Capitoul

Supervision des logs

avec

la pile

ELK

Qu'est ce qu'ELK ?

- ElasticSearch
  - Moteur de recherche et d'indexation
  - Flux de donnée Json
  - NoSQL
  - Mode Cluster
  - Lucene
  -
-

Qu'est ce qu'ELK ?

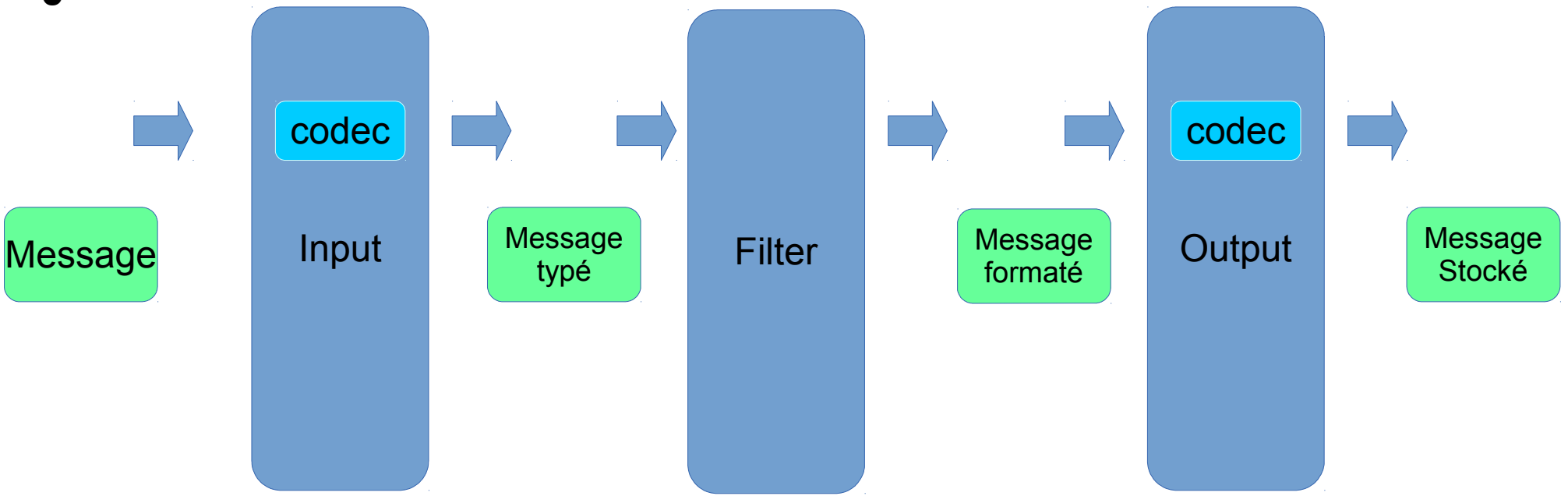
- Logstash
  - Administration des logs
  - Collecte
  - Analyse
  - Traitement
  - Stockage
-

Qu'est ce qu'ELK ?

- Kibana
  - Exploration
  - Visualisation

Qu'est ce qu'ELK ?

- Fonctionnement de logstash
-



Qu'est ce qu'ELK ?

