Tutoriel Kibana

Ce tutoriel a été conçu pour la version 7.5 d'Elasticsearch et de Kibana

INSTALLATION

https://www.elastic.co/fr/start

Elasticsearch

Lien de téléchargement : https://www.elastic.co/fr/downloads/elasticsearch

- Télécharger la version d'ElasticSearch correspondant à son système d'exploitation
- Dézipper le fichier
- Ouvrir un terminal dans le dossier elasticsearch-[version]¹
- Lancer la commande bin/elasticsearch (bin\elasticsearch.bat sur Windows) : veiller à avoir assez de place sur son ordinateur
- Pour vérifier qu'ElasticSearch s'est bien lancé, ouvrir un second terminal dans le dossier elasticsearch-[version] et exécuter la commande curl http://localhost:9200/



Une réponse similaire devrait apparaître sur le terminal

Kibana

Lien de téléchargement : https://www.elastic.co/fr/downloads/kibana

- Télécharger la version de Kibana correspondant à son système d'exploitation
- Dézipper le fichier
- Exécuter la commande bin/kibana (bin\kibana.bat sur Windows) dans un terminal ouvert dans le dossier kibana-[version]
- Ouvrir son navigateur à l'adresse <u>http://localhost:5601</u>
- Tada !

¹ Remplacer [version] par le numéro de la version effectivement téléchargée

RELANCER ELASTICSEARCH ET KIBANA

En fonction de la méthode d'installation d'Elasticsearch et Kibana, le processus de démarrage varie². Dans le cas d'une installation avec des paquets d'archives (comme expliqué précédemment) :

Elasticsearch

- Ouvrir un terminal dans le dossier elasticsearch-[version]
- Lancer la commande bin/elasticsearch (bin\elasticsearch.bat sur Windows)

Kibana

- Ouvrir un terminal dans le dossier kibana-[version]
- Lancer la commande bin/kibana (bin\kibana.bat sur Windows)

² Elasticsearch : <u>https://www.elastic.co/guide/en/elasticsearch/current/starting-elasticsearch</u> Kibana : <u>https://www.elastic.co/guide/en/kibana/current/start-stop</u>

IMPORTATION DE DONNÉES CSV

	D Ho	ne				0
Ø		Add Data to Kibana	nto pre-built dashboards and monitori	ng systems		
ŝ						
30					<u> </u>	
剑						
0		APM	Logging	Metrics	SIEM	
(;;)		APM automatically collects in- depth performance metrics and	Ingest logs from popular data sources and easily visualize in	Collect metrics from the operating system and services	Centralize security events for interactive investigation in	
â		errors from inside your applications.	preconfigured dashboards.	running on your servers.	ready-to-go visualizations.	
ſ			Add log data	Add metric data	Add security events	
P			Add log data	Add metric data	Add secondy events	
9				¥		
÷		Add sample data	Upload data	a from log file	Use Elasticsearch data	
9			u import a CSV, N	DUSON, or log me CC	Innect to your classicsealCh Index	

- Sur la page d'accueil de Kibana, cliquer sur "Upload data from log file" (ou dans l'onglet _ "Machine learning")
- Importer le fichier .csv choisi : Kibana parse le fichier automatiquement
 - Le chez oim fest,Musique,Annuelle,Juin,"50.3091545259,3.02186108116",Noyelles Sous Bellonne,62,Hauts-de-France,62490,2014 Art contemporain en milieu rural,Arts visuels,Annuelle,Juin,"48.5051745323,6.01397377452",Goviller,54,Grand Est,54330,1993 Les agites du bocal a nivillac,Théâtre,Annuelle,Juin,"47.5405533272,-2.24923467173",Nivillac,56,Bretagne,56130, Musiques metisses a colnar,Musique,Annuelle,Mai,"48.1099405789,7.38468690323",Colmar,68,Grand Est,68000,1997 Tendance clown,Théâtre,Annuelle,Mai,"43.2999009436,5.38227869795",Marseille,13,Provence-Alpes-Côte d'Azur,13001,2006 Festival berry lait,Musique,Annuelle,Mai,"46.8029617828,1.69399812001",Chateauroux,36,Centre-Val de Loire,36000,2014 Dixie folies,Musique,Annuelle,Anai,"46.6043972,-1.74657028357",La Rochelle,17,Nouvelle-Aquitaine,17000, 6

