

Introduction à la Suite Elastic (Elasticsearch & Kibana)

Maîtrisez les bases d'Elasticsearch et Kibana via elastic cloud

INDEX

1

Présentation

Aperçu suite Elastic



2

Installation/exploration

Login/access elastic cloud



3

Ateliers pratiques

Practice endpoints,
dataviz

Planning

- **Introduction (Slides 1-7):** 30 minutes
- **Aperçu de Logstash (Slide 8):** 5 minutes
- **Installation et configuration (Slides 9-12):** 30 minutes
- **Exploration d'Elasticsearch (Slides 13-18):** 45 minutes
- **Introduction à Kibana (Slides 19-23):** 45 minutes
- **Atelier pratique (Slides 24-26):** 60 minutes (incluant les exercices)
- **Questions/Réponses et Conclusion (Slides 27-30):** 15 minutes

Total: 4 heures

Sommaire

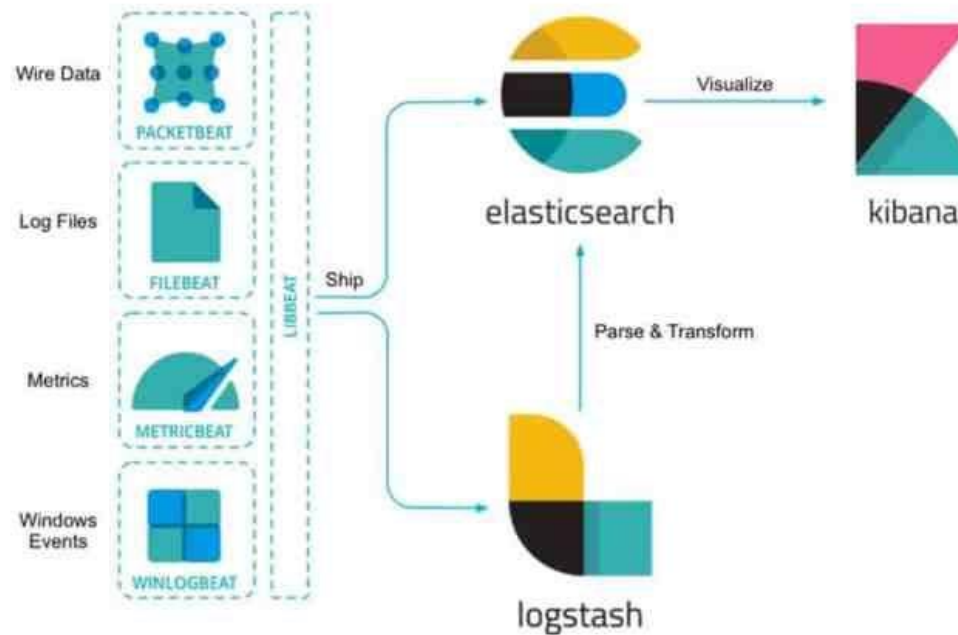
1. Présentation de la Suite Elastic
2. Présentation brève de Logstash
3. Points forts/points faibles elastic search
4. Installation et configuration
5. Exploration d'Elasticsearch
6. Introduction à Kibana
7. Atelier pratique (Exercices)
8. Questions / Réponses
9. Ressources supplémentaires

01

Présentation de la Suite Elastic

Qu'est-ce que la Suite Elastic?

