

## Basic Queries

| SYNTAX       | DESC              | EXAMPLE                          |
|--------------|-------------------|----------------------------------|
| Simple term  | Search any field  | <i>error</i>                     |
| Field value  | Match exact field | <i>status:200</i>                |
| Phrase       | Match exact text  | <i>message:"disk full"</i>       |
| Field exists | Has any value     | <i>status:*</i>                  |
| Nested       | Dot notation      | <i>kubernetes.pod.name:nginx</i> |

## Comparisons

| SYNTAX | DESC          | EXAMPLE                                 |
|--------|---------------|-----------------------------------------|
| >      | Greater than  | <i>bytes &gt; 1000</i>                  |
| <      | Less than     | <i>status &lt; 500</i>                  |
| >=     | Greater/equal | <i>@timestamp &gt;= "2023-01-01"</i>    |
| <=     | Less/equal    | <i>response.time &lt;= "2024-01-01"</i> |

## Wildcards

| SYNTAX   | DESC        | EXAMPLE          |
|----------|-------------|------------------|
| *        | Many chars  | <i>username*</i> |
| ?        | One char    | <i>user?name</i> |
| Prefix   | Starts with | <i>error*</i>    |
| Contains | Inside text | <i>*error*</i>   |
| Suffix   | Ends with   | <i>*.com</i>     |

## Arrays

| SYNTAX       | DESC              | EXAMPLE                        |
|--------------|-------------------|--------------------------------|
| Any match    | Match array value | <i>tags:(error or warning)</i> |
| All match    | All must match    | <i>tags:(error and info)</i>   |
| Exists       | Has any value     | <i>tags:*</i>                  |
| Empty        | No values         | <i>not_exists_:tags</i>        |
| Single match | One specif        | <i>tags:error</i>              |
| Exclude      | Remove match      | <i>not tags:error</i>          |

## Boolean Logic

| SYNTAX   | DESC           | EXAMPLE                                       |
|----------|----------------|-----------------------------------------------|
| AND      | Both match     | <i>status:200 and method:GET</i>              |
| OR       | Either matches | <i>status:(200 or 201)</i>                    |
| NOT      | Negate         | <i>not status:400</i>                         |
| Combined | Mix operators  | <i>status:200 and (user:john or user:svc)</i> |

## Lists &amp; Ranges

| SYNTAX          | DESC             | EXAMPLE                                      |
|-----------------|------------------|----------------------------------------------|
| Value list      | Any match        | <i>status:(200 or 201 or 204)</i>            |
| Number range    | Between values   | <i>status &gt;= 200 and status &lt;= 299</i> |
| Date range      | Time period      | <i>@timestamp &gt;= "now-24h"</i>            |
| Multi-field     | Match any field  | <i>labels.(app:nginx or env:prod)</i>        |
| Inclusive range | Include 1 and 10 | <i>[1 to 10]</i>                             |
| Exclusive range | Exclude 1 and 10 | <i>{1 to 10}</i>                             |

## Time Queries

| SYNTAX     | DESC             | EXAMPLE                       |
|------------|------------------|-------------------------------|
| Now        | Current time     | <i>@timestamp &gt;= now</i>   |
| Relative   | Time offset      | <i>@timestamp &gt; now-1h</i> |
| Calendar   | Round to unit    | <i>@timestamp &gt;= now/d</i> |
| Time units | m, h, d, w, M, y | <i>@timestamp &gt; now-7d</i> |

## Special Cases

| SYNTAX  | DESC        | EXAMPLE               |
|---------|-------------|-----------------------|
| Null    | Is null     | <i>tags:null</i>      |
| Boolean | True/false  | <i>active:true</i>    |
| IP      | CIDR format | <i>ip:10.0.0.0/24</i> |

