

Modul 02: Discover & Abfragen

Daten durchsuchen, filtern und analysieren mit Kibana Discover

Lernziele

Nach diesem Modul kannst du:

- Die Discover-Oberfläche in Kibana sicher bedienen
- Zeitfilter gezielt einsetzen, um relevante Zeiträume auszuwählen
- Mit der Kibana Query Language (KQL) präzise Abfragen formulieren
- Filter kombinieren, um Datenbestände einzugrenzen
- Spalten konfigurieren und Dokumente im Detail untersuchen
- Ergebnisse als CSV exportieren und gespeicherte Suchen teilen

Kibana Discover - Überblick

Discover ist dein zentrales Werkzeug, um Daten in Elasticsearch zu durchsuchen und zu erkunden.

Typische Anwendungsfälle bei Mustertech GmbH:

- Bestellungen eines bestimmten Zeitraums finden
- Umsätze nach Produktkategorie analysieren
- Kundenregionen auswerten
- Auffällige Bestellwerte identifizieren

Discover zeigt dir die Rohdaten - hier beginnst du jede Analyse.

Die Discover-Oberfläche

Bereich	Beschreibung
Suchleiste	KQL-Abfragen eingeben
Zeitfilter	Zeitraum auswählen (oben rechts)
Histogramm	Verteilung der Treffer über die Zeit
Felderliste	Verfügbare Felder (linke Seitenleiste)
Dokumententabelle	Trefferliste mit konfigurierbaren Spalten
Dokumentendetails	Einzelnes Dokument aufklappen
Filter-Leiste	Aktive Filter unterhalb der Suchleiste

Die Discover-Oberfläche - Kibana

The screenshot shows the Kibana Discover interface. At the top, there's the Elastic logo and a search bar. Below that, the 'Discover' tab is active, showing 'Kibana Sample Data eCommerce'. A bar chart displays data from Feb 10, 2026, to Feb 17, 2026, with an auto interval of 3 hours. The chart shows a fluctuating number of documents per hour, peaking around 25-30. Below the chart, a table of documents is displayed, sorted by 'order_date'. The table has columns for document ID, timestamp, and a truncated document body. The first document is from Feb 17, 2026, at 15:54:14.000, with category 'Women's Shoes' and customer 'Selena Lewis'. The second document is from Feb 17, 2026, at 15:44:10.000, with category 'Men's Clothing' and customer 'Jackson Simpson'. The third document is from Feb 17, 2026, at 15:26:53.000, with category '[Men's Shoes, Men's Clothing]' and customer 'Phil Henderson'. The fourth document is from Feb 17, 2026, at 15:15:22.000, with category '[Women's Shoes, Women's Clothing]' and customer 'Betty Rivera'. The fifth document is from Feb 17, 2026, at 15:15:22.000, with category '[Men's Shoes, Men's Clothing]' and customer 'Abd Morrison'. The sixth document is from Feb 17, 2026, at 15:13:55.000, with category '[Women's Clothing, Women's Accessories, Women's Shoes]' and customer 'Rabbia Al Cunningham'. The seventh document is from Feb 17, 2026, at 15:13:55.000, with category '[Men's Accessories, Men's Clothing]' and customer 'Abd Rios'. The interface includes a sidebar with 'Popular fields' and 'Available fields', a search bar for field names, and a 'Documents (1,042)' header with sorting options.

Data Views (ehemals Index Patterns)

Ein **Data View** legt fest, welche Elasticsearch-Indizes du durchsuchst.

Beispiele bei Mustertech GmbH:

- `mustertech-orders-*` -- alle Bestelldaten
- `mustertech-products-*` -- Produktkatalog
- `mustertech-customers-*` -- Kundendaten

So wählst du einen Data View aus:

1. Klicke oben links auf den Data-View-Namen
2. Wähle den gewünschten Data View aus der Liste
3. Die Felderliste und Daten aktualisieren sich automatisch

Der Data View bestimmt, welche Felder dir zur Verfügung stehen.

Zeitfilter und Zeitreihen

Der Zeitfilter ist eines der wichtigsten Werkzeuge in Discover. Er befindet sich oben rechts in der Oberfläche.

Zwei Arten der Zeitauswahl:

- **Relativ:** z. B. "Letzte 24 Stunden", "Letzte 7 Tage", "Letzte 30 Tage"
- **Absolut:** z. B. "01.01.2026 00:00" bis "31.01.2026 23:59"

Wann welche Variante nutzen?