Elastic (ELK) Stack Architecture



**la majorité du workshop se concentrera sur Elasticsearch et Kibana via Elastic Cloud*



elastic

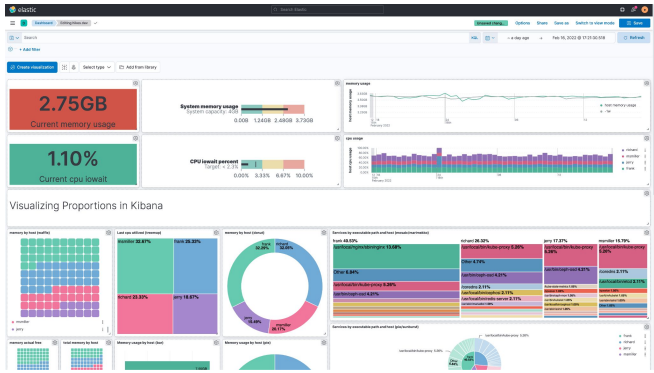


kibana

Cas d'utilisation typiques de la Suite Elastic



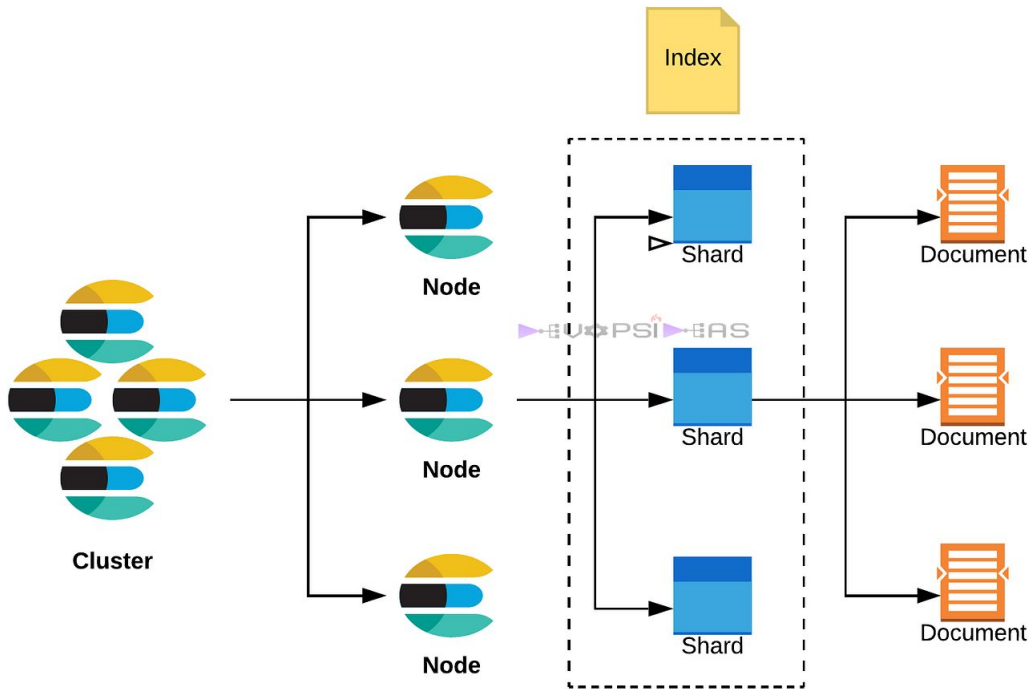
Recherche de données



Analyse de données



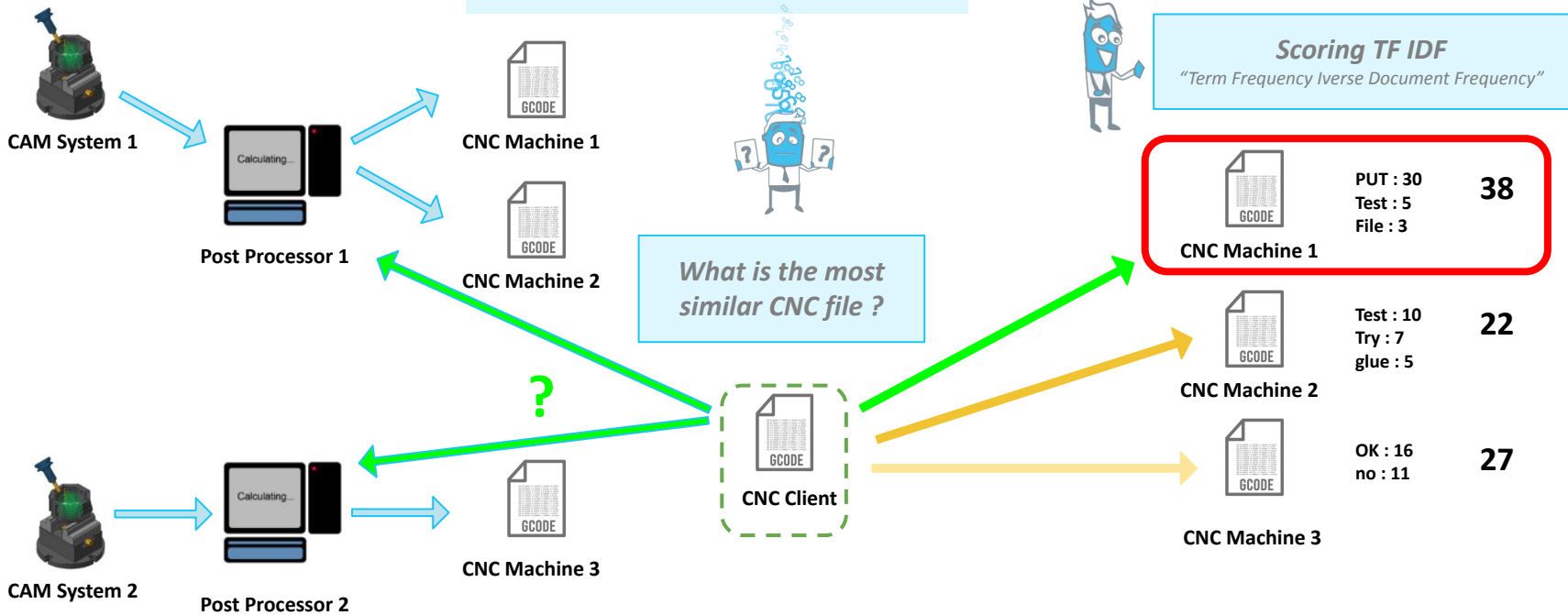
Elasticsearch Component Relation



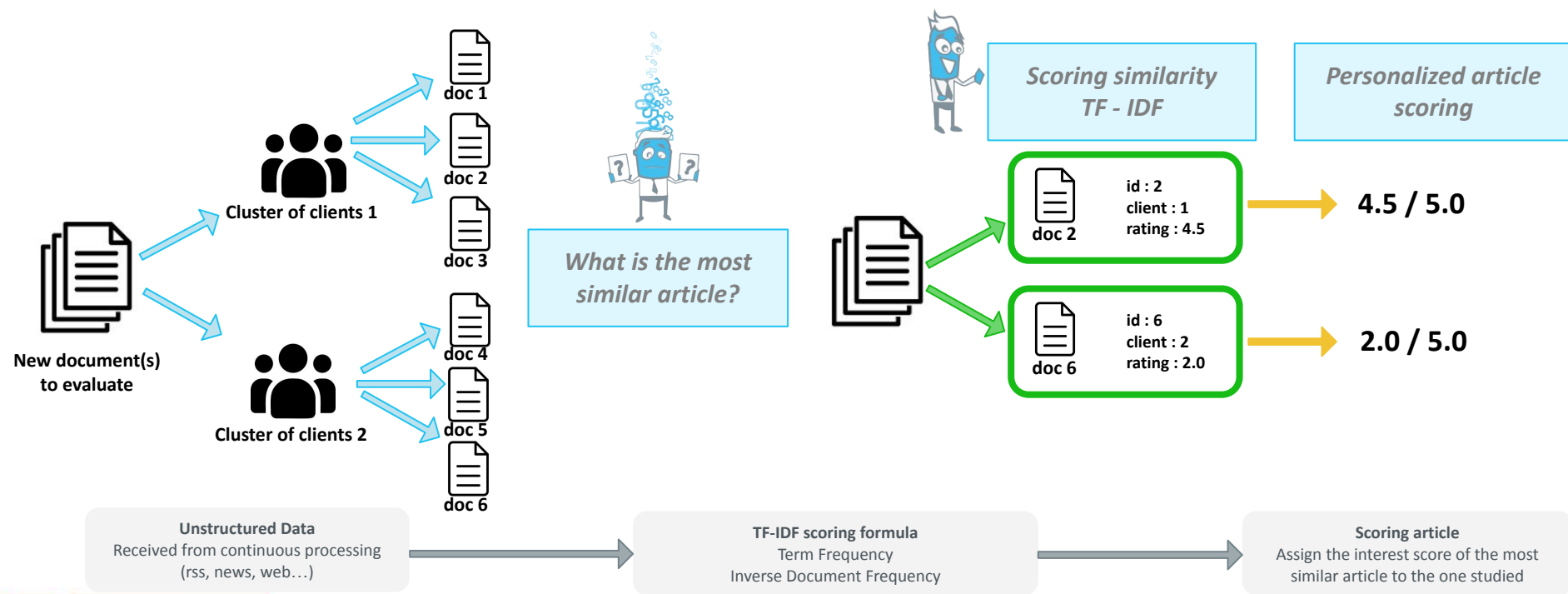
Cas d'usage HUPI

Optimisation du processus de mise en service des machines-outils

Scoring similarity



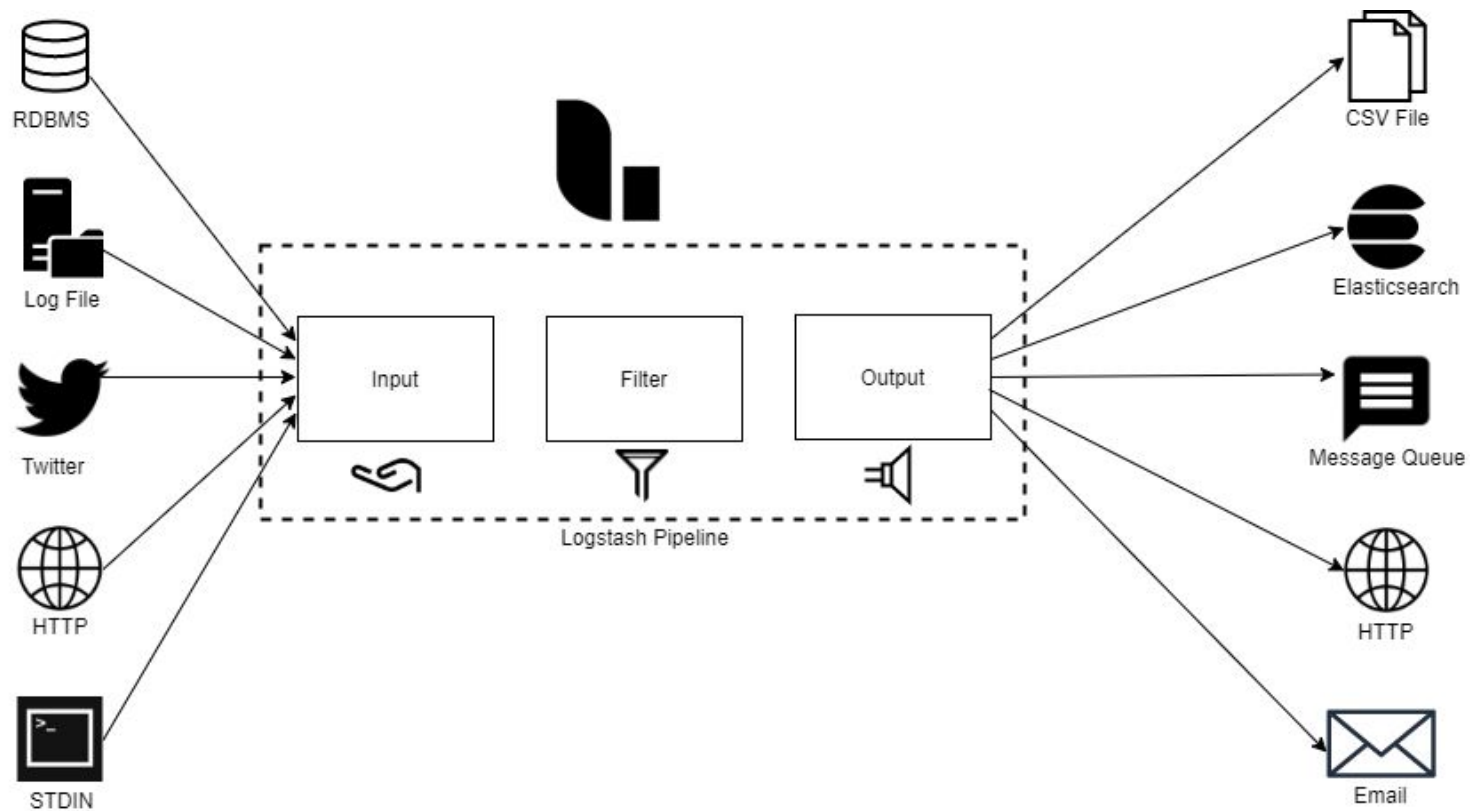
Prédiction du “niveau d’intérêt”
de documents personnalisé par clients



01

Présentation brève de Logstash

Aperçu de Logstash



01

Points forts, points faibles

Elastic search



“Comment Elasticsearch favorise une scalabilité horizontale, garantissant ainsi une recherche rapide et des performances analytiques.”



"Si Elasticsearch offre de puissantes fonctionnalités, il présente un certain niveau de complexité et peut être gourmand en ressources. "

Comparaison avec d'autres méthodes : TF-IDF en Python

```
In [98]: def computeIDF(docList):
import math
idfDict = {}
N = len(docList)

idfDict = dict.fromkeys(docList[0].keys(), 0)
for doc in docList:
    for word, val in doc.items():
        if val > 0:
            idfDict[word] += 1

for word, val in idfDict.items():
    idfDict[word] = math.log10(N / float(val))

return idfDict
```

```
In [94]: def computeTF(wordDict, bow):
tfDict = {}
bowCount = len(bow)
for word, count in wordDict.items():
    tfDict[word] = count/float(bowCount)
return tfDict
```

```
In [100]: def computeTFIDF(tfBow, idfs):
tfidf = {}
for word, val in tfBow.items():
    tfidf[word] = val*idfs[word]
return tfidf
```



Natural language processing

Elastic Search TF-IDF implement

Objectif : comment décomposer le score d'un document en fonction du résultat obtenu par Lucene.

```

16 ..... "multi_match": {
17 .....   "query": "Global economic implications of the Russia-Ukraine war",
18 .....   "fields": ["DocTitle", "DocContent"]
19 ..... }
20 ..... }
21 ..... ]
22 ..... }
  
