Installation stack ELK (Elasticsearch, Logstash, Kibana)

Introduction

La stack ELK, composée d'Elasticsearch, Logstash et Kibana, est une puissante suite d'outils utilisée pour gérer les journaux (logs) et analyser les données en temps réel. Chaque composant de cette suite joue un rôle spécifique dans ce processus :

1. **Elasticsearch** : Il s'agit du moteur de recherche et de stockage distribué qui permet de stocker, indexer et rechercher efficacement les données, y compris les logs.
2. **Logstash** : Logstash est l'outil de collecte et de transformation des logs. Il prend en charge la collecte de données à partir de diverses sources, les transforme en un format cohérent et les envoie à Elasticsearch pour le stockage.
3. **Kibana** : Kibana est l'interface utilisateur qui permet de visualiser et d'analyser les données stockées dans Elasticsearch. C'est un outil essentiel pour créer des tableaux de bord, des graphiques et des visualisations pour comprendre et surveiller les données en temps réel.

En combinant ces trois composants, la stack ELK offre une solution complète pour gérer les logs et obtenir des informations précieuses à partir de ces données, facilitant ainsi la résolution de problèmes, la surveillance en temps réel et l'analyse des tendances.

Installation

Elasticksearch

Étape 1 : Ajoutez la clé GPG pour télécharger le package Elasticsearch.

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add –

Étape 2 : Installez le support de transport HTTPS pour APT.

sudo apt install apt-transport-https

Étape 3 : Ajoutez le dépôt Elasticsearch à votre liste de sources.

echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

Étape 4 : Mettez à jour les dépôts et installez Elasticsearch.

sudo apt-get update -y && sudo apt-get install elasticsearch

Étape 5 : Configurez Elasticsearch (le fichier de configuration est /etc/elasticsearch/elasticsearch.yml). Pour le moment, laissez-le tel quel.

Étape 6 : Démarrez le service Elasticsearch.

sudo service elasticsearch start

Étape 7 : Pour que le service se lance automatiquement au démarrage, utilisez la commande suivante :

sudo systemctl enable elasticsearch

Cela simplifie la documentation tout en maintenant les étapes essentielles pour l'installation et la configuration d'Elasticsearch. Assurez-vous de fournir des explications plus détaillées si nécessaire dans votre documentation complète.

1. Pour que elasctícksearch sois accessible depuis le réseau lorsque nous sommes en lab pour vérifier que tout fonctionne il faut rajouter ces lignes dans le fichier de conf

```
#
http.port: 9200
cluster.name: my-cluster
node.name: SRVSISLOGPRD
network.host: 0.0.0.0
discovery.seed_hosts: ["172.16.5.37"]
```

network.host: 0.0.0.0 :

- Cette ligne indique à Elasticsearch d'écouter sur toutes les interfaces réseau disponibles sur la machine. L'adresse IP "0.0.0.0" signifie qu'Elasticsearch sera accessible via toutes les interfaces, y compris IPv4 et IPv6 si elles sont activées.

discovery.seed_hosts: ["172.16.5.37"] :

- Cela configure les nœuds que ce nœud Elasticsearch utilisera comme points d'initialisation pour la découverte du cluster. Dans cet exemple, il spécifie que le nœud Elasticsearch doit essayer de se connecter à un nœud ayant l'adresse IP "172.16.5.37" pour découvrir d'autres nœuds dans le cluster. Les nœuds de découverte sont essentiels pour former un cluster Elasticsearch.

