



Elasticsearch Query Language

ES|QL

David Pilato - @dadoonet
Developer | Evangelist

slides & demo



BNP PARIBAS
FORTIS



A brief history of Elasticsearch's analytical capabilities





ES|QL

- Language
- Engine
- Visualization

ES|QL

in action

<https://github.com/dadoonet/esql-demo>

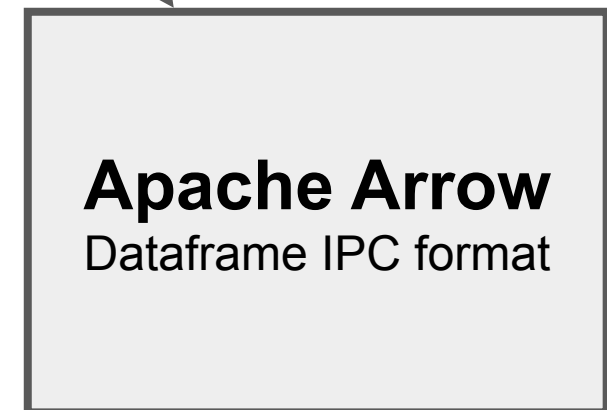
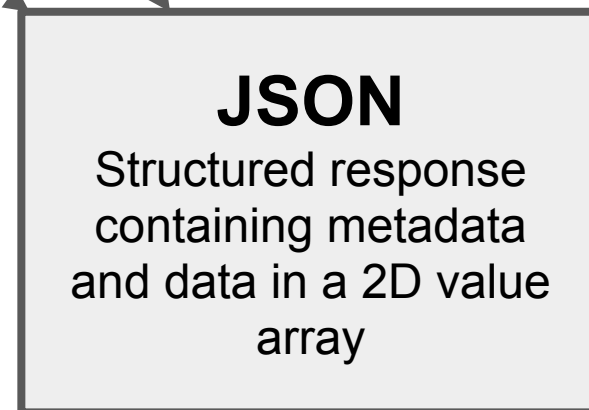
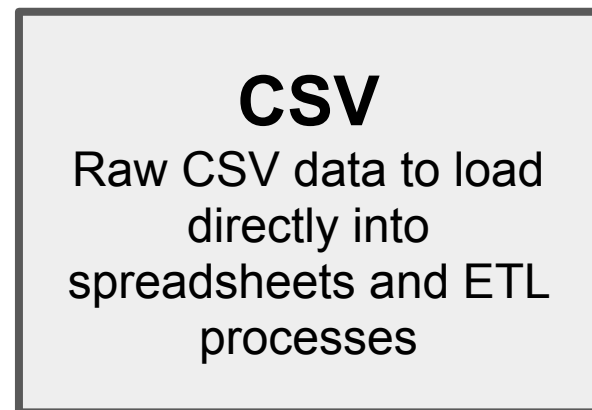
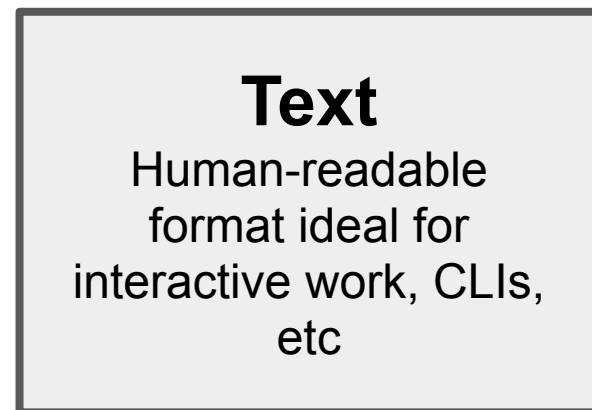
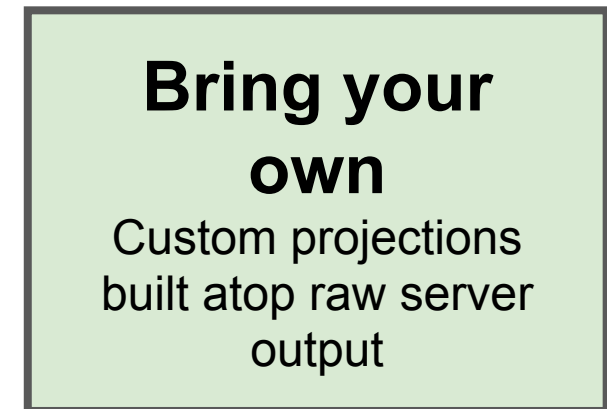
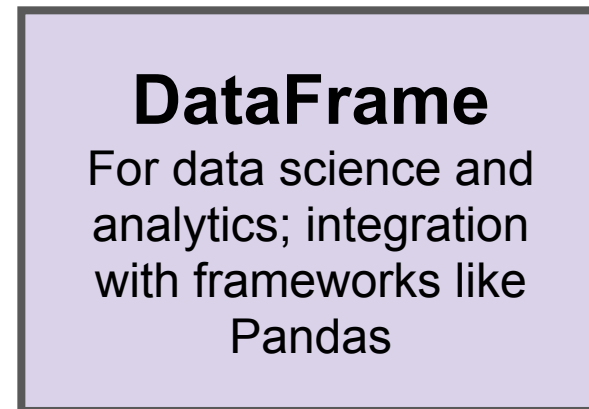
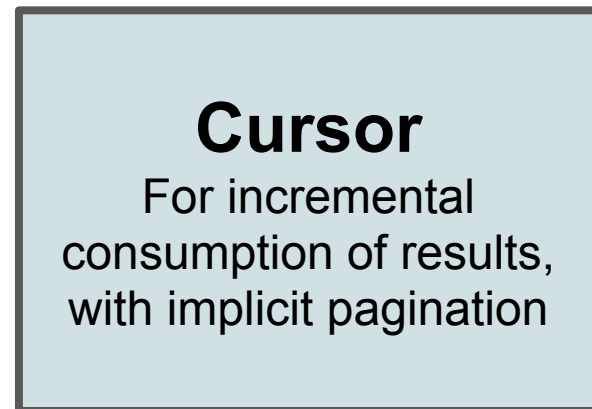
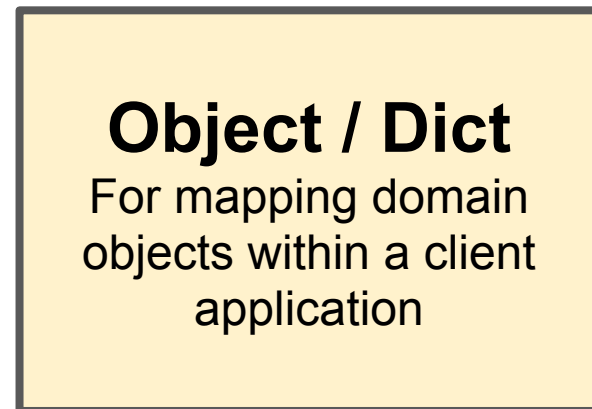
slides & demo



