Informe Proyecto Final

Monitoreo de infraestructura con Nagios

David A. Narvaez Salazar
Universidad Autónoma de Occidente
Santiago de Cali, Colombia
david_a.narvaez@uao.edu.co

Anderson L. Alvarez Perez
Universidad Autónoma de Occidente
Santiago de Cali, Colombia
anderson.alvarez@uao.edu.co

Alejandro Mejia Ortiz
Universidad Autónoma de Occidente
Santiago de Cali, Colombia
alejandro.mejia_ort@uao.edu.co

Abstract- The following report describes the solution for the monitoring of two machines with a different service, also displaying its status on a web page that generates the graphs according to the status of the customers. .

Keywords: Nagios, monitoring, NRPE, plugin.

I. INTRODUCCIÓN

El monitoreo de la información ha tomado gran importancia en los últimos años. En estos últimos años ha tenido cabida el despliegue de una infraestructura híbrida y en la nube. Para modelos híbridos, esto gira en torno al seguimiento y administración de los recursos locales y externos con igual facilidad y eficiencia. El monitoreo de una infraestructura trae consigo una amplia gama de beneficios como poder corregir automáticamente ciertos problemas con la definición de pasos definidos, administrar los permisos que tienen servicios que se basan en la nube, capacidad de ejecutar remotamente una serie de comandos para cortar el flujo de los datos. Con el notable aumento en la necesidad del monitoreo de infraestructuras este ha evolucionado más allá de los equipos locales, abarcando infraestructuras en la nube, servicios en la nube, dispositivos móviles como mecanismos IoT, entre otros. Esto fue lo que se realizó el proyecto final, se realizó la monitorización de dos máquinas virtuales mediante Nagios mostrando en un dashboard el estado de varios servicios que están implementados en las máquinas.

II. MARCO TEÓRICO

Nagios Core

Nagios Core anteriormente conocida como Nagios, es una aplicación de software informático libre y de código abierto utilizado para vigilar los equipos (hardware) y servicios (software). Nagios ofrece servicios de monitoreo y alerta para servidores, switches, aplicaciones y servicios. Permite alertar a los administradores cuando detecta un comportamiento no deseado en una máquina o un servicio y se notifica por segunda vez cuando el problema ha sido resuelto.

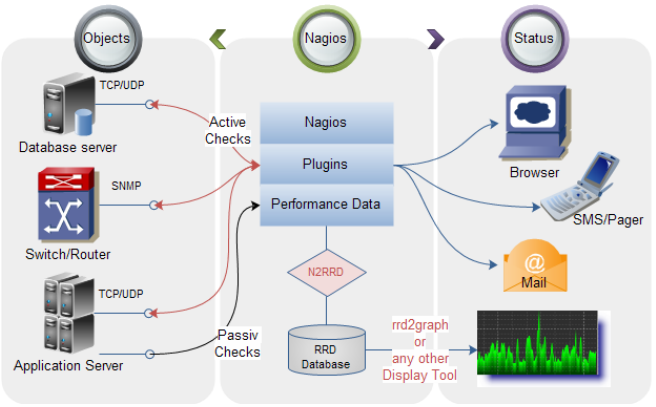

Figura 1. Funcionamiento de Nagios. [2]

El demonio o servicio de Nagios, ejecutado en el servidor, se comporta como un programador que ejecuta ciertos scripts en ciertos momentos. Este ejecuta periódicamente plugins que residen en el mismo servidor, se ponen en contacto con hosts o servidores en su red o en Internet. Los datos que se obtienen sobre el monitoreo son guardados para mostrar gráficas de su rendimiento. También se puede visualizar la información del estado de los sistemas usando una interfaz web.

Nagios permite la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP…), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos), posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de crear plugins específicos para nuevos sistemas o para propósitos específicos del administrador.

