# Gérer efficacement ses logs avec la stack ELK

## *ElasticSearch – Logstash – Kibana*

### DESCRIPTION

La stack ELK est très communément utilisée pour gérer facilement et efficacement ses logs applicatifs. Issue de l'open source, simple à installer et permettant de gérer toute sorte de documents (logs, messages divers, documents évènementiels, etc.), cette stack est un outil puissant qui peut cependant vite devenir incontrôlable. Cette formation vous donne des outils simples et pratiques pour dimensionner, configurer et gérer simplement votre cluster ELK.

### OBJECTIFS PÉDAGOGIQUES

Identifier les bonnes pratiques à mettre en place pour développer une application basée sur la stack ELK
Découvrir les bases de la gestion de messages avec Logstash
Appréhender les concepts de recherche full-text et de stockage de données massif avec ElasticSearch
Créer des visualisations représentatives et efficaces avec le dashboard Kibana
Configurer ces trois outils pour une application robuste et fiable

### PUBLIC CIBLE

Développeur
Architecte
Ops

### PRÉ-REQUIS

- Disposer de notions sur http.
- Connaissance de l'environnement sous Linux.

### MÉTHODE PÉDAGOGIQUE

Formation rythmée par des apports théoriques, des mises en pratique et des bonnes pratiques qui s'appuient sur les retours d'expérience de nos consultants-formateurs.

### PROFILS DES INTERVENANTS

Toutes nos formations sont animées par des consultants-formateurs expérimentés et reconnus par leurs pairs.

### MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION

L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique. Une évaluation à chaud sur la satisfaction des stagiaires est réalisée systématiquement en fin de session et une attestation de formation est délivrée aux participants mentionnant les objectifs de la formation, la nature, le programme et la durée de l'action de formation ainsi que la formalisation des acquis.

### POUR ALLER PLUS LOIN :

**Stage pratique en présentiel**
NOSQL

Code :
**ELK01**

Durée :
**2 jours (14 heures)**

Exposés :
**50%**

Cas pratiques :
**50%**

**Sessions à venir :**

27 - 28 mai 2019
Paris / 1 630 eur

21 - 22 nov. 2019
Paris / 1 630 eur

Tarif & dates intra :
**Sur demande**

- Toutes nos formations NoSQL
- Formation officielle "Déployer et gérer un cluster Couchbase" (Couchbase NoSQL Server Administration) (CS300)
- Formation officielle Couchbase "Requêtes, modélisation de données, optimisation et migration via N1QL" (Querying, Modeling, Tuning, and Migrating Data using N1QL) (CD210)
- Formation "Concevoir un moteur de recherche avec Elasticsearch : Dimensionnement - Administration - Recherche" (ELAS2)

# Programme pédagogique détaillé par journée

## Jour 1

### DÉCOUVRIR LA STACK ELK

- Qu'est-ce que Elasticsearch, Logstash et Kibana ?
- Cas d'utilisation
- Représentation des données dans Elasticsearch
- Présentation écosystème Elastic
- Modèle de pricing
- Architecture générale
- Principaux points de vigilance pour la mise en place

### DÉCOUVRIR ELASTICSEARCH

- Elasticsearch : une base de donnée ? un moteur de recherche ?
- Comment communiquer avec Elasticsearch ?
- Structure de l'API
- Format de stockage des données : Design by query

### RÉCUPÉRER SES LOGS AVEC L'ETL LOGSTASH

- Fonctionnement et concepts
- Positionnement des Beats par rapport à Logstash
- Installation et configuration de base
- Inputs / Outputs : que peut-on brancher sur ce tuyau ?
- Traitement automatique de la donnée avec les Filters
- Dimensionnement des index
- Cas pratique : "Agréger des logs et métriques système sur un noeud Elasticsearch avec Logstash, Filebeat et Metricbeat."

## Jour 2

### STOCKER INTELLIGEMMENT SES LOGS AVEC ELASTICSEARCH

- Installation, configuration de base et plugins
- Le rôle et l'importance du mapping
- Recherche basique
- Agrégats
- Cas pratique : "Rechercher et agréger sur des formats de logs hétérogènes"

### VISUALISER SES LOGS AVEC KIBANA

- Un dashboard conçu pour les cas d'utilisation ELK
- Installation, configuration de base et plugins
- Rechercher, agréger, visualiser, sauver, exporter
- Construire des graphes représentatifs du besoin
- Cas pratique : "Construire un outil de monitoring de logs simple et efficace avec différents types de logs sur plusieurs machines distantes."

### OPTIMISER LA GESTION OPÉRATIONNELLE D´UN CLUSTER ELK

- Monitoring et supervision
- Dimensionner Elasticsearch
- Dimensionner Logstash
- Retour sur les points de vigilance
- Une alternative à Logstash ?

## CLÔTURE

- Synthèse et rappel des points clés
- Plan d’action individuel