Integrasi Telegraf, InfluxDB OSS V2, dan Grafana dalam Monitoring Trafik Jaringan berbasis NetFlow

Firdaus[1)]

[1)] Komputer Dan Bisnis, Politeknik Negeri Tanah Laut
[1)] firdaus@mhs.politala.ac.id

Abstrak

Dalam dunia jaringan modern, pemantauan trafik sangat penting untuk menjaga stabilitas, efisiensi, dan keamanan sistem jaringan. Salah satu protokol yang digunakan untuk memantau trafik adalah NetFlow. Namun, dibutuhkan sistem yang dapat mengumpulkan, menyimpan, dan memvisualisasikan data NetFlow secara efisien. Penelitian ini membahas penerapan *stack open source* TIG (Telegraf, InfluxDB, Grafana) untuk membangun sistem monitoring trafik jaringan berbasis NetFlow. Sistem ini menggunakan Telegraf sebagai kolektor data, InfluxDB sebagai penyimpanan time-series, dan Grafana sebagai alat visualisasi. Dengan pendekatan ini, data trafik dapat divisualisasikan secara *real-time* dan historis melalui *dashboard* interaktif. Penelitian ini menggunakan metode eksperimen dengan lingkungan virtualisasi Docker. Hasil pengujian menunjukkan bahwa sistem ini efektif untuk monitoring trafik jaringan dalam skala kecil hingga menengah.

Kata kunci: *NetFlow, Telegraf, InfluxDB, Grafana,* Monitoring Jaringan

Abstract

In modern networking, traffic monitoring is essential for maintaining the stability, efficiency, and security of network systems. One of the protocols used for traffic monitoring is NetFlow. However, an efficient system is needed to collect, store, and visualize NetFlow data. This study discusses the implementation of the open-source TIG stack (Telegraf, InfluxDB, Grafana) to build a NetFlow-based network traffic monitoring system. The system uses Telegraf as the data collector, InfluxDB as the time-series data storage, and Grafana as the visualization tool. With this approach, traffic data can be visualized in real-time and historically through an interactive dashboard. This research uses an experimental method within a Docker-based virtualization environment. The test results show that the system is effective for monitoring network traffic in small to medium-scale

Keywords: *NetFlow, Telegraf, InfluxDB, Grafana, Network Monitoring*

1. PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, lalu lintas data jaringan menjadi aset penting bagi organisasi. Pemantauan lalu lintas jaringan (*network traffic monitoring*) menjadi hal esensial dalam memastikan keamanan, ketersediaan, dan efisiensi infrastruktur jaringan. NetFlow merupakan salah satu protokol yang banyak digunakan dalam memantau trafik jaringan karena mampu memberikan informasi rinci mengenai pola komunikasi antar host.

Solusi *open source* seperti Telegraf, InfluxDB, dan Grafana (dikenal sebagai stack TIG) menawarkan alternatif ringan dan fleksibel untuk pengumpulan, penyimpanan, serta visualisasi data jaringan. Telegraf bertindak sebagai agent pengumpul data, InfluxDB sebagai basis data time-series untuk menyimpan data, dan Grafana digunakan untuk visualisasi dalam bentuk *dashboard* interaktif.

2. TINJAUAN PUSTAKA

2.1 Pengertian *Netflow*

NetFlow adalah protokol dari Cisco yang digunakan untuk mengumpulkan informasi statistik tentang lalu lintas jaringan IP. NetFlow memungkinkan administrator untuk melihat siapa yang berbicara dengan siapa, kapan, dan dengan *volume* berapa.

2.2 *Pengertian Telegraf*

Telegraf adalah agent ringan berbasis plugin yang mengumpulkan dan mengirimkan data ke berbagai *backend* termasuk InfluxDB.

2.3 *Pengertian Influxdb*

InfluxDB merupakan *time-series* database yang dirancang untuk data performa sistem dan jaringan. Cocok digunakan untuk menyimpan data NetFlow.

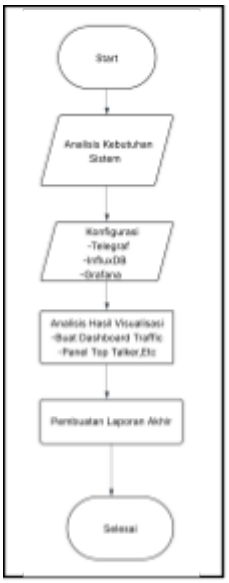
2.4 *Pengertian Grafana*

Grafana adalah alat *open source* untuk visualisasi data yang mendukung banyak sumber data termasuk InfluxDB.