```

```

108 {
109   "value": 53.718456,
110   "description": "sum of:",
111   "details": [
112     {
113       "value": 6.169303,
114       "description": "weight(DocTitle:global in 0) [PerFieldSimilarity], result of:",
115       "details": [
116         {
117           "value": 6.169303,
118           "description": "score(freq=1.0), computed as boost * idf * tf from:",
119           "details": [
120             {
121               "value": 2.2,
122               "description": "boost",
123               "details": []
124             },
125             {
126               "value": 5.054971,
127               "description": "idf, computed as log(1 + (N - n + 0.5) / (n + 0.5))",
128               "details": [
129                 {
130                   "value": 5.054971,
131                   "description": "idf, computed as log(1 + (N - n + 0.5) / (n + 0.5))",
132                   "details": [
133                     {
134                       "value": 5.054971,
135                       "description": "idf, computed as log(1 + (N - n + 0.5) / (n + 0.5))",
136                       "details": [
137                         {
138                           "value": 5.054971,
139                           "description": "idf, computed as log(1 + (N - n + 0.5) / (n + 0.5))",
140                           "details": [
141                             {
142                               "value": 5.054971,
143                               "description": "idf, computed as log(1 + (N - n + 0.5) / (n + 0.5))",
144                               "details": [
145                                 {
146                                   "value": 5.054971,
147                                   "description": "idf, computed as log(1 + (N - n + 0.5) / (n + 0.5))",
148                                   "details": [
149                                     {
150                                       "value": 5.054971,
151                                       "description": "idf, computed as log(1 + (N - n + 0.5) / (n + 0.5))",
152                                       "details": [
153                                         {
154                                           "value": 5.054971,
155                                           "description": "idf, computed as log(1 + (N - n + 0.5) / (n + 0.5))",
156                                           "details": [
157                                             {
158                                               "value": 5.054971,
159                                               "description": "idf, computed as log(1 + (N - n + 0.5) / (n + 0.5))",
160                                               "details": [
161                                                 {
162                                                   "value": 5.054971,
163                                                   "description": "idf, computed as log(1 + (N - n + 0.5) / (n + 0.5))",
164                                                   "details": [
165                                                     {
166                                                       "value": 5.054971,
167                                                       "description": "idf, computed as log(1 + (N - n + 0.5) / (n + 0.5))",
168                                                       "details": [
169                                                         {
170                                                           "value": 5.054971,
171                                                           "description": "idf, computed as log(1 + (N - n + 0.5) / (n + 0.5))",
172                                                           "details": [
173                                                             {
174                                                               "value": 5.054971,
175                                                               "description": "idf, computed as log(1 + (N - n + 0.5) / (n + 0.5))",
176                                                               "details": [
177                                                                 {
178                                                                  "value": 5.054971,
179                                                                  "description": "idf, computed as log(1 + (N - n + 0.5) / (n + 0.5))",
180                                                                  "details": [
181                                                                    {
182                                                                      "value": 5.054971,
183                                                                      "description": "idf, computed as log(1 + (N - n + 0.5) / (n + 0.5))",
184                                                                      "details": [
185                                                                      ]
186                                                                    }
187                                                                  ]
188                                                                }
189                                                              ]
190                                                            }
191                                                          ]
192                                                        }
193                                                      ]
194                                                    }
195                                                  ]
196                                                }
197                                              ]
198                                            }
199                                          ]
200                                        }
201                                      ]
202                                    }
203                                  ]
204                                }
205                              ]
206                            }
207                          ]
208                        }
209                      ]
210                    }
211                  ]
212                }
213              ]
214            }
215          ]
216        }
217      ]
218    }
219  }
  
```

Calcul du score pour le terme "global" :

