

Kibana Cheatsheet

Accessing Kibana

Open Kibana in a browser

`http://localhost:5601` (replace with your Kibana server URL)

Log in to Kibana

Use credentials configured for Elasticsearch/Kibana

Dashboard Management

Create a new dashboard

Click 'Dashboard' → 'Create dashboard'

Add visualization to dashboard

Click 'Add' or 'Edit' → select visualization

Save dashboard

Click 'Save' in the top menu

Export dashboard

Dashboard → 'Share' → 'Export'

Data Visualization

Create visualization

Click 'Visualize' → 'Create visualization'

Create lens visualization

Click 'Visualize' → 'Create visualization' → select 'Lens'

Create TSVB visualization

Click 'Visualize' → 'Create visualization' → select 'TSVB'

Create Vega visualization

Click 'Visualize' → 'Create visualization' → select 'Vega'

Discover/Search

Search data

Click 'Discover' → type query in search bar

Filter data

Click 'Add filter' or use KQL in search bar

View document details

Click expand arrow next to document

Change time range

Use time picker in top-right corner

Save search

Click 'Save' in top menu

Kibana Query Language (KQL)

Field equals value

`field: value`

Field contains value

`field: *value*`

Field does not equal

`NOT field: value`

AND condition

`field1: value1 AND field2: value2`

OR condition

`field1: value1 OR field2: value2`

Nested field query

`parent.child: value`

Range query

`field > 100 or field < 100 or field >= 100`

Dev Tools

Open Console

Click 'Dev Tools'

Execute query

Type query and press `Ctrl+Enter` or click the play button

View response

Response appears in the right panel

Clear Console

Click the trash icon

Index Pattern Management

Create index pattern

Click 'Stack Management' → 'Index Patterns' → 'Create index pattern'

Refresh field list

Click 'Stack Management' → 'Index Patterns' → select pattern → 'Refresh field list'

Set default index

Click 'Stack Management' → 'Advanced Settings' → 'defaultIndex'

Alerts & Monitoring

Create alert rule

Click 'Alerting' → 'Rules' → 'Create rule'

View triggered alerts

Click 'Alerting' → 'Alerts'

Monitor Elasticsearch

Click 'Stack Monitoring' → 'Elasticsearch'

Monitor Kibana

Click 'Stack Monitoring' → 'Kibana'