



Groupe Emetteur : Service informatique	
Objet : Utilisation dejavu	
Application :	Rédacteur : MÉNARD Lucas
Date : Responsables : Romain BERTIN	
Ordre de classement de la procédure :	
Destinataires	

Indice	Date	Libellé de la procédure	Pages Modifiées
V1.0		Utilisation de dejavu	

Nature de la dernière modification : Veillez détruire l'exemplaire à l'indice précédent	
VERIFICATEUR : Date :	APPROBATEUR : Date :





Zolux.com

ZOLUX SAINTES (F)

141 cours Paul Doumer - 17100 Saintes - France

contact@zolux.com – Tel : +33 (0)5 46 74 17 98



Table des matières

Comment utilisé Dejavu ?	3
Utilité ? :	3
Interface WEB	3
Voir les logs :	4
Pré-visualiser et modifier les logs	5
Voir tout index :	7





Comment utilisé Dejavu ?

Utilité ? :

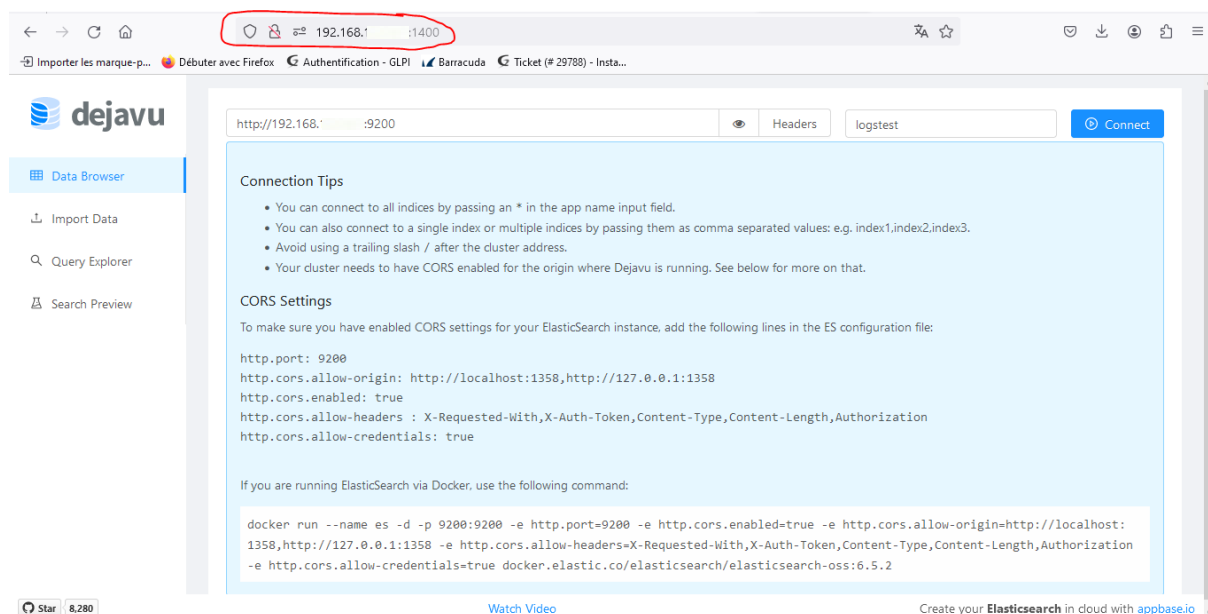
Dejavu facilite l'exploration et la visualisation des données stockées dans Elasticsearch. C'est un outil pratique pour interagir avec les index Elasticsearch, offrant une expérience simplifiée pour comprendre et analyser les données de manière efficace.

Interface WEB

Pour avoir accès à l'interface web de DEJAVU il faut entrer l'adresse @ip:port configuré lors de l'installations des services.

En aillant suivi les documents vous avez normalement : <http://192.168.xxx.xxx:1400/>