Lorsque via un navigateur j'accede à IP :9200 je vois que elasticksearch fonctionne correctement


```
{
    "name": "SRVSISLOGPRD",
    "cluster_name": "my-cluster",
    "cluster_uuid": "a4P4RGCpSvu-uxO6nW6teQ",
    "version": {
        "number": "7.17.13",
        "build_flavor": "default",
        "build_type": "deb",
        "build_hash": "2b211dbb8bfdecaf7f5b44d356bdfe54b1050c13",
        "build_date": "2023-08-31T17:33:19.958690787Z",
        "build_snapshot": false,
        "lucene_version": "8.11.1",
        "minimum_wire_compatibility_version": "6.8.0",
        "minimum_index_compatibility_version": "6.0.0-beta1"
    },
    "tagline": "You Know, for Search"
}
```

Installation de kibana

sudo apt install kibana

Fichier de conf : /etc/kibana/kibana.yml

Dans le fichier de conf on veut vérifier que l'url d'elasticksearch est correct

```
# The URLs of the Elasticsearch instances to use for all your queries.
#elasticsearch.hosts: ["http://localhost:9200"]
```

Elasticksearch est bien sur ma machine locale et il écoute sur le port 9200 en TCP

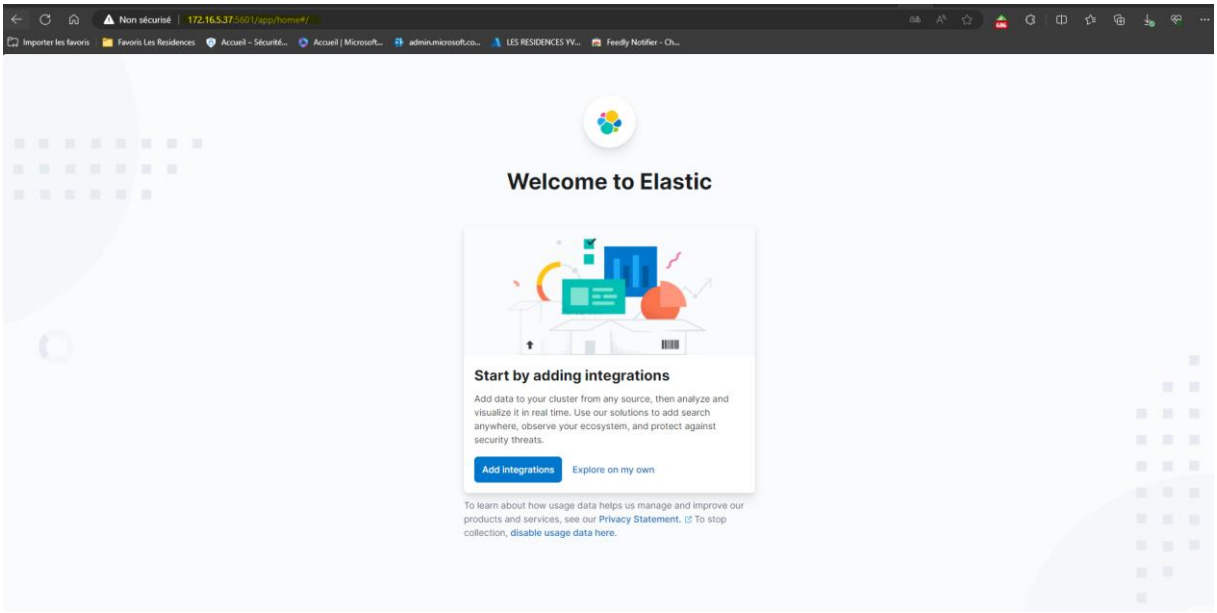
Par défaut il n'est accessible qu'en local je modifie cette directive pourqu'il écoute sur toute les interfaces

```
# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: 0.0.0.0
```

Pour que kibana se lance au démarrage du serveur tapez la commande :

sudo systemctl enable kibana

Page web kibana



Installation logstash

Étape 1 : Installez Java.

sudo apt install default-jre

Étape 2 : Installez Logstash.

sudo apt install logstash

Étape 3 : Configurez Logstash (le fichier de configuration se trouve à /etc/logstash/logstash.yml).

Étape 4 : Démarrez Logstash.