Ways to consume ES | QL results

RESULT DATA PROJECTIONS

Each language client will offer a selection of projections relevant to that language ecosystem.



Users can consume raw data directly from the server output in one of several formats.

Object API

<https://github.com/dadoonet/elasticsearch-java-client-demo>

```
String query = """
    FROM persons
    | WHERE name == "David"
    | KEEP name
    | LIMIT 1
    """;

Iterable<Person> persons = client.esql()
    .query(ObjectsEsqlAdapter.of(Person.class), query);
for (Person person : persons) {
    assertNull(person.getId());
    assertNotNull(person.getName());
}
```

ResultSet JDBC API

<https://github.com/dadoonet/elasticsearch-java-client-demo>

```
String query = ""
    FROM persons
    | WHERE name == "David"
    | KEEP name
    | LIMIT 1
    """;

try (ResultSet resultSet = client.esql()
    .query(ResultSetEsqAdapter.INSTANCE, query)) {
    assertTrue(resultSet.next());
    assertEquals("David", resultSet.getString(1));
}
```

A better dashboard experience with named parameters

```
POST /_query
{
  "query": ""
    from logs-*
    | stats x = ?function(?field) by ?breakdownField
    | where x >= ?value
  "",
  "params": [
    {"function": {"identifier": "avg"}},
    {"field": {"identifier": "network.bytes"}},
    {"breakdownField": {"identifier": "agent.name"}},
    {"value": 1000}
  ]
}
```


Run query

Filter your data using KQL syntax

Last 15 minutes

Refresh

Create visualization Add panel Add from library Controls

Table @timestamp & Effective_process.entity_id & Effective_process.executable &...

@timestamp	Effective_prc	Effective_prc	Effective_prc	Effective_prc
2024-10-21T -	-	-	-	-
2024-10-21T -	-	-	-	-
2024-10-21T -	-	-	-	-
2024-10-21T -	-	-	-	-
2024-10-21T -	-	-	-	-
2024-10-21T -	-	-	-	-
2024-10-21T -	-	-	-	-
2024-10-21T -	-	-	-	-

```

1 FROM nginx_logs*
2 | STATS mCount = COUNT(message) BY
  log.level, BUCKET(@timestamp, |

```

- Create control
- 1 day
- 1 hour
- 1 millisecond
- 1 minute
- 1 month
- 1 quarter
- 1 second

2 lines @timestamp

ES|QL Query Results

Visualization configuration

Suggestions 4

Cancel

Apply and close



Create ES|QL control

Filter your data using KQL syntax Last 15 minutes Refresh

Create visualization Add panel Add from library Controls

Table @timestamp & Effective_process.entity_id & Effective_process.executable &...

@timestamp	Effective_prc	Effective_prc	Effective_prc	Effective_prc
2024-10-21T -	-	-	-	-
2024-10-21T -	-	-	-	-
2024-10-21T -	-	-	-	-
2024-10-21T -	-	-	-	-
2024-10-21T -	-	-	-	-
2024-10-21T -	-	-	-	-
2024-10-21T -	-	-	-	-
2024-10-21T -	-	-	-	-

Type: Static values

Name: ?myInterval

Values: 5m, 10m, 1h, 3h, 12h, 1d, 7d, 14d
Comma separated values (e.g. 1h, 1m, 6h, 1d).

