KQL: Let’s start

Lab session

Agenda

Get familiar with Kusto Query Language (KQL)

Basic operation – exploring the data

Advanced operators – getting insights from the data

Hands on

KQL: Language concepts

Relational operators (filters, union, joins, aggregations, …)

Each operator consumes tabular input and produces tabular input

Can be combined with ‘|’ (pipe).

Similarities: OS shell, Linq, functional SQL…

Ease to write, read, change

Statements:

- Single statement query
- Use ‘let’ for reusing statements
- Multi-statement (‘;’) queries

Basic operators for data exploration

… | count

- Counts records in input table (e.g. T)

… | take 10

- Get few records - convenient to start get familiar with the data
- No actual order ensured

… | where Timestamp > ago(1) and UserId = ‘abdcdef’

- Filtering on a specific fields

… | project Col1, Col2, …

- Choose some columns (great if input table has dozens of coluns)

…| extend NewCol1=Col1+Col2

- Introduces new calculated columns

… | render timechart

- Plot the data (in KE and KWE) while exploring

Demo: start exploration

(more) Advanced Operators

Dynamic data types

- Nested objects are first-class citizents

… | **summarize** count(), dcount(Id) by Col1, Col2

- Analytics: aggregations

… | **top** 10 by count_ desc

- Find needle in the haystack

… | **join** (…) on Key1, Key2

- Joining data sets

… | **mvexpand** Col1,Col2 …

- Turn dynamic arrays to rows (multi-value expansion)

… | **parse** Col1 with <pattern>…

- Take care of unstructured data

Resources

- KQL documents:

https://docs.microsoft.com/en-us/azure/kusto/query/

- Self-study KQL course (Pluralsight):

https://www.pluralsight.com/courses/kusto-query-language-kql-from-scratch