinatario [2]. Es importante mencionar que un sistema de monitorización puede generar una gran cantidad de datos. Por tal motivo, se vuelve esencial establecer cuáles serán realmente información en términos de disponibilidad. No todos son realmente útiles e, incluso, pueden generar falsos positivos.

Como ejemplo, se puede pensar que, si el procesamiento de un servidor se encuentra por encima del 80%, podría generar una alerta a los administradores para que tomen acciones, incluso más si se da a las 03:00 a.m. de un lunes. Sin embargo, esto podría ser diferente si este servidor procesa calificaciones o estados de cuenta bancarios, y son los lunes a esa hora cuando se realizan procesos de consolidación o respaldo. Ese sería seguramente un parámetro normal y esperado. Esto deja ver como la información del sistema de monitoreo y adecuarlos a los sistemas en que son implementados permite identificar estos casos para saber si se trata de un proceso normal o es una desviación que se necesita revisar.

Depuración de la información

Los sistemas de monitorización buscan generar información, no sólo datos. Sin embargo, es importante que los administradores la analicen para mejorar la disponibilidad, contextualizándola y ajustándola a la realidad y el contexto de la organización.

> Retomando el caso anterior, los administradores no configuran sus alertas de forma granular, estableciendo un día y hora para recibir notificaciones, a pesar de saber, de antemano, que sus equipos realizarán un proceso que incrementará el uso de CPU en el equipo a las 03:00. Por lo tanto, recibirán alertas cuando se sobrepase el valor establecido en la configuración. Esto les permitirá, en cualquier otro momento, saber si existe una sobrecarga anormal en los equipos. Seguramente se acostumbrarán a tener demasiadas alertas, y como podría llegar a ser entendible desde su perspectiva, las silencian o las borran en automático. Esto puede ser un problema en este periodo de tiempo, porque si en ese momento hay una falla eléctrica que apague de forma no planeada el servidor, no se darán cuenta de ello hasta que los usuarios comiencen a tener problemas al acceder al servicio.

Una mala implementación conllevará a una saturación de alertas, de tal forma que se dejará de tomar acciones cuando suceda un evento. El exceso de notificaciones es tan poco útil, como su inexistencia, ya que después de algún tiempo todas las alertas comenzarán a ser ignoradas, se dejarán de tomar acciones (si es que alguna vez se comenzaron a realizar) y de forma regular se tratarán como falsos positivos [1].

Algunos sistemas de monitoreo permiten programar los días y los horarios de revisión, así como especificar ventanas de mantenimiento para evitar la generación de alertas, como notificaciones por correo electrónico.

Implementación desde el ser y no el deber ser

Sabemos que cada organización cuenta con su propia infraestructura y que cada una de ellas se adapta, crece y se modifica a partir de las necesidades, eventos y cambios. Por esta razón, al implementar un sistema de monitorización, se debe comenzar a partir de los elementos conocidos de la infraestructura, para familiarizarse con éste y saber el significado de las alertas emitidas, esto para conocer el comportamiento normal de los sistemas a monitorizar. Hacerlo en forma inversa, informará que los sistemas no se adaptan a lo deseado, teniendo métricas y parámetros que, en el mejor de los casos, mostrarán una falla constante, cuando en realidad es su comportamiento normal. En esto Josephsen menciona que "toda herramienta de monitorización requiere una fuerte inversión de tiempo en la personalización, antes de que comience a solucionar problemas" [1].

Diseñar conforme a la arquitectura existente y futura

Uno de los puntos más importantes al diseñar una estrategia de revisión de los equipos, se encuentra en posicionar el sistema de monitoreo, y si el procesamiento será centralizado (ejecutado por quien monitoriza) o descentralizado (realizado por quienes son monitorizados).

En la figura 1 se aprecia un sistema de monitoreo que es capaz de revisar los servidores ubicados en la locación A y B. La locación B puede ser un cuarto de telecomunicaciones alterno, con una ubicación geográfica distinta a la primera.

