

Fondamenti di basi di dati
Docente: Alessandro Fiori
Titolo argomento:
Kibana

Aggiungere i dati di esempio

I set di dati di esempio sono corredati da visualizzazioni di esempio, dashboard e altro ancora per aiutarvi a esplorare Kibana prima di aggiungere i vostri dati.

1. Nella pagina iniziale, fare clic su Try our sample data
2. Nella scheda Sample eCommerce orders, fare click su Add data

Add data

Try Integrations

All Logs Metrics Security **Sample data** Upload file

Sample eCommerce orders

Sample data, visualizations, and dashboards for tracking eCommerce orders.

Sample flight data

Sample data, visualizations, and dashboards for monitoring flight routes.

Sample web logs

Sample data, visualizations, and dashboards for monitoring web logs.

Add data

Add data

Add data

Esploarer i dati

Discover visualizza i dati in un istogramma interattivo che mostra la distribuzione dei dati, o dei documenti, nel tempo e in una tabella che elenca i campi di ogni documento che si confronta con il modello di indice. Per visualizzare un sottoinsieme di documenti, è possibile applicare filtri ai dati e personalizzare la tabella per visualizzare solo i campi che si desidera esplorare.

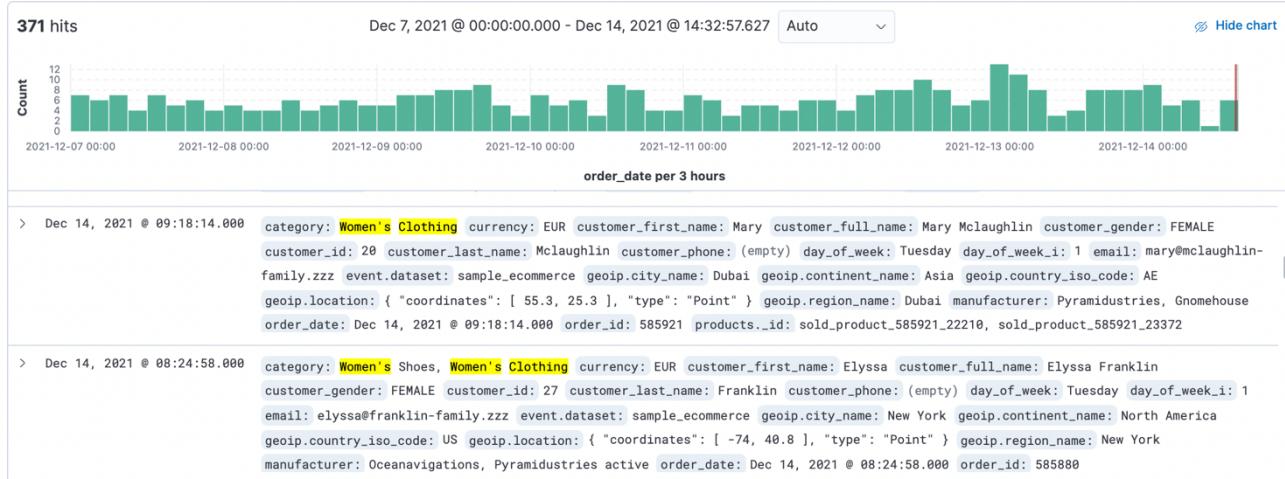
1. Aprire il menu principale, quindi fare clic su Discover
2. Cambiare il filtro temporale in Last 7 days

The screenshot shows the Kibana Discover interface with the following configuration:

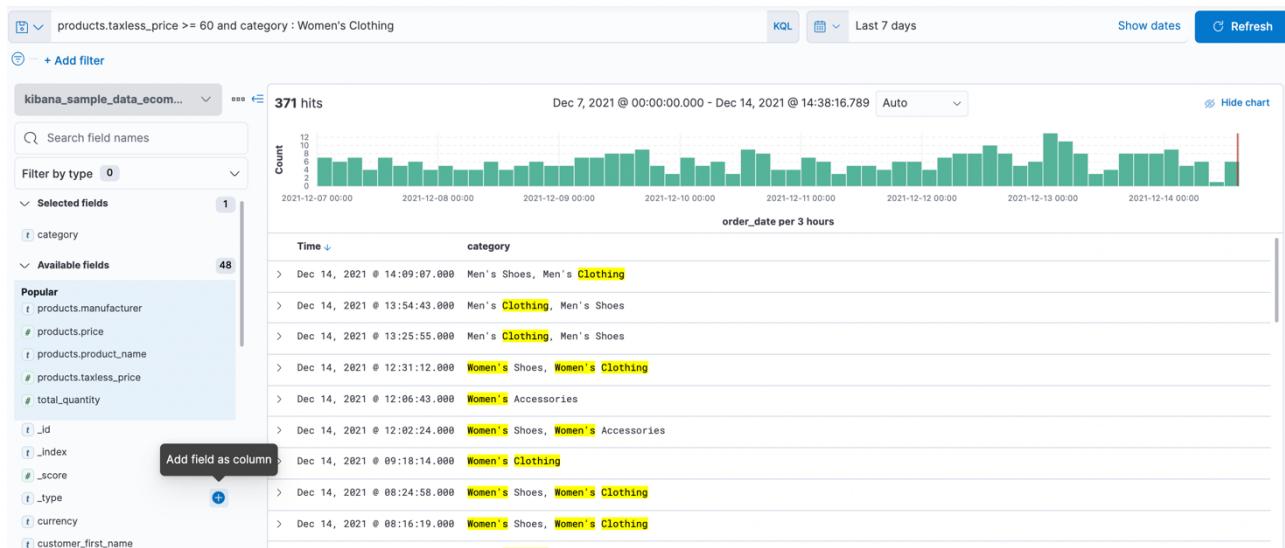
- Time range: ~ 15 minutes ago → now
- Quick select: Last 15 minutes
- Commonly used time ranges:
 - Today
 - This week
 - Last 15 minutes
 - Last 30 minutes
 - Last 1 hour
 - Last 24 hours
 - Last 7 days
 - Last 30 days
 - Last 90 days
 - Last 1 year
- Recently used date ranges: Last 7 days
- Refresh every: 0 seconds

3. Per visualizzare gli ordini di vendita di abbigliamento femminile di importo pari o superiore a 60 dollari, utilizzare il campo di ricerca KQL:

`products.taxless_price >= 60 and category : Women's Clothing`



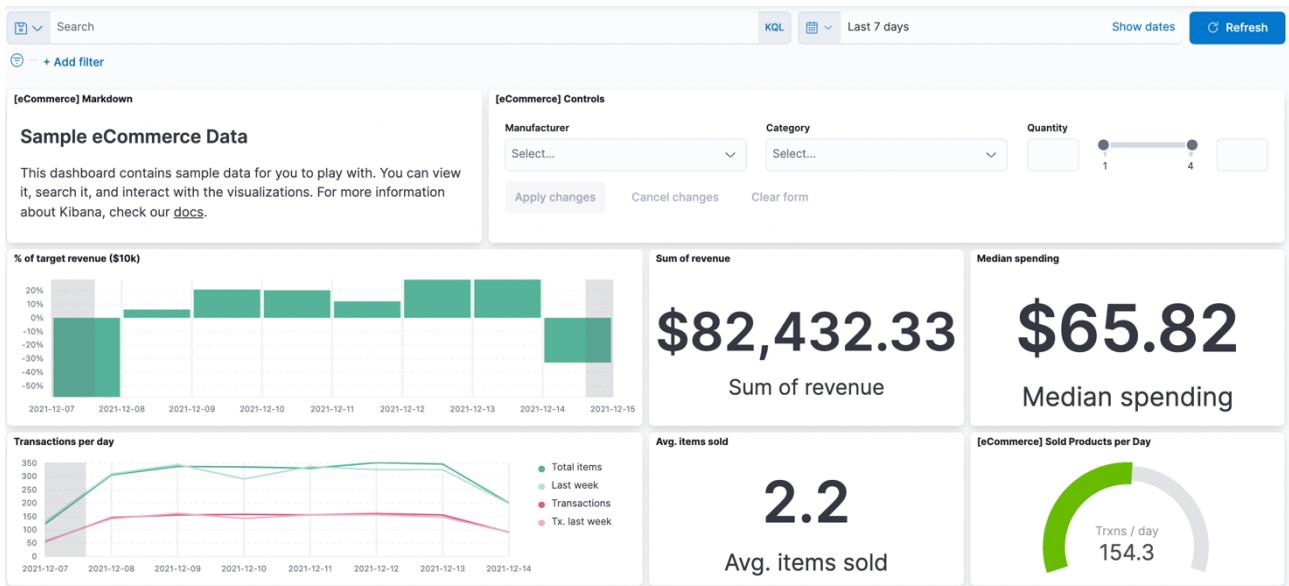
4. Per visualizzare solo le categorie di prodotti che contengono ordini di vendita, passare il mouse sul campo della categoria e fare clic su +.



Visualizzare e analizzare i dati

Una dashboard è una collezione di pannelli che possono essere utilizzati per visualizzare e analizzare i dati. I pannelli contengono visualizzazioni, controlli interattivi, testo e altro.

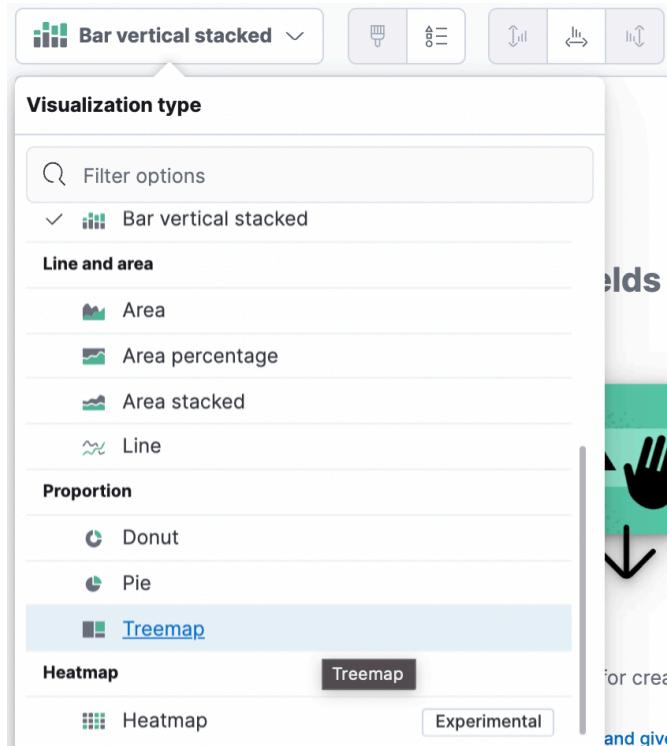
5. Aprire il menu principale, quindi fare clic su Dashboard.
6. Fare clic su [eCommerce] Revenue Dashboard



Creare un pannello di visualizzazione

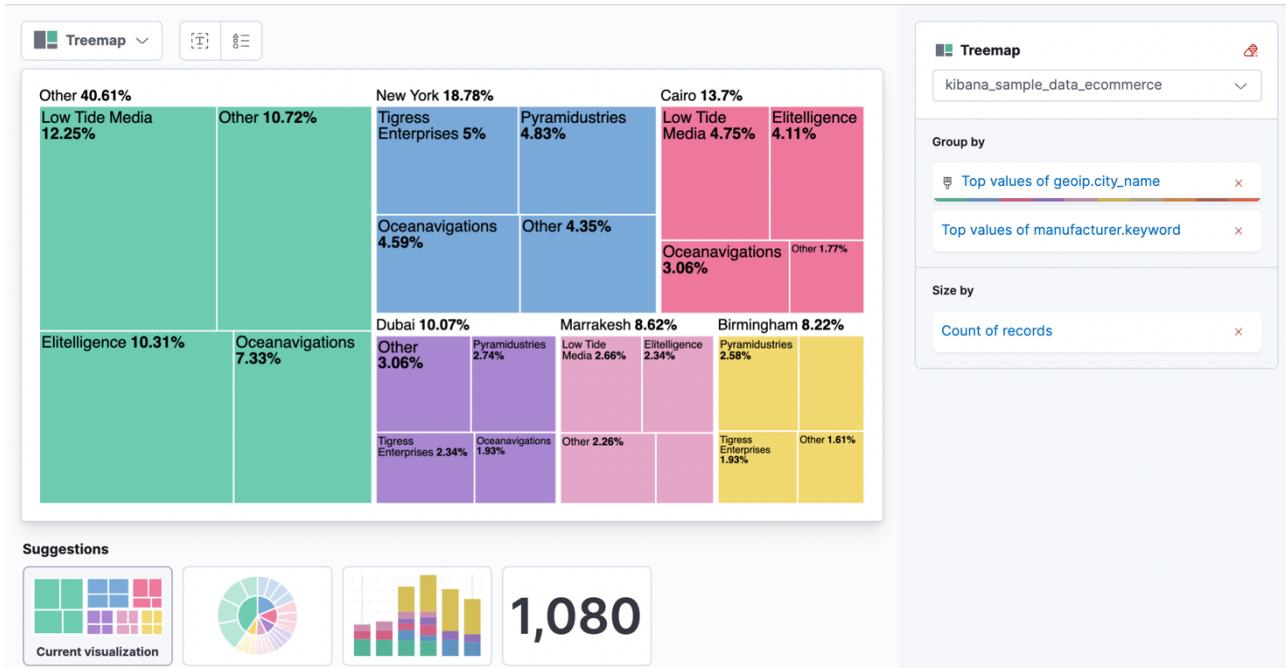
Creare un pannello treemap che mostri le principali regioni di vendita e i produttori, quindi aggiungere il pannello al dashboard.