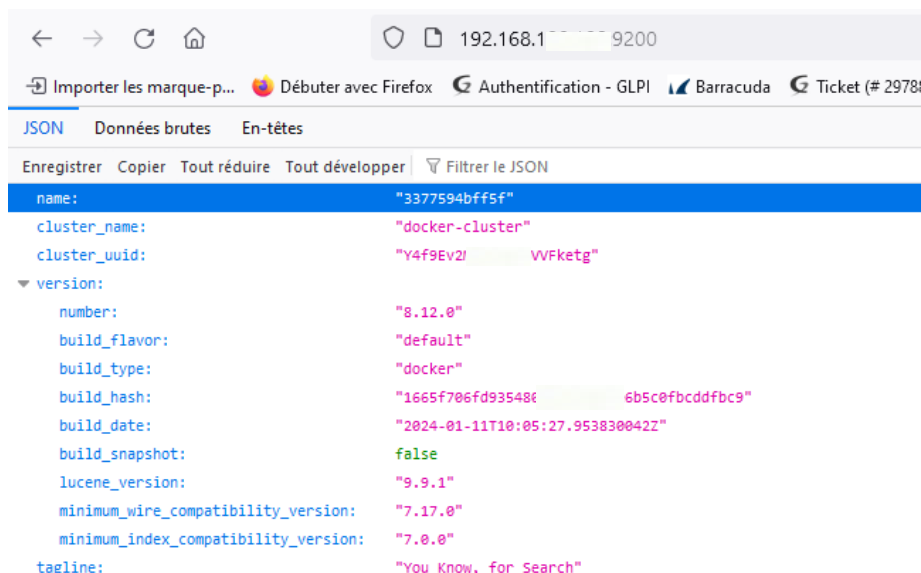
En entrant cela vous serez sur l'interface web de DEJAVU qui ressembleras à cela.



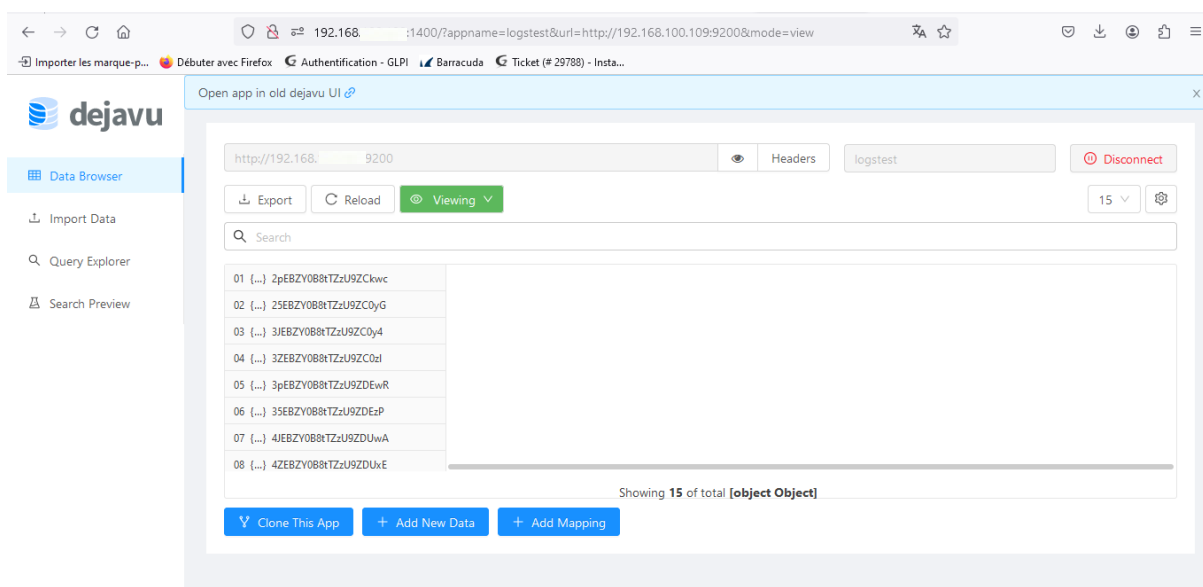


Voir les logs :

Pour voir des logs indexés de Elasticsearch il suffit d'entrer l'URL avec lequel on as accès à cette page :



Une fois l'URL entré à droite ont rempli la case avec le nom de l'index qu'on a créé et sur laquelle on a indexé le fichier logs.