 - 9
 - 10 11
 - ,17000,

12	Dixie folies, Musique, Annu	elle,Mai,"46.162064:	1972,-1.17465702836",La	Rochelle, 17, Not	velle-Aquitaine,
12	Eace Musique Annualle Mai	"AG 9545755693 _A A	70375077786" Processing	70 Nouvollo-Ag	itaino 70300

Number of lines analyzed	1000		
Format	delimited		
Delimiter	1		
Has header row	true		
File stats			
₽No	om	tDomaine	t Périodicité
企] 999 docum	ents (100%)	伦 999 documents (100%)	但 999 documents (100%)
🗞 998 disti	nct values	r distinct values	🗞 3 distinct values
top va	lues	ton values	top values

Pour modifier le titre des colonnes, le caractère délimiteur, etc., cliquer sur "Override _ settings" : cliquer ensuite sur "Import"

 Pour ajuster le type des différentes colonnes (notamment pour permettre des traitements ultérieurs), choisir le mode "Advanced" afin de modifier le mapping du fichier

Simple Advanced	
Index name	
index name	
Create index pattern	
Index pattern name	
Index settings	Mappings
<pre>1* { 2 "number_of_shards": 1 3 }</pre>	<pre>3 "type": "long" 4 }, 5 "Commune": { 6 "type": "keyword" 7 }, 8 "Coordonnees": { 9 "type": "geo_point" 10 }, 11 "Creation": {</pre>
	12 "type": "long" 13 },

Cela est nécessaire notamment pour forcer la reconnaissance de certains types de données (pour la liste de tous les types utilisés dans ElasticSearch : <u>c'est ici</u>). Par exemple :

- Géographiques (format "lat, long") : changer le type pour "geo_point"
- Temporelles (<u>formats</u>) : changer le type pour **"date"** et préciser un format. Par exemple :



- Choisir un nom (sans majuscule ni accent) pour son ensemble de données dans le champ "Index name" puis cliquer sur le bouton "Import"
- Les données sont ensuite converties en NDJSON et chargée dans votre base de données ElasticSearch !³



De plus amples informations à cette adresse.

³ Trois champs ont été créés automatiquement par elasticsearch : "_id", "_index" et "_type". Chaque enregistrement dispose ainsi d'un identifiant, et connaît à la fois l'index auquel il appartient et son type.

ONGLET "DISCOVER"

- Réorganiser les données en sélectionnant les champs à faire apparaître dans la barre latérale



 Ajouter/Modifier des filtres pour dégager des ensembles dans les données présentes : l'autocomplétion (au clic sur "Add filter") permet de formuler des filtres très facilement. Le nombre de "hits" qui apparaît au dessus des résultats correspond au nombre d'enregistrement de l'index correspondant à la recherche.



Tip : Une fois appliqué, en cliquant sur le filtre puis dans "Edit filter", lorsque l'on clique sur "Edit as Query DSL"⁴, le filtre est formulé en tant que requête au format JSON : cela permet d'avoir des requêtes écrites automatiquement.

ලා –	+ Add filter			© –	Commune: Paris × + Add filter	
fest	EDIT FILTER	Edit as Query DSL		fest	EDIT FILTER	Edit filter values
Selec				Selec		
t Co	Field	Operator	ıée ۽	t Co	Elasticsearch Query DSL	née
t Mc	Commune ~	is \checkmark	de l'	t Mc	1 - { 2 - "query": { 3 - "match": {	je
t No	Value			t No	4 - "Commune": {	
t Re	Paris	\sim		t Re	6 "type": "phrase" 7 }	
Avail			livre	Availa	8 } 9 }	_
# Co	○ × Create custom label	?	11016	# Co	10 }	liv
🛛 Co		Cancel Save		♀ Co		
⊘ Cre	aton		fest	O Cre		fe

- La barre de recherche propose également de l'autocomplétion pour formuler des requêtes.
- Si l'on souhaite conserver un état "filtré" d'un index, il suffit de cliquer sur "Save" en haut de l'écran. Cette requête peut être ensuite utilisée pour réaliser des visualisations sur des sous-ensembles d'un index.