1. Nella barra degli strumenti, fare clic su **Edit**
2. Nella dashboard, cliccare **Create visualization**
3. Nell'editor di visualizzazione drag-and-drop, aprire il menu a tendina **Visualization type** e selezionare **Treemap**.

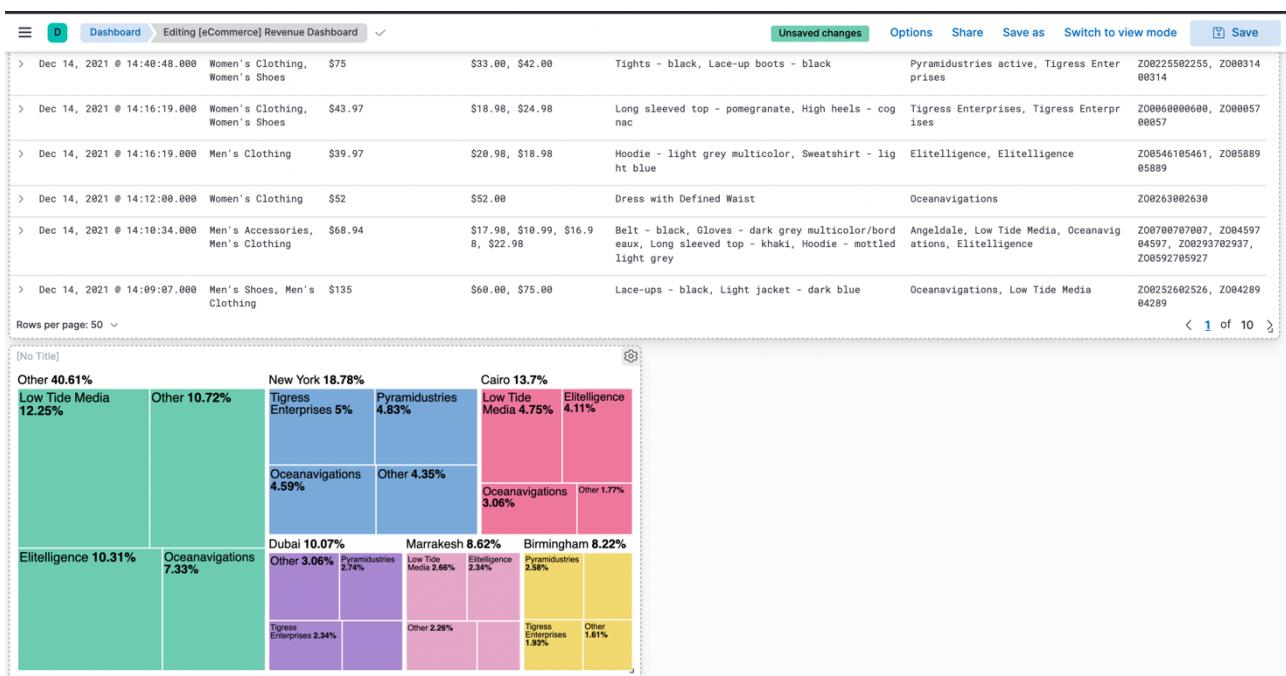


4. Dall'elenco Available fields, trascinare i seguenti campi nell'area di lavoro:

- geoip.city_name
- manufacturer.keyword



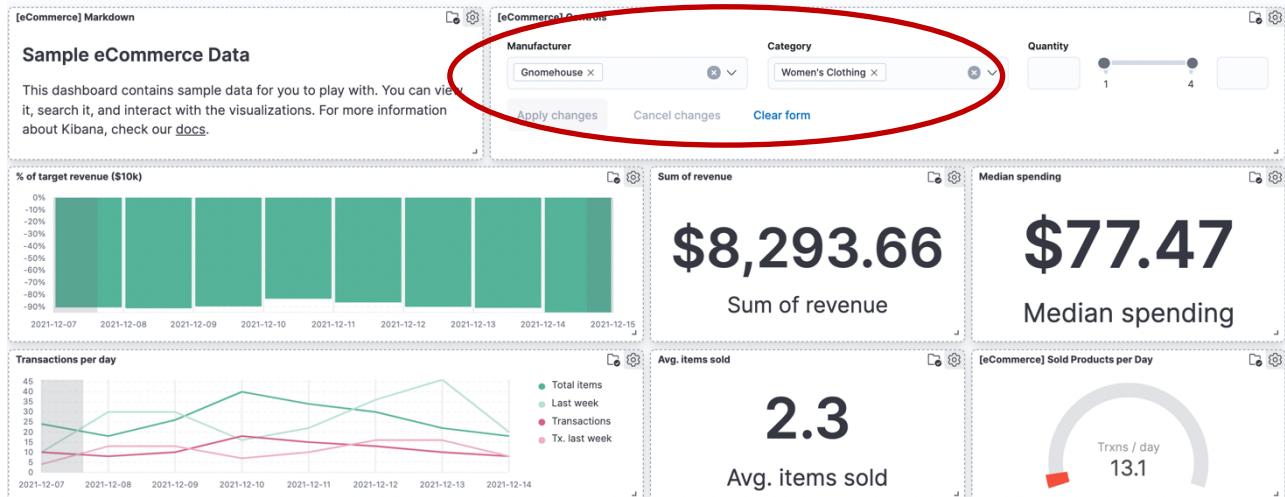
5. Cliccare . La treemap viene visualizzata come ultimo pannello di visualizzazione del cruscotto.



