Kusto Query Language (KQL) Cheat Sheet

Operators

where

Filters rows based on conditions.
Example: where Status == 200 filters for successful HTTP responses.

project

Selects specific columns.
Example: project Timestamp, User selects only Timestamp and User columns.

join

Combines two tables based on a condition.
Example: join kind=inner Logs on RequestId joins tables on RequestId.

union

Combines results from multiple tables or queries.
Example: union Table1, Table2 combines rows from Table1 and Table2.

search

Searches for a term across all columns.
Example: search "error" finds "error" in any column.

== (Equality)

Tests for exact matches.
Example: where User == "john" matches rows where User is "john".

!= (Inequality)

Filters rows not matching a value.
Example: where Status != 200 excludes successful responses.

in

Checks if a value is in a set.
Example: where Status in (400, 404, 500) matches specified status codes.

has

Matches if a column contains a term (case-sensitive).
Example: where Message has "error" finds rows with "error" in Message.

Functions

count()

Counts rows in a result set.
Example: summarize count() by Status counts rows grouped by Status.

avg()

Calculates the average of a numeric column.
Example: summarize avg(Duration) computes average Duration.

sum()

Sums a numeric column.
Example: summarize sum(Bytes) totals Bytes.

max()

Finds the maximum value in a column.
Example: summarize max(Duration) returns the highest Duration.

min()

Finds the minimum value in a column.
Example: summarize min(Latency) returns the lowest Latency.

ago()

Calculates a time relative to now.
Example: where Timestamp > ago(1h) filters for the last hour.

tostring()

Converts a value to a string.
Example: project tostring(Status) converts Status to string.

Syntax

| (Pipe)

Chains operations in a query.
Example: Table | where Status == 200 | project User filters and selects columns.

summarize

Groups and aggregates data.
Example: summarize count() by User counts rows per User.

order by

Sorts results by a column.
Example: order by Timestamp desc sorts by Timestamp, newest first.

take

Limits the number of rows returned.
Example: take 100 returns the first 100 rows.

extend

Creates calculated columns.
Example: extend ResponseTimeSec = Duration / 1000 converts Duration to seconds.

Range Queries

Filters within a range using between or comparisons.
Example: where Status between(400 .. 499) matches status codes 400–499.

Case Sensitivity

KQL operators are case-insensitive; string comparisons may vary.
Example: has "ERROR" and has "error" depend on has vs has_cs.

Comments

Use // for single-line comments.
Example: // This is a comment is ignored in the query.