Elasticsearch SQL Webinar

Arthur Gimpel
Solutions Architect

Agenda

1. What is Elasticsearch SQL?
2. Text operators and relevancy
3. Aggregations
4. Geographic queries

What is Elasticsearch SQL

SQL Interface to Elasticsearch

- SQL interpreter for Elasticsearch queries
- Based on Elasticsearch API's & ANSI SQL
- Lightweight and scalable

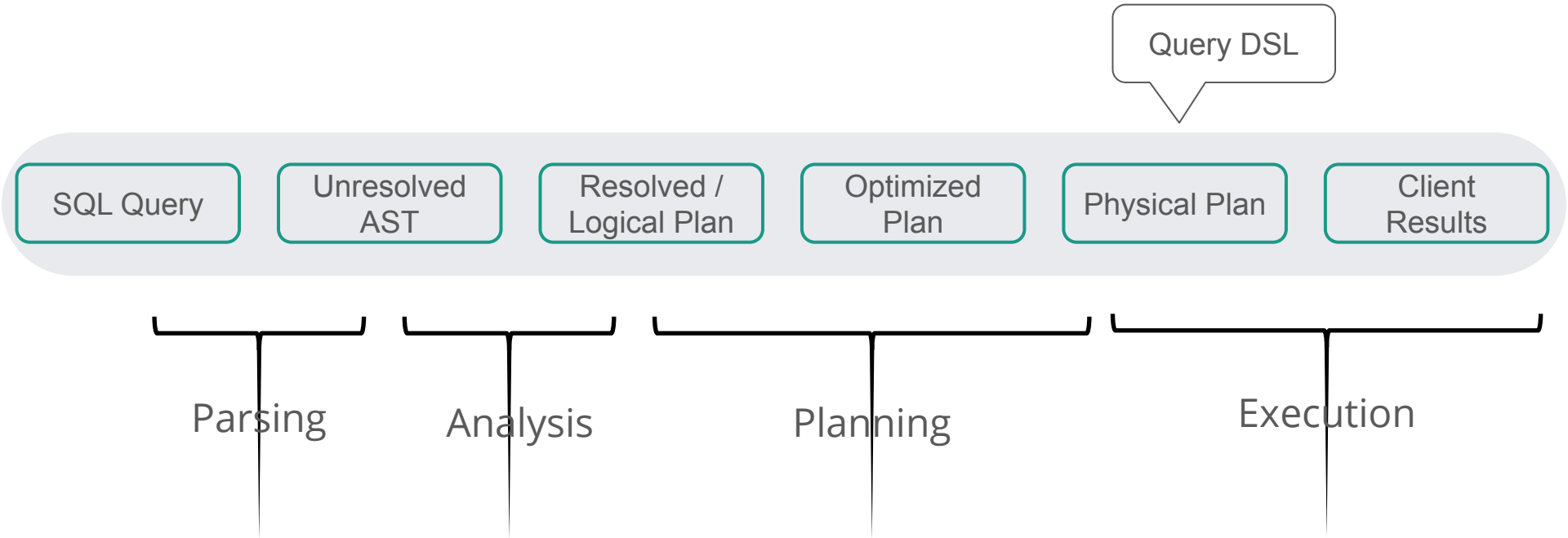
Elasticsearch SQL <> RDBMS

Terminological Differences

Relational Databases (RDBMS)	Elasticsearch SQL
Column	Field
Row	Document
Table	Index
View	Alias
Schema	- (Security can enforce “schema”)
Database / Catalog	-
Instance / Cluster	Cluster / Clusters (Federated via CCS)

Elasticsearch SQL Execution

SQL Interpreter Internals



Demo

Agenda

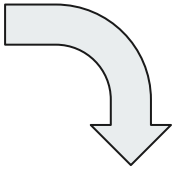
1. What is Elasticsearch SQL?
2. Text operators and relevancy
3. Aggregations
4. Geographic queries

Text Operators and Relevancy

Fulltext Search with Elasticsearch SQL

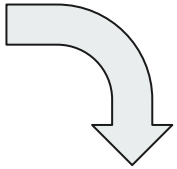
- Within the WHERE clause there are two predicates made for full text:
  - MATCH (field(s) to match, matching text, optional parameters)
  - QUERY (query_string, optional parameters)
- The SCORE() function is used to project the result of the scoring. Can be used in the scope of SELECT, ORDER BY clauses

```
"match" : {
  "full_name" : {
    "query" : "arthur gimpel",
    "operator" : "AND“
  }
}
```



```
SELECT
…
WHERE MATCH('full_name', 'arthur gimpel',
‘operator=and’);
```

```
"multi_match" : {
   "query" : "Lee",
   "fields" : [
     "first_name",
     "last_name^2.0"]
  }
```



```
SELECT
…
WHERE MATCH(‘first_name, last_name^2.0’ , ‘Lee’)
```

Demo

Agenda

1. What is Elasticsearch SQL?
2. Text operators and relevancy
3. Functions and Aggregations
4. Geographic queries

Functions and Aggregations

Types of Functions in Elasticsearch SQL

Aggregate Functions	Scalar Functions
Metric Aggregations: COUNT, SUM, MAX, AVG…	**Math:** ABS, SQRT, LOG, COS, SIN, ACOS, ASIN….
GROUPING (except GROUP BY): HISTOGRAM	**String:** RIGHT,LEFT,SUBSTRING,LENGTH, UCASE…
	Conversion: CAST,CONVERT
	Date: DAY, MONTH, YEAR, NOW, MONTH_NAME…
	Conditional: IIF, ISNULL, CASE, NULLIF, GREATEST…
	Geo: ST_AsWKT, ST_WKTToSQL, ST_X, ST_Y, ST_Z, ST_Distance…