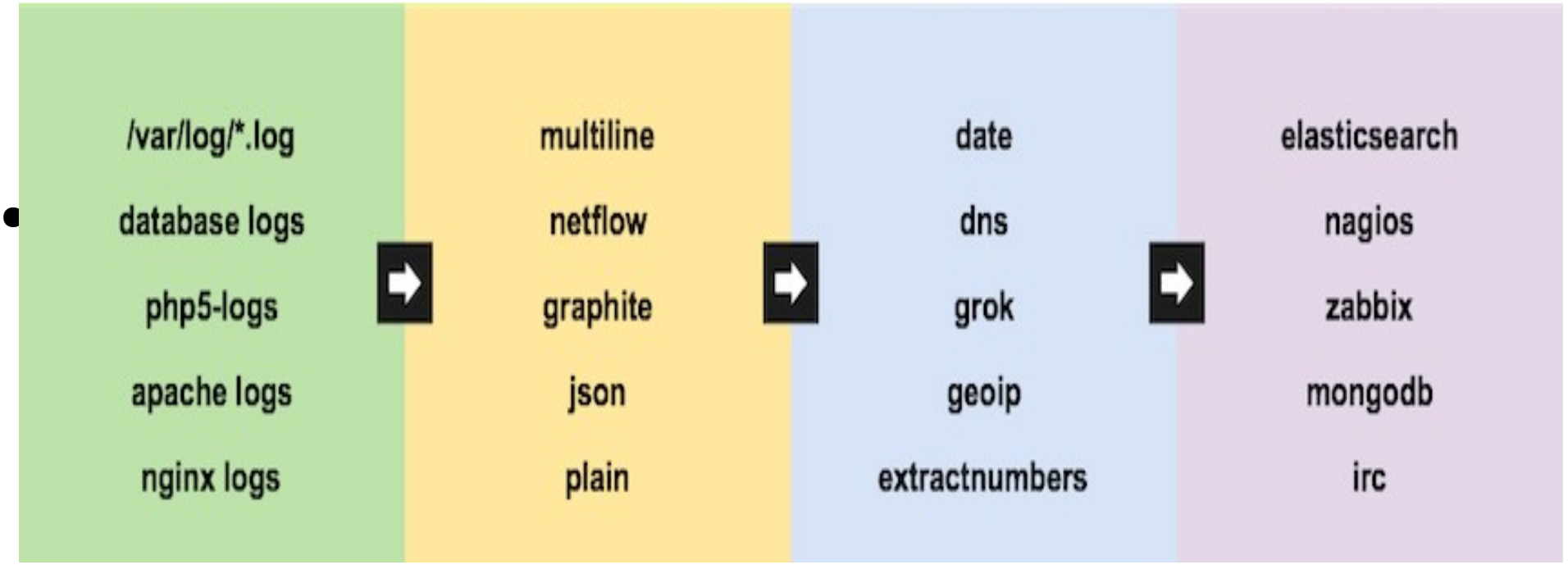
- Input : type d’entrée
- Codec : format du flux
- Filter : remaniement du message
- Output : résultat

–

•

Qu'est ce qu'ELK ?

- Entrées
- Encodeurs/Décodeurs
- Filtres
- Sorties



Qu'est ce qu'ELK ?

