https://doi.org/10.22201/dgtic.ctud.2024.2.2.53

Vol. 2, Núm. 2. abril-junio 2024, págs. 24 - 32

Representación gráfica de consultas recibidas en DNS recursivo de la UNAM

Información del reporte:

Para citar este reporte técnico:

Navarrete Guerra, L. I. (2024). Representación gráfica de consultas recibidas en DNS recursivo de la UNAM. Cuadernos Técnicos Universitarios de la DGTIC, 2 (2) páginas (24 - 32).

https://doi.org/10.22201/dgtic.ctud.2024.2.2.53

Luis Iván Navarrete Guerra

Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Universidad Nacional Autónoma de México

ivan_navarrete@unam.mx

ORCID: 0009-0008-4488-131X

Resumen:

Se describe la implementación de Grafana para la representación gráfica de consultas realizadas a los Sistemas de Nombres de Dominio recursivos de la Universidad Nacional Autónoma de México, así como el monitoreo del servicio de resolución de nombres. Se utiliza Prometheus como fuente de datos y los *dashboards* que ofrece Grafana, para mostrar gráficamente las métricas sobre el rendimiento del servidor así como las consultas realizadas a los diferentes registros del Sistema de Nombres de Dominio, lo que favorece al Centro de Información de RedUNAM tomar medidas preventivas que ayuden a mantener la disponibilidad del servicio y a la generación de reportes con la información obtenida.

Palabras clave:

DNS, DNS recursivo, monitoreo, Grafana, Prometheus, archivos de zona.

https://doi.org/10.22201/dgtic.ctud.2024.2.2.53 Vol. 2, Núm. 2. abril-junio 2024, págs. 25 - 32

1. INTRODUCCIÓN

En el Centro de Información de RedUNAM (NIC UNAM) de la Dirección General de Cómputo y de Tecnologías de la Información y Comunicación se ofrece el servicio de DNS (Sistema de Nombres de Dominio) a todas las entidades y dependencias de la Universidad Nacional Autónoma de México (UNAM). Este servicio involucra la asignación de dominios de red bajo "unam.mx"; alta, baja y actualización de registros, así como la administración de dominios externos como .mx, .edu.mx, .com, etc. Un dominio en cualquier entidad o dependencia les permite publicar cierta información en un sitio web que puede ser visualizado en todo el mundo, lo que coadyuva a la docencia, la investigación, la difusión de la cultura y la administración universitaria.

Es de suma importancia mantener siempre operando el servicio de DNS, para ello se sugiere contar con un sistema de monitoreo del servicio, que permita a los administradores visualizar gráficamente varios aspectos, como pueden ser las diferentes consultas o peticiones que recibe el DNS, procesamiento y estado del servidor.

La implementación de una plataforma como Grafana que es de código abierto (Open Source) y que se adecua fácilmente al sistema operativo donde se aloja el servicio de resolución de nombres de dominio, contribuirá a visualizar las consultas que recibe el servidor DNS recursivo en tiempo real y permitirá mantener las estadísticas después de un largo periodo para realizar análisis o generación de reportes con la información.

2. OBJETIVO

Proporcionar un sistema de monitoreo en tiempo real que permita visualizar gráficamente el número de consultas de los diferentes tipos de registros que recibe un DNS recursivo de la UNAM, así como el rendimiento de dicho servidor, para detectar posibles fallas y tomar medidas preventivas que ayuden a mantener la disponibilidad del servicio. Cabe señalar que los servidores DNS recursivos se encargan de proporcionar la dirección IP correcta del dominio deseado al host solicitante y es el intermediario entre los usuarios finales y los servidores DNS autoritativos (DNS autoritativo frente a recursivo,2023).