⁴ "Query DSL" est le langage de requête utilisé par Elasticsearch (équivalent à SQL pour une base de données relationnelle)

ONGLET "VISUALIZE"

- Cliquer sur "Create new visualization" et sélectionner le type de visualisation à réaliser
- Sélectionner l'index ou le sous-ensemble d'index (requête enregistrée) que l'on souhaite visualiser
- Configurer son graphique puis cliquer sur "Apply changes" pour voir la visualisation se mettre à jour



Tip : il est aussi possible d'avoir une vue d'ensemble sur un index dans l'onglet "Machine learning" avec l'outil "Data visualizer"

Pie chart

- Choisir la mesure ("Metrics") en cliquant dessus
- Configurer les buckets et la manière de les visualiser : "Split slices" répartit les données d'un même graphique dans plusieurs champs tandis que "Split chart" opère la répartition des données dans des graphiques différents. "Split chart" doit être fait avant "Split slices"
- L'agrégation de "Terms" correspond à la création de sous-ensemble de données partageant la même valeur pour un champ

"Order by" spécifie quels buckets doivent ressortir en premier : ceux premiers dans l'ordre alphabétique ? Premier en termes de nombre ? etc.

Ne pas oublier d'augmenter la taille – de base limitée à 5 – pour obtenir des données plus complètes (ce que je n'ai pas fait sur les screenshots)



ta Options	D X	
✓ Split slices	$\odot = \times$	
Sub aggregation	Terms help	
Terms	\sim	
Field		:
Region	\sim	
Order by		
Metric: Count	~	
Order Size		
Descending V 5		

0000

00000

Auvergne-Rhône-Alp..
 Occitanie
 Île-de-France
 Nouvelle-Aquitaine
 Provence-Alpes-Côt...

- Grand Est
- Normandie

Coordinate map

La carte ne peut être réalisée que si l'index à visualiser possède un de type "geo_point".

- Choisir la mesure ("Metrics")
- Définir un bucket à visualiser
- Cliquer sur l'icône "Fit data bounds" (pictogramme de recadrage) pour resserrer le zoom autour des points présents sur la carte. En zoomant, la carte se précise



- Avec l'outil "Draw a polygon" (pictogramme en pentagone) ou "Draw a rectangle" (pictogramme en carré), il est possible de filtrer pour ne garder que les données présentes dans un certain périmètre
- Dans les options, il est possible de changer les paramètres d'affichage et de créer une carte de chaleur



Line chart

- Choisir la mesure ("Metrics") associée à l'axe vertical ("Y-axis")
- Définir le bucket à visualiser sur l'axe horizontal
- Si l'on dispose d'un champ de type date, il est possible de choisir de réaliser un "Date histogram" : on va définir un intervalle de temps pour lequel la mesure sera effectué⁵



- Pour détailler le graphique en fonction d'un autre champ : ajouter un bucket de type "Split series"



- Si l'on souhaite changer le type de graphique : cliquer sur "Metrics & Axes" en haut du panneau de configuration et sélectionner le mode de visualisation

⁵ Par exemple, pour un jeu de données comprenant des dates précises, la fonction histogramme permet de considérer ces dates par cluster d'année plutôt qu'individuellement



- Pour zoomer sur une zone précise du graphique, utiliser la sélection avec la souris



ONGLET "DASHBOARD"

- Créer un dashboard puis cliquer sur le bouton "Add" : sélectionner toutes les visualisations à disposer sur le dashboard
- Disposer les différentes visualisations



 Sélectionner une donnée pour opérer un filtrage sur l'ensemble du dashboard : lorsque la donnée cliquée est ambigüe, une boîte de dialogue s'affiche pour proposer les différents filtres possibles



EXPORTER UNE VISUALISATION

- Pour exporter un dashboard, il est possible de cliquer sur le bouton "Share" en haut de l'écran pour avoir accès à différents modes d'export



