

Infraestructura y Tecnología de Redes

Curso 2020-2021

Práctica 4: *Monitores de red*

Introducción

A la hora de trabajar con una red, es muy importante la información que se pueda obtener de esta. Una información de calidad nos permitirá gestionar la red de forma sólida y evitar problemas.

Para obtener esta información, un tipo de herramienta imprescindible son los sistemas de monitorización, o monitores de red. Estos sistemas vigilan los equipos y los servicios que se especifican y generan alertas cuando los comportamientos (servidores caídos, poco espacio en disco, tiempo de respuesta demasiado altos, etc.) superan unos ciertos parámetros.

1. Herramienta utilizada: Nagios

Nagios [1] es un monitor de red muy potente, capaz de monitorizar servicios de red (SMTP, POP3, HTTP, SNMP) y los recursos de hardware de los equipos (carga de la CPU, espacio de disco, uso de la memoria, estado de los puertos, etc.). Nagios genera alertas que pueden ser enviadas de forma automática a través de correo electrónico o por SMS.

Nagios es multi-plataforma y tiene una GUI que puede ser accedida a través de un navegador Web. Además, permite la programación de plugins y add-ons avanzados.

Nagios Core tiene licencia GNU General Public License Version 2 publicada por la Free Software Foundation.

En esta práctica utilizaremos Nagios XI, una versión comercial de Nagios Core con varias funcionalidades preconfiguradas y listas para usar. Esta versión puede utilizarse durante 60 días de forma gratuita y puede descargarse de [2]. Para las prácticas en el laboratorio se ha optado por utilizar Nagios XI en un contenedor [3] basado en la tecnología Docker [4], con el objetivo de reducir el consumo de recursos de hardware y para agilizar tareas administrativas (inicio, apagado, pausa, importación o exportación).

2. Guión de la práctica

Todas las respuestas deben ir acompañadas de las gráficas correspondientes que demuestren los resultados de lo que se está explicando, configurando y/o requiriendo.

Cree un contenedor con la siguiente línea de comandos, donde XX hace referencia al grupo de trabajo. Por ejemplo: **itx-a1-nagiosxi**. (debe ejecutarlo una sola vez):

```
docker run -d -p 8080:80 -p 5666:5666
-p 5667:5667 --name itx-XX-nagiosxi
tgoetheyn/docker-nagiosxi
```

Recuerde utilizar el mismo ordenador para las dos sesiones de la práctica de Nagios.

2.1. Puesta en funcionamiento

1. Verifique que el contenedor se encuentra corriendo con el comando
`docker ps -a`.
2. Abra un navegador Web y acceda a la URL: `http://localhost:8080/nagiosxi/`.
3. Siga los pasos que aparecerán en pantalla (le pedirá que introduzca una contraseña para el usuario administrador). Cuando haya terminado, podrá utilizar el usuario **nagiosadmin** y el password que ha establecido para acceder a Nagios XI. Guarde el password que ha utilizado. (**NOTA:** Si pierde la contraseña tendrá que volver a empezar la práctica desde **cero**).

Password:

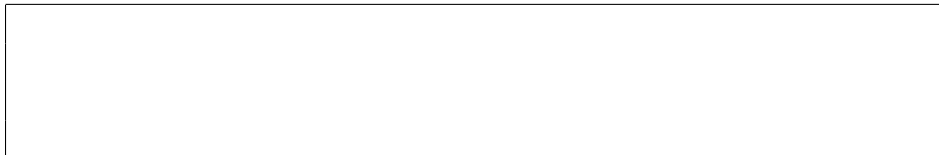
2.2. Monitorizar nodos

1. Vaya a “**Configure**” → “**Run the Auto-Discovery Wizard**”. Seleccione “**Start a new discovery job**” y seleccione como “**Scan Target**” la red `158.109.79.67/27`. Este proceso será lento, por lo tanto lo dejaremos corriendo.
2. Vuelva a lanzar otro “**discovery job**” seleccionando como “**Scan Target**” la dirección `158.109.95.225`.

3. Cuando acabe el auto-descubrimiento, deberá iniciar la segunda etapa de este proceso. Para ello, haga clic en “**1 New**” para abrir el “**Auto-Discovery Monitoring Wizard**”.
4. En el paso 3 (“**Step 3**”) deberá seleccionar los nodos que desee monitorizar (en este caso, sólo hay uno, selecciónelo). También puede ponerle un nombre (en este caso, utilice el nombre `www.uab.cat`).
5. En los pasos 4 y 5 deberá configurar los periodos de comprobación y de alerta. Como el tiempo de que disponemos para esta práctica es limitado, configure un tiempo de 2-3 minutos para evitar esperas innecesarias.
6. Ignore de momento el paso 6 y acabe con el proceso haciendo click en “**Finish**”.