Interagire con i dati

È possibile interagire con i dati del dashboard utilizzando i controlli che consentono di applicare filtri a livello di dashboard. Interagire con il pannello [eCommerce] Controls per visualizzare i dati relativi all'abbigliamento femminile del produttore Gnomehouse.

1. Dal menu a tendina Manufacturer, selezionare Gnomehouse
2. Dal menu a tendina Category, selezionare Women's Clothing
3. Cliccare Apply changes



Filtrare i dati

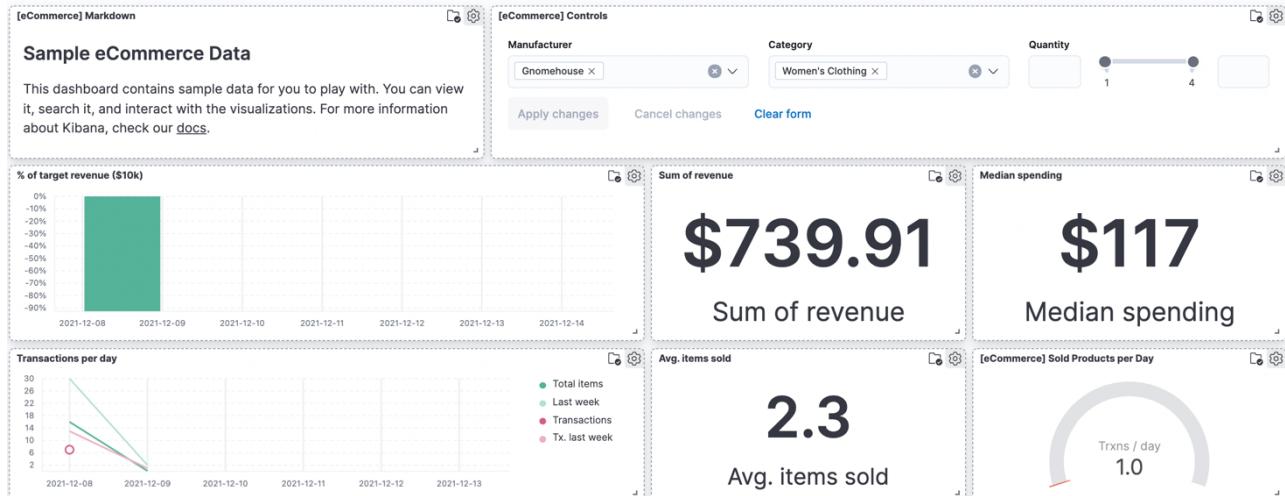
Per visualizzare un sottoinsieme di dati, è possibile applicare dei filtri ai pannelli del dashboard. Applicare un filtro per visualizzare i dati sull'abbigliamento femminile generati il mercoledì dal produttore Gnomehouse.

1. Cliccare Add filter
2. Dal menu a tendina Field, selezionare day_of_week
3. Dal menu a tendina Operator, selezionare is
4. Dal menu a tendina Value, selezionare Wednesday

The screenshot shows the "Edit filter" dialog box with the following fields:

- Field:** day_of_week
- Operator:** is
- Value:** Wednesday
- Buttons:** Cancel and Save
- Other:** A "Create custom label?" checkbox.

5. Cliccare Save



Costruire la propria dashboard

Caricare un set di dati in Elasticsearch

Questa esercitazione richiede tre insiemi di dati:

- Le opere complete di William Shakespeare, opportunamente analizzate in campi. Scaricare [shakespeare.json](#)
- Un insieme di conti finti con dati generati in modo casuale. Scaricare [accounts.zip](#)
- Un insieme di file di log generati in modo casuale. Scaricare [logs.jsonl.gz](#)

Decomprimere i file compressi.

Struttura dei set di dati

L'insieme di dati di Shakespeare ha questa struttura:

```
{  
    "line_id": INT,  
    "play_name": "String",  
    "speech_number": INT,  
    "line_number": "String",  
    "speaker": "String",  
    "text_entry": "String",  
}
```

L'insieme dei dati contabili è strutturato come segue:

```
{  
    "account_number": INT,  
    "balance": INT,  
    "firstname": "String",  
    "lastname": "String",  
    "age": INT,  
    "gender": "M or F",  
    "address": "String",  
    "employer": "String",  
    "email": "String",  
    "city": "String",  
    "state": "String"  
}
```

Il set di dati log ha decine di campi diversi. Ecco i campi importanti per questa esercitazione:

```
{  
    "memory": INT,  
    "geo.coordinates": "geo_point"  
    "@timestamp": "date"  
}
```

Impostare le mappature

Prima di caricare i set di dati Shakespeare e log, è necessario impostare le mappature per i campi. Le mappature dividono i documenti dell'indice in gruppi logici e specificano le caratteristiche dei campi. Queste caratteristiche includono la ricercabilità del campo e la sua eventuale tokenizzazione, ovvero la suddivisione in parole separate.

In Kibana **Dev Tools > Console**, impostare una mappatura per il set di dati Shakespeare:

```
PUT /shakespeare
{
  "mappings": {
    "properties": {
      "speaker": {"type": "keyword"},
      "play_name": {"type": "keyword"},
      "line_id": {"type": "integer"},
      "speech_number": {"type": "integer"}
    }
  }
}
```

Questa mappatura specifica le caratteristiche del campo per il set di dati:

- I campi speaker e play_name sono campi di parole chiave. Questi campi non vengono analizzati. Le stringhe vengono trattate come una singola unità anche se contengono più parole.
- I campi line_id e speech_number sono numeri interi.

Il set di dati dei log richiede una mappatura per etichettare le coppie di latitudine e longitudine come luoghi geografici, applicando il tipo geo_point.

```
PUT /logstash-2015.05.18
{
  "mappings": {
    "properties": {
      "geo": {
        "properties": {
          "coordinates": {
            "type": "geo_point"
          }
        }
      }
    }
  }
}
```

```
PUT /logstash-2015.05.19
{
  "mappings": {
    "properties": {
      "geo": {
        "properties": {

```

```
        "coordinates": {
          "type": "geo_point"
        }
      }
    }
  }
}
```

```
PUT /logstash-2015.05.20
{
  "mappings": {
    "properties": {
      "geo": {
        "properties": {
          "coordinates": {
            "type": "geo_point"
          }
        }
      }
    }
  }
}
```

Il set di dati dei conti non richiede alcuna mappatura.

