Elastic Stack : Elasticsearch, Logstash et Kibana

Référence : **BDDELA002** Durée : **2 jours (14 heures)** Certification : **Aucune**

CONNAISSANCES PRÉALABLE

- Connaissances en bases de données et JSON

PROFIL DES STAGIAIRES

- Data engineers, DevOps, analystes

OBJECTIFS

- Indexer et rechercher des données avec Elasticsearch
- Créer des pipelines ETL avec Logstash
- Visualiser et analyser les données avec Kibana

CERTIFICATION PRÉPARÉE

- Aucune

MÉTHODES PÉDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique pendant le stage
- La formation est constituée d'apports théoriques interactif, démonstrations en direct, travaux dirigés, ateliers collaboratif, mises en situation professionnelles, projet fil rouge, études de cas réels, d'ateliers d'analyse de d'optimisation.
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement par demi-journée de formation

FORMATEUR

- Consultant-formateur expert Data Engineer et Elastic Stack

MÉTHODES D'ÉVALUATION DES ACQUIS

- Validation des prérequis envoyée en amont de la formation. En l'absence de réponse d'un ou plusieurs participants, un temps sera consacré en ouverture de session pour prendre connaissance du positionnement de chaque stagiaire sur les objectifs pédagogiques évalués
- Validation progressive des compétences tout au long de la formation via exercices pratiques, quiz techniques, études de cas, réalisation des différents composants de la chaîne Elastic Stack et restitution des travaux réalisés dans le cadre du projet fil rouge
- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

ACCESSIBILITÉ DE LA FORMATION

- Si vous avez besoin d'un aménagement pour suivre votre formation dans de bonnes conditions, nous vous invitons à contacter notre référent handicap au 01 71 19 70 30 ou à l'adresse referent.handicap@edugroupe.com. Un échange en amont nous permettra d'étudier avec vous les adaptations possibles.

CONTENU DU COURS

1. JOUR 1 - Collecter, indexer et rechercher les données (7h)

2. Comprendre l'architecture Elastic Stack (2h)

- Présentation de l'Elastic Stack
- Cas d'usage : observabilité, analyse de logs, reporting et recherche
- Architecture Elasticsearch
- Notions de cluster, nœud et index
- Documents JSON
- Architecture Logstash
- Architecture Kibana
- Flux de données dans Elastic Stack
- 💡 *Mises en pratique : Découverte d'un environnement Elastic Stack ; Exploration des composants ; Analyse d'une architecture type*

3. Indexer et rechercher des données avec Elasticsearch (3h)

- Création d'index
- Mapping et types de données
- Analyseurs et tokenisation
- Indexation de documents JSON
- Requêtes de recherche
- Filtres et agrégations
- Recherche plein texte
- Principes de scoring
- 💡 *Mises en pratique : Création d'index ; Importation de données ; Réalisation de recherches simples et avancées ; Construction d'agrégations*

4. Optimiser l'organisation et l'exploitation des données (2h)

- Gestion des mappings
- Templates d'index
- Shards et replicas
- Cycle de vie des index
- Optimisation des performances
- Bonnes pratiques de modélisation
- 💡 *Mises en pratique : Création de templates ; Analyse de performances ; Optimisation d'un index existant*

5. JOUR 2 - Transformer et visualiser les données (7h)

6. Construire des pipelines de transformation avec Logstash (3h)

- Architecture Logstash
- Inputs
- Filters
- Outputs
- Traitement des fichiers de logs
- Parsing et enrichissement
- Manipulation de données JSON
- Gestion des erreurs
- 💡 *Mises en pratique : Création de pipelines Logstash ; Transformation de données ; Enrichissement de flux ; Envoi vers Elasticsearch*

7. Créer des visualisations et tableaux de bord avec Kibana (2h)

- Découverte de Kibana
- Data Views
- Visualisations
- Graphiques
- Tableaux
- Filtres interactifs
- Dashboards
- Cas d'usage métiers
- 💡 *Mises en pratique : Création de visualisations ; Construction d'un tableau de bord ; Analyse de jeux de données réels*

8. Atelier de synthèse : construire une chaîne complète Elastic Stack (2h)

- Collecte des données
- Transformation via Logstash
- Indexation dans Elasticsearch
- Recherche et agrégation
- Création de visualisations
- Construction d'un tableau de bord décisionnel
- Mises en pratique : Réalisation d'un cas pratique complet ; Mise en œuvre d'un pipeline Elastic Stack de bout en bout ; Construction d'indicateurs et tableaux de bord ; Restitution et débriefing collectif