Plugins

Son ejecutables o scripts compilados (scripts Perl, scripts shell, etc.) que se pueden ejecutar desde una línea de comandos para comprobar el estado o un host o servicio. En muchos casos también es frecuente que algunos programas con bastante peso desarrollen sus propios plugins para otros softwares. Nagios utiliza los resultados de los complementos para determinar el estado actual de los hosts y servicios en su red.

Virtual Box

Oracle VM VirtualBox es un hipervisor de tipo 2 (estos hipervisores se ejecutan en un sistema operativo convencional al igual que otros programas informáticos, un sistema operativo invitado se ejecuta como un proceso en el host) para virtualización x86 desarrollado por Oracle Corporation.

VirtualBox puede instalarse en Microsoft Windows, macOS, Linux, Solaris y OpenSolaris. Admite la creación y administración de máquinas virtuales invitadas que ejecutan Windows, Linux, BSD, OS/2, Solaris, Haiku y OSx86. Los usuarios de la virtualización pueden cargar varios sistemas operativos dentro de un único sistema operativo. Las máquinas en las que se alojan estos sistemas operativos pueden ser iniciadas, pausadas o apagadas sin la necesidad de que se altere el sistema operativo del anfitrión.

NRPE

Nagios Remote Plugin Executor (NRPE) es una herramienta de extensión de Nagios, utilizada en el host monitoreado. Puede proporcionar información local del host al servidor de monitoreo de nagios. Algunos ejemplos de los recursos que puede monitorear son:

- Carga de CPU
- Uso de memoria
- Capacidad del disco
- Número de usuarios registrados
- Cantidad total de procesos
- Número de procesos zombies
- Uso de partición de intercambio

Para su funcionamiento es necesario el plugin *check_nrpe* en la máquina de monitoreo local y el demonio NRPE en la máquina remota de linux que en este caso es el servidor de monitoreo. Cuando el servidor ejecuta el complemento *check_nrpe* indicando qué servicios o recursos debe verificar, este complemento se conecta con el demonio de NRPE en la máquina monitoreada. Cuando la máquina recibe esta orden, el demonio NRPE ejecuta los plugins de Nagios encargados de verificar el servicio o recurso. Finalmente los resultados de dicha comprobación son entregados del demonio NRPE al plugin *check_nrpe*, que posteriormente devuelve los resultados de la comprobación. La conexión segura mediante SSL es opcional.

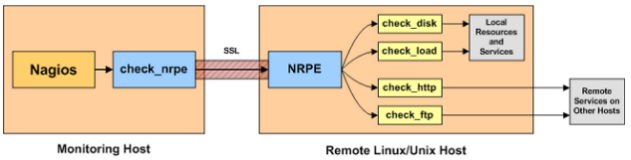

Figura 2. Modo de operación de NRPE. [6]

Se pueden hacer dos tipos de checks (comprobaciones) desde el servidor:

- Checks directos: Utilizados para revisar recursos locales de la máquina que está siendo monitoreada. Este tipo de comprobaciones se hacen a los recursos previamente enunciados.
- Checks indirectos: Utilizado para comprobar indirectamente los servicios y recursos "públicos" de los servidores remotos que es posible que no se pueda acceder directamente desde el host de supervisión.

PNP4Nagios

PNP4Nagios es un complemento para Nagios que analiza los datos de rendimiento obtenidos por los plugins y los almacena automáticamente en bases de datos RDD (Round Robin Databases). La base de datos RRD es un tipo de almacenamiento muy especial diseñado para mantener estadísticas agregadas de series de tiempo en archivos, su ventaja principal es la velocidad de inserción extremadamente rápida, importante para el monitoreo en tiempo real.

Figura 3. Insignia de PNP4Nagios. [7]

III. PLANTEAMIENTO DEL PROBLEMA

La empresa de componentes electrónicos Texas Instruments ha reportado pérdidas millonarias en los últimos meses y tras un análisis detallado de todos los procesos de la compañía se ha identificado que el debacle se debe en gran medida a problemas de disponibilidad de los servidores donde están su página web, que es uno de sus principales canales de comunicación y comercialización con sus clientes y su servicio de FTP; que juega un papel relevante en los procesos internos de la compañía ya que es que permite transferir los documentos internos entre las distintas dependencias de la compañía y por tanto no se puede implementar un plan de control y mejora continua que garantice el desempeño de la empresa.