Relativ	Absolut
Laufende Überwachung	Monatsberichte
Tagesaktuelle Analyse	Quartalsvergleiche
Dashboards mit Auto-Refresh	Reproduzierbare Auswertungen

Zeitfilter - Quick Menu

The screenshot shows the Elastic Discover interface for the 'Kibana Sample Data eCommerce' dataset. A 'Quick select' menu is open, displaying various time range options. The main interface shows a bar chart and a table of documents.

Quick select menu options:

- Last 7 Days (selected)
- Today
- This week
- Last 1 minute
- Last 15 minutes
- Last 30 minutes
- Last 1 hour
- Last 24 hours
- Last 7 days
- Last 30 days
- Last 90 days
- Last 1 year

Document Table:

order_date	Summary
Feb 17, 2026 @ 15:54:14.000	category Women's Shoes currency EUR customer_first_name Se... E customer_id 42 customer_last_name Lewis customer_phone (... -family.zzz event.dataset sample_ecommerce geoip.city_name
Feb 17, 2026 @ 15:44:10.000	category Men's Clothing currency EUR customer_first_name J... E customer_id 13 customer_last_name Simpson customer_phone (... mpson-family.zzz event.dataset sample_ecommerce geoip.city...
Feb 17, 2026 @ 15:26:53.000	category [Men's Shoes, Men's Clothing] currency EUR custom... n customer_gender MALE customer_id 50 customer_last_name Henderson customer_phone (empty) day_of_week Tuesda... y day_of_week_i 1 email phil@henderson-family.zzz event.dataset sample_ecommerce geoip.continent_name Europ...
Feb 17, 2026 @ 15:15:22.000	category [Women's Shoes, Women's Clothing] currency EUR customer_first_name Betty customer_full_name Betty River... a customer_gender FEMALE customer_id 44 customer_last_name Rivera customer_phone (empty) day_of_week Tuesda... y day_of_week_i 1 email betty@rivera-family.zzz event.dataset sample_ecommerce geoip.city_name New Yor...
Feb 17, 2026 @ 15:15:22.000	category [Men's Shoes, Men's Clothing] currency EUR customer_first_name Abd customer_full_name Abd Morriso... n customer_gender MALE customer_id 52 customer_last_name Morrison customer_phone (empty) day_of_week Tuesda... y day_of_week_i 1 email abd@morrison-family.zzz event.dataset sample_ecommerce geoip.city_name Cair...
Feb 17, 2026 @ 15:13:55.000	category [Women's Clothing, Women's Accessories, Women's Shoes] currency EUR customer_first_name Rabbia A... 1 customer_full_name Rabbia Al Cunningham customer_gender FEMALE customer_id 5 customer_last_name Cunningha... m customer_phone (empty) day_of_week Tuesday day_of_week_i 1 email rabbia_al@cunningham-family.zzz event.dataset sampl...
Feb 17, 2026 @ 15:13:55.000	category [Men's Accessories, Men's Clothing] currency EUR customer_first_name Abd customer_full_name Abd Rio... s customer_gender MALE customer_id 52 customer_last_name Rios customer_phone (empty) day_of_week Tuesda... y day_of_week_i 1 email abd@rios-family.zzz event.dataset sample_ecommerce geoip.city_name Cairo geoip.continent_name...

Das Histogramm nutzen

Das Histogramm oben in Discover zeigt die **Verteilung der Treffer über die Zeit.**

So nutzt du es effektiv:

- **Überblick verschaffen:** Erkenne auf einen Blick, wann besonders viele Bestellungen eingegangen sind
- **Hineinzoomen:** Klicke und ziehe, um einen Zeitbereich auszuwählen
- **Intervall anpassen:** Kibana wählt das Intervall automatisch, du kannst es aber manuell ändern (z. B. stündlich, täglich)

Auffällige Spitzen oder Lücken im Histogramm sind oft der Ausgangspunkt für tiefere Analysen.

Kibana Query Language (KQL)

KQL ist die Abfragesprache in Kibana. Sie ist speziell für Analysten konzipiert.

Grundprinzip:

```
feldname: wert
```

Beispiel:

```
product.category: "Smartphones"
```

KQL-Abfragen gibst du in die Suchleiste oben in Discover ein.