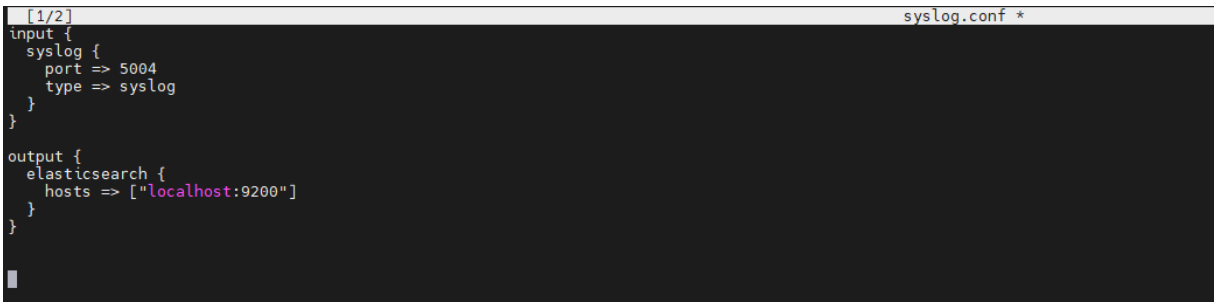
sudo systemctl start logstash

Étape 5 : Pour que Logstash démarre automatiquement avec le système, utilisez la commande suivante :

sudo systemctl enable logstash

Étape 6 : Dans le répertoire /etc/logstash/conf.d/, créez un fichier nommé syslog.conf pour configurer Logstash en fonction de vos besoins.

Cette version simplifiée résume les étapes essentielles pour l'installation et la configuration de Logstash. Vous pouvez fournir des détails plus spécifiques dans votre documentation complète si nécessaire.



Étape 1 : Modifiez la configuration de rsyslog.

Ouvrez le fichier de configuration de rsyslog en éditant le fichier **/etc/rsyslog.conf** :

sudo nano /etc/rsyslog.conf

Ajoutez la ligne suivante pour rediriger les logs vers Logstash sur le port 5004 en localhost :

. @@localhost:5004

Sauvegardez et fermez le fichier.

Étape 2 : Redémarrez le service rsyslog.

Après avoir modifié la configuration, redémarrez le service rsyslog pour appliquer les modifications :

sudo systemctl restart rsyslog

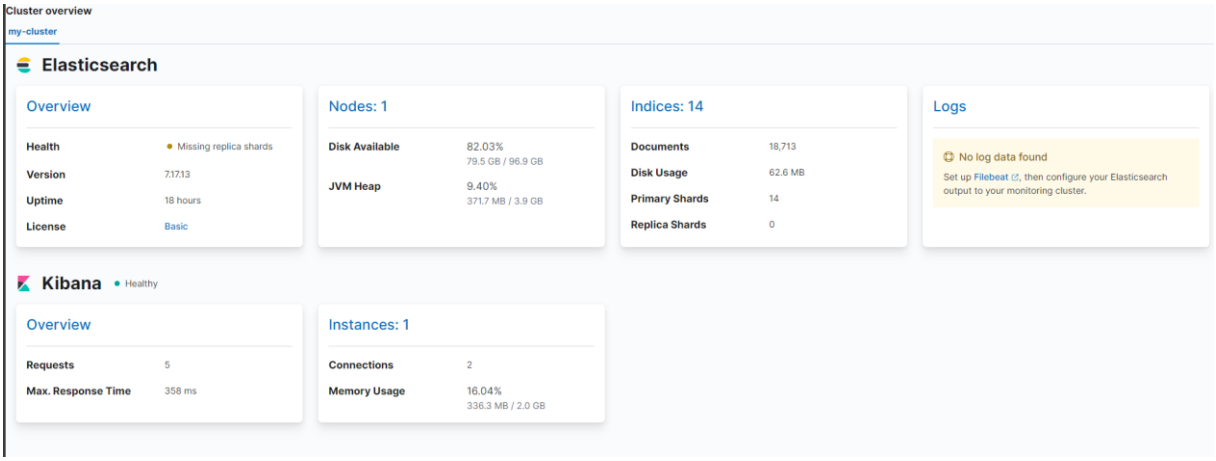
Cela redirigera tous les logs vers Logstash sur le port 5004 en localhost.