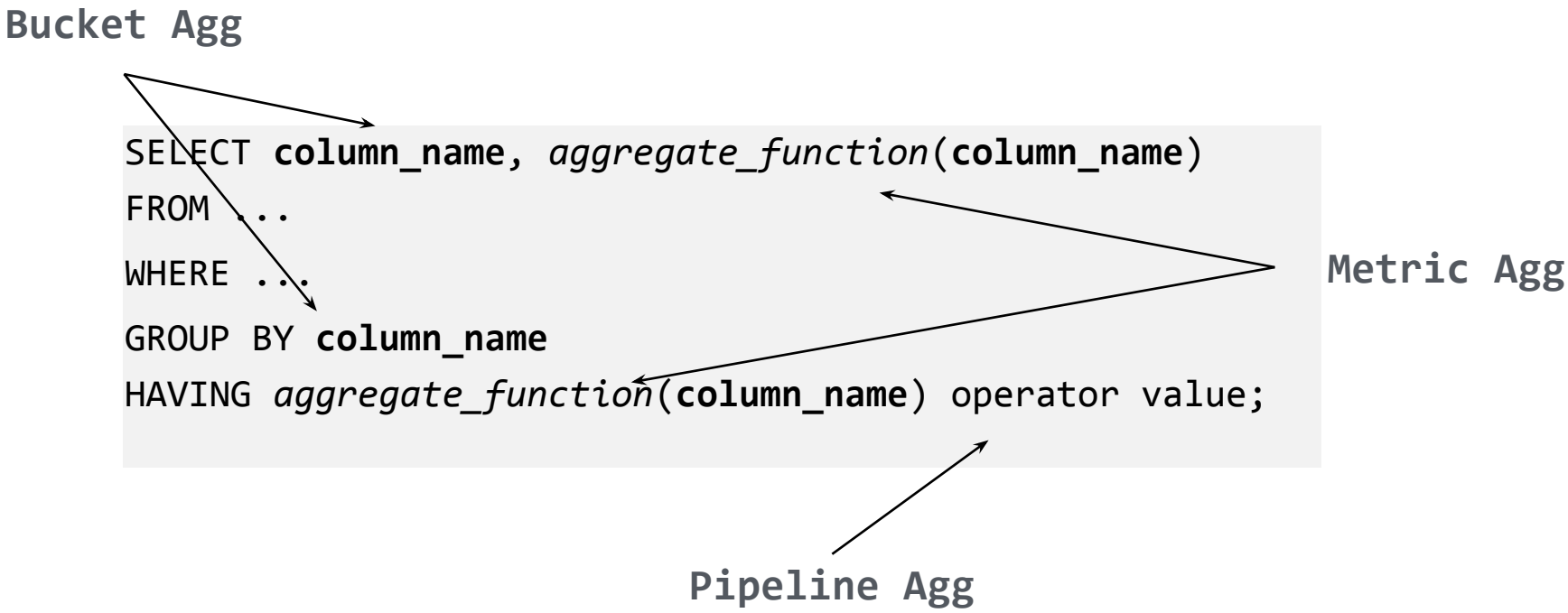
Functions and Aggregations

Group By & Having

```
SELECT column_name, aggregate_function(column_name)
FROM ...
WHERE ...
GROUP BY column_name
HAVING aggregate_function(column_name) operator value;
```

Functions and Aggregations

Group By & Having



Demo

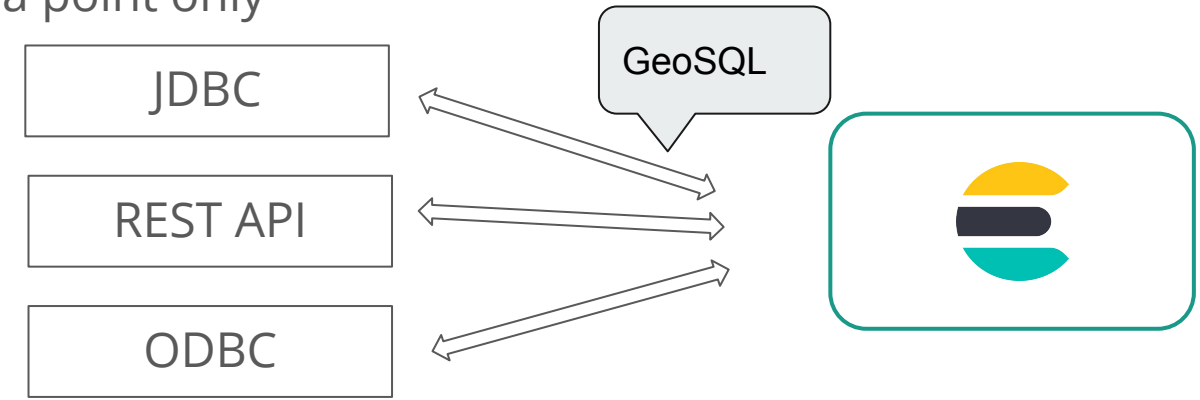
Agenda

1. What is Elasticsearch SQL?
2. Text operators and relevancy
3. Functions and Aggregations
4. Geographic queries

Geographic Queries

Standard GeoSQL Implementation on top of Elasticsearch

- Implements OpenGIS Simple Features Implementation Specification for SQL
- Currently supports ST_AsWKT, ST_WKTToSQL, ST_GeometryType, ST_X, ST_Y, ST_Z, ST_Distance
- Internally the Elasticsearch types supported are geo_point and geo_shape containing a point only



Demo

Q & A

Thank you