KQL - Freitextsuche

Ohne Feldnamen durchsuchst du alle Felder gleichzeitig:

```
Samsung Galaxy
```

Findet alle Dokumente, die "Samsung" **und** "Galaxy" in beliebigen Feldern enthalten.

Anführungszeichen für exakte Phrasen:

```
"Samsung Galaxy S24"
```

Findet nur Dokumente mit genau dieser Zeichenkette.

Abfrage	Ergebnis
Samsung Galaxy	Beide Wörter (beliebige Reihenfolge)
"Samsung Galaxy"	Exakte Phrase

KQL - Feld:Wert-Abfragen

Die präziseste Art zu suchen: Gib das Feld explizit an.

Abfrage	Beschreibung
<code>customer.city: "Berlin"</code>	Kunden aus Berlin
<code>product.category: "Laptops"</code>	Kategorie Laptops
<code>order.status: "shipped"</code>	Versendete Bestellungen
<code>customer.region: "Bayern"</code>	Kunden aus Bayern

Wichtig:

- Feldnamen sind case-sensitive
- Textwerte mit Leerzeichen in Anführungszeichen setzen
- Kibana bietet Autovervollständigung für Feldnamen und Werte

KQL - Vergleichsoperatoren

Für numerische Felder und Datumswerte stehen Vergleichsoperatoren zur Verfügung:

Operator	Bedeutung	Beispiel
>	Größer als	<code>order.total > 500</code>
>=	Größer oder gleich	<code>order.total >= 100</code>
<	Kleiner als	<code>order.total < 50</code>
<=	Kleiner oder gleich	<code>order.items_count <= 3</code>

Praxisbeispiel Mustertech GmbH:

Alle Bestellungen über 1000 Euro finden:

```
order.total > 1000
```

KQL - Boolesche Operatoren

Kombiniere Bedingungen mit **AND**, **OR**
und **NOT** :

AND - beide Bedingungen müssen zutreffen:

```
product.category: "Laptops" AND order.total > 800
```

OR - mindestens eine Bedingung trifft zu:

```
customer.region: "Bayern" OR  
customer.region: "Baden-Württemberg"
```

NOT - Bedingung ausschließen:

```
order.status: "completed" AND  
NOT product.category: "Zubehör"
```

KQL - Klammern und Priorität

Verwende Klammern, um die Auswertungsreihenfolge festzulegen:

Ohne Klammern (mehrdeutig):

```
product.category: "Laptops" OR  
product.category: "Tablets" AND  
order.total > 500
```

Mit Klammern (eindeutig):

```
(product.category: "Laptops" OR  
product.category: "Tablets") AND  
order.total > 500
```

Nutze immer Klammern, wenn du **AND** und **OR** in einer Abfrage kombinierst. So vermeidest du unerwartete Ergebnisse.

KQL - Wildcards

Das Sternchen * steht für beliebig viele Zeichen:

Abfrage	Findet
<code>product.name: Samsung*</code>	Samsung Galaxy, Samsung Tab, ...
<code>customer.email: *@firma.de</code>	Alle Firmen-E-Mails
<code>product.sku: LPT-*</code>	Alle Laptop-Artikelnummern

Existenzprüfung - hat ein Feld überhaupt einen Wert?

```
customer.phone: *
```

Findet alle Dokumente, bei denen das Feld

```
customer.phone
```

 vorhanden und nicht leer ist.

Wildcards sind nützlich, können aber bei sehr großen Datenmengen langsam sein.

KQL - Übersicht der Syntax

Element	Syntax	Beispiel
Freitext	text	Samsung
Exakte Phrase	"text"	"Samsung Galaxy"
Feld:Wert	feld: wert	customer.city: "Berlin"
Größer als	feld > wert	order.total > 500
Kleiner als	feld < wert	order.total < 50
UND	AND	a: 1 AND b: 2
ODER	OR	a: 1 OR a: 2
NICHT	NOT	NOT a: 1
Wildcard	*	name: Sam*
Klammern	()	(a: 1 OR a: 2) AND b: 3
Existenz	feld: *	phone: *

KQL in Aktion

customer_gender: FEMALE AND taxful_total_price > 100

The screenshot shows the Elastic Kibana Discover interface. At the top, the Elastic logo and a search bar are visible. Below that, the 'Discover' tab is active, and the query 'customer_gender: FEMALE AND taxful_total_price > 100' is entered in the search bar. The interface is divided into several sections:

- Left Panel:** Contains 'Popular fields' (products.manufacturer, products.price, products.product_name, total_quantity) and 'Available fields' (category, currency, customer_first_name, customer_full_name, customer_gender, customer_id, customer_last_name, customer_phone, day_of_week, day_of_week_i, email, event.dataset, geoip.city_name, geoip.continent_name, geoip.country_iso_code, geoip.location, geoip.region_name).
- Top Right:** Includes 'Try ES|QL', 'Inspect', 'Alerts', and a 'Save' button.
- Search Bar:** Shows the query 'customer_gender: FEMALE AND taxful_total_price > 100' and a 'Refresh' button.
- Visualizations:** A bar chart at the top shows data distribution over time (Feb 10, 2026 to Feb 17, 2026).
- Documents (109):** A list of search results is displayed, each with a timestamp and a summary of the document's fields. The first few results are:
 - Feb 17, 2026 @ 15:15:22.000: customer_gender FEMALE, category [Women's Shoes, Women's Clothing], currency EUR, customer_first_name Betty, customer_full_name Betty Rivera, customer_id 44, customer_last_name Rivera, customer_phone (empty), day_of_week Tuesday, day_of_week_i 1, email betty@rivera-family.zzz, event.dataset sample_ecommerce, geoip.city_name New York.
 - Feb 17, 2026 @ 15:13:55.000: customer_gender FEMALE, category [Women's Clothing, Women's Accessories, Women's Shoes], currency EU, customer_first_name Rabbia A, customer_full_name Rabbia A, customer_id 5, customer_last_name Cunningham, customer_phone (empty), day_of_week Tuesday, day_of_week_i 1, email rabbia_al@cunningham-family.zzz, event.dataset sample_ecommerce, geoip.city_name New York.
 - Feb 17, 2026 @ 14:58:05.000: customer_gender FEMALE, category [Women's Clothing, Women's Accessories], currency EUR, customer_first_name Rabbia A, customer_full_name Rabbia A, customer_id 5, customer_last_name Ball, customer_phone (empty), day_of_week Tuesday, day_of_week_i 1, email rabbia_al@ball-family.zzz, event.dataset sample_ecommerce, geoip.city_name Dubai.
 - Feb 17, 2026 @ 13:53:17.000: customer_gender FEMALE, category [Women's Shoes, Women's Clothing], currency EUR, customer_first_name Rabbia A, customer_full_name Rabbia A, customer_id 5, customer_last_name Harper, customer_phone (empty), day_of_week Tuesday, day_of_week_i 1, email rabbia_al@harper-family.zzz, event.dataset sample_ecommerce, geoip.city_name Dubai.
 - Feb 17, 2026 @ 12:12:29.000: customer_gender FEMALE, category [Women's Clothing, Women's Shoes], currency EUR, customer_first_name Gwen, customer_full_name Gwen Powell, customer_id 26, customer_last_name Powell, customer_phone (empty), day_of_week Tuesday, day_of_week_i 1, email gwen@powell-family.zzz, event.dataset sample_ecommerce, geoip.city_name Los Angeles.
 - Feb 17, 2026 @ 09:09:36.000: customer_gender FEMALE, category Women's Clothing, currency EUR, customer_first_name Elyssa, customer_full_name Elyssa Cook, customer_id 27, customer_last_name Cook, customer_phone (empty), day_of_week Tuesday, day_of_week_i 1, email elyssa@cook-family.zzz, event.dataset sample_ecommerce, geoip.city_name New York, geoip.continent_name North America.
 - Feb 17, 2026 @ 06:47:02.000: customer_gender FEMALE, category [Women's Clothing, Women's Shoes], currency EUR, customer_first_name Elyssa, customer_full_name Elyssa Martin, customer_id 27, customer_last_name Martin, customer_phone (empty), day_of_week Tuesday, day_of_week_i 1, email elyssa@martin-family.zzz, event.dataset sample_ecommerce, geoip.city_name New York.

Filter verwenden

Neben KQL-Abfragen bietet Kibana eine **grafische Filter-Leiste** unterhalb der Suchleiste.