N'oubliez pas de configurer également Logstash pour écouter sur le port 5004 et traiter les logs entrants correctement. Assurez-vous que la configuration Logstash dans le fichier **/etc/logstash/conf.d/syslog.conf** (comme mentionné précédemment) correspond à ce que vous attendez en termes de traitement des logs reçus.

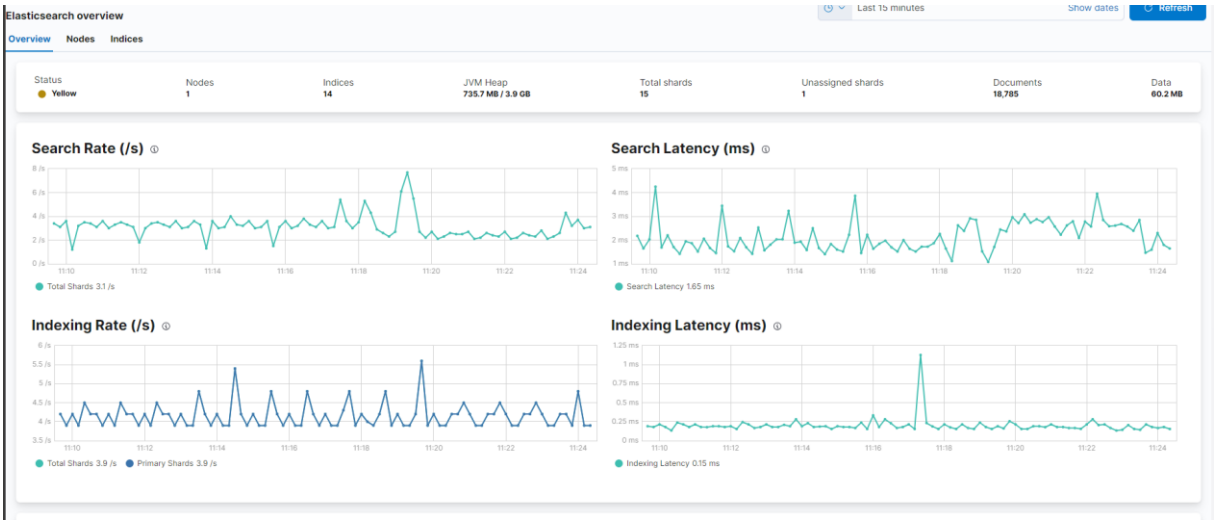
Configuration Kibana

Repartir sur l'ip du serveur web port 5601

Je fais défiler le menu à gauche et je vais dans Managment > stackmonitoring



Si j'appuie sur overview en dessous Elasticsearch cela me montre cela



Le nombre de log que je reçois si il y’a un pic d’activités ou non

J’ai fait un script qui redémarre le serveur 500 fois et je vais regarder si il y’a un pic à un moment

D’abord on peut dire à logstash de chercher les logs directement dans syslog comme ceci