El mejor lugar para posicionar un sistema de monitorización dependerá de diversas características, que podrían depender de los siguientes puntos:

- **Activos identificados como críticos.** Sin duda, deben ser identificados aquellos equipos que soportan las operaciones de la organización, por lo que deben tener mayor prioridad para ser monitorizados. Así, si los equipos o servicios más importantes se ubican en sólo una locación, podría pensarse en poner en este lugar el sistema de monitorización.
- **Ancho de banda entre locaciones.** Si la conectividad es limitada, sería poco viable establecer el monitoreo desde un solo punto, por lo que debe de ponderarse el ancho de banda utilizado para monitorizar, de tal forma que éste no interfiera en las operaciones regulares de la organización.
- **Resultados de monitoreo en tiempo real.** Si ambas locaciones dependen de equipos diferentes, es probable que se pueda establecer la revisión de equipos desde cada locación, sólo para quienes solucionarán los problemas locales.
- **Enlace de conexión deja de funcionar.** En ocasiones es preferible tener planes de contingencia. Por ejemplo, tener una estructura jerárquica, donde los

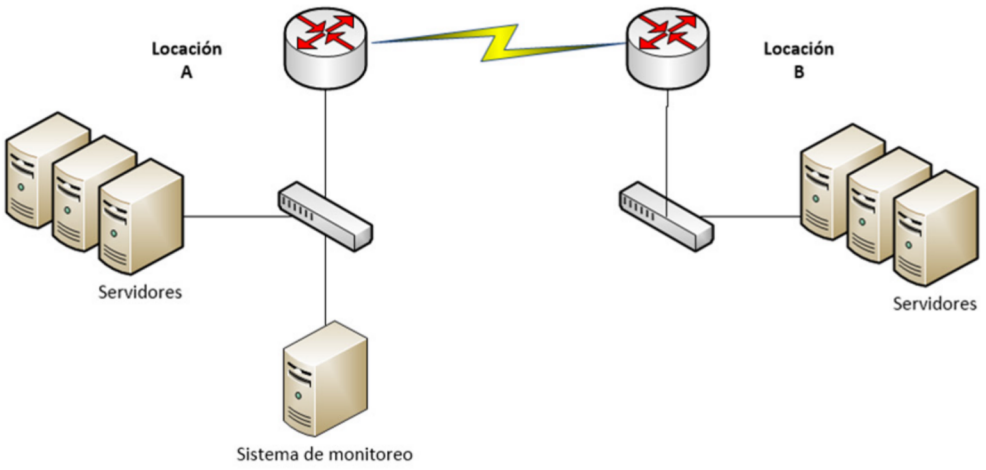

Figura 1.
Locaciones remotas. 2019. Fuente: elaboración propia.

equipos de monitorización locales reporten a uno de consolidación, de tal manera que permita una visualización de la mayor parte de la infraestructura, para que en caso de que algún enlace falle, se pueda notificar por otro medio (por ejemplo, por una llamada telefónica).

- **Crecimiento del sistema de monitorización.** Uno de los grandes problemas que hemos visto en la implementación de sistemas de monitorización, es que comienza como un proyecto pequeño, crece de forma exponencial y los recursos actuales se vuelven insuficientes, o bien, el diseño no permite que se escale, teniendo que implementarse más de un sistema no coordinado, viéndose dificultada la unificación de la información. Puede incluso, pensarse en un sistema distribuido desde el primer nodo.
- **Recursos destinados a la monitorización**. Si se tienen recursos limitados para la monitorización, se asumirá que habrá posibles puntos de fallos. Asimismo, se debe diseñar una estrategia, teniendo como parámetro de decisión qué tendría menor impacto.
- **Administrador del sistema de monitorización.** Si se cuenta con personal dedicado a la monitorización, se puede establecer un monitoreo más detallado para cada equipo y servicio. En algunas organizaciones educativas sucede que esta tarea se agrega a un equipo de soporte ya existente, que deberá optimizar y afinar el sistema de monitoreo para requerir el mínimo de su intervención, ya que cuando se produzca alguna alerta se tendrá la certeza de que algo sucedió y necesita atención.

Los puntos anteriores permitirán considerar diferentes implementaciones basadas en la red de datos, recursos y activos de la organización, así como determinar si se utilizará una base de datos centralizada o distribuida, ya que dependerá de si habrá uno o más sistemas de monitoreo.