3. DESARROLLO TÉCNICO

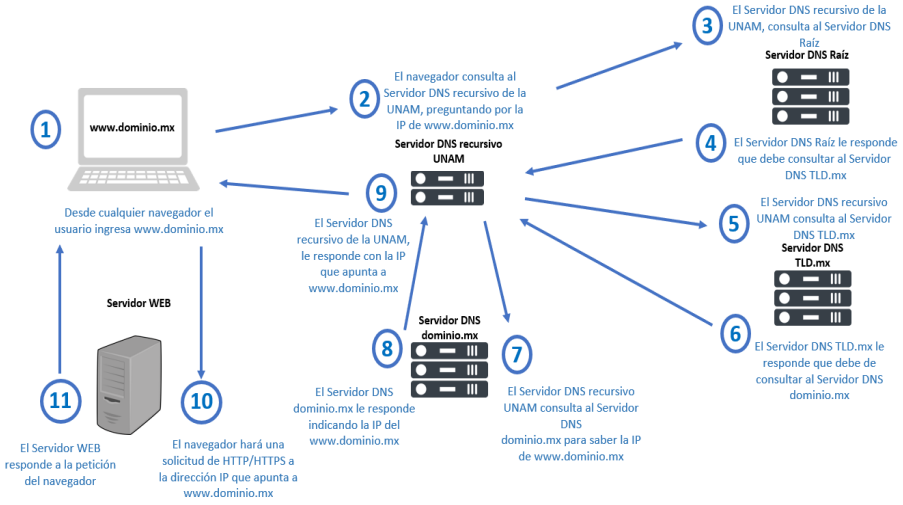
3.1 ANTECEDENTES

El DNS es un protocolo de Internet cuya función principal es la resolución de nombres de dominio, es decir, la traducción de un nombre de dominio como www.unam.mx en una dirección IP, la cual es utilizada para hacer la consulta en el servidor web y que este devuelva el contenido del sitio web en el navegador, de esta manera se facilita a los usuarios de Internet a que sólo introduzcan en la barra de direcciones del navegador nombres de dominio fáciles de recordar. Por lo tanto, si el servidor de DNS no está disponible no será visible el sitio Web si se coloca el nombre de dominio en el navegador. En la Figura 1 se muestra el proceso para la resolución de un nombre de dominio a través del Servidor DNS recursivo de la UNAM, administrado por Network Information Center (NIC UNAM).

https://doi.org/10.22201/dgtic.ctud.2024.2.2.53 Vol. 2, Núm. 2. abril-junio 2024, págs. 26 - 32

Figura 1

Proceso de resolución de nombre de dominio



El NIC UNAM realiza la administración del dominio “unam.mx” mediante 2 servidores DNS autoritativos y 8 recursivos, se administran miles de registros que se traducen en aproximadamente 700 archivos de zona que contienen los registros (A, AAAA, TXT, MX CNAME) de las diferentes instancias de la UNAM. Los diferentes registros con los que cuentan los archivos de zona son los siguientes:

- A: Relaciona una IPv4 a un nombre de dominio.

  Ejemplo: www.fca.unam.mx IN A 10.0.2.2

- AAAA: Relaciona una IPv6 a un nombre de dominio.

  Ejemplo: www.fca.unam.mx IN AAAA db8:ffa:3ef1:2001::123

- CNAME: Mayormente llamado alias, redirecciona un nombre de dominio hacia otro, sin perder el nuevo nombre dado por este registro.

  Ejemplo: nuevo.fca.unam.mx IN CNAME www.fca.unam.mx

- MX: Se utiliza para la referencia de los servidores de correo electrónico, se utiliza una prioridad en caso de tener más de uno.

  Ejemplo: correo.fca.unam.mx IN MX 0 10.0.2.2

- TXT: Permite tener notas de texto, normalmente utilizado para validación y actividades de seguridad para el correo electrónico.

  Ejemplo: correo.fca.unam.mx IN TXT “texto de seguridad para correo”

- NS: Indica el nombre de dominio o la dirección IP de los servidores de nombres en los cuales se encuentran alojados los demás registros, este registro es indispensable para la configuración de un

https://doi.org/10.22201/dgtic.ctud.2024.2.2.53 Vol. 2, Núm. 2. abril-junio 2024, págs. 27 - 32

archivo de zona.

Ejemplo: fca.unam.mx. IN NS ns1.unam.mx.

- SRV: Es utilizado para indicar servicios específicos como SIP, y son relacionados a servidores específicos.

  Ejemplo: _sip._udp IN SRV 10 10 5060 zero.redes

- PTR: Generalmente llamado inverso, se encarga de referenciar una IP a un nombre de dominio, se le llama inverso por realizar la resolución reversa de un registro A.