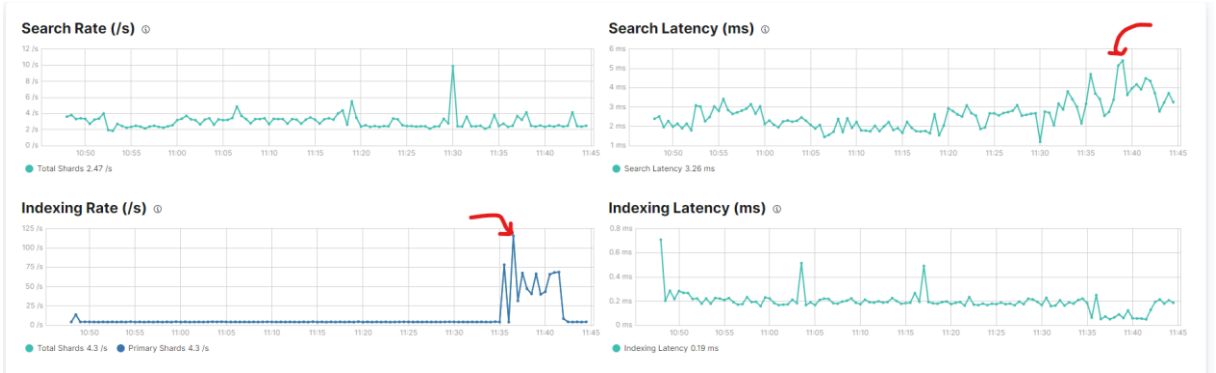
```
input {

file {
    path => "/var/log/syslog"
    start_position => "beginning" # Vous pouvez également utiliser "end" pour lire le fichier à partir de la fin.
  }

}

output {
  elasticsearch {
    hosts => ["localhost:9200"]
  }
}
```

Le moment ou j’ai lancé le script vers 11h38



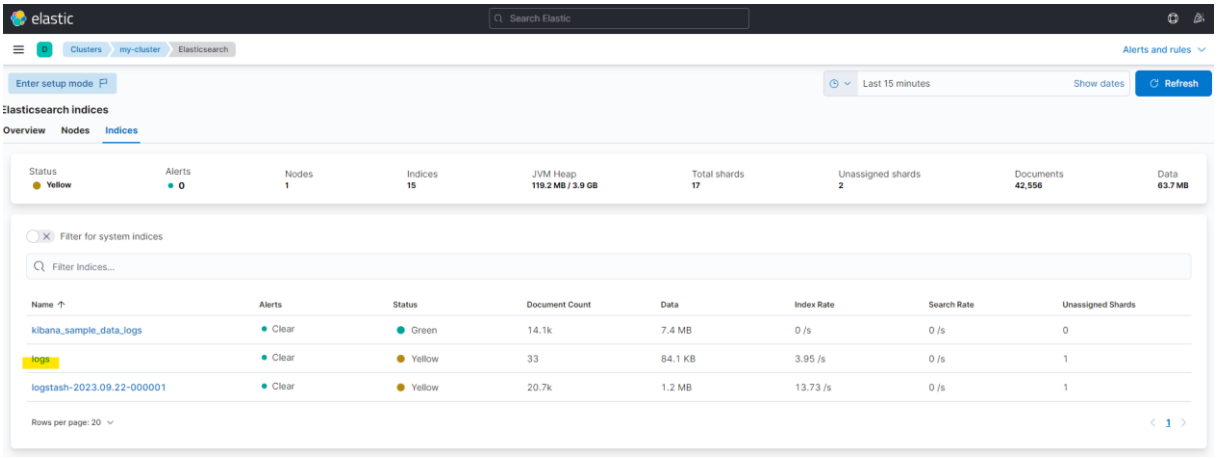
Je peux aussi séparer les logs dans logstash pour que ça soit beaucoup plus clair

```
input {

file {
    path => "/var/log/syslog"
    start_position => "beginning" # Vous pouvez également utiliser "end" pour lire le fichier à partir de la fin.
  }

}

output {
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "logs"
  }
}
```

