Formation ELK (Elasticsearch, Logstash et Kibana)

Durée :	3 jours
Public :	Opérationnels, Développeurs, Chefs de projets
Pré-requis :	Connaissances en développement et en administration du système d'exploitation Windows ou Linux
Objectifs :	Maîtriser l'utilisation d'Elasticsearch, logstash et Kibana pour indexer, chercher et visualiser des données et des documents
Référence :	BUS100545-F
Demandeurs d'emploi :	Contactez-nous pour connaître les remises Pôle Emploi

Découvrir la Suite Elastic

Introduction à la recherche d'information
Indexation des données : concepts, formes
Présentation de la suite Elastic : produits, contextes d'utilisation
Découverte du moteur de recherche ElasticSearch
Connecteurs et outils de transformation de Logstash
Kibana pour l'analyse et la visualisation
Distributions de la suite
Atelier : Architecture et installation de la stack ELK

Maîtriser l'utilisation du moteur de recherche ElasticSearch

ElasticSearch : origine, détail du moteur de recherche, technologies / fonctionnalités
Notions fondamentales : Index, Document, Cluster, Noeud, Réplique
Présentation des APIs disponibles (REST) : Indexation, recherche
Indexation : gestion des index, documents et mapping, méta-données
Types de champs
Analyseurs
Utilisation de filtres
Recherche avec le moteur : types, filtres, score de pertinence, recherche à facette
Agrégation, Bucket, Mesure
Gestion de la géolocalisation : points, précision, formes
Mesure des performances
Modélisation de données
Atelier : création et modifications d'index - manipulation de l'API de recherche - utilisation d'analyseurs

Ingérer des données provenant d'une multitude de sources avec Logstash

Gestion des données en entrée : plugins, formats supportés
Gestion des données en sortie
Filtres
DSL Logstash

Atelier : configuration de Logstash et gestion de données

Analyser et visualiser des données avec Kibana

Kibana : fonctionnalités, architecture, plugins disponibles
Recherches
Templates de Visualisations
Visualisations personnalisées
Atelier : utilisation de visualisations prédéfinies - création de visualisations personnalisées et mise en forme.

Mettre en place une architecture avancée (scalabilité et clustering)

La suite ELK dans un environnement à haute disponibilité (HA)
Mise en place d'un cluster Elasticsearch
Gestion de plusieurs instances Logstash : architecture, file de message, filebeat
Kibana pour la distribution des requêtes Elasticsearch
Tuning et monitoring
Atelier : mise en oeuvre d'une architecture HA avec la suite Elastic

Administrer et déployer la suite Elastic

Optimisation du déploiement de la suite
Gestion des ressources matérielles et réseau
Outils de monitoring (Metrics)
Sauvegarde et restauration
Atelier : utilisation d'un outil de monitoring et tests de charge - mise en place d'une stratégie de sauvegarde et de restauration.