

Tabla de Contenido

| | |
|---|-----------|
| 1. Introducción | 1 |
| 1.1. Sistema de Nombres de Dominio | 1 |
| 1.1.1. Importancia del sistema DNS | 1 |
| 1.2. Motivación | 2 |
| 1.3. Objetivos | 3 |
| 1.3.1. Objetivos generales | 3 |
| 1.3.2. Objetivos específicos | 3 |
| 1.4. Trabajos Relacionados | 4 |
| 2. Marco Teórico | 5 |
| 2.1. Funcionamiento del DNS | 5 |
| 2.2. Administración de Nombres de dominio | 5 |
| 2.3. Paquetes DNS | 6 |
| 2.4. Captura de paquetes DNS | 7 |
| 2.4.1. Fievel | 8 |
| 2.4.2. Packetbeat | 8 |
| 2.4.3. Collectd | 8 |
| 2.4.4. DNS Statistics Collector | 9 |
| 2.4.5. gopassivedns | 9 |
| 2.5. Almacenamiento de datos | 10 |
| 2.5.1. Prometheus | 11 |
| 2.5.2. Druid | 12 |
| 2.5.3. ClickHouse | 13 |
| 2.5.4. InfluxDB | 13 |
| 2.5.5. ElasticSearch | 14 |
| 2.5.6. OpenTSDB | 14 |
| 2.6. Visualización de datos | 15 |
| 2.6.1. Kibana | 15 |
| 2.6.2. Grafana | 15 |
| 2.6.3. Graphite Web | 16 |
| 3. Definición del Problema y Análisis de Softwares Open Source | 17 |
| 3.1. Especificación del problema | 17 |
| 3.1.1. Métricas DNS a medir | 17 |
| 3.1.2. Captura de datos | 18 |
| 3.1.3. Almacenamiento | 18 |

| | | |
|------------|---|-----------|
| 3.1.4. | Visualización | 18 |
| 3.2. | Análisis de softwares a utilizar | 19 |
| 3.2.1. | Captura de datos | 19 |
| 3.2.2. | Almacenamiento de datos | 20 |
| 3.2.2.1. | Benchmark de sistemas de almacenamiento | 20 |
| 3.2.2.1.1. | Bases de datos a evaluar | 20 |
| 3.2.2.1.2. | Datos de prueba | 21 |
| 3.2.2.1.3. | Mediciones a realizar | 21 |
| 3.2.2.1.4. | Carga de prueba | 22 |
| 3.2.2.1.5. | Ejecución de pruebas | 22 |
| 3.2.2.1.6. | Resultados | 22 |
| 3.2.2.2. | Análisis de resultados | 24 |
| 3.2.3. | Visualización | 25 |
| 4. | Implementación de la Solución | 26 |
| 4.1. | Trabajo a desarrollar | 26 |
| 4.2. | Arquitectura de la solución | 26 |
| 4.3. | Implementación | 27 |
| 4.3.1. | Captura de datos | 27 |
| 4.3.2. | Almacenamiento y agregación | 28 |
| 4.3.3. | Visualización | 28 |
| 4.3.4. | Integración y ejecución | 28 |
| 4.4. | Pruebas de funcionamiento | 29 |
| 4.4.1. | Datos de prueba | 29 |
| 4.4.2. | Validación de captura | 29 |
| 4.4.3. | Prueba de inserción paralela de datos y visualización | 30 |
| 4.4.4. | Prueba de carga por inundación | 33 |
| 4.4.5. | Prueba de alertas | 33 |
| 4.4.6. | Utilización de ancho de banda y encriptación | 34 |
| 5. | Conclusión | 36 |
| 5.1. | Trabajo Futuro | 37 |
| 6. | Bibliografía | 39 |
| 7. | Apéndice | 42 |
| 7.1. | Apéndice 1: Resultado benchmarks | 42 |
| 7.1.1. | 5 Dominios más consultados | 42 |
| 7.1.1.1. | Utilización total de CPU | 42 |
| 7.1.1.2. | Utilización de CPU media | 43 |
| 7.1.1.3. | Utilización de memoria principal | 44 |
| 7.1.1.4. | Utilización de memoria secundaria | 45 |
| 7.1.1.5. | Tiempo de consulta | 46 |
| 7.1.2. | Máscaras de red IPv4 | 47 |
| 7.1.2.1. | Utilización total de CPU | 47 |
| 7.1.2.2. | Utilización de CPU media | 48 |
| 7.1.2.3. | Utilización de memoria principal | 49 |

| | | |
|----------|---|----|
| 7.1.2.4. | Utilización de memoria secundaria | 50 |
| 7.1.2.5. | Tiempo de consulta | 51 |
| 7.1.3. | Largo de paquetes de respuesta | 52 |
| 7.1.3.1. | Utilización total de CPU | 52 |
| 7.1.3.2. | Utilización de CPU media | 53 |
| 7.1.3.3. | Utilización de memoria principal | 54 |
| 7.1.3.4. | Utilización de memoria secundaria | 55 |
| 7.1.3.5. | Tiempo de consulta | 56 |
| 7.2. | Apéndice 2: Consultas para generación de base de datos | 57 |
| 7.3. | Apéndice 3: Consultas para obtención de métricas para Grafana | 59 |
| 7.4. | Apéndice 4: Ejecución de los servicios a través de Docker Compose | 61 |