DevOps - Logging & Monitoring

Pengantar Elastic Stack

Pesantren Teknologi Informasi dan Komunikasi
Jln. Mandor Basar No. 54 RT 01/RW 01 Rangkapanjaya,
Pancoran Mas, Depok 16435 | Telp. (021) 77 88 66 91
Koordinat (-6.386680 S, 106.777305 E)
www.petik.or.id

Elastic Stack

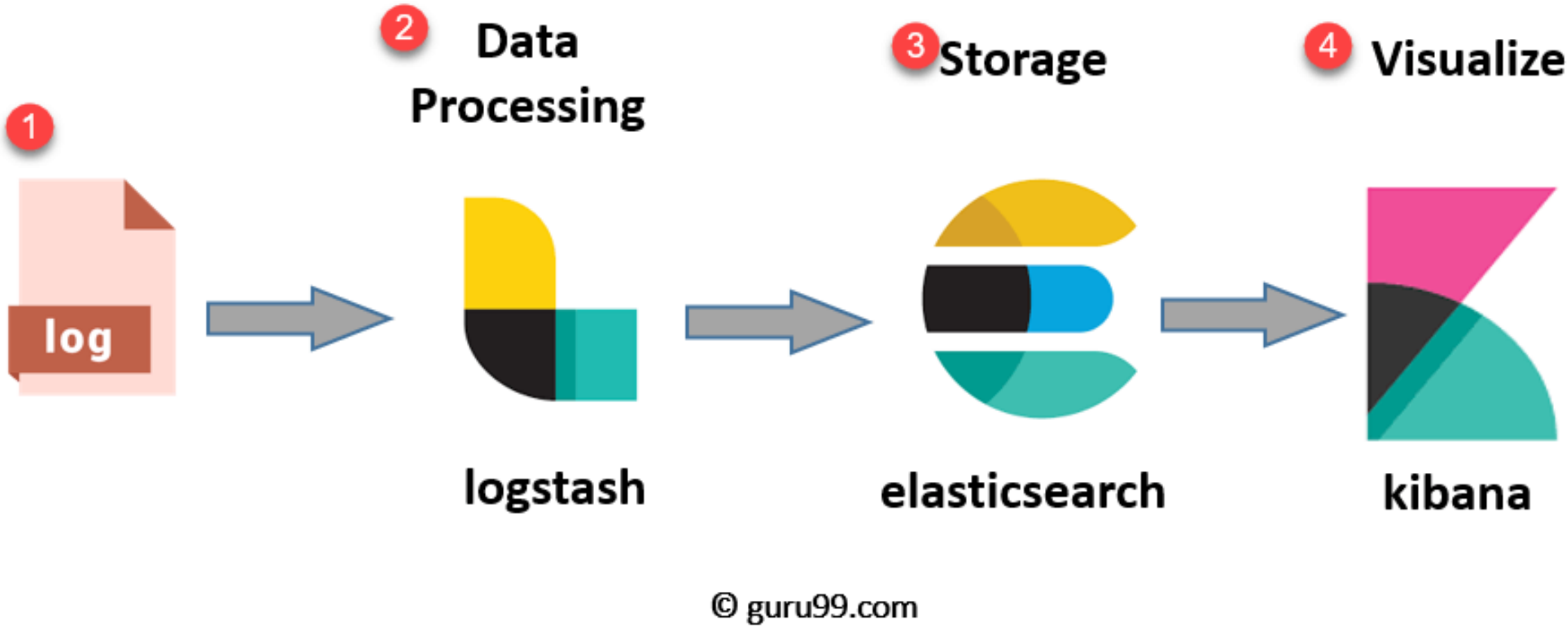
- Elastic Stack – sebelumnya dikenal sebagai ELK Stack – adalah kumpulan software open-source yang dibuat oleh Elastic yang memungkinkan untuk mencari, menganalisis dan memvisualisasikan log yang dihasilkan dari sumber apapun dan dalam format apapun, lebih dikenal dengan istilah logging terpusat.
- Logging terpusat sangat berguna ketika mencoba mengidentifikasi masalah dengan server atau aplikasi Anda karena memungkinkan Anda untuk mencari semua log Anda di satu tempat.

Komponen Elastic Stack

Elastic Stack terdiri dari empat komponen utama, yaitu:

- Elasticsearch, mesin pencari RESTful terdistribusi yang menyimpan semua data yang dikumpulkan.
- Logstash, komponen pemrosesan data yang akan mengirimkan data yang masuk ke Elasticsearch.
- Kibana, antarmuka web untuk mencari dan memvisualisasikan log.
- Beats, lightweight single-purpose data shippers yang dapat mengirimkan data dari ratusan bahkan ribuan mesin baik ke Logstash maupun ke Elasticsearch.