  10.0.2.2 IN PTR www.fca.unam.mx.

3.2 IMPLEMENTACIÓN

Dadas las características de los servidores UNIX en donde se encuentra instalado BIND (Berkeley Internet Name Domain), el cual brinda servicio de resolución de nombre que contienen actualmente los DNS de la UNAM, se buscó una solución de código abierto que se pudiera integrar adecuadamente a las características de dichos servidores.

Al hablar de soluciones para cumplir el objetivo planteado, pueden surgir muchos nombres de software para este propósito, pero al final se elige Grafana como el software a utilizar, derivado del caso de éxito en la implementación realizada por el NOC de RedUNAM de la DGTIC llevada a cabo en la publicación de Ramírez (2023) en donde se menciona que "después de una evaluación, se consideró a Grafana por la facilidad de crear gráficos a partir de diferentes fuentes de información".

"Grafana es una solución que sirve para ejecutar análisis de datos, extraer métricas que dan sentido ante enormes cantidades de datos y monitorear aplicaciones y recursos hardware con la ayuda de atractivos paneles de control personalizables" (Openwebinars,2021). Para esta implementación se usaron *dashboards* ya diseñados para monitorear el servicio de DNS con BIND.

Instalación

Es importante y recomendable que antes de llevar a cabo la instalación del sistema de monitoreo en Grafana, se tengan el sistema operativo y los repositorios actualizados, posteriormente es necesario instalar los siguientes paquetes, como se muestra en la Figura 2.

Figura 2

Instalación de paquetes para la implementación

```
root@ndns:~ # pkg install prometheus grafana node_exporter bind_exporter
```

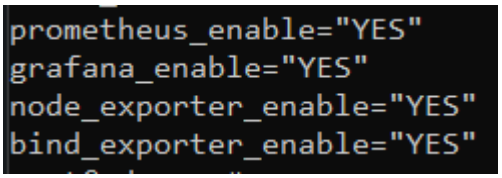
- Prometheus: es una aplicación que nos permite recolectar los datos del servidor donde se encuentra el servicio de DNS.
- Node_exporter: es un servicio que permite exporta los datos del servidor como lo es el CPU, RAM, almacenamiento y que son enviados a Prometheus.
- Bind_exporter: es un servicio que permite exporta los datos del servicio de BIND , como el tipo y número de consultas recibidas en el DNS y que son enviados a Prometheus.

https://doi.org/10.22201/dgtic.ctud.2024.2.2.53 Vol. 2, Núm. 2. abril-junio 2024, págs. 28 - 32

Una vez que se han instalado los paquetes anteriores, es necesario agregarlos al inicio del sistema con el comando *sysrc "nombre del servicio"_enable=YES* y se puede verificar en el archivo rc.conf, , como se muestra en la Figura 3.

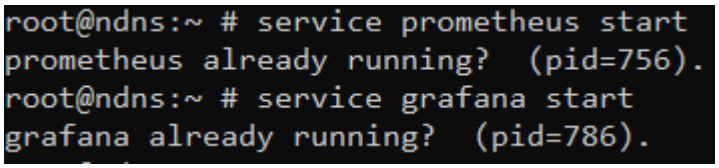
Figura 3

Servicios agregados al inicio del sistema



Es importante iniciar los servicios de Prometheus y Grafana, como se muestra en la Figura 4, para que posteriormente se pueda verificar vía interfaz web su funcionamiento.