Load the data sets

A questo punto, si è pronti a usare l'API bulk di Elasticsearch per caricare i set di dati:

```
curl --user elastic:changeme -H 'Content-Type: application/x-ndjson' -XPOST 'localhost:9200/bank/account/_bulk' --data-binary @accounts.json
```

```
curl --user elastic:changeme -H 'Content-Type: application/x-ndjson' -XPOST 'localhost:9200/shakespeare/_bulk' --data-binary @shakespeare_6.0.json
```

```
curl --user elastic:changeme -H 'Content-Type: application/x-ndjson' -XPOST 'localhost:9200/_bulk' --data-binary @logs.jsonl
```

L'esecuzione di questi comandi potrebbe richiedere del tempo, a seconda delle risorse informatiche disponibili.

Verificare l'avvenuto caricamento dalla Dev console:

```
GET /_cat/indices?v
```

Definire gli index patterns

Gli index pattern indicano a Kibana quali indici Elasticsearch si desidera esplorare. Un index pattern può corrispondere al nome di un singolo indice o includere un carattere jolly (*) per confrontare più indici.

Ad esempio, Logstash crea tipicamente una serie di indici nel formato logstash-YYYY.MM.DD. Per esplorare tutti i dati di log di maggio 2018, si potrebbe specificare il pattern di indice logstash-2018.05*.

Verranno creati dei pattern per il set di dati Shakespeare, che ha un indice chiamato shakespeare, e per il set di dati accounts, che ha un indice chiamato bank. Questi set di dati non contengono dati di serie temporali.

1. In Kibana, aprire Stack Management, e cliccare Index Patterns.
2. Se si tratta del primo modello di indice, la pagina Create index pattern si apre automaticamente. Altrimenti, cliccare **+ Create index pattern** in alto a sinistra.
3. Immettere shak* nel campo Index pattern.

The screenshot shows the 'Create index pattern' interface. On the left, there's a form with a 'Name' field containing 'shak*' and a 'Timestamp field' dropdown set to 'Select a timestamp field'. A note below the timestamp field says 'No matching data stream, index, or index alias has a timestamp field.' On the right, a summary bar indicates 'Your index pattern matches 1 source.' with 'shakespeare' listed under 'Index'. Below the summary, there's a 'Rows per page: 10' dropdown. At the bottom of the screen, there are 'Close' and 'Create index pattern' buttons.

4. Fare clic su **Create index pattern**. Per questo modello non è necessario configurare alcuna impostazione.
5. Definire un secondo modello di indice denominato ba*. Non è necessario configurare alcuna impostazione per questo modello.
6. Creare ora un modello di indice per il set di dati Logstash. Questo set di dati contiene dati di serie temporali.
7. Definire un modello di indice denominato logstash*.
8. Selezionare @timestamp nel menu a discesa del nome del campo Timestamp.

Scoprire ed esplorare i dati

Utilizzando l'applicazione Discover, è possibile inserire una query Elasticsearch per cercare i dati e filtrare i risultati.

1. Aprire Discover.
2. Il modello di indice corrente appare sotto la barra dei filtri, in questo caso scosse*. Potrebbe essere necessario fare clic su Nuovo nella barra dei menu per aggiornare i dati.
3. Fare clic sul cursore a destra del modello di indice corrente e selezionare ba*.
4. Nel campo di ricerca inserire la seguente stringa:
account_number<= 100 and balance >= 47500

5. Cliccare 

Document
> account_number: 32 address: 702 Quentin Street age: 34 balance: 48,086 city: Veguita email: dillardmcpherson@qualcom.com employer: Qualcom firstname: Dillard gender: F lastname: Mcpherson state: IN _id: 32 _index: bank _score: 2 _type: account
> account_number: 78 address: 834 Amber Street age: 23 balance: 48,656 city: Dunbar email: elvirapatterson@assistix.com employer: Assistix firstname: Elvira gender: F lastname: Patterson state: TN _id: 78 _index: bank _score: 2 _type: account
> account_number: 85 address: 212 Irving Avenue age: 20 balance: 48,735 city: Kipp email: wilcoxsellers@confrenzy.com employer: Confrenzy firstname: Wilcox gender: M lastname: Sellers state: MT _id: 85 _index: bank _score: 2 _type: account
> account_number: 97 address: 512 Cumberland Walk age: 40 balance: 49,671 city: Fredericktown email: karentrujillo@tsunamia.com employer: Tsunamia firstname: Karen gender: F lastname: Trujillo state: MO _id: 97 _index: bank _score: 2 _type: account
> account_number: 8 address: 699 Visitation Place age: 35 balance: 48,868 city: Wakulla email: janburns@glasstep.com employer: Glasstep firstname: Jan gender: M lastname: Burns state: AZ _id: 8 _index: bank _score: 2 _type: account

Per impostazione predefinita, tutti i campi vengono visualizzati per ogni documento confrontato. Per scegliere quali campi visualizzare, passare il puntatore sull'elenco dei Campi disponibili e fare clic su Aggiungi accanto a ciascun campo che si desidera includere come colonna nella tabella.

Ad esempio, se si aggiunge il campo numero_conto, la visualizzazione cambia in un elenco di cinque numeri di conto.

The screenshot shows the Kibana search interface. At the top, there is a search bar with the query "account_number<= 100 and balance >= 47500". Below the search bar are filter options: "Selected fields" (account_number) and "Available fields" (_id, _index, _score). On the right, a table titled "5 hits" lists five account numbers: 32, 78, 85, 97, and 8.

Visualize data

Nell'applicazione Visualize è possibile modellare i dati utilizzando una serie di grafici, tabelle, mappe e altro ancora. Verranno create quattro visualizzazioni: un grafico a torta, un grafico a barre, una mappa di coordinate e un widget Markdown.

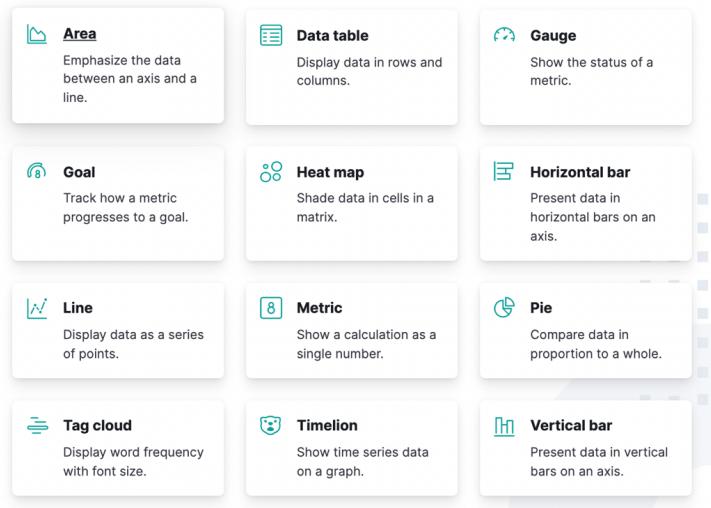
1. Aprire Visualize Library
2. Fare clic su [+ Create visualization](#). Verranno visualizzati tutti i tipi di visualizzazione in Kibana.