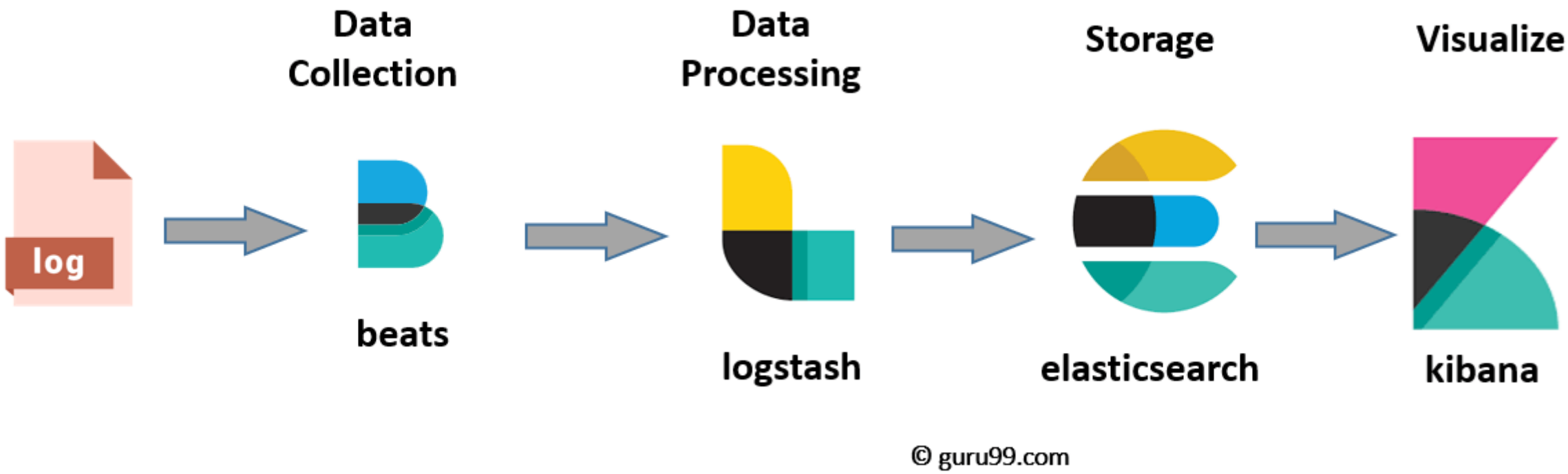
Arsitektur Klasik ELK



Arsitektur Klasik ELK

- Logs: Server log yang perlu dianalisis diidentifikasi
- Logstash: Mengumpulkan log dan data peristiwa, juga mem-parsing dan mengubah data
- ElasticSearch: Data yang diubah dari Logstash disimpan dan dibuatkan index
- Kibana: Kibana menggunakan database Elasticsearch untuk dieksplorasi, divisualisasi dan di-*share*

Arsitektur Elastic Stack



Arsitektur Elastic Stack

- Diperlukan satu komponen lagi untuk mengumpulkan data yang disebut Beats. Hal ini menyebabkan Elastic mengubah nama ELK menjadi Elastic Stack.

Apa itu Elasticsearch?

- Elasticsearch adalah basis data NoSQL.
- Dibuat dengan basis mesin pencari Apache Lucene, dan dibangun dengan RESTful APIS.
- Menawarkan penyebaran sederhana, keandalan maksimum, dan manajemen yang mudah.
- Juga menawarkan Query lanjutan untuk melakukan analisis detail dan menyimpan semua data secara terpusat. Sangat membantu untuk melakukan pencarian cepat dokumen.

Apa itu Logstash?

- Logstash adalah pipeline tool pengumpulan data.
- Mengumpulkan input data dan memasukkannya ke dalam Elasticsearch.
- Mengumpulkan semua jenis data dari sumber yang berbeda dan membuatnya tersedia untuk digunakan lebih lanjut.

Komponen Logstash

Logstash terdiri dari tiga komponen:

- Input: meneruskan log untuk memprosesnya menjadi format yang dapat dimengerti mesin
- Filter: serangkaian kondisi untuk melakukan tindakan atau peristiwa tertentu
- Keluaran: Pengambil keputusan untuk peristiwa atau log yang diproses

Apa itu Kibana?

- Kibana adalah visualisasi data yang melengkapi ELK stack.
- Digunakan untuk memvisualisasikan dokumen Elasticsearch.
- Dasbord Kibana menawarkan berbagai diagram interaktif, data geospasial, dan grafik untuk memvisualisasikan permintaan yang kompleks.

Apa itu Filebeat?

- Filebeat adalah pengirim ringan (lightweight shipper) untuk meneruskan dan memusatkan data log.
- Diinstal sebagai agen di server Anda, Filebeat memantau file log atau lokasi yang Anda tentukan, mengumpulkan peristiwa log, dan meneruskannya ke Elasticsearch atau Logstash untuk pengindeksan.

Pesantren Teknologi Informasi dan Komunikasi

PeTIK

Creates Future Skilled Professionals

Jalan Mandor Basar Nomor 54, RT. 01/001, Rangkapanjaya, Pancoran Mas, Kota Depok 16435

www.petik.or.id

021 7788 6691

info@petik.or.id