Figura 4

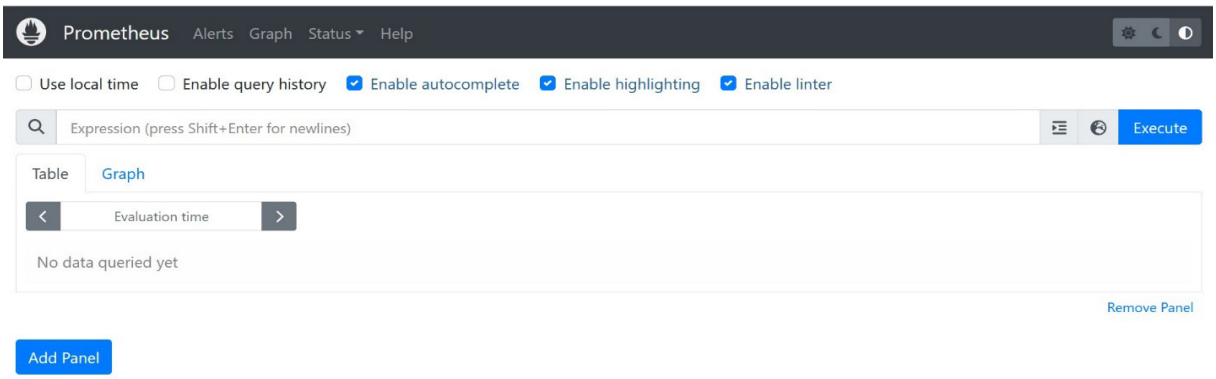


Se inician los servicios de Prometheus y Grafana

Una vez iniciado el servicio de Prometheus se puede verificar que se encuentre activo y sin ningún error, mediante un navegador web, ingresando http://<ip servidor>:9090, se desplegará una página como se muestra en la Figura 5.

Figura 5

Interfaz de Prometheus

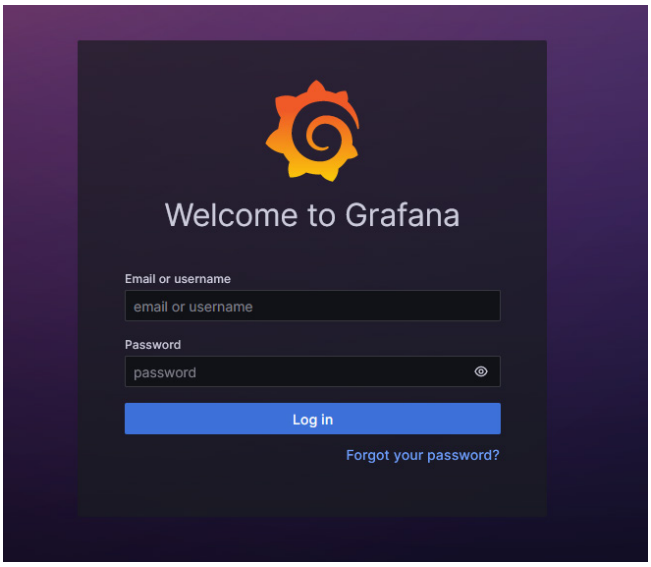


De la misma manera, una vez iniciado el servicio de Grafana, se puede verificar al ingresar http://<ip_servidor>:3000 y mostrará una interfaz como en la Figura 6.

https://doi.org/10.22201/dgtic.ctud.2024.2.2.53 Vol. 2, Núm. 2. abril-junio 2024, págs. 29 - 32

Figura 6

Interfaz de Grafana



Una vez verificado que Grafana y Prometheus están funcionando correctamente, se comienza a configurar Prometheus para concentrar la información tanto de Bind_exporter como de Node_exporter; en el archivo: /usr/local/etc/prometheus.yml se debe configurar los parámetros para lograr la conexión con los servicios antes mencionados, y se deben insertar los parámetros siguientes al final del archivo, como se muestra en la Figura 7.