Filter hinzufügen - drei Wege:

1. **Über die Felderliste:** Klicke auf ein Feld in der linken Seitenleiste und wähle einen Wert aus
2. **Über die Dokumententabelle:** Klicke auf ein Lupensymbol neben einem Feldwert
3. **Manuell:** Klicke auf "Add filter" in der Filter-Leiste

Filter und KQL-Abfragen ergänzen sich. Nutze Filter für häufig wechselnde Bedingungen und KQL für komplexere Abfragen.

Filter hinzufügen - Dialog

The screenshot shows the Elastic Discover interface with the 'Add filter' dialog box open. The dialog is positioned over a table of search results. The dialog has a search field for field names, a dropdown for operators, and a text input for a custom label. The background table shows columns for event date, customer gender, category, currency, and customer details.

Dialog Content:

- Search field: Search field names
- Operator: Select operator
- Field selection: Please select a field first...
- Custom label (optional): Add a custom label here
- Buttons: Cancel, Add filter

Table Content (Visible Rows):

Event Date	Summary
Feb 17, 2026 @ 15:15:22.000	customer_gender FEMALE category [Women's Shoes, Women's Clothing] currency EUR customer_first_name Betty customer_full_name Betty Rivera customer_id 44 customer_last_name Rivera customer_phone (empty) day_of_week Tuesday day_of_week_i 1 email betty@rivera-family.zzz event.dataset sample_ecommerce geoip.city_name New Yor...
Feb 17, 2026 @ 15:13:55.000	customer_gender FEMALE category [Women's Clothing, Women's Accessories, Women's Shoes] currency EU R customer_first_name Rabbia Al customer_full_name Rabbia Al Cunningham customer_id 5 customer_last_name Cunningha m customer_phone (empty) day_of_week Tuesday day_of_week_i 1 email rabbia al@cunningham-family.zzz event.dataset sampl...
Feb 17, 2026 @ 14:58:05.000	customer_gender FEMALE category [Women's Clothing, Women's Accessories] currency EUR customer_first_name Rabbia A l customer_full_name Rabbia Al Ball customer_id 5 customer_last_name Ball customer_phone (empty) day_of_week Tuesda y day_of_week_i 1 email rabbia al@ball-family.zzz event.dataset sample_ecommerce geoip.city_name Duba...
Feb 17, 2026 @ 13:53:17.000	customer_gender FEMALE category [Women's Shoes, Women's Clothing] currency EUR customer_first_name Rabbia A l customer_full_name Rabbia Al Harper customer_id 5 customer_last_name Harper customer_phone (empty) day_of_week Tuesda y day_of_week_i 1 email rabbia al@harper-family.zzz event.dataset sample_ecommerce geoip.city_name Duba...
Feb 17, 2026 @ 12:12:29.000	customer_gender FEMALE category [Women's Clothing, Women's Shoes] currency EUR customer_first_name Gwe n customer_full_name Gwen Powell customer_id 26 customer_last_name Powell customer_phone (empty) day_of_week Tuesda y day_of_week_i 1 email gwen@powell-family.zzz event.dataset sample_ecommerce geoip.city_name Los Angele...
Feb 17, 2026 @ 09:09:36.000	customer_gender FEMALE category Women's Clothing currency EUR customer_first_name Elyssa customer_full_name Elyssa Coo k customer_id 27 customer_last_name Cook customer_phone (empty) day_of_week Tuesday day_of_week_i 1 email elyssa@cook-f amily.zzz event.dataset sample_ecommerce geoip.city_name New York geoip.continent_name North Americ...
Feb 17, 2026 @ 06:47:02.000	customer_gender FEMALE category [Women's Clothing, Women's Shoes] currency EUR customer_first_name Elyss a customer_full_name Elyssa Martin customer_id 27 customer_last_name Martin customer_phone (empty) day_of_week Tuesda y day_of_week_i 1 email elyssa@martin-family.zzz event.dataset sample_ecommerce geoip.city_name New Yor...

Filter - Aktionen

Jeder aktive Filter bietet dir mehrere Aktionen per Klick:

Aktion	Beschreibung
Aktivieren/Deaktivieren	Filter temporär ein-/ausschalten
Pinnen	Filter bleibt beim Wechsel zwischen Tabs erhalten
Invertieren	Gegenteil anzeigen (z. B. alles außer "Laptops")
Bearbeiten	Filterbedingung nachträglich ändern
Löschen	Filter entfernen

Praxisbeispiel:

Du filterst auf `product.category: "Laptops"`. Durch Invertieren siehst du alle Bestellungen **ohne** Laptops.

