Formation **Kibana**

Cette formation vous initie à l'univers de Kibana, l'interface de visualisation et d'analyse de la stack Elastic. À travers des explications techniques, des démonstrations et des ateliers pratiques, vous découvrirez comment interroger efficacement vos données, créer des visualisations pertinentes, construire des tableaux de bord dynamiques, configurer des alertes, et exploiter les capacités de machine learning intégrées. Une attention particulière est portée à l'intégration avec Elasticsearch et à la maîtrise des différentes fonctionnalités de Kibana, des plus fondamentales aux plus avancées.

Durée

2 jours

Objectifs pédagogiques

- Comprendre l'architecture générale de la stack Elastic et le rôle spécifique de Kibana.
- Manipuler l'interface de Kibana, notamment les sections Discover, Visualize, Dashboard et Stack Management.
- Rechercher et filtrer les données dans Elasticsearch via la console Dev Tools et le langage KQL.
- Créer et personnaliser des visualisations à partir d'agrégations simples ou complexes.
- Construire des tableaux de bord interactifs et adaptés aux besoins métier.
- Mettre en place des alertes automatisées et générer des rapports dans Kibana.
- Exploiter les fonctionnalités de détection d'anomalies basées sur le machine learning.
- Gérer les droits d'accès, les espaces de travail et les options avancées de configuration.

Public

Data analystes, administrateurs systèmes, devops, développeurs, chefs de projet, marketing...

Prérequis

Connaissances de base en administration système et en traitement de données.

Programme de formation

Phase d'inclusion

Introduction à la formation Kibana

Les grands principes de la stack Elastic et le rôle particulier de Kibana
Déploiement de l'environnement de formation

Quelques notions à propos du fonctionnement d'Elasticsearch

Elasticsearch et les notions de noeuds, shards, index et mapping
Index versus Data Stream
Les types de mappings et les types de champs
Les spécificités des formats « text » et « keyword »
Le format JSON des documents (champs, valeurs, métadonnées)

Dev Tools, la console Elasticsearch au sein de Kibana

Les APIs Elasticsearch
Requêtes (Query DSL), recherche et filtres dans la console

Lab : exercice pratique avec la console

L'interface graphique de Kibana et l'onglet Discover

Les principales sections de Kibana
Ajout d'un index pattern / dataview
L'onglet « Discover »
Ajustement de l'intervalle calendaire de travail
Présentation des langages KQL et LUCENE et utilisation de la barre de recherche
Création de filtres
Sauvegarde, partage et export des résultats d'une recherche

Lab : exercice pratique dans l'onglet Discover

Les familles d'agrégations

Les agrégations métriques
Les agrégations en « buckets »
Les agrégations de type « pipeline »

Quiz rapide sur les agrégations

L'onglet « Visualize Library »

Les diVérents types de visualisations
Les visualisations basées sur les agrégations
La visualisation Lens
Les visualisations « complexes » : TSVB, Timelion et Vega

Sauvegarder, partager et exporter une visualisation

Lab : exercice de création de visualisations

L'onglet « Dashboard »

Création d'un dashboard dynamiques avec des paramètres de filtrage avancés
Ajout de visualisations et personnalisation du dashboard
Les drilldowns
Partage et export de tableaux de bord
Le reporting dans Kibana

Lab : Exercice de création d'un dashboard

L'alerting et le reporting avec Kibana

Le fonctionnement des alertes avec Kibana
Les notions de « rules », « case » et de « connector »

Lab : exercice de mise en place d'un alerte

La détection d'anomalies grâce au machine learning dans Kibana

Le « data visualizer » et l'analyse statistiques des données d'un index
Présentation de l'onglet « Anomaly Detection »
Les modèles généraux de jobs d'anomaly detection
Les modèles spécifiques (Apache, NGINX, etc.)

Lab : exercice de création d'un job de détection d'anomalie sur les données d'un index

Utilisation avancée de Kibana

L'administration de Kibana, utilisateurs et droits
Les spaces
La gestion avancée des options des index via l'onglet « Stack Management »
Les runtime fields
Les index « transform » pour synthétiser les données par des métriques calculées

Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques (hors formation de type séminaire).
- Les participants bénéficient des retours d'expérience terrains du formateur ou de la formatrice
- Un support de cours numérique est fourni aux stagiaires

Modalités d'évaluation

- **En amont de la session de formation**, un questionnaire d'auto-positionnement est remis aux participants, afin qu'ils situent leurs connaissances et compétences déjà acquises par rapport au thème de la formation.

- **En cours de formation**, l'évaluation se fait sous forme d'ateliers, exercices et travaux pratiques de validation, de retour d'observation et/ou de partage d'expérience, en cohérence avec les objectifs pédagogiques visés.

- **En fin de session**, le formateur évalue les compétences et connaissances acquises par les apprenants grâce à un questionnaire reprenant les mêmes éléments que l'auto-positionnement, permettant ainsi une analyse détaillée de leur progression.