New

Elastic Stack : Elasticsearch, Logstash et Kibana

Indexer, rechercher, transformer et visualiser des données avec Elasticsearch, Logstash et Kibana

Présentiel ou en classe à distance

2 jours (14 h)

Prix inter : 1.750,00 € HT
Forfait intra : 5.690,00 € HT

Réf.: BD516

La formation **Elastic Stack : Elasticsearch, Logstash et Kibana** permet de maîtriser une plateforme de référence pour l'**indexation**, la **recherche**, la **transformation** et la **visualisation de données**. Elle couvre la création d'index avec **Elasticsearch**, la conception de pipelines ETL avec **Logstash**, l'exploitation de **Kibana** pour l'analyse et les tableaux de bord, ainsi que les bonnes pratiques d'ingestion de données. Une formation idéale pour déployer des projets de **data analytics**, d'**observabilité** et de **cybersécurité** en environnement professionnel.

A qui s'adresse cette formation ?

Pour qui

- Data engineers, DevOps, analystes

Prérequis

- Connaissances en bases de données et JSON
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Introduction à Elastic Stack et à l'architecture d'Elasticsearch

- Présentation des composants de la suite Elastic : Elasticsearch, Logstash, Kibana et Beats
- Découverte des principaux cas d'usage : recherche applicative, observabilité des logs, des métriques et de l'APM, et sécurité avec un SIEM
- Architecture distribuée d'Elasticsearch : nodes, clusters, shards primaires et répliques
- Rôle des différents nodes : master, data, ingest, coordinating, machine learning et voting-only
- Modèle de données Elasticsearch : documents JSON, index et alias
- Modes de déploiement : environnement autogéré, Docker ou Docker Compose, Elastic Cloud et ECK pour Kubernetes
- Mécanismes de sécurité natifs : authentification, chiffrement TLS et contrôle des accès
- Présentation de l'Elastic Common Schema (ECS) pour standardiser les champs et assurer l'interopérabilité des données au sein d'Elastic Stack

Atelier

Démarrer un cluster Elasticsearch local avec Docker Compose, comprenant Elasticsearch et Kibana

Vérifier l'état du cluster à l'aide des API _cluster/health et _cat

Configurer l'authentification et créer un premier utilisateur

Interroger l'API REST avec curl et la console Kibana Dev Tools

Consulter les logs d'un node Elasticsearch et identifier les messages de démarrage clés tels que selected-as-master et started

2 - Indexation et modélisation des données dans Elasticsearch

- Gestion des documents et des index avec les opérations CRUD : PUT, GET, POST et DELETE
- Définition du mapping et des types de champs : text, keyword, numeric, date, geo_point, nested, object et dense_vector
- Comparaison entre mapping dynamique, mapping strict et runtime fields selon les besoins de flexibilité, de performance et de gouvernance
- Fonctionnement des analyzers et des tokenizers et incidence sur la recherche full-text
- Création et gestion des templates d'index et de leurs composants
- Stratégies de dimensionnement des shards et gestion de la réplication
- Utilisation des API Reindex et Update By Query pour faire évoluer un mapping sans interruption de service
- Gestion du cycle de vie des index avec Index Lifecycle Management (ILM) : phases hot, warm, cold, frozen et delete
- Création de snapshots et restauration des données Elasticsearch

3 - Recherche avec Query DSL et agrégations Elasticsearch

- Présentation de Query DSL, le langage de requête d'Elasticsearch
- Création de requêtes full-text avec match, multi_match et match_phrase
- Utilisation des requêtes term-level : term, terms, range, exists, prefix et wildcard
- Construction de requêtes booléennes avec bool, must, should, must_not et filter
- Gestion de la pertinence et du scoring avec BM25, function_score et boost
- Tri, pagination avec from/size ou search_after, et mise en évidence des résultats avec le highlighting
- Création d'agrégations métriques : avg, sum, min, max, stats et cardinality
- Utilisation des bucket aggregations : terms, date_histogram, range et filters
- Mise en oeuvre d'agrégations pipeline avec derivative, cumulative_sum et bucket_script
  Atelier

  Définir un mapping adapté à un jeu de données métier

  Indexer un volume de documents avec l'API Bulk

  Construire des requêtes full-text et term-level au sein d'une requête booléenne

  Utiliser l'API Reindex pour modifier le mapping d'un champ

  Créer des agrégations bucket et metric afin de répondre à des questions analytiques