Filter kombinieren

Mehrere Filter werden standardmäßig mit **AND** verknüpft.

Beispiel-Szenario bei Mustertech GmbH:

Du möchtest alle Laptop-Bestellungen aus Bayern mit einem Wert über 1000 Euro finden:

1. Filter: `product.category: "Laptops"`

2. Filter: `customer.region: "Bayern"`

3. KQL-Abfrage: `order.total > 1000`

Alle drei Bedingungen müssen gleichzeitig erfüllt sein.

Tip: Gepinnte Filter bleiben aktiv, auch wenn du zwischen verschiedenen Discover-Tabs oder Dashboards wechselst.

Spalten konfigurieren

In der Standardansicht zeigt Discover nur die Spalte `_source` mit dem gesamten Dokumentinhalt. Das ist unübersichtlich.

Spalten hinzufügen:

- Klicke in der Felderliste links auf das **Plus-Symbol** neben einem Feldnamen
- Oder klicke im aufgeklappten Dokument auf das Spaltensymbol neben einem Feld

Empfohlene Spalten für Bestellanalysen:

- `order.date`
- `customer.name`
- `product.category`
- `product.name`
- `order.total`

Spalten verwalten

Spalten neu anordnen:

- Ziehe Spaltenüberschriften per Drag & Drop an die gewünschte Position

Spalten entfernen:

- Klicke auf das X-Symbol in der Spaltenüberschrift

Spaltenbreite anpassen:

- Ziehe den Rand einer Spaltenüberschrift

Sortierung ändern:

- Klicke auf eine Spaltenüberschrift, um aufsteigend oder absteigend zu sortieren
- **Mehrfachsortierung:** Halte die Umschalttaste gedrückt

Dokumente im Detail untersuchen

Klicke auf einen Pfeil links neben einem Dokument, um es aufzuklappen.

Die Detailansicht zeigt:

- **Tabelle:** Alle Felder mit Werten übersichtlich dargestellt
- **JSON:** Das Rohdokument im JSON-Format

Nützliche Aktionen in der Detailansicht:

- Feldwert als Filter hinzufügen (Plus-Symbol)
- Feldwert als Ausschlussfilter setzen (Minus-Symbol)
- Spalte zur Tabelle hinzufügen
- Feld in die Zwischenablage kopieren

Die Detailansicht ist ideal, um einzelne Bestellungen genau zu prüfen.

Dokumente im Detail - Kibana

The screenshot shows the Kibana Discover interface. At the top, there's an Elastic logo and a search bar. Below that, the 'Discover' tab is active. The main area is divided into several sections:

- Left Sidebar:** Contains 'Popular fields' (4 items) and 'Available fields' (45 items).
- Top Center:** A search bar with the text 'Filter your data using KQL syntax'. Below it, a date range selector is set to 'Last 7 days' with a 'Refresh' button.
- Top Right:** A 'Document' header showing '1 of 500' documents. Below it are actions: 'View single document' and 'View surrounding documents'.
- Main Table:** A table with columns for document ID, timestamp, and a summary of fields. The first document is highlighted in orange.
- Right Pane:** A 'JSON' view of the selected document, showing a key-value structure for fields like '_id', '_score', 'category', 'currency', 'customer_first_name', 'customer_full_name', 'customer_gender', 'customer_id', 'customer_last_name', 'customer_phone', and 'day_of_week'.

Verfügbare Felder - Die Seitenleiste

Die linke Seitenleiste zeigt alle verfügbaren Felder des aktuellen Data Views.

Feldtypen erkennen:

- **t** -- Textfeld (z. B. `customer.name`)
- **#** -- Numerisches Feld (z. B. `order.total`)
- **Kalender** -- Datumsfeld (z. B. `order.date`)
- **?** -- Boolean (z. B. `order.is_returned`)

Feldstatistiken:

Klicke auf ein Feld, um eine Schnellübersicht der häufigsten Werte zu sehen. So erkennst du z. B. sofort die beliebtesten Produktkategorien.