En este sentido y para tomar acciones correctivas que mejoren la disponibilidad de sus servicios la empresa se ha propuesto a implementar un servidor capaz de monitorear en tiempo real la disponibilidad de sus servicios críticos y él estado de las máquinas que los alojan.

IV. HERRAMIENTAS PARA EL MONITOREO

Existe una diversa variedad de herramientas utilizadas para el monitoreo de infraestructuras, a continuación se describen algunas muy empleadas en este campo:

PRTG: Es un software de monitorización de red sin agente de Paessler AG. Este es capaz de monitorear y clasificar las condiciones del sistema, como el uso del ancho de banda o el tiempo de actividad que tiene un usuario.

SolarWinds: Es un software desarrollado para las empresas que les permite administrar sus redes, sistemas e infraestructuras. El principal producto que brinda a las empresas es el monitoreo de redes de forma segura para el análisis de rutas, proporciona escalabilidad y correlación de datos en toda la pila a fin de reducir las interrupciones de la red. También ofrece el servicio de administración de bases de datos con integración de Microsoft SQL.

V. SOLUCIÓN FINAL

Inicialmente se crearon dos máquinas (clientes) para ser monitoreadas y un servidor donde se encuentra Nagios. Todos los nombres de los archivos se encuentran en el repositorio en github donde está el proyecto, aquellos códigos que no se muestran aquí se encuentran en dicho repositorio.

Configuración del servidor

En el servidor se realizó la mayor parte de la configuración. Se tuvo que hacer la descarga e instalación de Nagios, los plugins para el servidor y NRPE. Con esto se puede realizar el monitoreo básico de los clientes, se creó el archivo *linux.cfg* y en él se puso los datos de los servidores que se monitorean tales como el nombre, el alias, la constancia con la que se va a verificar su estado y su dirección ip, también se debe aclarar si este pertenece a un grupo y las máquinas que lo conforman. Luego de esto se agregaron los servicios que tienen los clientes con una estructura similar a la anterior, se definió el grupo en el que están ambas máquinas, el tipo de servicio, el tiempo en minutos con el que se verificó el servicio y el comando de chequeo. Los comandos de chequeo que se implementaron fueron:

- check_hda1
- check_uptime
- check_load
- check_swap
- check_ping
- check_users
- check_mem

Para el monitoreo del servicio http se adicionaron la definición de los siguientes servicios indicando solo el cliente 1.

- check_apache
- check_tcp!80
- check_proc_apache
- check_http

Para el monitoreo del servicio de ftp se adicionó este servicio pero indicando que es solamente para el cliente 2.

- check_ftp!21

Configuración del cliente 1

En el primer cliente se instalaron los plugins de Nagios y NRPE, además de otras dependencias para la instalación de Nagios. Para el monitoreo del hardware del cliente se creó el archivo *check_mem* para el monitoreo de la memoria RAM de este cliente. Este archivo se encuentra dentro del cliente 1 con el nombre de *check_mem.pl*. También en el archivo *nrpe.cfg* del cliente 1 (con path /usr/local/nagios/etc/nrpe.cfg) se tuvo que agregar los siguientes comandos para que se pudiera realizar la revisión de los recursos.

```
command[check_users]=/usr/local/nagios/libexec/check_users -w 5 -c 10
command[check_load]=/usr/local/nagios/libexec/check_load -r -w .15,.10,.05 -c .30,.25,.20
command[check_hda1]=/usr/local/nagios/libexec/check_disk -w 20% -c 10% -p /dev/sda1
command[check_zombie_procs]=/usr/local/nagios/libexec/check_procs -w 5 -c 10 -s Z
command[check_total_procs]=/usr/local/nagios/libexec/check_procs -w 150 -c 200

command[check_swap]=/usr/local/nagios/libexec/check_swap -w 20% -c 10%
command[check_uptime]=/usr/local/nagios/libexec/check_uptime

#Agregue la siguiente linea#
command[check_mem]=perl /usr/local/nagios/libexec/check_mem.pl -f -C -w 20% -c 10%
```

Figura 4. Configuración de nrpe.cfg.

