ElasticStack pour administrateurs

CB022

Durée: 2 jours

1 570 €

13 au 14 mars
19 au 20 juin

25 au 26 septembre
22 au 23 décembre

Public :

Architectes techniques, ingénieurs système, administrateurs, ...

Objectifs :

Comprendre le fonctionnement d'Elastic Stack, savoir l'installer en cluster, le configurer, le surveiller, savoir installer / configurer kibana pour le mapping sur les données Elasticsearch.

Connaissances préalables nécessaires :

Connaissances générales des systèmes d'information, et des systèmes d'exploitation (Linux ou Windows). Les travaux pratiques sont réalisés sur Linux.

Programme :

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

Installation et configuration

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

Clustering

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

Fonctionnement

Notion de noeud maître,
stockage des documents, shard primaire et réplicat,
routage interne des requêtes.

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

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

Exploitation

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