Figura 7

Configuración de Prometheus

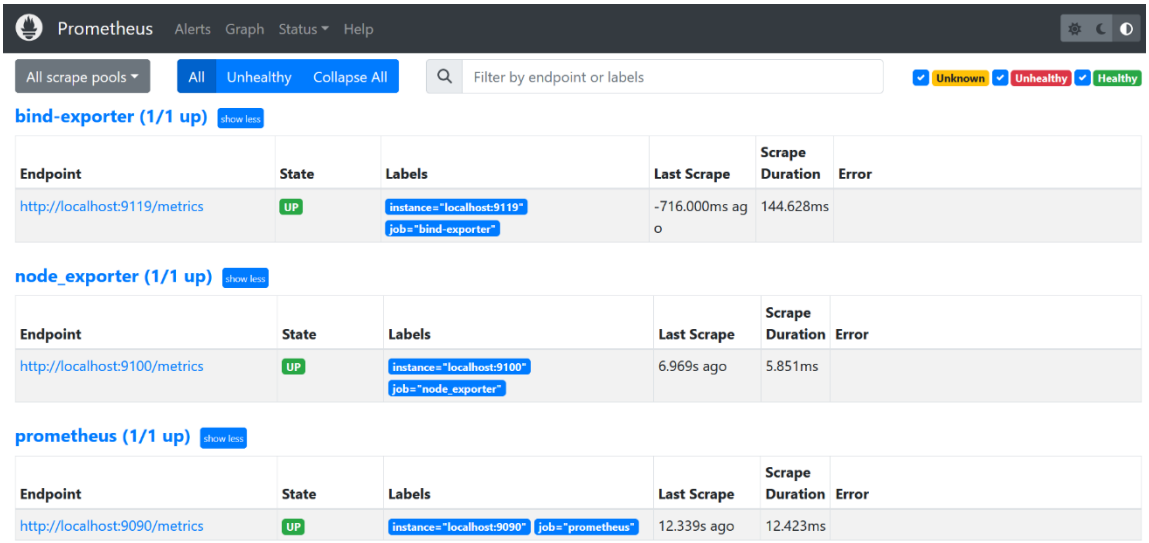
```
- job_name: "prometheus"

  # metrics_path defaults to '/metrics'
  # scheme defaults to 'http'.

  static_configs:
    - targets: ["localhost:9090"]

- job_name: "node_exporter"
  static_configs:
    - targets: ["localhost:9100"]

- job_name: "bind-exporter"
  static_configs:
    - targets: ["localhost:9119"]
```

https://doi.org/10.22201/dgtic.ctud.2024.2.2.53 Vol. 2, Núm. 2. abril-junio 2024, págs. 30 - 32

Para observar que la configuración esté correcta y se vea reflejada en Prometheus, se realiza una consulta en los targets desde la interfaz de Prometheus como se muestra en la Figura 8.

Figura 8

Targets Prometheus



Promethus ya comenzará almacenar la información de los datos obtenidos por Bind_exporter, el cual contiene las métricas de las consultas que se realizan en el DNS mediante el servicio de ind y a su vez Node_exporter contiene las métricas del servidor. Posteriormente se debe integrar como una fuente de datos a Grafana para que comience a desplegar las métricas de manera gráfica con la ayuda de los *dashboards* Bind9 Exporter DNS(Grafana_Dashboard-12309,2024) y Node Exporter FreeBSD (Grafana_Dashboard-4260, 2024), los que permiten monitorear el servicio de DNS.

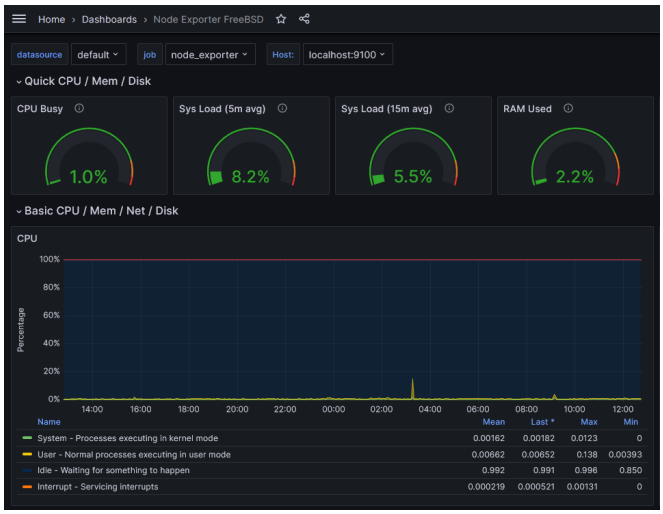
4. RESULTADOS

Al tener configurada la fuente de datos con Prometheus e instalados los *dashboards* Bind9 Exporter DNS y Node Exporter FreeBSD, se puede visualizar las métricas del servidor como se muestra en la Figura 9. De esta manera se monitoreará el servidor, lo que permitirá detectar posibles fallas o un estado anormal del sistema que pueda impactar en el servicio.