- boost = 2.2
- idf = 5.054971
- tf = 0.5547467

=> score = boost*idf*tf

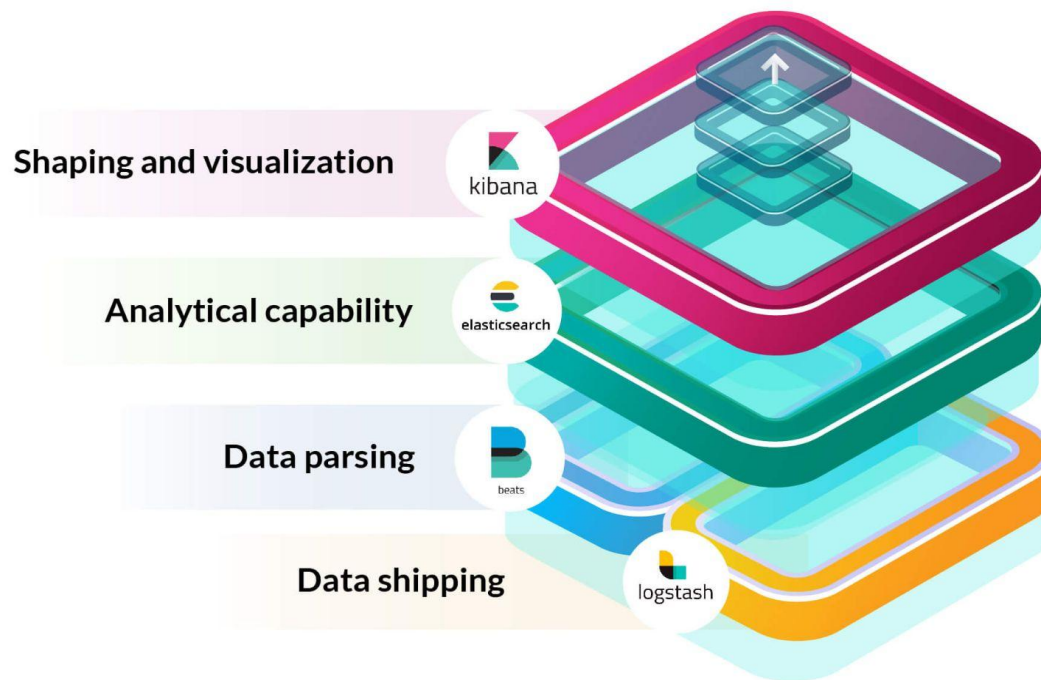
Zoom de IDF

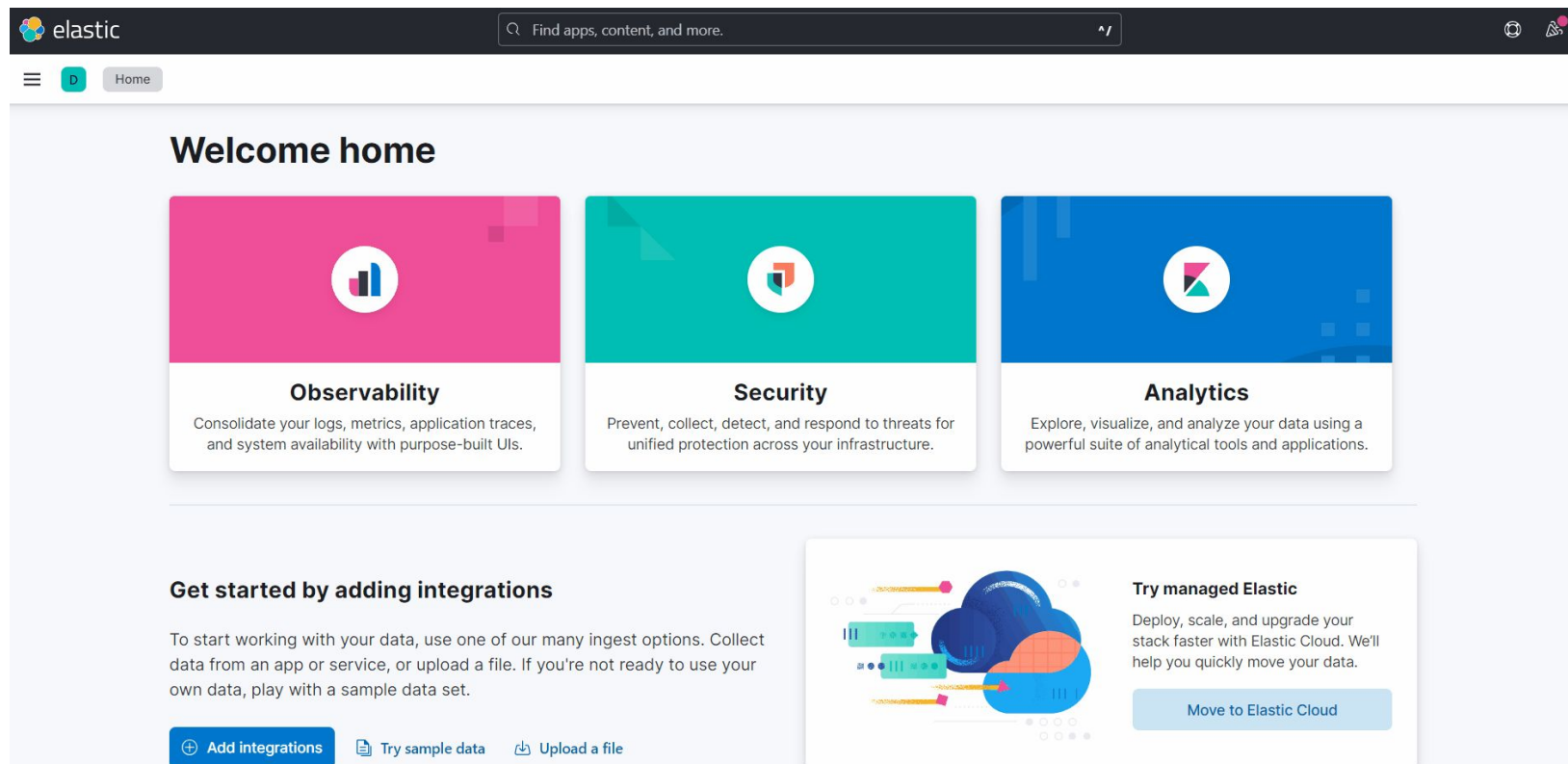
Zoom de TF

* Explain peut expliquer pourquoi un document ne correspond pas à une requête aussi

01


Installation et configuration (Elastic Cloud)






The screenshot shows the Elastic Cloud dashboard interface. At the top is a dark navigation bar with the Elastic logo, a search bar containing the text "Find apps, content, and more.", and user profile icons. Below the navigation bar is a "Home" button. The main content area features a "Welcome home" heading followed by three large colored cards: "Observability" (pink), "Security" (teal), and "Analytics" (blue). Each card contains an icon and a brief description of its capabilities. Below these cards is a section titled "Get started by adding integrations" with a paragraph of text and three buttons: "Add integrations", "Try sample data", and "Upload a file". To the right of this section is a "Try managed Elastic" box with a diagram of a cloud stack and a "Move to Elastic Cloud" button.

Welcome home




Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.



Security

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.




Analytics

Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, play with a sample data set.

[+ Add integrations](#) [Try sample data](#) [Upload a file](#)



Try managed Elastic

Deploy, scale, and upgrade your stack faster with Elastic Cloud. We'll help you quickly move your data.

[Move to Elastic Cloud](#)

Création d'un compte sur Elastic Cloud

cloud.elastic.co/registration?fromURI=%2Fhome

Apps

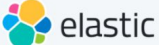
2021-03-16 Doce...

USAA - Centralize...

Public Training Ma...

Courses - Educati...

» | Other Bookmarks | Reading List



Already have an account? [Log in](#)

Start your free Elastic Cloud trial

No credit card required

Email

Password

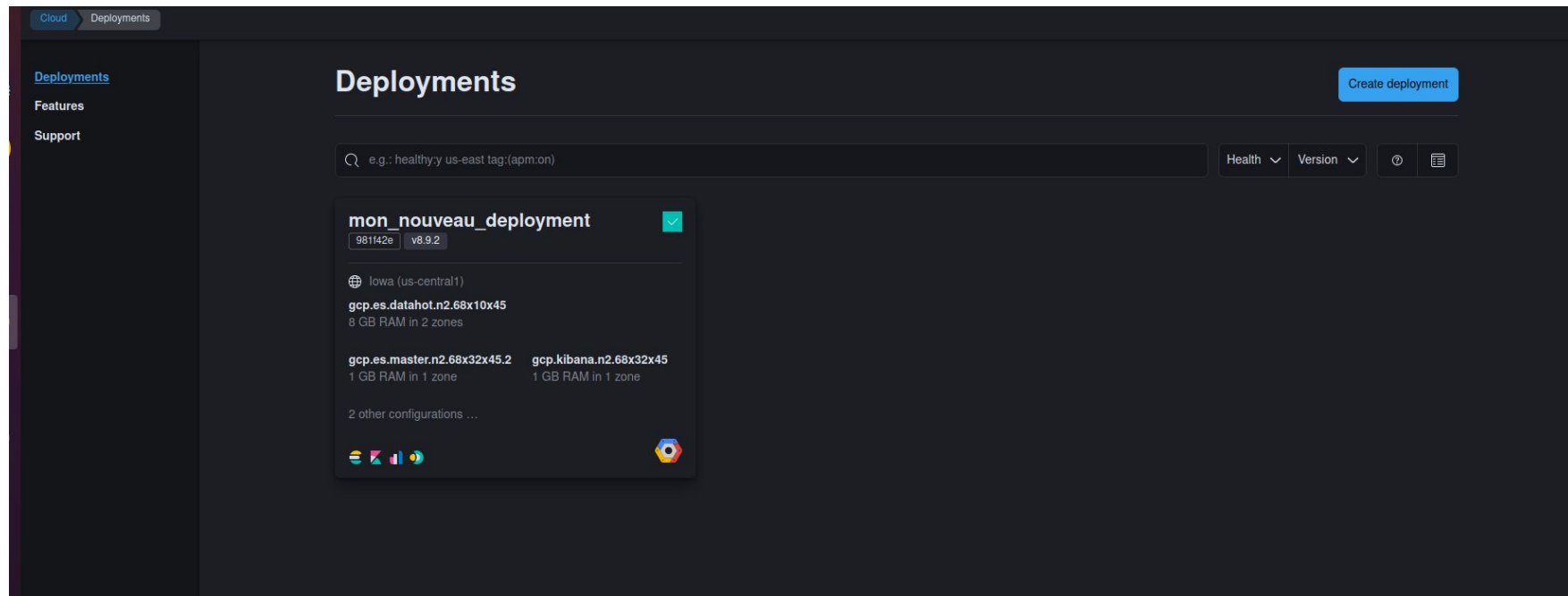
Start free trial

Or sign up with

Google

Microsoft

By signing up, you acknowledge that you've read and agree to our [Terms of Service](#) and [Privacy Statement](#).