Algunos aspectos de seguridad

Finalmente, hay que tomar en cuenta que la información reportada, o que generan estos sistemas, describe el comportamiento de la infraestructura. Por ello es importante protegerla. Algunas recomendaciones específicas de seguridad para los sistemas de monitoreo en general, son:

- Cifrar la información entre el sistema de monitorización y el equipo que reporta.
- Los clientes de monitoreo o agentes se instalan en los equipos que van a ser revisados. Procesan bitácoras y obtienen información del equipo donde se instaló, misma que es enviada al sistema de monitoreo. Cuando se usan clientes en los equipos, se recomienda asignar los permisos necesarios para su funcionamiento, de tal manera que solo puedan realizar las tareas para las que están diseñados. Con ello se reduce la superficie de ataque.
- En caso de realizar el monitoreo en forma centralizada, en la medida de lo posible debe hacerse al menor número de puertos o servicios posibles. Algunos sistemas, como Nagios, permiten establecer revisiones que simulen ser la acción de un usuario. Por ejemplo, puede inspeccionar el comportamiento de un sitio web, y con ello vigilar el sistema web, la base de datos de la que hace uso y el sistema de autenticación en un solo paso, obteniendo de cada equipo el uso de la memoria, el procesador y el número de conexiones [3].
- Es posible que existan alertas que requieran información complementaria a la reportada por el sistema de monitorización. Se puede vincular con otras herramientas, como un SIEM (*Security Information and Event Management*, por sus siglas en inglés). Estos sistemas permiten recopilar y correlacionar eventos e incidentes de diversas fuentes, para poder realizar predicciones.

Nagios como herramienta de monitorización

Nagios es un sistema de licencia libre, modular y escalable, que permite personalizar el tipo de datos que se desea revisar. Su elemento primario es Nagios Core, que puede entenderse como el sistema base. Permite a su vez realizar la monitorización, tanto por plugins como por módulos [4].

Un *plugin* es un archivo ejecutable o programa, que hace una tarea de revisión o reporte específico en los equipos remotos, que reportan hacia el sistema de monitorización, siendo ejecutado por un componente llamado NRPE (*Nagios Remote Plug-in Executor*). Un tipo de *plugin* que merece una mención especial es *End-to-End* (E2E), que hace posible la realización de acciones automatizadas y actuar como lo haría un usuario normal, ampliando las capacidades de monitorización desde Nagios mismo [3].

Por otro lado, los módulos dependen de NEB (*Nagios Event Broker*), un *API* (Interfaz de Programación de Aplicaciones, por sus siglas en inglés) que permite modificar, complementar o crear flujos de trabajo a partir de los resultados de los diferentes plugins implementados. Ambos suelen ser desarrollados por la comunidad de Nagios, pero la flexibilidad y la escalabilidad de este sistema permite crear uno ajustado a las necesidades específicas de cada organización [5].

La configuración de Nagios suele ser muy moldeable y, en principio, sencilla en su estructura. Depende de archivos de texto, modificables desde cualquier herramienta básica de edición, sin embargo, éstos pueden volverse más complejos conforme se agregan especificaciones o arquitecturas de red al mismo sistema [4]. La puesta a punto de los mismos archivos puede ser una tarea lenta, que requiere de una buena cantidad de ensayos para ser exitoso. Por otra parte, es importante respaldar la configuración y la información recabada por el sistema de monitoreo.

como NagiosPHP, que permite ampliar y modificar la original, extendiendo las capacidades de visualización de Nagios [4].

Por defecto, Nagios cuenta con un mapa de infraestructura (el cual debe personalizarse como se muestra en la figura 3), en el que pueden visualizarse los hosts y los servicios monitoreados, grupos de host (*hostgroups*), grupos de servicios (*servicegroups*), reportes de disponibilidad, alertas, notificaciones y bitácoras de eventos [6]. En la *figura 3* se muestra un ejemplo de personalización en la visualización de recursos en un sistema Nagios. Las imágenes permiten identificar diversos equipos, como sensores de red que utilizan Snort [19] y equipos de red (conmutadores y puntos de acceso inalámbrico, entre otros).

La implementación de este sistema suele ser sencilla, una vez que se ha diseñado una estrategia y se tiene claro qué es lo que se desea monitorizar [11].

Algunas de las características adicionales en la infraestructura de Nagios, son [3]:

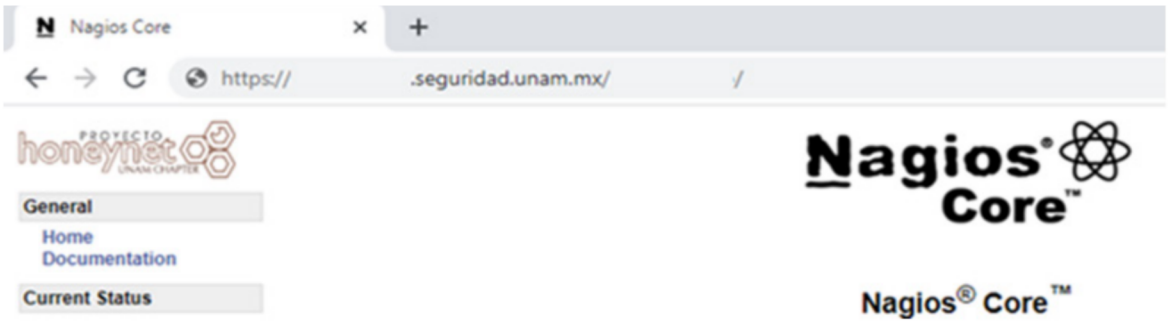

Figura 2.
Nagios Core, "Personalización de nagios cores," 2019. [Fotografía]. Disponible en: Sistema Nagios [Consultado en septiembre 20, 2019].