2.3. Descubrir la red

1. Vaya a “**Home**” → “**Details**” → “**Host Detail**” y seleccione el nodo `www.uab.cat`. En esta página puede obtener información sobre el estado del nodo, reconfigurarlo, etc.
2. (2 puntos) Seleccione “**Traceroute a este host**” y tome nota de los routers que hay entre su máquina y `www.uab.cat` (sólo hay nombre y dirección IP). Si no aparece el nombre de las máquinas, puede utilizar el comando `host` para averiguarlo. Coloque una captura de pantalla de la salida del `traceroute`.



3. Ahora debe repetir todos los pasos de la sección anterior (**Monitorizar nodos**) para cada uno de los elementos que el `traceroute` haya encontrado. Puede realizar este proceso en paralelo, poniendo en marcha más de un “**Discovery job**” a la vez.
 - Ponga a cada nodo su nombre. Puede utilizar el comando `host ip` para averiguar los nombres que no conozca.
 - Cuando llegue al paso 6, seleccione quién es el “**Parent host**” de cada nodo. Piense que la información que ha obtenido con el `traceroute` puede servir para imaginar cómo es la estructura jerárquica de la red. Si descubre cuál es el “**Parent host**” de un nodo después de haberlo

configurado, puede ir al “**Host Detail**” del nodo en cuestión y volver a configurarlo.

4. Vaya a “**Configure**” → “**Advanced Configuration**” → “**Core Config Manager**”. Vaya a “**Monitoring**” → “**Host Groups**” → “**Add new**” y cree un nuevo grupo de hosts llamado **Laboratorio-dEIC**.
5. Volvemos al primer proceso de descubrimiento, si ya ha terminado debería haber más de un nodo, añada todos los nodos **excepto** el 158.109.79.65. Añádalos al *Hostgroup* que ha creado en el punto anterior. Nombre los nodos utilizando la siguiente tabla:

158.109.79.66	deic-dc0
158.109.79.67	deic-dc1
158.109.79.68	deic-dc2
158.109.79.69	etc...

6. (2 puntos) Cuando finalice, coloque una captura de pantalla de “**Host Detail**” y “**Service Detail**” donde se vean los 10 primeros nodos monitorizados.



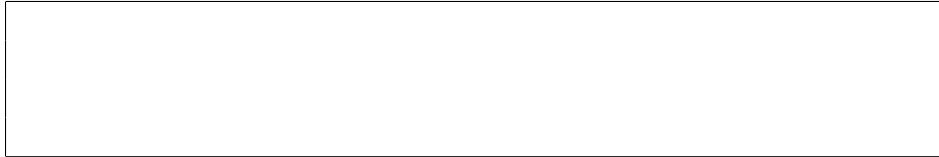
2.4. Monitorizar la red

1. Utilice el navegador para acceder a la GUI de Nagios XI.
2. (3 puntos) Vaya a “**Home**” → “**Maps**” → “**Hypermap**”. Cuando considere que el diagrama se ajusta a la realidad de la red puede tomar una captura de pantalla para adjuntarla al informe. Si cree que hay algo mal, debe solucionarlo modificando los “**Parents**” de los nodos afectados.



3. Vaya a “**Dashboards**” → “**Add New Dashboard**” y cree uno con el nombre “**Práctica 4 ITX**”.

4. **(3 puntos)** Vaya a “**Add Dashlets**” → “**Available Dashlets**” y añada unos cuantos *Dashlets* a tu *Dashboard*. Elija los *Dashlets* que cree que le serán más útiles. Coloque una captura de pantalla donde divise los *Dashlets* más relevantes para el entendimiento de la red monitorizada por Nagios.

A large, empty rectangular box with a thin black border, intended for the user to paste a screenshot of their Nagios dashboard showing selected dashlets.

5. Para finalizar esta sesión haga “**Logout** ” en su navegador y en un terminal ejecute la siguiente línea de comandos para apagar el contenedor:
- ```
docker stop itx-XX-nagiosxi
```

### 3. Calendario

A continuación se describe el calendario de los hitos relativos a la práctica:

- **Práctica:** El 26/03/2021.
- **Entrega:** El 08/04/2021 hasta las 23:55.

### 4. Condiciones de entrega

- La entrega de la práctica se hará a través del campus virtual.
- No se aceptarán informes entregados fuera de plazo.
- Cada grupo debe entregar un informe en formato **PDF que contenga el número de práctica, el número de grupo y el primer apellido de cada alumno** (ej. p1-a1-carpio-miranda.pdf) y las respuestas a los diferentes apartados de la práctica. En caso de **no** seguir el formato se **restará 1 punto de la nota**.

### Referencias

- [1] Nagios. Nagios - The Industry Standard. <http://nagios.com/>.
- [2] Nagios. Nagios XI Downloads. <https://www.nagios.com/downloads/nagios-xi/>.
- [3] Container. Red Hat Container. <https://www.redhat.com/en/topics/containers/whats-a-linux-container/>.
- [4] Docker. Docker. <https://www.docker.com/resources/what-container/>.