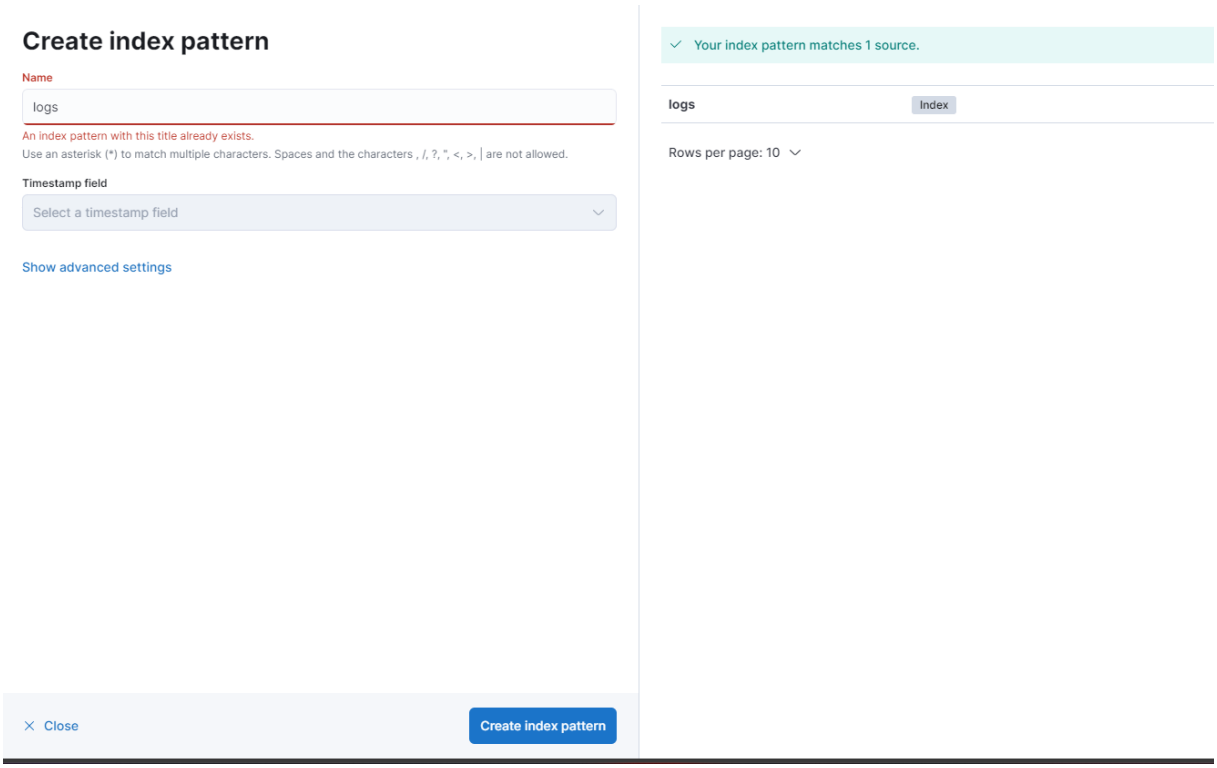


Maintenant pour visualiser ces logs dans kibana

Il faut aller dans stack management comme on a dit et aller dans Index Pattern

Ensuite sélectionner « Create Index Pattern »