 Le mode "Embed code" permet d'obtenir le code d'une iframe HTML pour l'insert du dashboard au sein d'une page HTML. Une iframe est une fenêtre sur l'application Kibana, ce qui signifie que si Elasticsearch et Kibana ne sont pas lancés sur le serveur où le dashboard est créé, le dashboard intégré à la page HTML ne s'affichera pas ; ainsi, un dashboard créé sur un localhost ne sera visible que depuis le même ordinateur

D Dash	hboard / dashboard			Ø 🖂
Full screen	Share Clone Edit			
₿ ∨ S€	< EMBED CODE		KQL $\qquad \boxplus \sim \qquad$ Last 15 minutes	Show dates C Refresh
🗇 - + Adc	Generate the link as			
Camembert	Saved object	● Jan 1, 2015 @ 01:	Carte	BELGIUM GERMANY Dresden
	Copy iFrai You can share this URL to let them load the mo saved version of this da	with people Jan 1, 2011 @ 01:0 st recent Jan 1, 2017 @ 01:0 shboard. Jan 1, 2017 @ 01:0	•	Le Havre LÜXEMBOURG CZECHI
\circ	0000	Jan 1, 2005 @ 01: Jan 1, 2005 @ 01: Jan 1, 2013 @ 01:	•	FRANCE SWITZERLAND AUSTRIA

- Pour un affichage minimal du dashboard, copier le code dans un template de page HTML comme suit :

- Enregistrer ce code dans un fichier au format .html puis l'ouvrir dans un navigateur pour voir le résultat.

L'option "Permalink" permet d'obtenir directement un lien partageable. Les mêmes fonctionnalités existent également pour les visualisations seules.

L'export de visualisation au format .pdf, .svg et .png est possible avec l'extension <u>Reporting</u> contenu dans le X-Pack, c'est-à-dire la version payante de la suite Elastic.

ONGLET "DEV TOOLS"

C'est l'onglet pour écrire des requêtes dans le langage d'elasticsearch. Pour se familiariser avec ces requêtes : <u>quelques exemples simples</u>. Des nombreuses fonctionnalités d'autocomplétion sont proposées ce qui rend la formulation des requêtes particulièrement facile⁶ : attention, le JSON doit être parfaitement valide, c'est-à-dire, interdiction d'utiliser des guillemets simples pour les chaînes de caractères et d'oublier une virgule à la fin d'une liste.

Search

Ø	Console Search Profiler Grok Debugger		
☆	1 GET festival/_search		1- [
	2-{ 3- "query": {		2 "took" : 0, 3 "timed_out" : false,
80	4- "match": {		4 - "_shards" : {
6	6 * }		6 successful": 1,
~	7- }		7 "skipped" : 0,
8	8 * }		8 "failed" : 0
69			10- "hits" : {
			11- "total": {
			12 Value : 1981, 13 "relation" : "ea"
I	;	:	14 * },
_			15 "max_score" : 0.45941275,
6			17- {
া			18 "_index" : "festival",
Ŭ			19
۵			21 "_score" : 0.45941275,
9			22 "
4			24 "Domaine" : "Musique",
ŵ			25 "Périodicité": "Annuelle",

La réponse renvoyée par l'API d'elasticsearch est toujours structurée de la même manière : c'est une longue chaîne de caractères en JSON avec un certain nombre de clefs :

- "took" : temps en milliseconde pris par elasticsearch pour répondre à la requête
- "time_out" : si la requête a expiré (généralement "false")
- "_shards" : informations vis-à-vis des shards utilisés ("éclats" de la base de données)
- "hits" : informations relatives aux réponses de la requête
 - "total" : nombre de résultats obtenus ("value") et si le nombre donné est exact ("eq") ou s'il est en dessous du véritable nombre de réponses ("gte")
 - "max_score" : score maximal récolté parmi les réponses, c'est-à-dire le score de la réponse la plus pertinente par rapport à la requête
 - "hits" : liste (array [...]) des résultats obtenus