https://doi.org/10.22201/dgtic.ctud.2024.2.2.53 Vol. 2, Núm. 2. abril-junio 2024, págs. 31 - 32

Figura 9

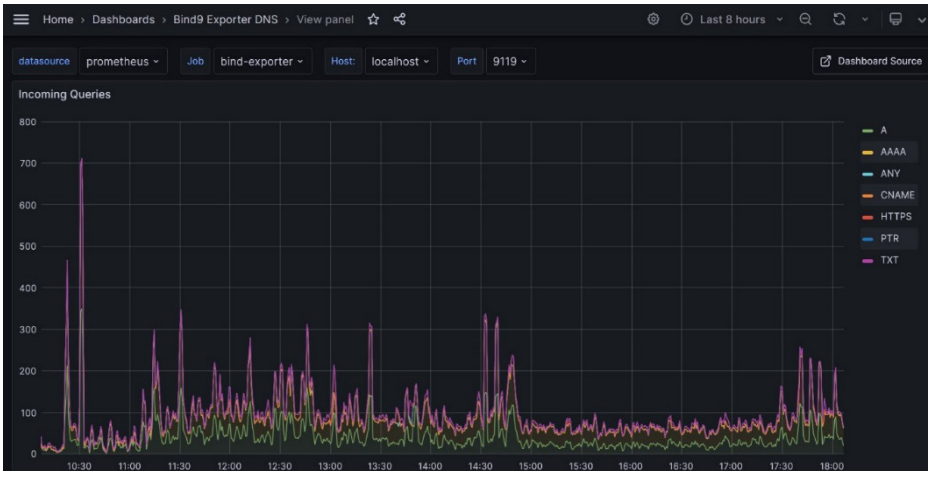
Monitoreo del sistema operativo en FreeBSD



El resultado obtenido para el servicio de Bind se muestra en la Figura 10, en donde se logra monitorear y obtener las métricas de las consultas que recibe el servidor DNS recursivo de la UNAM, tales consultas se clasifican con base en el tipo de registros que se tienen configurados en los DNS.

Figura 10

Gráfica de consultas recibidas en DNS



Además de permitir visualizar en tiempo real las consultas que recibe el DNS, también los administradores del servicio pueden observar la información de días anteriores, meses e incluso años, de acuerdo con la configuración elegida, lo que da oportunidad a realizar análisis o generación de reportes con la información.

https://doi.org/10.22201/dgtic.ctud.2024.2.2.53 Vol. 2, Núm. 2. abril-junio 2024, págs. 32 - 32

5. CONCLUSIONES

La implementación del sistema de monitoreo y visualización de consultas recibidas en el DNS con Grafana y con la fuente de datos de Prometheus, se logró integrar exitosamente al servidor que brinda el servicio de DNS recursivo en la UNAM, con la ayuda de los *dashborads* Bind9 Exporter DNS y Node Exporter FreeBSD que ofrece Grafana que permiten la representación gráfica de los datos exportados.

Al obtener los resultados que se plantearon en el objetivo, dicha implantación se propondrá para llevar a cabo en los DNS autoritativos de la UNAM, para ofrecer las mismas métricas y brindar un sistema de monitoreo interno en el NIC-UNAM de la DGTIC a los administradores del servicio.

REFERENCIAS

DNS autoritativo frente a recursivo (9 de agosto de 2023). https://powerdmarc.com/es/authoritative-vs-recursive-dns/

Grafana_Dashboard-12309. (2024). Bind9 Exporter DNS. https://grafana.com/grafana/dashboards/12309-bind9-exporter-dns/

Grafana_Dashboard-4260. (2024). Node Exporter FreeBSD. https://grafana.com/grafana/dashboards/4260-node-exporter-freebsd/

Openwebinars (27 de diciembre de 2021). https://openwebinars.net/blog/que-es-grafana-y-primeros-pasos/

Ramírez Fernández, E. R. (2023). *Implementación de técnicas de observabilidad en el Centro de Monitoreo de la Red*. Cuadernos Técnicos Universitarios de la DGTIC, 1 (1), páginas (169 - 184). https://doi.org/10.22201/dgtic.ctud.2023.1.1.17