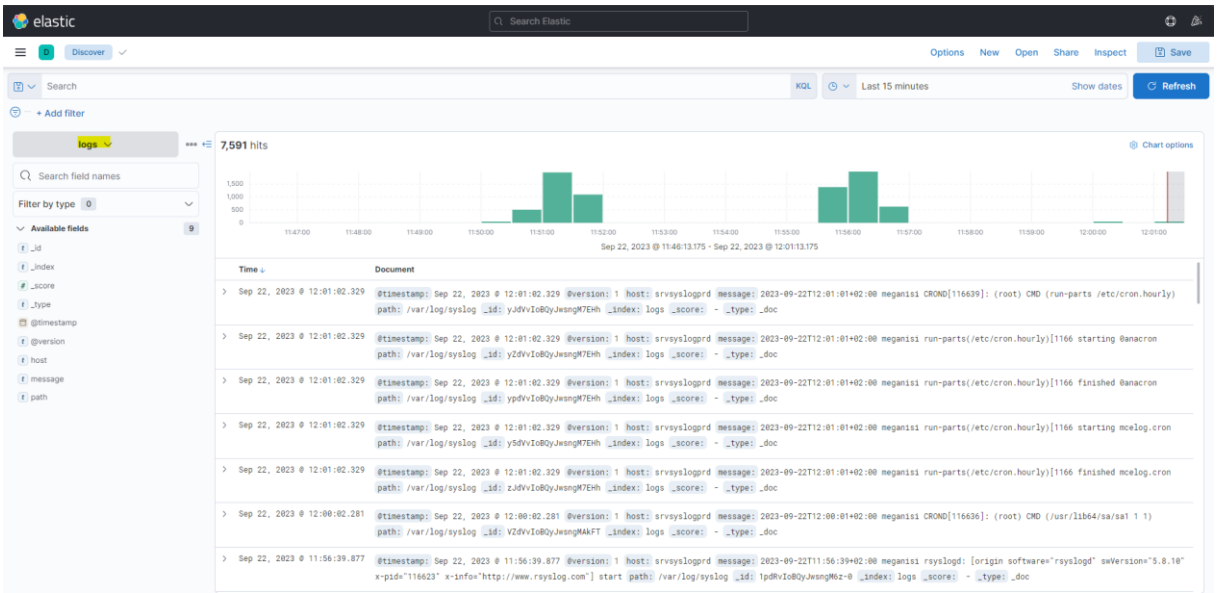
Ensuite il faut taper le nom de l'index qu'on a définis dans logstash



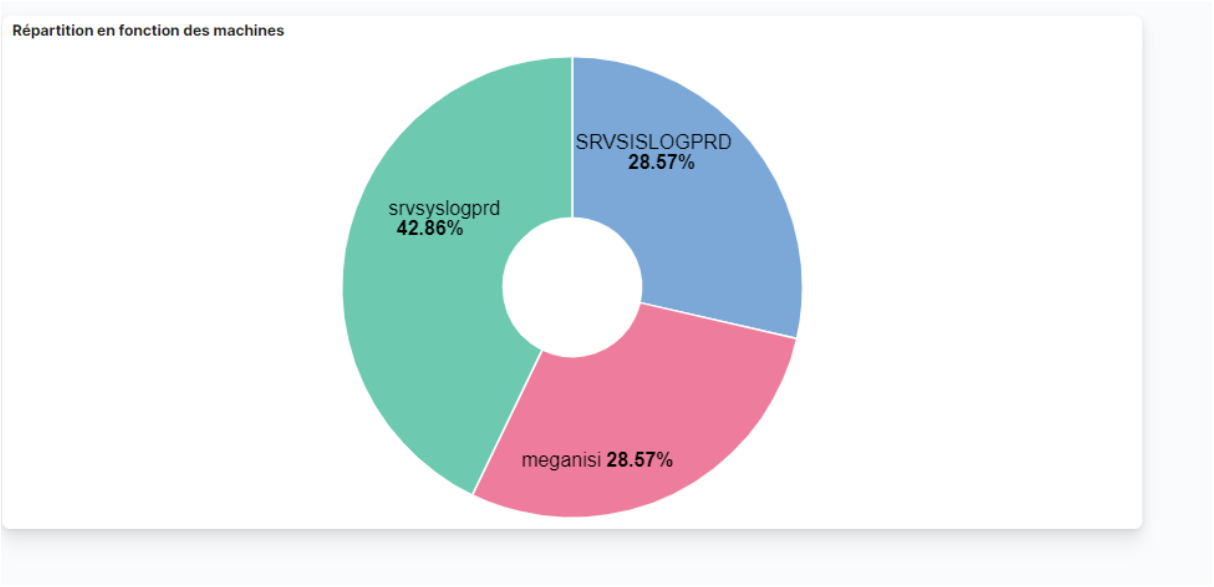
Ensuite appuyer sur Create Index Pattern

Je me rends ensuite dans discover

En haut a gauche je selectionne la source dans notre cas « logs »



Résultat


Répartition en fonction des machines
SRVSISLOGPRD
28.57%
srvsyslogprd
42.86%
meganisi 28.57%