Un último elemento se encuentra en la interfaz web de visualización. Esta interfaz se basa en tecnología *CGI* (Interfaz de Entrada Común, por sus siglas en inglés), método por el cual un servidor web puede interactuar con programas externos de generación de contenido [16]. En algunos aspectos es posible personalizar la página web a las necesidades de cada organización [6], pero cuenta con limitaciones. Por ejemplo, en la *figura 2* se muestra una personalización realizada en un sistema Nagios, para la monitorización de los recursos del Capítulo UNAM del Honeynet Project. Sin embargo, existen alternativas

- Nagios generalmente opera a través de un cliente en los dispositivos que monitoriza, lo que le permite realizar comprobaciones sobre controles específicos, aunque puede hacer una revisión externa, como conexión a un equipo o puerto, o bien, interacciones E2E.
- Las revisiones se realizan de forma programada.
- Las configuraciones se realizan en archivos de texto, lo que simplifica su uso.
- Permite el envío de alertas por diversos medios, como SMS, mensajería instantánea, redes sociales y correo electrónico, entre otros [7].

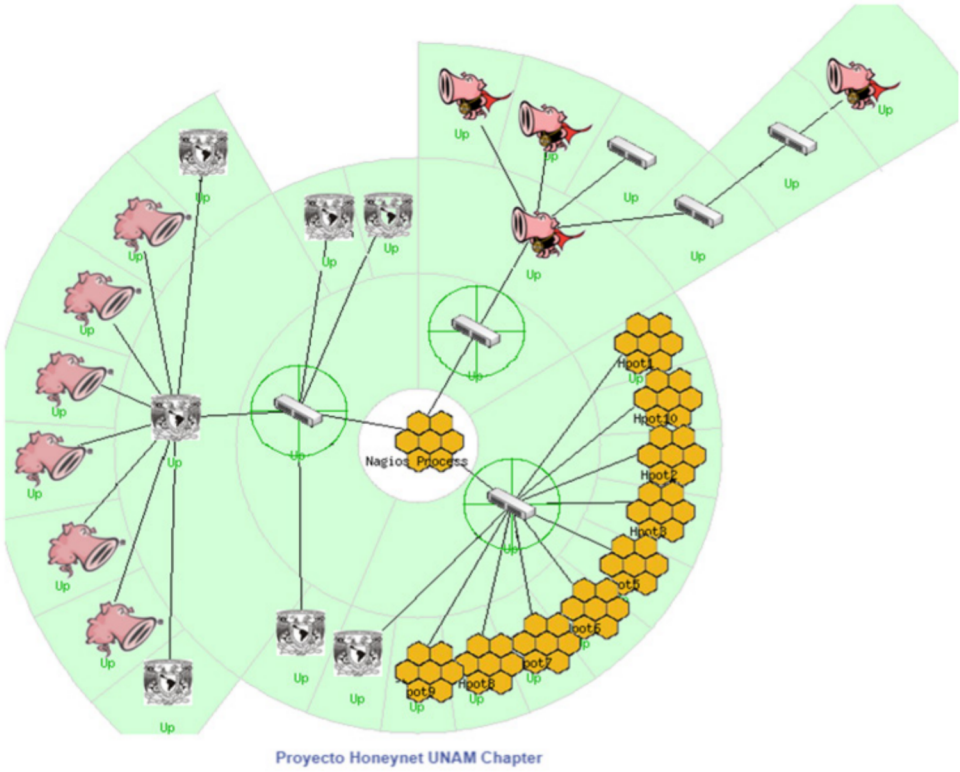

Figura 3.
Proyecto Honeynet UNAM, "Mapa de nagios core," 2019. Fuente: elaboración propia.

- Está diseñado para funcionar de forma óptima en sistemas basados en GNU/Linux y UNIX.