Sur : http://logstash.net/docs/1.4.2/

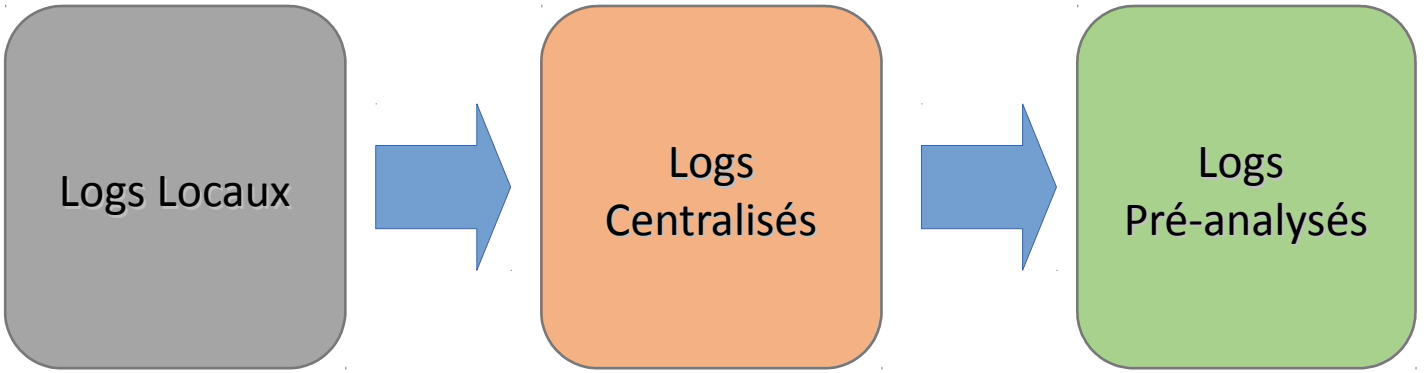
41 inputs

20 codecs

50 filtres

54 outputs

Evolution des logs

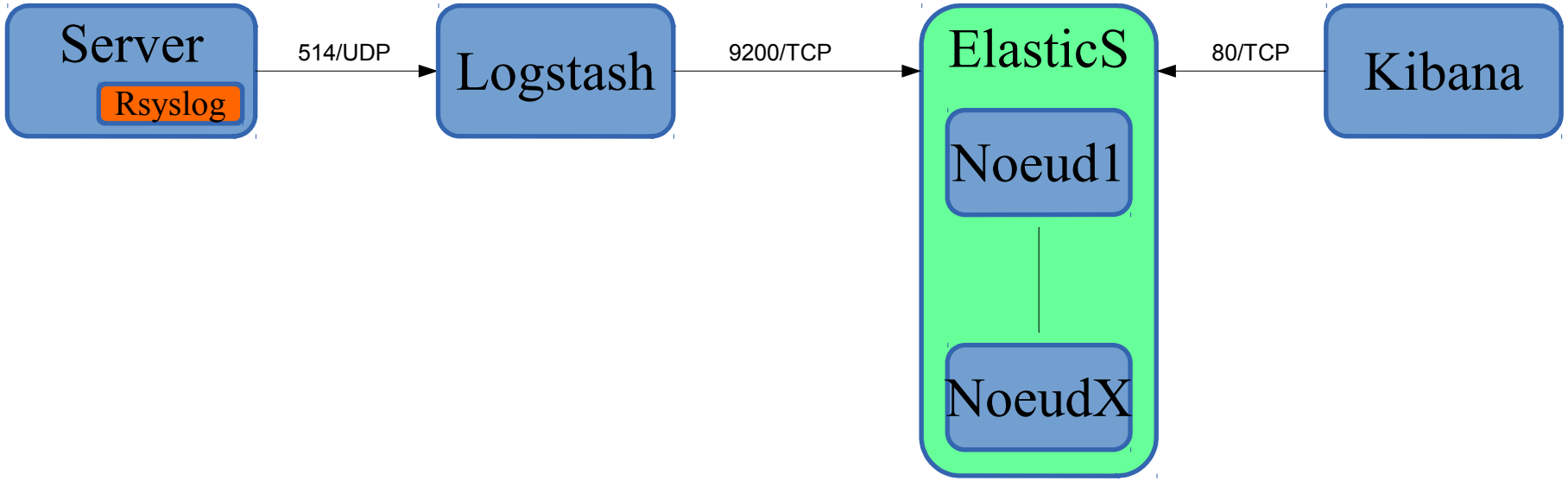


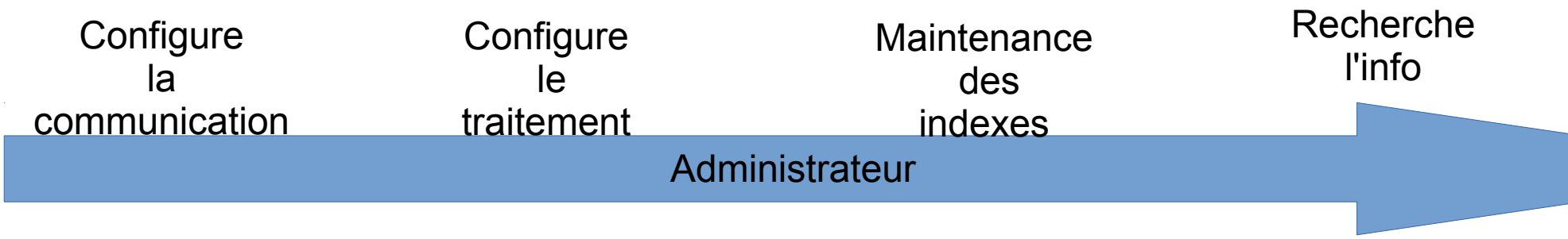
Installation

- Très Simple
- .deb, .rpm ou tar.gz disponibles sur le site
- Configuration de base à adapter légèrement
- Complexité = choix d’architecture
  -
  -
  -