3. METODE PENELITIAN

3.1 Diagram Alir

Gambar 3.1 dibawah adalah kerangkan penelitian yang digunakan dalam Integrasi Telegraf, InfluxDB, dan Grafana dalam Monitoring Trafik Jaringan berbasis NetFlow



Gambar 3.1 Diagram Yang Dipakai

Adapun langkah langkah yang akan dilakukan meliputi

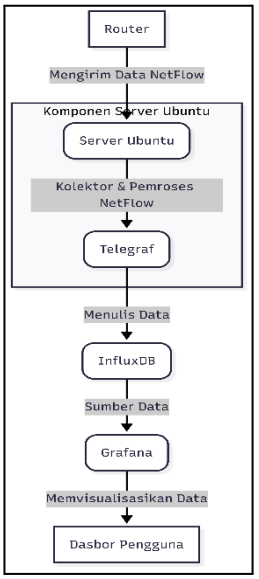
1. Konfigurasi Telegraf sebagai NetFlow *collector*
2. Konfigurasi InfluxDB sebagai basis data *time-series*
3. Konfigurasi data source di Grafana
4. Analisis hasil visualisas

3.2 Rancangan Sistem

Sistem ini dirancang untuk memantau dan memvisualisasikan lalu lintas jaringan secara komprehensif menggunakan kombinasi Telegraf, InfluxDB, dan Grafana, dengan NetFlow sebagai sumber data utama. Alur kerjanya dimulai dengan router yang dikonfigurasi untuk mengirimkan data NetFlow ke server Ubuntu. Di server tersebut, Telegraf berperan sebagai

p-ISSN: 3031-7118
e-ISSN: 3026-7870

agen pengumpul metrik, menangkap *stream* data NetFlow, memprosesnya, dan mengubahnya ke format yang sesuai sebelum dimasukkan ke dalam InfluxDB. Sebagai basis data *time-series*, InfluxDB sangat ideal untuk menyimpan metrik lalu lintas jaringan yang berubah seiring waktu, dengan *timestamp* yang akurat. Setelah data tersimpan dengan aman di InfluxDB, Grafana kemudian terhubung ke sana sebagai sumber data. Grafana memungkinkan pengguna untuk membuat *dashboard* interaktif, menampilkan metrik lalu lintas jaringan dalam berbagai format visual yang mudah dipahami. Sistem ini memberikan keuntungan signifikan dalam pemantauan *real-time*, analisis mendalam, peningkatan visibilitas jaringan, serta skalabilitas dan fleksibilitas berkat penggunaan tools open-source.



Gambar 3.2 Alur Kerja Sistem

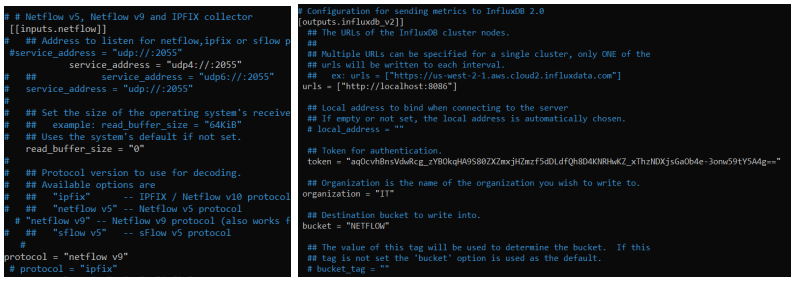
4. PEMBAHASAN

4.1 Implementasi Sistem

Router dikonfigurasi mengirim NetFlow v9 ke port UDP 2055 Menuju server Telegraf. Telegraf membaca data dan menulisnya ke InfluxDB sesuai konfigurasi plugin NetFlow. Dashboard Grafana dikustomisasi untuk menampilkan metrik seperti bandwidth usage, top talkers, dan penggunaan protokol.

4.1.2 Konfigurasi Telegraf

Konfigurasi Telegraf dilakukan dengan mengaktifkan input NetFlow menggunakan service_address, IP, dan port untuk menerima data trafik. Untuk menyimpan data ke InfluxDB v2, lalu aktifkan output InfluxDB v2 dengan mengisi URL server, token, nama organisasi, dan bucket.