Por otro lado, es importante también establecer algunas limitaciones de este sistema, como [3]:

- Cuenta con una interfaz base simple y poco amigable.
- La configuración puede ser compleja al inicio, y en caso de requerir un módulo muy específico.
- No cuenta con una herramienta de descubrimiento automatizado de dispositivos.
- Por sí mismo, no diferencia entre tipos de dispositivos, aunque esto puede especificarse.
- Sin importar su naturaleza, Nagios trata a cualquier dispositivo como un *host*.

A continuación, se mencionan cinco ejemplos de implementación para diferentes propósitos:

- Es usado en la Universidad de Extremadura (UEX) para el control de disponibilidad del entorno del Campus Virtual y situaciones que deben ser atendidas por el personal técnico [8].
- Sirve en la Universidad de Granma, como en el Instituto Tecnológico Superior "Portoviejo", para el monitoreo del desempeño de la red, donde se establecieron parámetros específicos para revisar, en función de los servicios que tiene cada equipo [7].
- En una implementación en Cuba se utilizó para la monitorización de un servidor revisado por Nagios y, en general, un procedimiento para el despliegue seguro de aplicaciones basado en buenas prácticas, estándares y elementos tradicionales de desarrollo de software [8].
- En el Proyecto Honeynet UNAM (https://www.honeynet.unam.mx) se utiliza para la monitorización de los servicios y el estado de los sensores de monitoreo, incluyendo la honeynet.
- En el UNAM-CERT se usa para monitorizar los servicios públicos y privados en tiempo real, con el fin de prevenir y responder ante incidentes de infraestructura tecnológica.

Por ejemplo, el Proyecto Honeynet UNAM-Chapter utiliza Nagios para monitorear los servidores, la infraestructura de red (conmutadores), los servicios y los equipos que son utilizados como sensores de monitoreo y honeypots, por medio de *plugins* personalizados, desarrollados en el lenguaje Perl y Shell Script, que permiten obtener el estado y la respuesta de cada uno para así poder mostrarlo en la interfaz web. Así se aprovechan las ventajas de tener un sistema de monitoreo, debido a que se mantiene un registro y se reciben alertas por correo electrónico cuando se detecta algún cambio. Esto permite atender de manera oportuna los diversos eventos que se presentan. Además, es posible identificar fechas y horarios específicos en los registros que ayudan a identificar la causa del problema y proporcionan información útil para ajustar las notificaciones, los intentos e intervalos de sondeo.

Finalmente, algunos otros productos de monitorización que existen en el mercado, son [9]:

- Icinga
- ZENOSS
- HP BTO
- CiscoWorks LAN Management Solutions
- NAGIOS XI (Versión comercial de Nagios Core)
- PANDORA FMS
- Munin
- Cacti
- Zabbix

Conclusión

La monitorización de servicios, equipos o redes, permite establecer mejores niveles de disponibilidad. No solo sirve para alertar sobre un problema actual, sino también para informar sobre los parámetros que permitan predecir o prevenir una crisis dentro de la infraestructura del centro de datos.

Sin embargo, la implementación de un sistema de monitoreo requiere que se adapte a la naturaleza y las necesidades de la organización donde será instalado. También requiere el conocimiento de la organización y el tiempo de aprendizaje sobre la misma herramienta y los sistemas o servicios que monitorizará. Así, la información generada deberá ser suficiente para responder ante eventualidades, no excesivas, para que éstas no sean ignoradas por el personal que atenderá las incidencias.

Una opción para la implementación de un sistema de monitorización es Nagios Core, una herramienta eficaz y flexible, que permite establecer una monitorización específica para cada dispositivo o tipo de dispositivo, siendo escalable y adaptativo a las necesidades actuales y futuras de cada organización.

BIBLIOGRAFÍA

[1] D. Josephsen, *Building a Monitoring Infrastructure with Nagios*, Boston: Prentice Hall, 2007.

[2] L. de Haan y T. Koppelaars, *Applied Mathematics for Database Professionals*, Estados Unidos: Apress, 2007.

[3] S. Mongkolluksamee, P. Pongpaibool y C. Issariyapat, "Strengths and Limitationsof Nagios as a Network Monitoring Solution," *DOCPLAYER*, [En línea]. Disponible en: https://docplayer.net/1264602-Strengths-and-limitations-of-nagios-as-a-network-monitoring-solution.html [Consultado en septiembre 20, 2019].

[4] C. Issariyapat, P. Pongpaibool, S. Mongkolluksamee et al., "Using Nagios as a Groundwork for Developing a Better Network Monitoring System, 2012 Proceedings of PICMET '12" Vancouver: IEEE 2012, pp. 2771-2777.