Architecture Simple

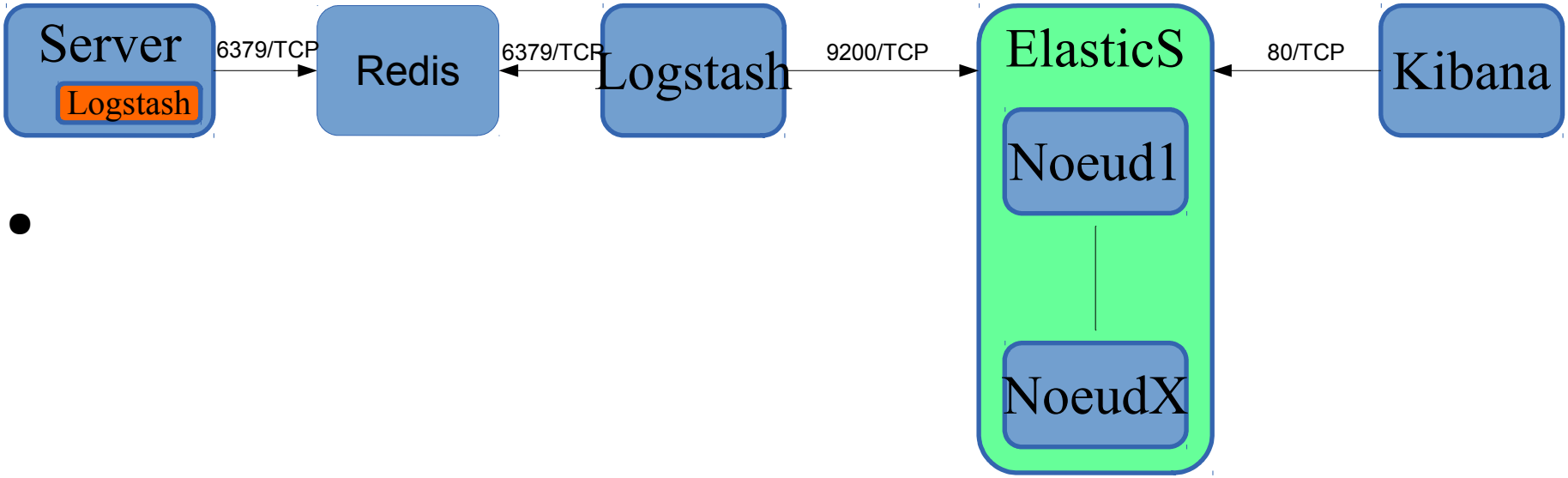
- ELK et rsyslog

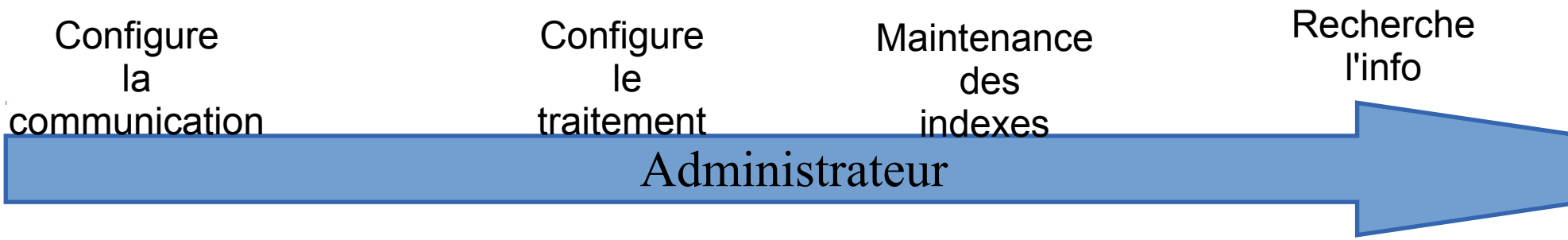




Architecture Fiable

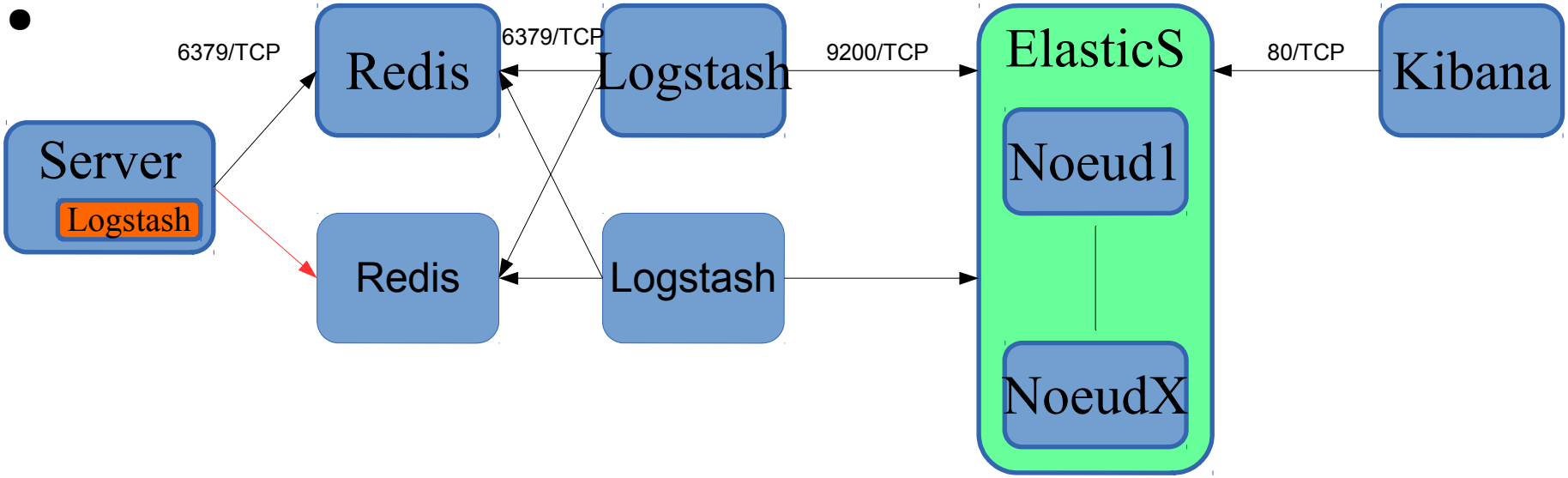
- ELK et Redis

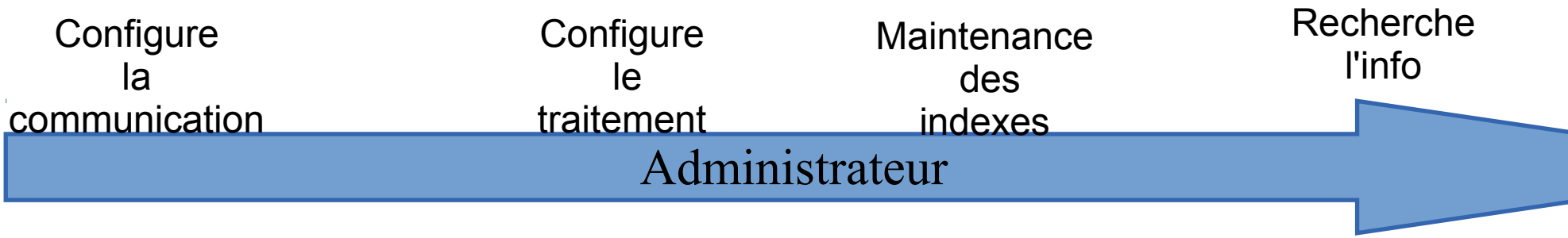




Architecture solide

- ELK, Redis et redondance
-





Nos tests

- Dhcp, radius, Active Directory, Apache, Syslog
-
- Grok
-
- Récupération de Métriques
-
- La sécurité est ailleurs

Difficultés rencontrées

- Mémoire pour ES (8GB)
-
- CPU (4CPU Bi-Core, VM WMware)
-
- La remontée d’alerte avec Nagios
-
- File d’attente sur syslog
-
- L’espace disque (61 GB de données au 27/04, ~6 serveurs sources, <59M d'évènements en < 2 mois)
-

Conclusion

- Très bon outil
- Un peu gourmand
- Très pratique
- Facile à configurer pour une utilisation simple
- Mais utilisable aussi pour des requêtes complexes
-
- Va être mis en place à l'INSA et à l'ISAE
-