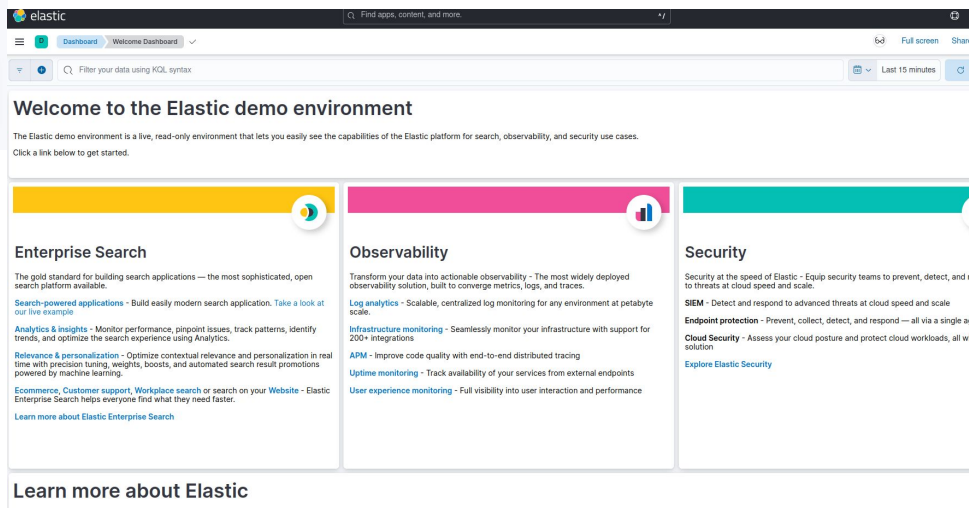
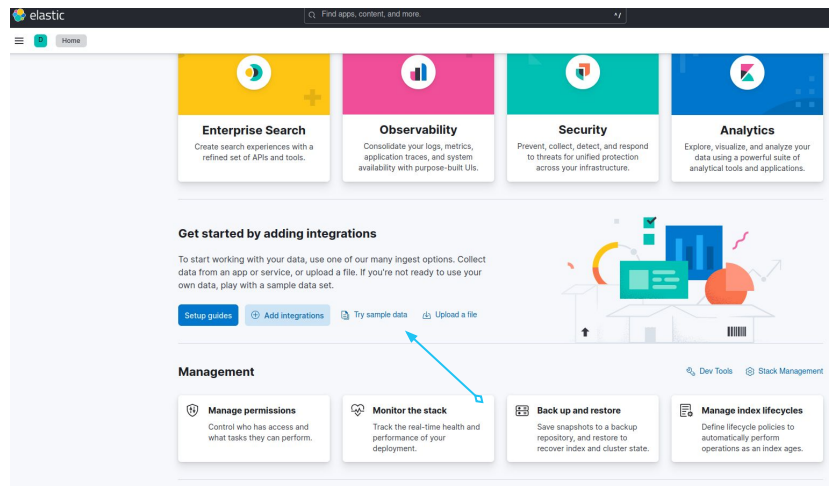
The screenshot shows the Elastic Cloud 'Deployments' page. On the left is a sidebar with 'Cloud' and 'Deployments' tabs, and links for 'Deployments', 'Features', and 'Support'. The main area is titled 'Deployments' and includes a 'Create deployment' button. A search bar contains the text 'e.g.: healthy-y us-east tag:(apm:on)'. Below the search bar, a deployment card for 'mon_nouveau_deployment' is shown with a green checkmark. The card displays the ID '981142e' and version 'v8.9.2'. It lists the region 'Iowa (us-central1)' and the instance types: 'gcp.es.datahot.n2.68x10x45' (8 GB RAM in 2 zones), 'gcp.es.master.n2.68x32x45.2' (1 GB RAM in 1 zone), and 'gcp.kibana.n2.68x32x45' (1 GB RAM in 1 zone). It also mentions '2 other configurations ...' and shows icons for various cloud providers.

Rechercher des jeux de données avec des données textuelles :

- <https://www.kaggle.com/datasets/abdallahwagih/books-dataset>
- <https://www.kaggle.com/datasets/thedevastator/books-sales-and-ratings>

Libre choix dans la recherche de données.

Accès et configuration initiale de Kibana via Elastic Cloud



02

Exploration d'Elasticsearch

Cloud

Deployments

mon_nouveau_deployment

Deployments

mon_nouveau_deployment...

Edit

Monitoring

Health

Logs and metrics

Performance

Elasticsearch

Snapshots

API console

Kibana

Integrations Server

Enterprise Search

Activity

Security

Features

Support

mon_nouveau_deployment

HEALTHY

GCP - Iowa (us-central1)