[5] Nagios, "What can Nagios Help You Do?," *nagios.org,* 2019. [En línea]. Disponible en: https://www.nagios.org/ [Consultado en septiembre 20, 2019].

[6] A. A. Cevallos, *Análisis, diseño e implementación de una herramienta de monitoreo y control de Data Center basada en herramientas Open Source. Aplicado al Banco de Guayaquil*, Universidad Politécnica Salesiana, Colombia, 2015.

[7] M. L. Alvaro, L. S. Parrales y K. M. Parrales, "Capítulo IX: Implementación de los sistemas de gestión de la red en dos universidades americanas" en *Investigaciones Cualitativas en Ciencia y Tecnología*. 2017: VI Congreso Internacional de Investigación Cualitativa en Ciencia y Tecnología, España: 3Ciencias, 2017, pp. 101-114.

[8] A. D. Domínguez, J. G. Pulido y J. R. Guerrero, "Metodología previa a la aplicación de sistemas analíticos sobre entornos virtuales de aprendizaje," en *I Congreso Internacional de Campus Digitales en Educación Superior*, España: Extremadura, 2018, pp. 79-82.

[9] A. H. Yeja y J. P. Rubier, "Procedimiento para la seguridad del proceso de despliegue de aplicaciones web," *Revista Cubana de Ciencias Informáticas*, junio, 2016. [En línea]. Disponible en: http://scielo.sld.cu/scielo.php?pid=S2227-18992016000200004&script=sci_arttext&tlng=en [Consultado en septiembre 20, 2019].

[10] R. O. Prada, "Fator de eficácia na implementação de Marketing Digital em negócios de Varejo," *Revista EAN*, 2016. [En línea]. Disponible en: http://www.scielo.org.co/scielo.php?pid=S0120-81602016000100008&script=sci_abstract&tlng=pt [Consultado en septiembre 20, 2019].

[11] E. Imamagic y D. Dobrenic, "Grid Infrastructure Monitoring System Based on Nagios," *Proceedings of the 2007 workshop on Grid monitoring*, Estados Unidos: California, 2007, pp. 23-28.

[12] Icinga, "Monitor Your Entire Infrastructure," *Icinga*, 2009. [En línea]. Disponible en: https://icinga.com/ [Consultado en septiembre 20, 2019].

[13] Munin, "Munin is a Networked Resource Monitoring Tool that can Help Analyze Resource Trends and "What Just Happened to Kill our Performance?" Problems. It is Designed To Be Very Plug and Play. A default Installation Provides a lot of Graphs with Almost no Work," *Munin*, 2003. [En línea]. Disponible en: http://munin-monitoring.org/ [Consultado en septiembre 20, 2019].

[14] Cacti, "The Complete RRDTool-Based Graphing Solution," *Cacti*, 2004. [En línea]. Disponible en: https://www.cacti.net/ [Consultado en septiembre 20, 2019].

[15] Zabbix, "Deploy Zabbix in the Cloud," *Zabbix*, 2001. [En línea]. Disponible en: https://www.zabbix.com/ [Consultado en septiembre 20, 2019].

[16] Apache, "Tutorial de apache: contenido dinámico con CGI," *Apache*, 2019. [En línea]. Disponible en: https://httpd.apache.org/docs/trunk/es/howto/cgi.html [Consultado en septiembre 20, 2019].

[17] Zenoss, "Zenoss Recognized in Gartner Market Guide for AIOps Platforms," *Zennos Own It*, 2005. [En línea]. Disponible en: https://www.zenoss.com/ [Consultado en septiembre 20, 2019].

[18] Nagios, "Nagios Core is the Monitoring and Alerting Engine that Serves as the Primary Application Around which Hundreds of Nagios Projects are Built," *nagios.org*, https://www.nagios.org/projects/nagios-core/ [Consultado en septiembre 20, 2019].

[19] Snort, "Network Intrusion Detection & Prevention System," *Snort*, 2020. [En línea]. Disponible en: https://snort.org/ [Consultado en noviembre 16, 2020].

Cómo se cita

M. I. Quintero Martínez y S. A. Tovar Balderas, "Monitorización de infraestructura tecnológica como mejora en centros de datos," *TIES, Revista de Tecnología e Innovación en Educación Superior*, vol. 2, n.o. 1, abril, 2021. [En línea]. Disponible en: http://ties.unam.mx/ [Consultado en mes día, año].