  Mettre en place une politique ILM simple sur un index

4 - Logstash : architecture et pipelines ETL

- Présentation de Logstash et de son positionnement au sein de la suite Elastic
- Architecture d'un pipeline Logstash : inputs, filters et outputs
- Utilisation des plugins d'entrée : file, Beats, Kafka, JDBC, HTTP et Syslog
- Utilisation des plugins de filtrage : grok pour l'analyse des logs non structurés, mutate, date, geoip, json et csv
- Utilisation des plugins de sortie : Elasticsearch, file, stdout et Kafka
- Gestion de la persistance et des files d'attente : memory queue et persistent queue
- Configuration de plusieurs pipelines avec le fichier pipelines.yml
- Présentation des alternatives complémentaires : Beats Filebeat et Metricbeat , Elastic Agent, Fleet Server et Ingest Pipelines
- Surveillance de Logstash avec l'API node/stats et intégration de Metricbeat pour le monitoring en production
  Atelier

  Configurer une entrée file pour lire un fichier de logs applicatifs

  Analyser les lignes de logs avec le filtre grok et extraire des champs structurés

  Enrichir les événements avec les filtres date, geoip et mutate, puis convertir les types de données

  Configurer une sortie Elasticsearch afin d'indexer les événements transformés

  Vérifier l'ingestion et explorer les données avec Kibana Discover

5 - Kibana : exploration des données avec Discover

- Présentation de Kibana et organisation de son interface : Spaces et applications
- Configuration et gestion des Data Views, anciennement appelées Index Patterns
- Utilisation de Discover pour explorer les données indexées dans Elasticsearch
- Recherche et filtrage des données avec KQL et la syntaxe Lucene : usages, différences et cas d'emploi
- Utilisation d'ES|QL, Elasticsearch Query Language, et de sa syntaxe fondée sur les pipelines pour explorer les données dans Discover
- Configuration des filtres, des plages temporelles et des recherches sauvegardées
- Utilisation de la console Kibana Dev Tools pour interagir avec les API Elasticsearch

6 - Création de visualisations et de dashboards avec Kibana

- Création de visualisations avec Kibana Lens et son interface en glisser-déposer
- Principaux types de visualisations : graphiques en barres, courbes, aires, secteurs, heatmaps, treemaps et jauges

- Création de visualisations géographiques avec Kibana Maps
- Utilisation des fonctions time series et d’ES|QL dans Lens pour réaliser des analyses temporelles avancées
- Création et organisation de dashboards regroupant plusieurs visualisations
- Application de filtres globaux, exploration par drill-down et partage des dashboards
- Présentation des mécanismes de notification et d’alerting de Kibana
  Atelier

  Configurer une Data View sur l’index alimenté par Logstash

  Explorer les données avec Kibana Discover et KQL

  Utiliser ES|QL dans Discover afin de créer une requête fondée sur un pipeline

  Créer plusieurs visualisations avec Kibana Lens : répartition, séries temporelles et classement des principales valeurs

  Composer un dashboard cohérent intégrant des filtres globaux et des plages temporelles

  Partager le dashboard et exporter une visualisation

Les objectifs de la formation

- Indexer, rechercher et optimiser des données avec Elasticsearch
- Concevoir et automatiser des pipelines ETL performants avec Logstash
- Analyser des données en temps réel pour faciliter la prise de décision
- Exploiter les fonctionnalités d'Elasticsearch, Logstash et Kibana dans un projet

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Une pédagogie orientée pratique alternant apports théoriques et ateliers pour manipuler concrètement Elastic Stack (ELK). Les nombreux exercices permettent de prendre en main Elasticsearch, Logstash et Kibana dans des situations proches des besoins de l'entreprise
- Une approche complète de la chaîne de traitement des données : de l'ingestion avec Logstash, à l'indexation et la recherche avec Elasticsearch, jusqu'à la visualisation et l'analyse des données avec Kibana

Dates et villes 2026 - Référence BD516

Dernières places disponibles Session garantie

A distance

du 21 oct. au 22 oct.	du 14 déc. au 15 déc.

Paris

du 21 oct. au 22 oct.	du 14 déc. au 15 déc.