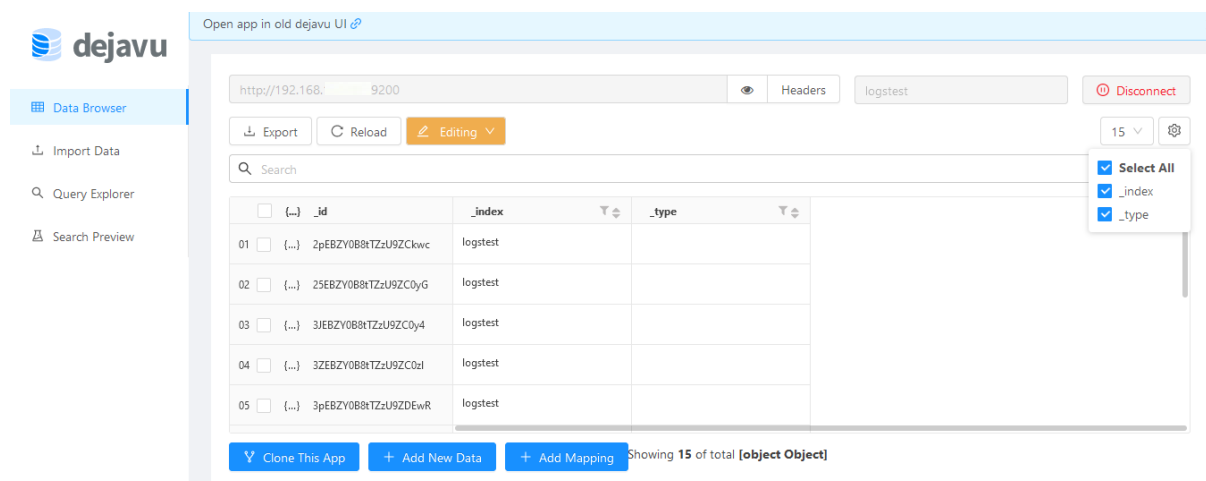




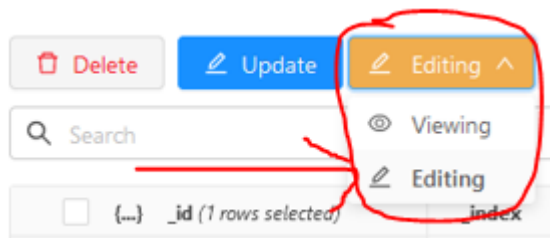
Pré-visualiser et modifier les logs

Comme on l'a vu 'DEJAVU' permet d'avoir une interface web pour Elasticsearch.

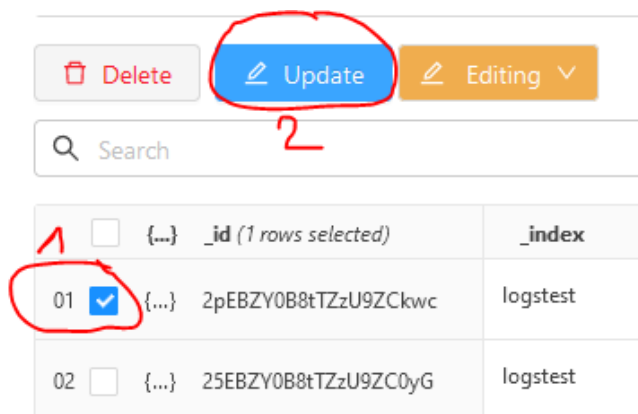
On peut donc pré-visualiser et modifier les logs de la façon suivante et on peut aussi voir sur quelle index les fichiers se trouvent :



Ensuite il faut se mettre en mode « editing » de la façon suivante :



Dès lors on peut cocher un fichier puis faire update :





Maintenant on peut à la fois visualiser les logs au format brut (.jsonl) et on peut modifier les données dans le fichier.

Index:

Type:

logstest

Document Id:

2pEBZY0B8tTZzU9ZCkwc

JSON document:

```
1 {
2   "@timestamp": "2015-05-18T09:03:25.877Z",
3   "ip": "185.1. 2.126",
4   "extension": "gif",
5   "response": "404",
6   "geo": {
7     "coordinates": {
8       "lat": 36.518375,
9       "lon": -86.05828083
10    },
11   "src": "PH",
12   "dest": "MM",
13   "srcdest": "PH:MM"
14 }
```

Cancel

OK

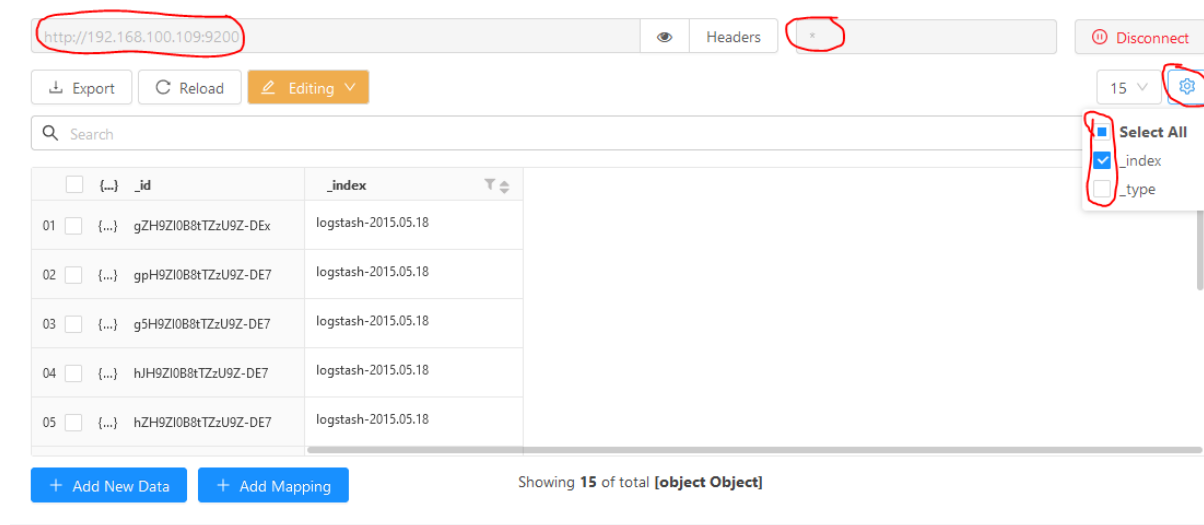




Voir tout index :