The screenshot shows the "New visualization" library. It features several cards:

- Lens**: Create visualizations with our drag and drop editor. Switch between visualization types at any time. Recommended for most users.
- Maps**: Create and style maps with multiple layers and indices.
- TSVB**: Perform advanced analysis of your time series data.
- Custom visualization**: Use Vega to create new types of visualizations. Requires knowledge of Vega syntax.
- Aggregation based**: Use our classic visualize library to create charts based on aggregations. [Explore options →](#)
- Tools**:
 - Text**: Add text and images to your dashboard.
 - Controls**: Add dropdown menus and range sliders to your dashboard.

3. Cliccare Aggregation based

New visualization

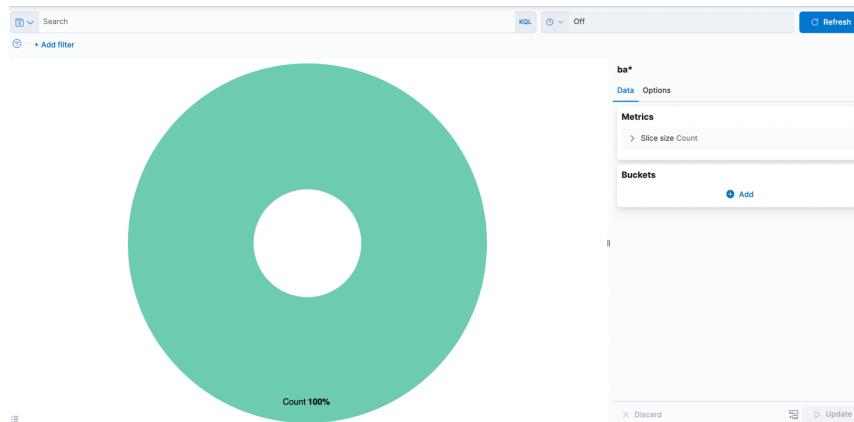


4. Cliccare Pie

5. In New Search, selezionare il modello di indice ba*. Il grafico a torta verrà utilizzato per ottenere informazioni sui saldi dei conti correnti nei dati dei conti bancari.

Pie chart

Inizialmente, la torta contiene una sola "fetta". Questo perché la ricerca predefinita ha confrontato tutti i documenti.



Per specificare quali fette visualizzare nella torta, si utilizza un'aggregazione di bucket di Elasticsearch. Questa aggregazione ordina i documenti che si confrontano con i criteri di ricerca in diverse categorie, note anche come bucket.

Utilizzate un'aggregazione di bucket per stabilire più intervalli di saldi dei conti e scoprire quanti conti rientrano in ciascun intervallo.

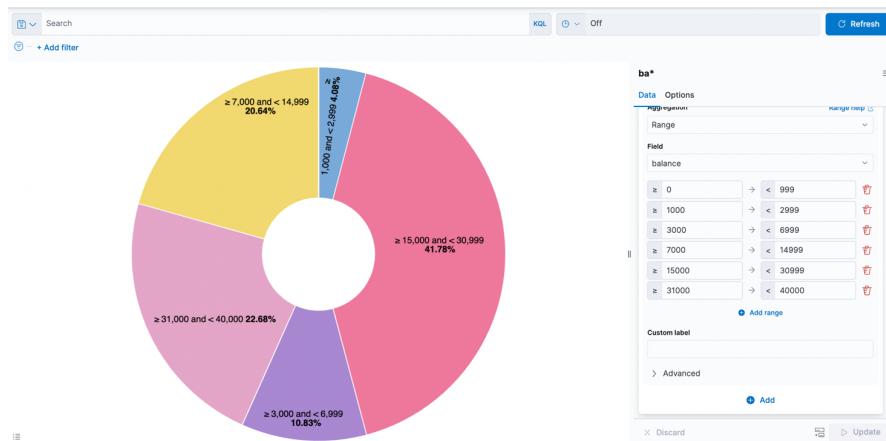
1. Nel riquadro Buckets, fare clic su Add e poi su Split Slices.
2. Nel menu a tendina Aggregation, selezionare Range.
3. Nel menu a tendina Field, selezionare balance.

4. Fare clic su Add Range quattro volte per portare il numero totale di intervalli a sei.
5. Definire i seguenti intervalli:

0	999
1000	2999
3000	6999
7000	14999
15000	30999
31000	50000

6. Cliccare 

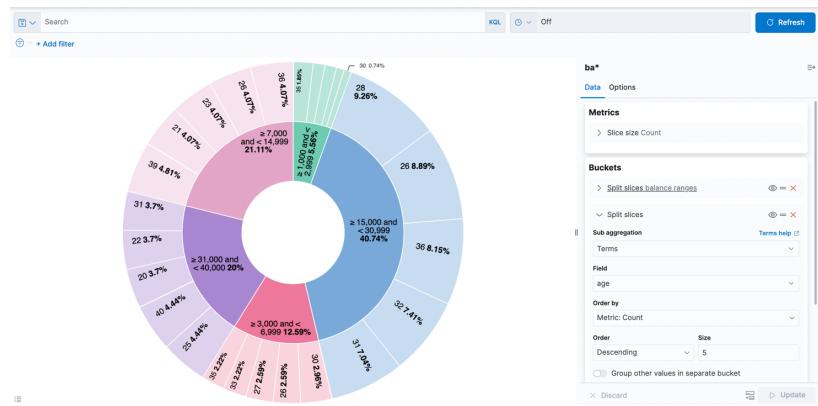
Ora è possibile vedere quale percentuale dei 1000 conti rientra in ciascuna fascia di saldo.



Aggiungere un'altra aggregazione di bucket che consideri l'età dei titolari dei conti.

1. Nella parte inferiore del riquadro Buckets, cliccare Add.
2. In Select buckets type, cliccare Split Slices.
3. Nel menu a tendina Sub Aggregation, selezionare Terms.
4. Nel menu a tendina Field, selezionare age.
7. Cliccare il pulsante .

