Elastic Stack (ELK) - Pour administrateurs

Administration et optimisation pour des analyses de données performantes

Présentiel ou en classe à distance

2 jours (14 h) | Prix inter : 1.600,00 € HT | Réf.: BD522

Elastic Stack (ELK) est une puissante suite d'outils d'analyse et de recherche. En acquérant les compétences nécessaires pour la maîtriser, il est possible de configurer, gérer et optimiser Elasticsearch, Logstash et Kibana pour l'indexation et l'analyse des données à grande échelle.
En tant qu'administrateur, vous pourrez améliorer la performance, la sécurité et l'efficacité opérationnelle de votre infrastructure, optimisant ainsi la visualisation et la compréhension des données pour des prises de décisions plus éclairées.
Cette formation ouvre de nombreuses opportunités dans des domaines tels que l'analyse de données, la sécurité et l'administration système.

A qui s'adresse cette formation ?

Pour qui

- Architectes techniques, ingénieurs système, administrateurs

Prérequis

- Connaissances générales des systèmes d'information et des systèmes d'exploitation (Linux ou Windows)

Programme

1 - Introduction

- Présentation de la pile Elastic
- Positionnement d'ElasticSearch et des produits complémentaires : Kibana, Logstash, Beats, X-Pack
- Principe : base technique Lucene et apports d'ElasticSearch
- Fonctionnement distribué

2 - Installation et configuration

- prérequis techniques
- Installation depuis les RPM
- Premiers pas dans la console Devtools
- Étude du fichier : elasticsearch.yml et kibana.yml
- Mise en place de la surveillance d'un cluster ES

3 - Clustering

- Définitions : cluster, noeud, sharding
- Nature distribuée d'ElasticSearch
- Présentation des fonctionnalités : stockage distribué, calculs distribués avec ElasticSearch, tolérance aux pannes

4 - Fonctionnement

- Notion de noeud maître
- Stockage des documents : shard primaire et réplica, routage interne des requêtes

5 - Gestion du cluster

- Outils d'interrogation : /_cluster/health
- Création d'un index : définition des espaces de stockage (shard), allocation à un noeud
- Configuration de nouveaux noeuds : tolérance aux pannes matérielles et répartition du stockage

6 - Cas d'une panne

- Fonctionnement en cas de perte d'un noeud : élection d'un nouveau noeud maître si nécessaire, déclaration de nouveaux shards primaires

7 - Exploitation

- Gestion des logs : ES_HOME/logs
- Paramétrage de différents niveaux de logs : INFO, DEBUG, TRACE
- Suivi des performances
- Sauvegardes avec l'API snapshot

Les objectifs de la formation

- Comprendre le fonctionnement d'Elastic Stack
- Savoir installer Elastic Stack en cluster
- Comprendre comment configurer et surveiller Elastic Stack
- Apprendre à installer et configurer kibana pour le mapping sur les données ElasticSearch

Evaluation

- Cette formation fait l'objet d'une évaluation formative.

Les points forts de la formation

- Une formation pratique qui permet aux participants d'apprendre le fonctionnement et comment administrer Elastic Stack.
- Les travaux pratiques effectués au cours de la formations sont réalisés sur Linux.
- 90% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Dates et villes 2026 - Référence BD522

Dernières places disponibles Session garantie

A distance

du 19 janv. au 20 janv.	du 28 mai au 29 mai	du 19 nov. au 20 nov.
du 26 mars au 27 mars	du 24 sept. au 25 sept.	

Paris

du 19 janv. au 20 janv.	du 28 mai au 29 mai	du 19 nov. au 20 nov.
du 26 mars au 27 mars	du 24 sept. au 25 sept.	