Quand on est connecté à Elasticsearch et quand index on entre le symbole « * » alors ensuite on peut trier les index est c'est ici qu'on les voit tous avec le nombres de fichier indexé a l'intérieur.

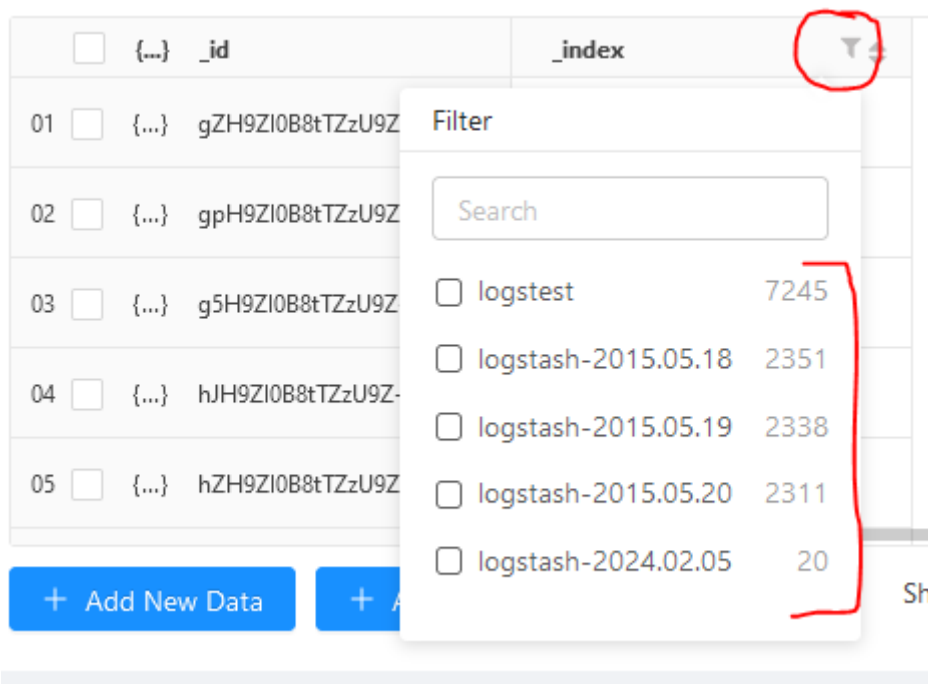
Pour ce faire on fait comme les screens ci-dessous :



The screenshot shows the Elasticsearch Kibana interface. The address bar contains 'http://192.168.100.109:9200'. The 'Headers' tab is selected. The 'Index' dropdown menu is open, showing the selected index pattern '*'. The 'Select All' checkbox is checked. The table below shows the list of indices and their document counts.

	_id	_index
01	{...}	gZH9ZI0B8tTZzU9Z-DEx
02	{...}	gpH9ZI0B8tTZzU9Z-DE7
03	{...}	g5H9ZI0B8tTZzU9Z-DE7
04	{...}	hJH9ZI0B8tTZzU9Z-DE7
05	{...}	hZH9ZI0B8tTZzU9Z-DE7

Showing 15 of total [object Object]



The screenshot shows the Elasticsearch Kibana interface. The 'Filter' dropdown menu is open, showing the list of indices and their document counts. The 'logstash-2024.02.05' index is highlighted.

	_id	_index
01	{...}	gZH9ZI0B8tTZzU9Z
02	{...}	gpH9ZI0B8tTZzU9Z
03	{...}	g5H9ZI0B8tTZzU9Z
04	{...}	hJH9ZI0B8tTZzU9Z
05	{...}	hZH9ZI0B8tTZzU9Z

Filter

	_id	_index
01	{...}	gZH9ZI0B8tTZzU9Z
02	{...}	gpH9ZI0B8tTZzU9Z
03	{...}	g5H9ZI0B8tTZzU9Z
04	{...}	hJH9ZI0B8tTZzU9Z
05	{...}	hZH9ZI0B8tTZzU9Z

logtest 7245

logstash-2015.05.18 2351

logstash-2015.05.19 2338

logstash-2015.05.20 2311

logstash-2024.02.05 20