Ora è possibile vedere la suddivisione dell'età dei titolari dei conti, visualizzata in un anello intorno agli intervalli di saldo.



Per salvare questo grafico

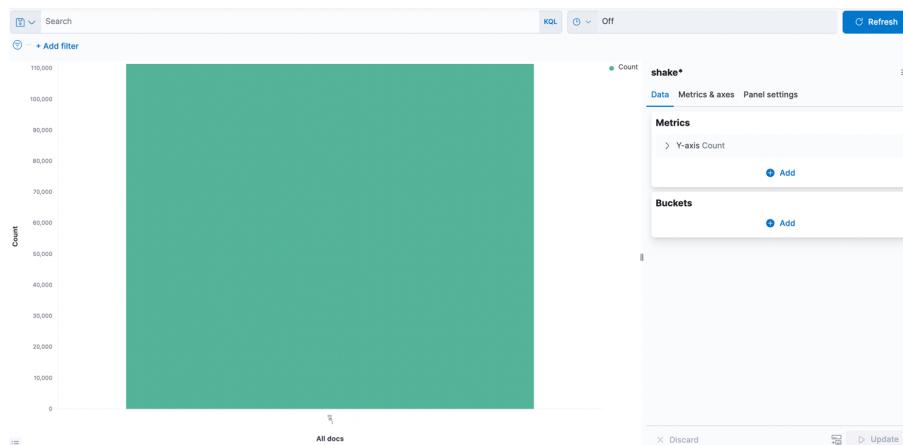
1. Cliccare Save nella barra dei menu superiore e inserire Pie Example
2. Selezionare None nell'opzione Add to dashboard
3. Cliccare **Save and add to library**

Bar chart

Utilizzerete un grafico a barre per esaminare il set di dati di Shakespeare e confrontare il numero di parti parlate nelle opere teatrali.

Creare un grafico **Vertical Bar** e impostare l'origine della ricerca su **shakes***.

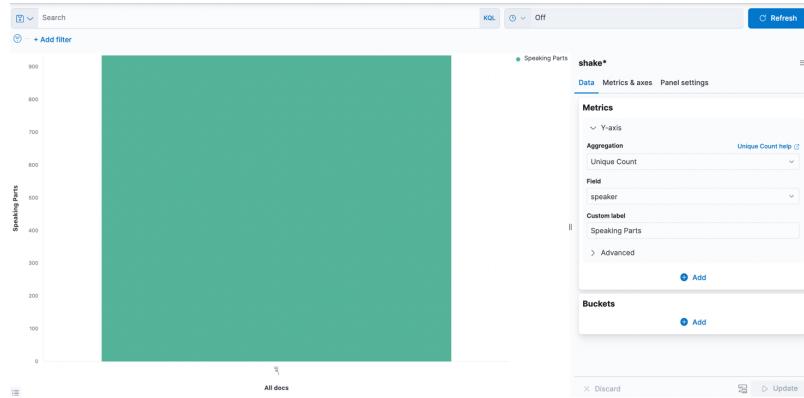
Inizialmente, il grafico è costituito da una singola barra che mostra il numero totale di documenti che si confrontano con la query jolly predefinita.



Mostrare il numero di parti parlanti per rappresentazione lungo l'asse Y. Questo richiede la configurazione dell'aggregazione delle metriche dell'asse Y. Questa aggregazione calcola le metriche in base ai valori dei risultati della ricerca.

1. Nel riquadro Metrics espandere Y-Axis
2. Impostare Aggregation su Unique Count
3. Impostare il campo Field a speaker
4. Nella casella Custom Label, inserire Speaking Parts

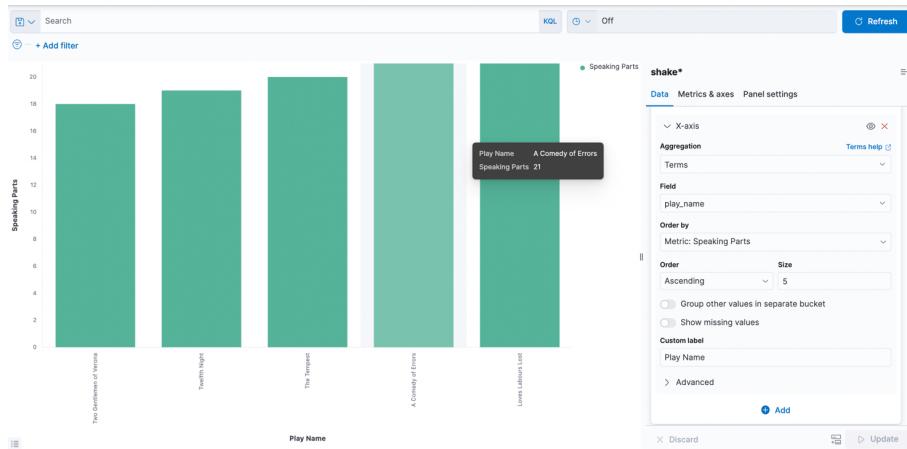
5. Cliccare 



Mostrare le rappresentazioni lungo l'asse X.

1. Nel riquadro Buckets, Cliccare Add e poi X-Axis.
2. Impostare Aggregation a Terms e Field a play_name.
3. Per elencare le opere in ordine alfabetico, nel menu a discesa Order, selezionare Ascending.
4. Assegnare all'asse un'etichetta personalizzata, Play Name.
5. Cliccare 

Se si passa il mouse su una barra, viene visualizzato un tooltip con il numero di parti parlanti per quell'opera.



Si noti come i nomi dei singoli spettacoli vengano visualizzati come frasi intere, invece che suddivisi in singole parole. Questo è il risultato della mappatura effettuata all'inizio dell'esercitazione, quando si è contrassegnato il campo play_name come non analizzato.

