# Elastic Stack ELK (Elasticsearch, Logstash & Kibana)

Formation Informatique / Développement logiciel / Frameworks Javascript

ElasticSearch est un puissant moteur de recherche reconnu et utilisé par de grands acteurs internationaux (Sony, IGN, Stackoverflow , github, SoundCloud, Mozilla…). Orienté "document" au sens NoSQL du terme, toutes les données sont stockées sous forme de documents JSON structurés. Tous les champs sont indexés par défaut, et tous les index peuvent être utilisés dans une même requête, pour retourner les résultats correspondant à une recherche à une vitesse impressionnante. Dans cette formation vous aborderez l'utilisation d'ELK V6 qui est l'association de 4 outils: Elasticsearch, Logstash, Kibana et Beats. Elasticsearch est le moteur de recherche distribué utilisé pour le stockage. Beats permet de collecter et d'envoyer simplement des données. Logstash permet d'extraire les logs, les transférer, les parser, et enfin les indexer dans Elasticsearch. Kibana permet d'exploiter les données stockées dans Elasticsearch, de produire des requêtes, d'en faire des tableaux de bord depuis un navigateur web. Comme dans toutes nos formations, celle-ci vous présentera la toute dernière version de d'ELK / Elastic Stack (à la date de rédaction de l'article : Elastic Stack / ELK 6.3.1).

## OBJECTIFS

- Découvrir Elasticsearch et les dernières nouveautés d'Elastic Stack
- Connaissance de la stack ELK (avec Beats ELKB / BELK)
- Alimenter Elasticsearch avec de nombreuses sources de données
- Structurer et enrichir des données hétérogènes
- Transférer des données brutes depuis un fichier ou un broker
- Produire des tableaux de bords / dashboards avec Kibana
- Monitoring système, JMX, Métier et BI
- Administration avancée (Module optionnel)

## PUBLIC

Développeurs, Architectes, Administrateurs systèmes, DevOps

## PRE-REQUIS

- Connaissances de base d'un système Unix

## PROGRAMME

**Introduction et vue d'ensemble**

- L'écosystème d'Elasticsearch
- Le rôle d'Elasticsearch, Logstash, Kibana et Beats
- Simplifier la gestion des versions avec The Elastic Stack V5
- Principes et fonctionnement
- Exemples d'architectures
- Cas d'utilisations

**Elasticsearch – Indexation, Recherche et analyse de données**

- Introduction à Elasticsearch
- Indexation et recherche
- Analyse de données
- Mappings et configuration de l'analyse
- Requêtage avec Elasticsearch
- Système de plugins & Configuration
- Queries et Filters
- Agrégations
- Réplication et partitionnement
- TP: Installation et configuration
- Serveur ElasticSearch
- Mettre en place un cluster
- Les rôles des noeuds

**Logstash – Transformez et formatez vos données pour les utiliser depuis Elasticsearch**

- Concepts: Input, Output, Filter (filtre), Codecs…
- Les Inputs: File, Redis, RabbitMQ…
- Les Filters: Grok, Date, Mutate…
- Les Outputs: File, Elasticsearch, Redis…
- Threading et haute-disponibilité

**Kibana – Visualisez les données d'Elasticsearch et Créez vos rapports**

- Installation et configuration

### A retenir

Durée : **3 jours** soit 21h.
Réf. **ELK**

01 42 93 52 72

### Dates des sessions

**Cette formation est également proposée en formule INTRA-ENTREPRISE.**

### Inclus dans cette formation

**Coaching Après-COURS**

Pendant 30 jours, votre formateur sera disponible pour vous aider. CERTyou s'engage dans la réalisation de vos objectifs.

**Votre garantie 100% SATISFACTION**

Notre engagement 100% satisfaction vous garantit la plus grande qualité de formation.

- Découverte des données et construction des requêtes / Queries
- Agrégations et construction de Visualizations
- Panels
- Création des vues
- Mise en place d'un tableau de bord
- TP: Créer un rapport avec une visualisation en temps-réel

**Beats – Collectez, Parsez et envoyez simplement vos données**

- Introduction aux Data Shippers et au monitoring temps réel
- Monitorez votre réseau grâce à PacketBeat
- Monitorez vos fichiers grâce à FileBeat
- Monitorez vos Windows event logs grâce à WinlogBeat
- Récupérer les métriques importantes de vos serveurs grâce à Metricbeat

**Monitoring et analyse**

- Mise en pratique
- Monitoring Système
- Monitoring JVM / JMX
- Log As A Service
- Analyse Métier & BI (Business Intelligence)

**Modules avancés d'administration (optionnels)**

- X-Pack: Sécurisez et protégez vos données et soyez alerté grâce à des rapports sur l'état de santé de vos services Elastic Stack !
- ES-Hadoop
- Elastic Cloud: Elasticsearch as a Service
- Graph
- Tuning et architectures avancés
- Supervision (Kopf, Marvel) et monitoring (Cluster, Nodes, Cat)
- Sauvegardes : Snapshots et Restore

## Horaires, Planning et Déroulement de cette formation

**Horaires**

• Formation de 9h00 (9h30 le premier jour) à 17h30.
• Deux pauses de 15 minutes le matin et l'après-midi.
• 1 heure de pause déjeuner

**DEROULEMENT**

• Les horaires de fin de journée sont adaptés en fonction des horaires des trains ou des avions des différents participants.
• Une attestation de suivi de formation vous sera remise en fin de formation.
• Cette formation est organisée pour un maximum de 14 participants.

## PROCHAINES FORMATIONS

Réussir la Certification Gestion de Projet PMP du PMI
Réussir la Certification PRINCE2 Foundation
Réussir les Certifications PRINCE2 Foundation et PRINCE2 Practitioner
Réussir la Certification ITIL Foundation
Réussir la Certification Agile certifié SCRUM Master
Réussir les Certifications TOGAF Certified et TOGAF Foundation

Retrouvez cette formation sur notre site :
Elastic Stack ELK (Elasticsearch, Logstash & Kibana)