Label: Enter label (Optional)

Minimum width: Small Medium Large

Expand width to fit available space



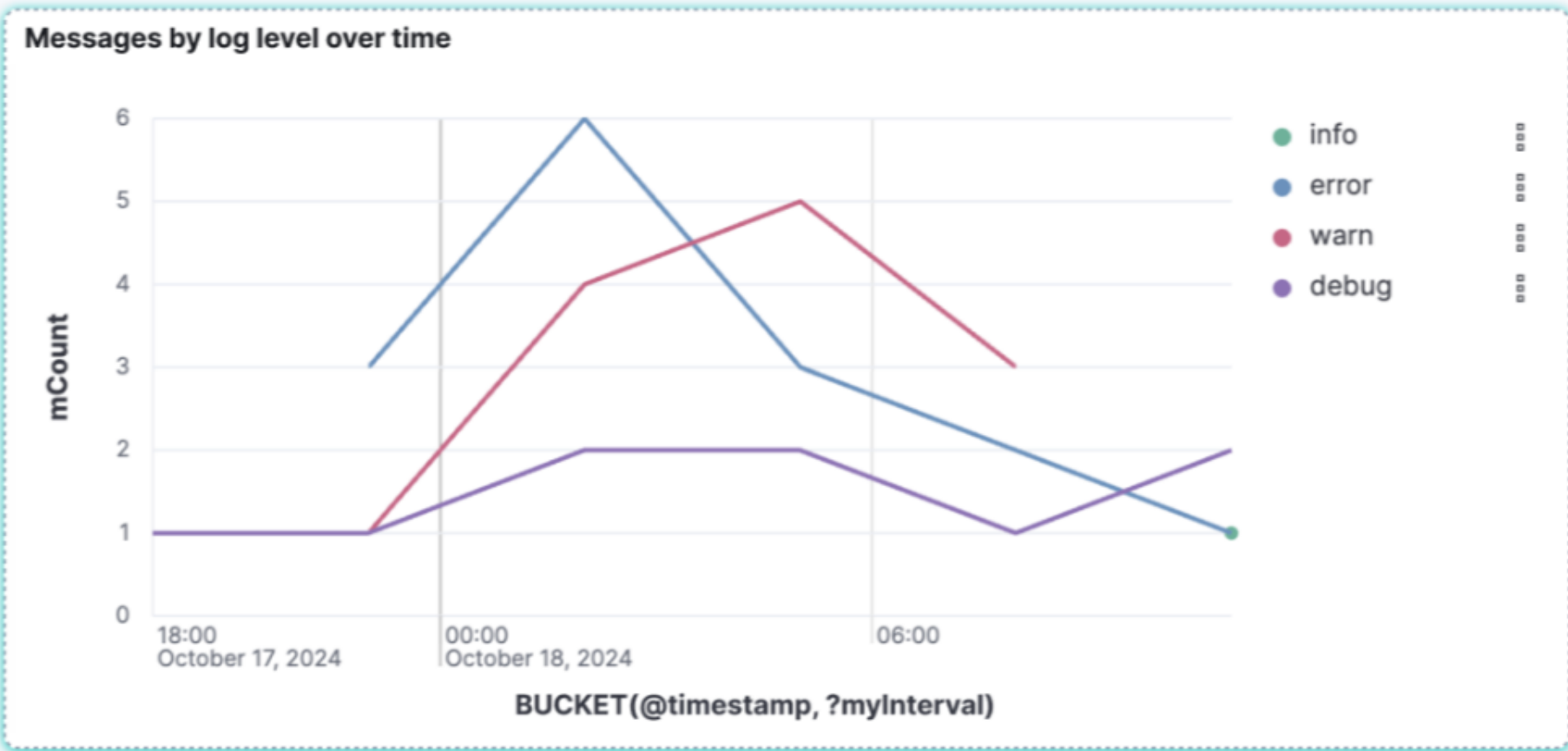
Filter your data using KQL syntax

Last 15 minutes

Refresh

Create visualization Add panel Add from library Controls

Interval 1 5m



Coming next

```
WHERE MATCH(actors, "Marlon*")  
WHERE QSTR("bytes:[1024 TO 2048]")
```

Coming next

```
WHERE KQL("bytes>=1024")
```

TBD

JOINS!

```
joinType JOIN indexName (AS qualifier)? condition?
```

```
joinType: LOOKUP | LEFT | RIGHT | INNER
```

```
condition:
```

```
  ON identifier == identifier  
| USING identifier
```

```
INLINESSTATS total_visits = COUNT()
```

```
FROM employees
```

```
| SORT emp_no
```

```
| LOOKUP JOIN languages_lookup ON language_code
```

```
| KEEP emp_no, language_name
```

- No need to create an enrich policy
- A drag and drop experience in the UI



Elasticsearch Query Language

ES|QL

David Pilato - @dadoonet
Developer | Evangelist

slides & demo



BNP PARIBAS
FORTIS