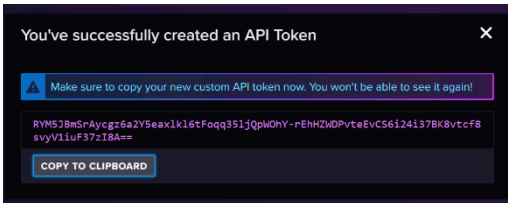


Gambar 4.1.2 Konfigurasi Telegraft

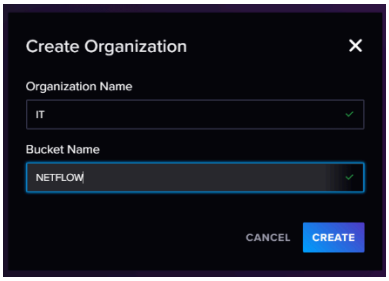
4.1.2 Konfigurasi InfluxDB OSS V2

Konfigurasi influxdb dilakukan dengan membuat organization nama bucket dan api

p-ISSN: 3031-7118
e-ISSN: 3026-7870



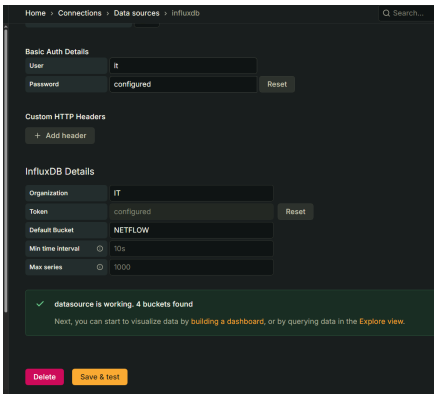
Gambar 4.1.2.1 Token Dibuat



Gambar 4.1.2.2 Membuat Organisasi Dan Bucket

4.1.3 Konfigurasi Grafana

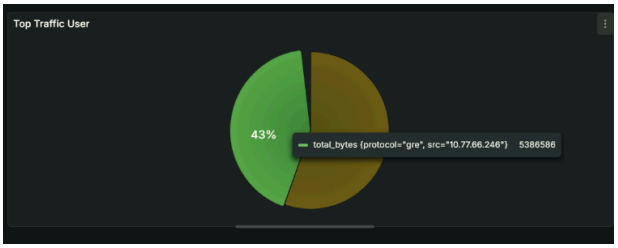
Konfigurasi grafana untuk menampilkan data netflow yang dikumpulkan oleh telegraf dan disimpan dalam influxdb oss v2 melalui cara menambah data *source* influxdb dengan mengisi *cresedensial ,form* url *,token,organization,bucket* dan melakukan *test & sav*e jika



Gambar 4.1.3 isi Konfigurasi Dan Test Data Di Grafana

4.2 Analisis Hasil Visualisasi

Dibab ini akan dilakukan uji coba terkait penarikan data dari influxdb untuk di tampilkan di dashboard grafana



Gambar 4.2.1 *Top Traffic User*

p-ISSN: 3031-7118
e-ISSN: 3026-7870

Gambar 4.2.2 Gambar Protocol Yang Sering Dipakai

5. Kesimpulan

1) Telegraf, InfluxDB , Grafana berhasil diterapkan untuk monitoring trafik NetFlow secara efisien.
2) Telegraf mampu mengoleksi data NetFlow dengan stabil dan ringan.
3) Visualisasi melalui Grafana membantu dalam menganalisis lalu lintas jaringan secara *real-time* dan historis.
4) Solusi ini cocok untuk digunakan di lingkungan jaringan kecil hingga menengah.

6. Terima Kasih

Penulis mengucapkan terima kasih kepada dosen pembimbing dan semua pihak yang telah mendukung penulisan ini, serta kepada komunitas *open source Tool* yang dipakai atas dokumentasinya sangat membantu selama proses pengembangan

7. Daftar Pustaka

[1] Cisco Systems. “Introduction to Cisco NetFlow.” Cisco.com, 2020.
[2] InfluxData. “Telegraf Documentation.” https://docs.influxdata.com/telegraf/, 2024.
[3] Grafana Labs. “Grafana Documentation.” https://grafana.com/docs/, 2024

Biodata Penulis

Firdaus, lahir di Pelaihari 16 Oktober 2002. Mahasiswa Program Studi D4 Teknologi Rekayasa Komputer Jaringan di Politeknik Negeri Tanah Laut. Aktif dalam pengembangan sistem jaringan, open source, dan monitoring sistem. Saat ini sedang menyelesaikan PKL tentang **ANALISIS INTEGRASI TOOL MONITORING *OPEN SOURCE* TERHADAP TRAFIK USER DAN PERFORMA PERANGKAT JARINGAN**