Verfügbare Felder - Feldstatistiken

The screenshot shows the Elastic Kibana Discover interface. At the top, there's a search bar with the text "Find apps, content, and more." Below it, the "Discover" tab is active. The main view shows a bar chart with the x-axis representing dates from Feb 10, 2026 to Feb 17, 2026. The y-axis represents the count of documents, ranging from 0 to 30. The chart shows a relatively stable number of documents per day, with a slight peak on Feb 13th.

On the left sidebar, under "Available fields", the "category" field is selected. The "Field statistics" panel for "category" shows the following top values:

Category	Percentage
Men's Clothing	27.4%
Women's Clothing	26.2%
Women's Shoes	15.4%
Men's Shoes	12.6%
Women's Accessories	10.9%
Men's Accessories	7.4%

Below the top values, there's a "Summary" section showing sample documents for the "category" field. The first document is:

```
category Women's Shoes currency EUR customer_first_name Selena customer_full_name Selena Lewis customer_gender FEMALE customer_id 42 customer_last_name Lewis customer_phone (empty) day_of_week Tuesday day_of_week_i 1 email selena@lewis-family.zzz event.dataset sample_ecommerce geoip.city_name Marrakesh geoip.continent_name Africa...
```

The second document is:

```
category Men's Clothing currency EUR customer_first_name Jackson customer_full_name Jackson Simpson customer_gender MALE customer_id 13 customer_last_name Simpson customer_phone (empty) day_of_week Tuesday day_of_week_i 1 email jackson@simpson-family.zzz event.dataset sample_ecommerce geoip.city_name Los Angeles geoip.continent_name North America...
```

The third document is:

```
category [Men's Shoes, Men's Clothing] currency EUR customer_first_name Phil customer_full_name Phil Henderson customer_gender MALE customer_id 50 customer_last_name Henderson customer_phone (empty) day_of_week Tuesday day_of_week_i 1 email phil@henderson-family.zzz event.dataset sample_ecommerce geoip.continent_name Europe...
```

The fourth document is:

```
category [Women's Shoes, Women's Clothing] currency EUR customer_first_name Betty customer_full_name Betty Rivera customer_gender FEMALE customer_id 44 customer_last_name Rivera customer_phone (empty) day_of_week Tuesday day_of_week_i 1 email betty@rivera-family.zzz event.dataset sample_ecommerce geoip.city_name New York...
```

The fifth document is:

```
category [Men's Shoes, Men's Clothing] currency EUR customer_first_name Abd customer_full_name Abd Morrison customer_gender MALE customer_id 52 customer_last_name Morrison customer_phone (empty) day_of_week Tuesday...
```

Daten exportieren - CSV

Du kannst die aktuelle Trefferliste als CSV-Datei herunterladen:

1. Führe deine Suche mit Filtern und KQL durch
2. Klicke auf **Share** in der oberen Leiste
3. Wähle **CSV Reports** oder **Download CSV**
4. Warte, bis der Export erstellt ist
5. Lade die Datei herunter

Hinweise:

- Der Export enthält die aktuell sichtbaren Spalten
- Zeitfilter und Abfragen werden berücksichtigt
- Bei sehr großen Datenmengen kann der Export einige Zeit dauern

Gespeicherte Suchen

Speichere häufig genutzte Abfragen, um sie schnell wiederzuverwenden:

Suche speichern:

1. Konfiguriere deine Abfrage, Filter und Spalten
2. Klicke auf **Save** in der oberen Leiste
3. Vergib einen aussagekräftigen Namen

Beispiele für sinnvolle Namen:

- "Laptop-Bestellungen Bayern > 1000 EUR"
- "Retouren letzte 30 Tage"
- "Bestellungen ohne Versandbestätigung"

Gespeicherte Suchen können auch in Dashboards eingebettet werden - dazu mehr

Zusammenfassung

Discover ist dein Einstiegspunkt für jede Datenanalyse in Kibana:

- **Zeitfilter** grenzen den Zeitraum ein - relativ für laufende Analysen, absolut für Berichte
- **KQL** bietet dir eine mächtige, aber einfache Abfragesprache mit Feld: Wert-Suche, Vergleichen, Wildcards und boolescher Logik
- **Filter** ergänzen KQL und lassen sich per Klick ein-/ausschalten, pinnen und invertieren
- **Spalten** konfigurierst du individuell für jede Analyse
- **Gespeicherte Suchen** und **CSV-Export** machen deine Ergebnisse nachhaltig nutzbar