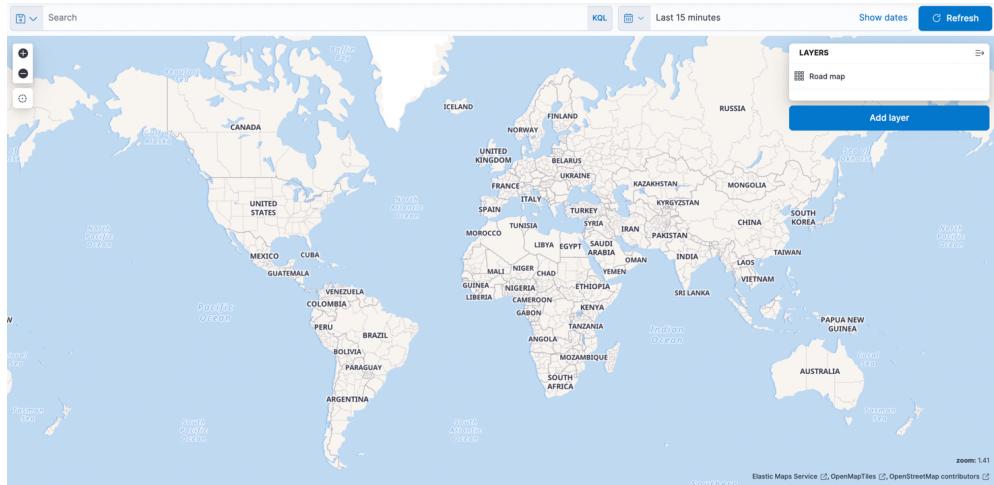
Per salvare questo grafico

1. Fare clic su Save nella barra dei menu in alto e immettere Bar Example
2. Selezionare None nell'opzione Add to dashboard
3. Cliccare 

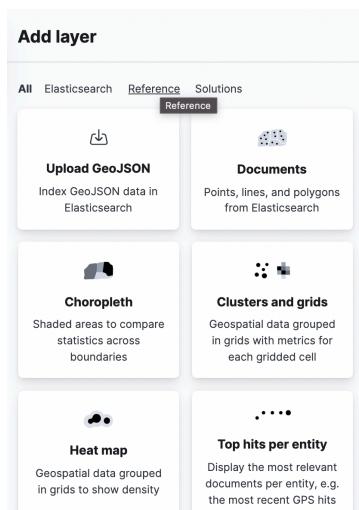
Map

Utilizzando una mappa, è possibile visualizzare le informazioni geografiche nei dati di esempio del file di log.

1. Tra i tipi di visualizzazione selezionare Map

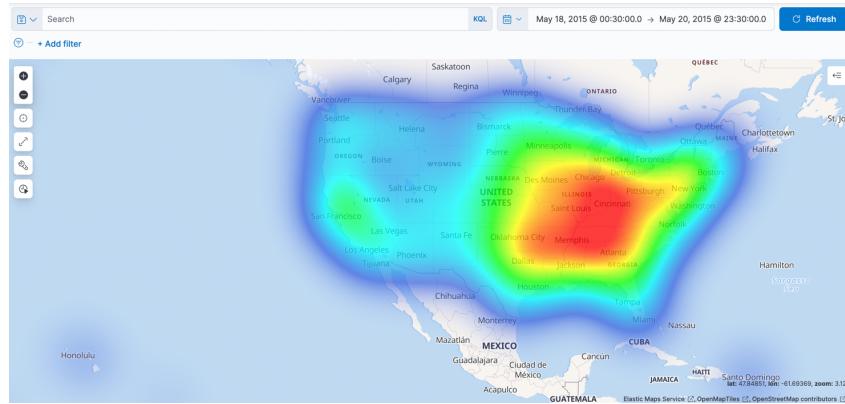


2. Cliccare Add layer
3. Selezionare Heat map



4. Nel menu index patter selezionare logstash*
5. Cliccare **Add layer →**
6. Inserire il nome events
7. Cliccare **Save & close**
8. Nella barra dei menu in alto, fare clic sul selezionatore dell'ora all'estrema destra.
9. Cliccare Absolute.
10. Impostate l'ora di inizio al 18 maggio 2015 e l'ora di fine al 20 maggio 2015.

11. Cliccare Update.



Per salvare questo grafico

1. Fare clic su Save nella barra dei menu in alto e inserire Map Example
2. Selezionare None nell'opzione Add to dashboard
3. Cliccare Save and add to library

Text

La visualizzazione finale è un widget Markdown che rende il testo formattato.

1. Nel menu del tipo di visualizzazione, selezionare Text sotto Tools
2. Nella casella di testo, inserite quanto segue:

```
# This is a tutorial dashboard!
The Markdown widget uses **markdown** syntax.
> Blockquotes in Markdown use the > character.
```

3. Cliccare D Update

Il Markdown viene visualizzato nel riquadro di anteprima:

This is a tutorial dashboard!

The Markdown widget uses markdown syntax.

> Blockquotes in Markdown use the > character.

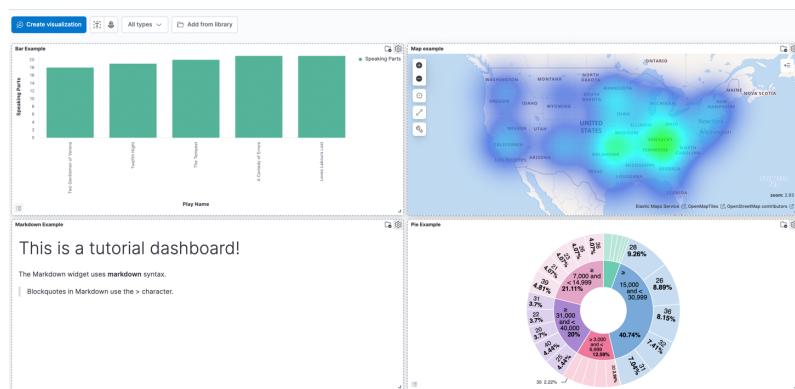
Per salvare questo grafico

1. Cliccare Save nella barra dei menu in alto e inserire Markdown Example
2. Selezionare None nell'opzione Add to dashboard
3. Cliccare **Save and add to library**

Aggiungere visualizzazioni a un dashboard

Una dashboard è una collezione di visualizzazioni che si possono organizzare e condividere. Si costruirà una dashboard che contiene le visualizzazioni salvate durante questa esercitazione.

1. Aprire Dashboard
2. Cliccare **+ Create dashboard**
3. Cliccare **Add from library**
4. Aggiungere Bar Example, Map Example, Markdown Example, e Pie Example.



È possibile riorganizzare le visualizzazioni facendo clic sull'intestazione di una visualizzazione e trascinandola. L'icona dell'ingranaggio in alto a destra di una visualizzazione visualizza i controlli per modificare e cancellare la visualizzazione. In basso a destra è presente un controllo di ridimensionamento.

Per ottenere un link da condividere o un codice HTML per incorporare il dashboard in una pagina web, salvare il dashboard.

Il pulsante Share consente di condividere il dashboard come codice incorporato, Permalink, report PDF e PNG.