Sumo Logic query examples

gist.github.com/danhodge/b56537bcbeb398188f7b70cd507fa09a

262588213843476

Setting the source

```
_sourceName=*service* _sourceName=*service*env_name
```

JSON parsing

```
... | json auto | json auto field=message
```

JSON + where

```
... | WHERE field_name = <value>
```

JSON + where field not missing

```
... | WHERE !(field_name = null)
```

Cast Field to Number

```
... | number(duration)
```

Math Operations

```
... | round(duration / 1000) as duration_secs
```

Statistical Calculations

`... | avg(field)` or `... | avg(field1) as field1, avg(field2) as field2` when multiple

Percentiles

```
... | pct(field, 50, 95, 99)
```

Timesliced Comparisons

Shows `avg(field)` in 15 minutes timeslices grouped by day over the past 8 days

```
... | timeslice 15m | avg(field) by _timeslice | compare with timeshift 1d 8
```

Timesliced Graphs

Graphs `count(status, path, _timeslice)` with the X axis = timeslice and Y axis = count, with one line per unique (status, path)

```
... | timeslice 5m | count by status, path, _timeslice | transpose row _timeslice column path, status
```

Count By Field(s)

```
... | count by field1, field2
```

Escaping Escaped Quotes in Regex

Number of backslashes in regex = (2 * number_of_backslashes_in_message) + 1

String Contains

```
... | where contains(field, "str")
```

Split String

```
... | split <field> delim='/' extract 4 as <name>
```