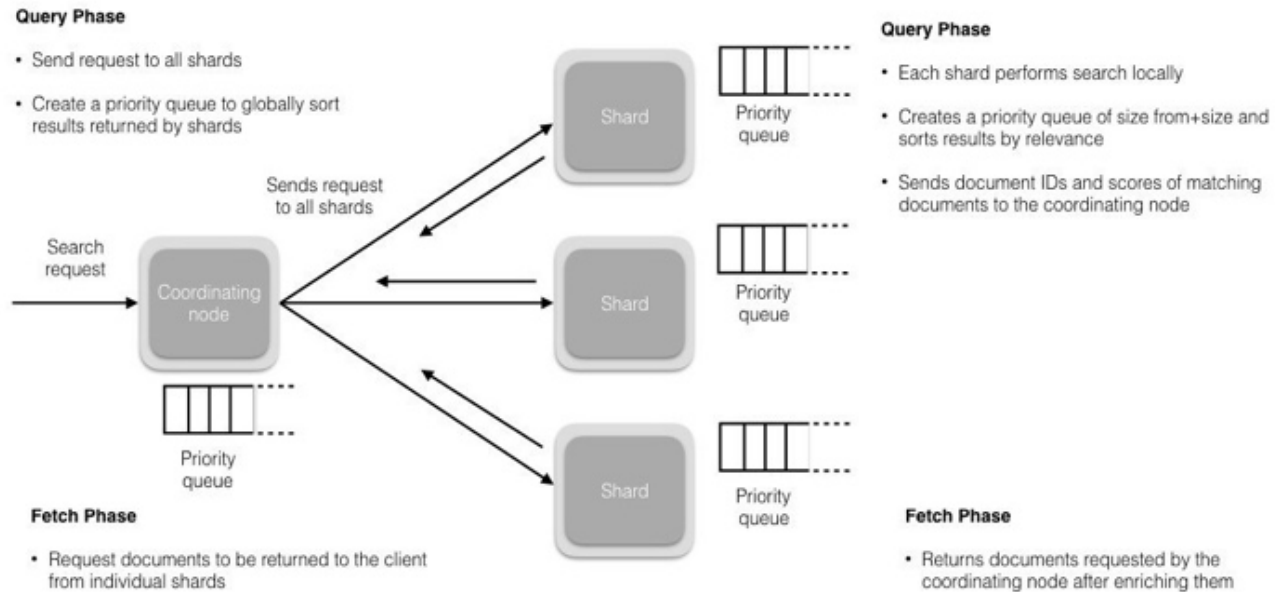


Elasticsearch & Kibana

Elasticsearch

- Full-text search engine.
- Based on the Lucene library.
- HTTP web interface and schema-free JSON documents.






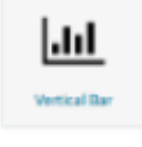


Understanding Kibana aggregations



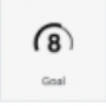
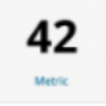
- There are two types of aggregations
 - **Bucket** aggregations groups documents together in one bucket according to your logic and requirements
 - **Metric** aggregations are used to calculate a value for each bucket based on the documents inside the

Metric aggregations	Bucket aggregations
<ul style="list-style-type: none"> • Count • Sum • Average • Media • Min • Max • Unique Count • Standard Deviation • Percentiles • Percentile Ranks 	<ul style="list-style-type: none"> • Date Histogram • Date Range • Filters • Histogram • IPv4 Range • Range • Terms • Significant Terms • Geohash



Basic Charts

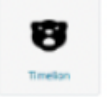

 Area	For visualizing time series data and for splitting lines on fields	Users over time
 Heat Map	For showing statistical outliers and are often used for latency values	Latency and outliers
 Horizontal Bar	Good for showing relationships between two fields	URL and referrer
 Line	are a simple way to show time series and are good for splitting lines to show anomalies	Average CPU over time by host
 Pie	Useful for displaying parts of a whole	Top 5 memory consuming system procs
 Vertical Bar	Great for time series data and for splitting lines across fields	URLs over time





Data

	Best way to split across multiple fields in a custom way	Top user, host, pod, container by usage
	A way to show the status of a specific metric using thresholds you define	Memory consumption limits
	Similar to a Gauge, useful for monitoring a specific metric defined as a goal	No. of errors per service
	Useful visualization for displaying a calculation as a single number	No. of Docker containers run.

Map, Time series, and Others

		Help add a geographical dimension to IP-based logs	Geographic origin of web server requests.
--	--	--	---

		Allows you to create more advanced queries based on time series data	Percentage of 500 errors over time
---	---	--	------------------------------------

	Experimental - Allows you to create selectors or sliders for alternating between options.	Switch between
	A great way to add a customized text or image based visualization to your dashboard based on markdown syntax	Company logo or a description of a dashboard
	Helps display groups of words sized by their importance	Countries sending requests to a web server
	Experimental - allows you to add custom visualizations based on Vega and VegaLite	-

(chungut@soict.hust.edu.vn)