LOGZILLA DOCUMENTATION

Query Types —- Event Queries

LogZilla event query reference for Search, EventRate, TopN, and LastN, including parameters, sort fields, pagination, and result structures

LogZilla API · Generated May 3, 2026 · logzilla.ai/docs/logzilla-api/event-query-types

© LogZilla Corporation · logzilla.ai

Query Types —- Event Queries

These queries operate on event data and require the main storage/search services. All parameters and fields are verified against the current implementation in `lib/logzilla/query.py`.

- Search
- EventRate
- TopN
- LastN

Search

Returns counts plus a paginated list of matching events.

Parameters:

- `time_range`: Time period.
- `filter`: Filter expression (see Query API Parameters).
- `sort`: Array of sort fields. Defaults to `["first_occurrence", "-counter"]`.
- `page`, `page_size`, `offset`: Pagination controls.

Result structure (high level):

- `totals.ts_from`, `totals.ts_to`, `totals.count`
- `events.objects` with pagination fields (`page_number`, `page_size`, `item_count`, `page_count`)

Notes:

- Valid sort field name is `first_occurrence` (spelling verified).

EventRate

Returns total count and per-period counts for the given range.

Parameters:

- `time_range`: Time period.
- `filter`: Filter expression (optional).

© LogZilla Corporation · logzilla.ai

Result structure (high level):

- `totals.ts_from`, `totals.ts_to`, `totals.count`
- `details[]` with `ts_from`, `ts_to`, `count`

TopN

Returns the top N values for a field in the specified period, with optional subperiod details and subfield breakdowns.

Parameters:

- `time_range`
- `field` (default: `host`)
- `with_subperiods` (bool)
- `top_periods` (bool)
- `filter`
- `limit`
- `show_other` (bool)
- `ignore_empty` (bool, default true)
- `subfields` (list of field names)
- `subfield_limit`

Result structure (high level):

- `totals.ts_from`, `totals.ts_to`
- `totals.values[]` of `{name, count}`
- Optional subfield breakdowns per value when `subfields` provided

LastN

Returns the last N values for a field during the period, sorted by recency.

Parameters:

- `time_range`
- `field` (default: `host`)
- `filter`

- `limit`
- `ignore_empty` (bool)
- `last_seen_threshold` (number)

Result highlights:

- Same overall structure as TopN totals, with `last_seen` information for each value and sorting by recency instead of counts.

Export formats

See Query Export Formats (https://www.logzilla.ai/docs/logzilla-api/query-export) for supported exports by query type.