EMGS GROUP
CONSULTING | RECRUITMENT | TRAINING

Contact
☎ 01 75 43 05 58
✉ training@emgsgroup.com

Gérer efficacement ses logs avec la stack ELK

Code formation : EMELK
Durée : 2 jours – 14h de cours
Format : Inter-entreprise*

2 jours
14 heures de cours

**Cette formation est également disponible en « Intra-entreprise », nous contacter pour plus d'infos.*

| Description

La stack ELK est très communément utilisée pour gérer facilement et efficacement ses logs applicatifs. Issue de l'open source, simple à installer et permettant de gérer toute sorte de documents (logs, messages divers, documents évènementiels, etc.), cette stack est un outil puissant qui peut cependant vite devenir incontrôlable. Cette formation vous donne des outils simples et pratiques pour dimensionner, configurer et gérer simplement votre cluster ELK.

| Objectifs pédagogiques

- Identifier les bonnes pratiques à mettre en place pour développer une application basée sur la stack ELK
- Découvrir les bases de la gestion de messages avec Logstash
- Appréhender les concepts de recherche full-text et de stockage de données massif avec ElasticSearch
- Créer des visualisations représentatives et efficaces avec le dashboard Kibana
- Configurer ces trois outils pour une application robuste et fiable

| Publics

- Développeur
- Architecte
- Ops

| Pré-requis

- Disposer de notions sur http.
- Connaissance de l'environnement sous Linux.

| Méthode pédagogique

Formation rythmée par des apports théoriques, des mises en pratique et des bonnes pratiques qui s'appuient sur les retours d'expérience de nos consultants-formateurs.

| Programme détaillé

Jour 1

Découvrir la stack ELK

- ElasticSearch, Logstash et Kibana
- Cas d'utilisation
- Principaux points de vigilance pour la mise en place

Stocker intelligemment ses logs avec Elasticsearch

- ElasticSearch : une base de données ? Un moteur de recherche ?
- Installation, configuration de base et plugins
- Architecture générale
- Structure de l'API
- Le rôle et l'importance du mapping
- Recherche basique
- Agrégats
- Cas pratique : "Rechercher et agréger sur des formats de logs hétérogènes"

Jour 2

Récupérer ses logs avec l'ETL LOGSTASH

- Fonctionnement et concepts
- Installation et configuration de base
- Inputs / Outputs : que peut-on brancher sur ce tuyau ?
- Traitement automatique de la donnée avec les Filters
- Dimensionnement des index
- Cas pratique : "Agréger des logs sur un nœud ElasticSearch avec Logstash"

Visualiser ses logs avec Kibana

- Un dashboard conçu pour les cas d'utilisation ELK
- Installation, configuration de base et plugins
- Rechercher, agréger, visualiser, sauver, exporter
- Construire des graphes représentatifs du besoin
- Cas pratique : "Construire un outil de monitoring de logs simple et efficace avec différents types de logs sur plusieurs machines distantes"

Optimiser la gestion opérationnelle d'un cluster ELK

- Monitoring et supervision
- Dimensionner ElasticSearch
- Dimensionner Logstash
- Retour sur les points de vigilance
- Une alternative à Logstash ?

Clôture