Deployment ID 981f42

Deployment name

mon_nouveau_deployment

Edit

Custom endpoint alias

Create an alias

Applications

Elasticsearch

Kibana

API

Fleet

Enterprise Search

Copy endpoint

Copy cluster ID

Copy component ID

Copy component ID

Copy component ID

Open

Open

Open

Open

Hardware profile

Storage optimized

Edit

Tags

Add tags

Instances

Zone us-central1-a

Tiebreaker #2

Healthy · v8.9.2 · 1 GB RAM · GCP.ES.MASTER.N2.68X32X45.2 · master eligible

Disk allocation 1 MB / 45 GB 0 %

Zone us-central1-b

Instance #0

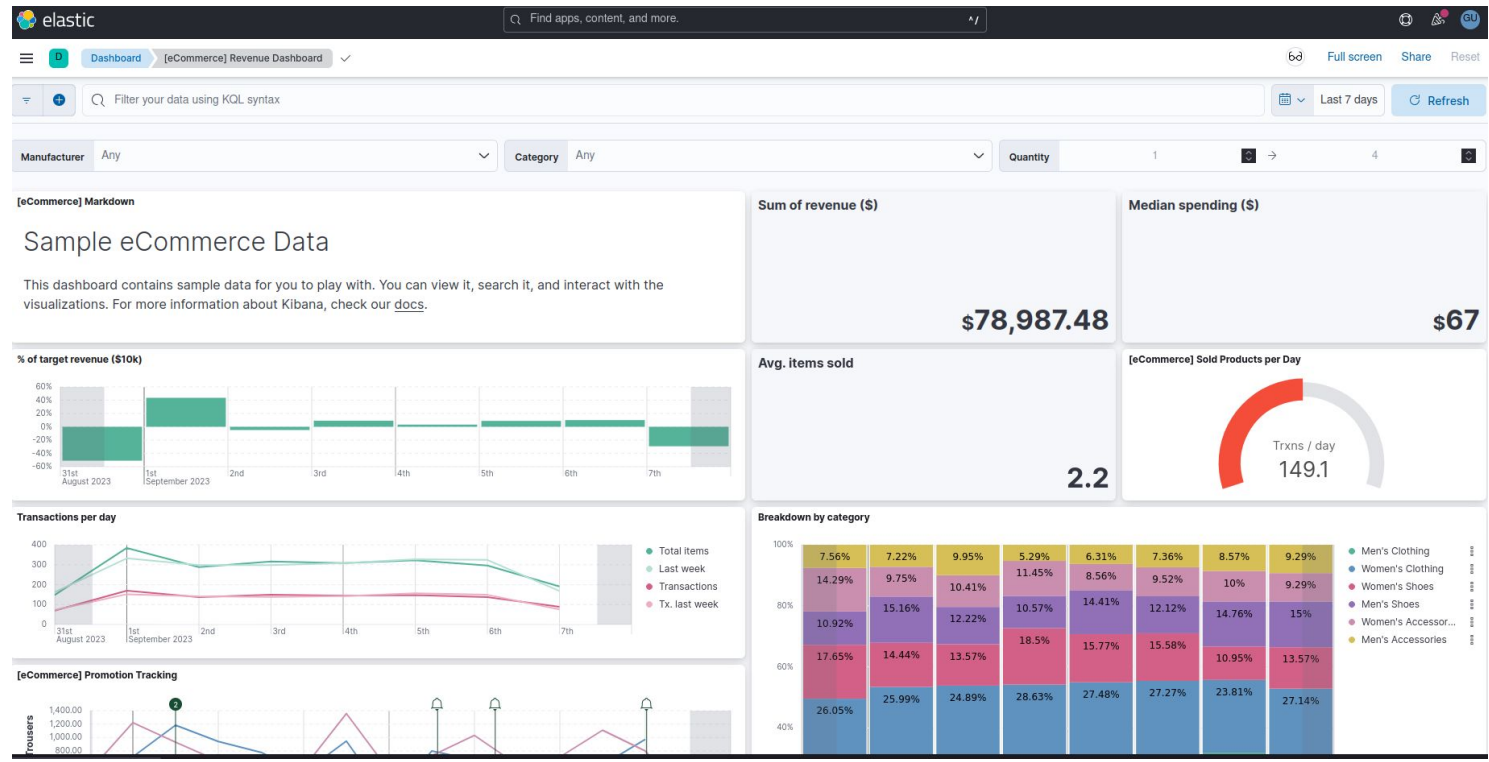
Healthy · v8.9.2 · 4 GB RAM · GCP.ES.DATAHOT.N2.68X10X45 · data_hot · data_content · master · coordinating · ingest

