

## Programme de formation

Formation « Elasticsearch »

### But de la formation

- Comprendre le fonctionnement de Elastic Stack
- Savoir installer et configurer un cluster Elastic Stack
- Être capable d'indexer des volumes importants de données
- Être capable de visualiser des données et créer des tableaux de bord
- Maîtriser l'administration et l'exploitation de la solution

### Pré-requis

- Solides connaissances des systèmes d'exploitation

### Type de public

- Administrateur système
- Architecte annuaire
- Analystes et membres d'un SOC
- Toute personne souhaitant utiliser Elastic Stack pour la visualisation de données

### Moyens pédagogiques

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

### Sanction de la formation

- À l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h00 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification Elasticsearch par HS2.
- Formation délivrée [en partenariat avec HS2](#)

### Méthodes pédagogiques

- Cours magistral
- Démonstrations
- Exercices de mise en œuvre

### Durée

35 heures (5 jours).

# Programme

---

## Chapitre 1 - Présentation d'Elasticsearch

- Fonctionnalités et potentiels d'ElasticSearch
- Ecosystème
- Les alternatives à ElasticSearch
- Comprendre Lucene, son coeur
- Les apports spécifiques d'Elasticsearch.

## Chapitre 2 - Installation et configuration

- Installation en local
- Installation sur un serveur
- Déploiement sur plusieurs serveurs en mode cluster

## Chapitre 3 - Requêtes de recherche

- Principe d'une API REST, et les principaux points d'entrée
- Index, mapping et templates
- Rechercher des données
- Fonctionnalités avancées de recherches

## Chapitre 4 - L'analyse

- La base de l'analyse : l'agrégation
- Les agrégations metric et bucket
- L'analyse avancées

## Chapitre 5 - Surveiller Elasticsearch

- Les métriques
- Les slowlogs
- Sauvegardes et restaurations
- La fonction Monitoring des Stack Features
- Les API pour les admins

## Chapitre 6 - Collecte d'information depuis des beats

- Rappels sur Elastic Stack
- Rappels sur l'installation d'un noeud standalone
- Mise en place de collecte avec Filebeat
- Mise en place de collecte avec Packetbeat
- Mise en place de collecte avec Metricbeat

## Chapitre 7 - Exploration de données depuis Kibana

- Concepts de base
- Découverte de données
- Le Lucene Query DSL
- Extraction et partage de données

## Chapitre 8 - Création de visualisations et dashboards

- Les différents types de visualisations
- Création de visualisations et dashboards
- Dashboards interactifs
- Création de rapports

## Chapitre 9 - Visualisations des séries de données

- Introduction à timelion
- Utilisation de timelion
- Le visual builder

## Chapitre 10 - Management de Kibana

- - Personnalisation
- - Les objets sauvegardés
- - Import/export de configuration

## Chapitre 11 - Configuration du cluster

- Configuration du cluster Elasticsearch
- Préparation du cluster Elasticsearch pour le traitement des gros volumes
- Configuration des noeuds
- Gestion des modèles

## Chapitre 12 - Collecte et indexation de données avec Logstash

- Les possibilités offertes par Logstash
- Le monitoring par les Beats
- Activation de la géolocalisation IP dans Logstash
- Activation du monitoring de performance

## Chapitre 13 - Administration du cluster

- Surveillance du cluster
- Sécurisation du cluster
- L'allocation des noeuds
- Alias d'index. Greffons Elasticsearch

## Examen de certification