Para el monitoreo del servicio de apache se tuvo que instalar el servicio de http y agregar los siguientes comandos en el archivo *httpd.conf* (con path /etc/httpd/conf/httpd.conf) para permitir las solicitudes

que se hacen desde el servidor. También se tuvo que habilitar el puerto 80 en el caso de tener el firewall activado.

```
<location /server-status>
        setHandler server-status
        Order deny,allow
        Deny from all
        Allow from 192.168.50.0/24
</location>
```

Figura 5. Configuración en httpd.conf.

Después de esto se tuvo que otorgarle a NRPE el comando de acceso a este servicio para el posterior envío de la información, de forma similar como se hizo con los recursos en el monitoreo de hardware del cliente.

```
command[check_proc_apache]=/usr/local/nagios/libexec/check_procs -c 1: -C httpd
```

Figura 6. Configuración de nrpe.cfg para http.

Configuración del cliente 2

De forma similar como en el cliente 1 se instalaron los plugins y dependencias necesarios, se creó el archivo *check_mem* y se agregaron las mismas líneas de comando que se muestran en la figura 4. A diferencia del cliente 1, en este cliente se monitoreo el servicio de ftp. Para ello se tuvo que instalar el servicio de ftp en el cliente y habilitar que el servicio arranque desde que se prende la máquina con el comando *chkconfig vsftpd on.* El resto de la configuración para el monitoreo de este servicio se realizó en el servidor.

VI. CONCLUSIONES

- La implementación del proyecto nos ayudó a aplicar los conocimientos adquiridos durante el curso, en donde monitoreamos los servicios de HTTP y FTP para los clientes que se definieron en la configuración de Nagios. También nos brinda la posibilidad de escalar el proyecto a empresas que cuenten con redes medianas o más complejas, el reto puede ser mayor, pero ya vimos que Nagios cuenta con un amplio soporte y una comunidad grande que ofrece soluciones a problemas que se puedan llegar a presentar.

- La generación de reportes y gráficas mediante Nagios brinda una amplia gama de opciones para los administradores de una infraestructura tanto de máquinas como también de redes y servicios en la nube que resultan de gran ayuda en el momento de conocer el estado de una infraestructura sin la necesidad de ejecutar largas líneas de comandos dentro del servidor.

- Nagios, al ser un programa de código abierto, le brinda a las personas y a las empresas una mayor agilidad en la gestión de la tecnología, y una mayor practicidad en la seguridad ya que corre sobre SSL.

VII. REFERENCIAS

[1]https://www.e-dea.co/blog/que-debe-tener-una-solucion-de-monitoreo-de-infraestructura-tecnologica

[2] https://en.wikipedia.org/wiki/Nagios

[3]https://www.edureka.co/blog/nagios-tutorial/#:~:text=Nagios%20runs%20on%20a%20server,SMS%20notifications%20if%20something%20happens.

[4] https://en.wikipedia.org/wiki/VirtualBox

[5] https://www.bujarra.com/nagios-monitorizando-nrpe/

[6] [En inglés] Nagios. (2017 nov 17). "*NRPE Documentation"*. [En línea]. Obtenido de: https://assets.nagios.com/downloads/nagioscore/docs/nrpe/NRPE.pdf

[7]https://www.ochobitshacenunbyte.com/2017/03/28/anadir-graficas-a-icinga2-con-pnp4nagios/

[8] https://www.solarwinds.com/es/