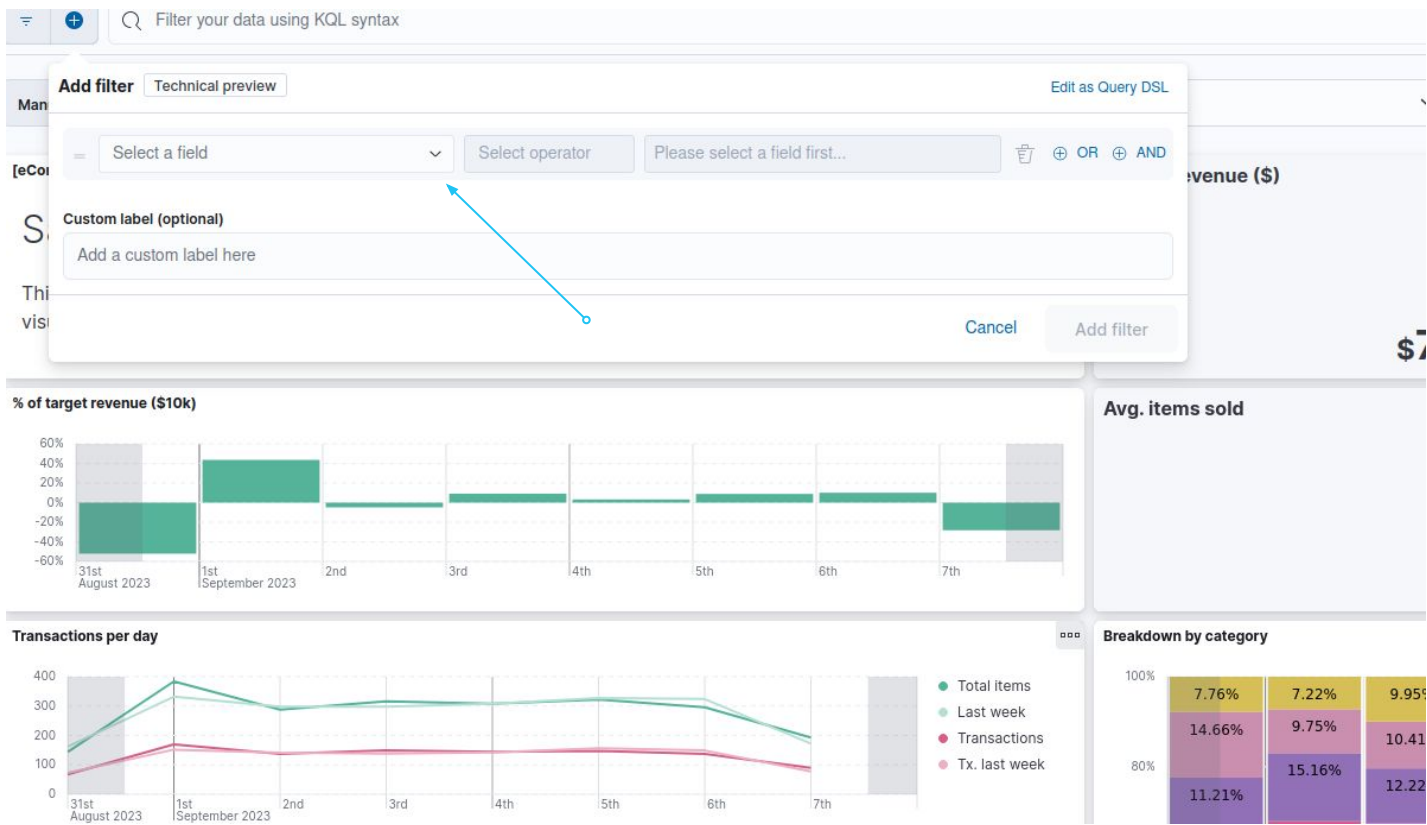
Disk allocation



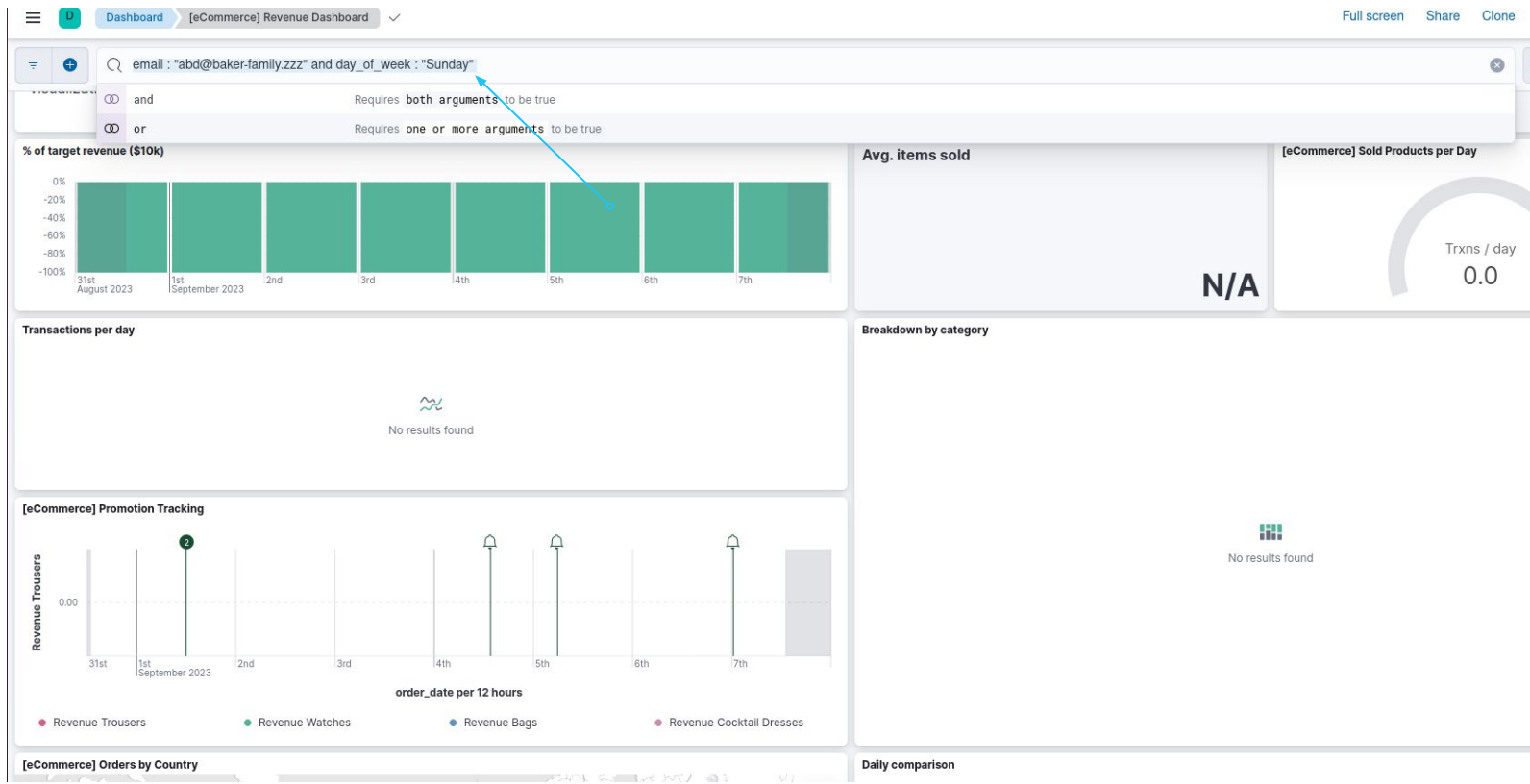
03 Kibana

Accès à Kibana via Elastic Cloud (eCommerce dataset)





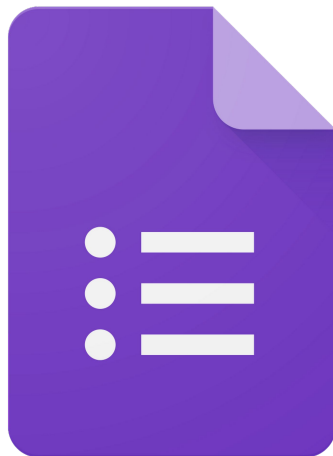
Exemple dataviz kibana cloud





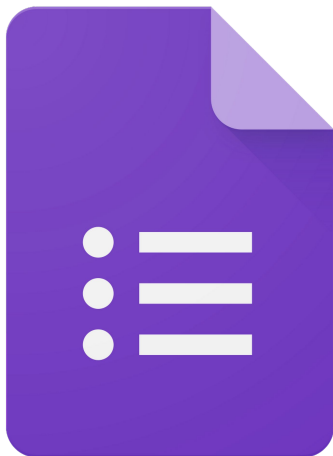
MILESKER
–
MERCİ

QCM Retour Formation



[Lien QCM Retour expérience](#)

QCM Evaluation



“Garapen ekonomikoa xedea baino gehiago, baliabide bat da”

“Le Développement Économique est un Moyen et pas une Finalité”

HUPI S.A.S.

Technopole Izarbel
45 allée Théodore Monod
64210 Bidart

HUPI IBERICA S.L.U.

Gipuzkoako Parke Teknologikoa
Paseo Miramon N°170
20009 Donostia

contact@hupi.fr