**ELATIC SEARCH**

Table des matières

[Chapitre 1 Introduction 2](#_Toc105526640)

[Chapitre 2 Ecosystème ELK (Es Logstash Kibana) 2](#_Toc105526641)

[1-Avant : 2](#_Toc105526642)

[2-Après : 3](#_Toc105526643)

[Chapitre 3 3](#_Toc105526644)

[Titre 1 3](#_Toc105526645)

[Chapitre 4 3](#_Toc105526646)

[Titre 1 3](#_Toc105526647)

[Chapitre 5 3](#_Toc105526648)

[Titre 1 3](#_Toc105526649)

[Chapitre 6 3](#_Toc105526650)

[Titre 1 3](#_Toc105526651)

# 

# Introduction

Elasticsearch = ES

ES est une base de données noSql orientée documents distribuée, moteur d’indexation de recherche.

ES n’est pas sur HDFS ( a son propre cluster), peut être déployé sur windows

Indexe = base de données.

Apache Lucene : moteur d’indexation non distribué (un seul nœud.

Es basé sur Appache Lucene (chaque nœud) : intéressant mais compliqué à gérer (code)

Google à chaque nouveau site, il le détecte, il indexe les éléments importants du site, par des requêtes https puis l’algorithme

Recherche multi critères très compliquée sur une page (Lucene) (il se passe beaucoup de traitements derrière code java) et ES masque la complexité qui existe derrière.

ES stock les données en Json.

API Rest est supportée par tous les langages d’api Rest ( postman, SOPWI)

Pugin pour tout

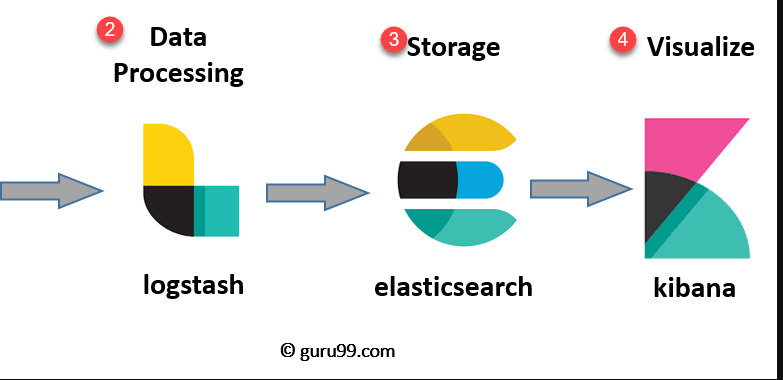
CMS (Content management system) : framework qui permet de créer des pages web facilement

# Ecosystème ELK (Es Logstash Kibana)

## 1-Avant :

Au début ES est dédié à Logstash des logs

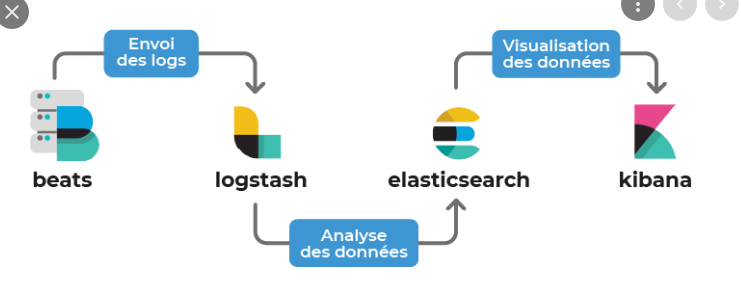
Logstash = ETL : récupère les logs les transformes et les charger dans ES.



## 2-Après :

Agent logstash ES consomme de la mémoire donc remplacé par beats (agent light)

Beats : log shipping (sans transformation)



**Application**

Serveur d’application

Serveur

Cluster ES

Agent BEATS

KIBANA

Logstash

Agent BEATS

Agent BEATS

Autres serveurs

Serveur web clients externe

# 

## Titre 1

# 

## Titre 1

# 

## Titre 1

# 

## Titre 1