Chaque hit est contenu dans un "dictionnaire" (object $\{\ldots\}$) structuré ainsi :

- "_index" : nom de l'index auquel appartient le hit
- "_type" : son type
- "_id" : son identifiant
- "_score" : son score vis-à-vis de la requête
- "_source" : ses champs de métadonnées

⁶ Kibana garde un historique des requêtes

La requête de base pour retirer tous les enregistrements d'un index se formule ainsi :

```
GET festival/_search
{
    "query": {
        "match_all": {}
    }
}
```

Le nombre de résultats renvoyé est de base limité à 10 : pour augmenter cette taille, il suffit de rajouter une clef à la requête comme suit : "size": \${nombre-de-resultats}

Put

Il est aussi possible d'ajouter de nouveaux enregistrements à ses index via la console de l'onglet "Dev tools"



Les visualisations et dashboards créés se mettront à jour en fonction des ajouts.

Delete

De la même manière, il est possible de retirer des données d'un index en donnant son identifiant

1	DELETE festival/_doc/KBKa4W4BsUDiea9PT8_y 🛛 ▶ 🍭		1- {
2			<pre>2 "_index" : "festival",</pre>
3			3 "_type" : "_doc",
4			<pre>4 "_id" : "KBKa4W4BsUDiea9PT8_y",</pre>
5			5 "_version" : 2,
6			6 "result" : "deleted",
7			7 • "_shards" : {
8			8 "total" : 2,
9			9 "successful" : 1,
10			10 "failed" : 0
11			11 - },
12			12 "_seq_no" : 3138,
13			13 "_primary_term" : 1
14		:	14 * }

Communiquer avec l'API hors Kibana

Pour formuler une requête SEARCH dans une URL (dans un navigateur) :

- "http://\${port-elasticsearch}/"
 - + "\${nom-index}/_search?source_content_type=application/"
 - + "json&source=\${requete}"

Par exemple :

```
http://localhost:9200/festival/_search?source_content_type=application/json&so
urce={"query":{"match_all": {}}
```

Pour formuler une requête SEARCH sous forme cURL (dans un terminal)⁷ :

curl -XGET "http://localhost:9200/festival/_search" -H 'Content-Type: application/json'-d'{"query":{"match_all":{}}}'

⁷ En cliquant sur la clef à molette dans la console Kibana, il y a une fonctionnalité pour transposer la requête en cURL

SUPPRIMER UN INDEX

- Se rendre dans l'onglet "Management", tout en bas de la barre latérale
- Dans la partie "Elasticsearch", aller dans l'onglet "Index Management"
- Sélectionner l'index à supprimer et cliquer sur "Manage index" puis "Delete index"

Elasticsearch Index Management Index Lifecycle Policies Rollup Jobs Cross-Cluster Replication	Index Man	Show index settings Show index mapping Show index stats				() Index	Management docs
Remote Clusters Snapshot and Restore License Management	Update your Elasticsea	Edit index settings			X Include rollu	o indices	Include system indices
8.0 Upgrade Assistant	Manage index $ \sim $	Close index					C Reload indices
🟅 Kibana	Name	Force merge index	Status	Primaries	Replicas	Docs count	Storage size
Index Patterns Saved Objects	estival	Clear index cache	open	1	1	3136	569.9kb
Spaces Reporting	bloupi	Flush index	open	1	1	3136	597.3kb
Advanced Settings	Rows per page: 10 $ \smallsetminus $	Freeze index					
		Delete index					

- Dans la partie "Kibana", aller dans l'onglet "Index Patterns"
- Cliquer sur l'index à supprimer

= 1	lasticsearch		
1	ndex Management ndex Lifecycle Policies	Index patterns ③	① Create index pattern
(Rollup Jobs Cross-Cluster Replication Remote Clusters Snapshot and Restore	Q Search	
5		Pattern 🔨	
8	8.0 Upgrade Assistant	bloupi Default	
Κ Ι	(ibana	festival	
1	ndex Patterns Saved Objects	Rows per page: 10 🗸	
F	Reporting		
,	dvanced Settings		

- Cliquer sur l'icône de suppression

