

Mis à jour le 03/06/2024

S'inscrire

## Formation EFK

3 jours (21 heures)

### Présentation

EFK (ElasticSearch, Fluentd et Kibana) est une solution de [journalisation centralisée](#) populaire. Avec notre formation EFK vous pourrez collecter, traiter et visualiser les journaux.

Lors de ce cours, vous comprendrez le fonctionnement des services permettant d'aider à trier et à analyser rapidement un volume conséquent de données de journaux produites par les pods.

Avec Elasticsearch, vous pourrez faire des recherches en texte intégral et structurées ainsi que des analyses, Kibana pour la visualisation de données, Fluentd afin de collecter, transformer et envoyer les [données de journaux](#) au backend Elasticsearch.

Grâce à cette formation, vous serez capable de gérer une quantité importante de données et de fournir des informations en temps réel sur le comportement de systèmes complexes.

Comme pour toutes nos formations, celle-ci vous sera présentée avec les dernières fonctionnalités de l'outil.

### Objectifs

- Comprendre les composants et l'architecture de la Stack EFK
- Installer et configurer Elasticsearch, Fluentd et Kibana
- Créer et gérer des visualisations et des tableaux de bord dans Kibana
- Optimiser et surveiller les performances des pipelines de logs en production

### Public visé

- Développeurs
- Ingénieurs de données
- Architectes

## Pré-requis

- Connaissance des bases de données
- Familiarité avec les formats de logs et les systèmes de journalisation

## PROGRAMME DE NOTRE FORMATION EFK

### INTRODUCTION À L'EFK

- Présentation de la Stack EFK
- Cas d'utilisation
- Avantages de l'EFK par rapport aux autres solutions
- Aperçu des composants Elastic, Fluentd et Kibana
- Architecture et flux de données

### INSTALLATION ET CONFIGURATION

- Installation et configuration d'Elastic
- Concepts clés : Index, Shards et Replicas
- Sauvegarde et restauration des données
- Sécurisation de l'installation

### DÉCOUVERTE DE FLUENTD

- Introduction à Fluentd et son architecture
- Installation de Fluentd
- Configuration des entrées (Inputs) et sorties (Outputs)
- Utiliser des filtres pour transformer les données
- Meilleures pratiques pour optimiser les performances de Fluentd

### VISUALISATION AVEC KIBANA

- Installation et configuration de Kibana
- Navigation dans l'interface de Kibana
- Créer des visualisations basiques
- Dashboards et panels : création et gestion
- Utiliser Kibana pour l'analyse des journaux

### INTÉGRATION DE FLUENTD AVEC ELASTICSEARCH

- Configuration de Fluentd pour envoyer des logs vers Elasticsearch
- Gestion des schémas de données et des templates d'index

- Monitoring et troubleshooting des pipelines de logs
- Optimisation des performances et tuning des paramètres
- Cas pratique : ingestion de logs applicatifs avec Fluentd et Elastic

## ANALYSE ET SURVEILLANCE AVANCÉES AVEC KIBANA

- Requêtes avancées et analyse des données avec Lucene
- Utiliser correctement les alertes et les notifications
- Exploration des logs en temps réel
- Intégration avec d'autres outils de surveillance et d'alerte
- Cas pratique : création de tableaux de bord complexes

## BONNES PRATIQUES ET DÉPLOIEMENT EN PRODUCTION

- Stratégies de déploiement de la Stack EFK en production
- Sauvegarde et récupération des données
- Sécurité et gestion des accès
- Actualisation et gestion des versions de la Stack EFK

## Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

## Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

## Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

## Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

## Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte

des compétences.

## Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.