

ElasticSearch : infrastructure et administration

Durée: 2 jours

1220 €

8 au 9 mars
21 au 22 juin

27 au 28 septembre
13 au 14 décembre

Public:

Architectes techniques, ingénieurs système, administrateurs..

Objectifs:

Comprendre le fonctionnement d'Elasticsearch, savoir l'installer et le configurer, gérer la sécurité avec X-Pack, et 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 Elasticsearch, fonctionnalités, licence
Positionnement d'Elasticsearch et des produits complémentaires : Watcher, Kibana, Logstash, Beats, X-Pack
Principe : base technique Lucene et apports d'ElasticSearch
Fonctionnement distribué
- Installation et configuration** : Prérequis techniques.
Installation depuis les RPM.
Utilisation de l'interface X-Pack monitoring.
Premiers pas dans la console Sense.
Etude du fichier : elasticsearch.yml
- Kibana** : Présentation : objectifs, collecte de données, logs, ... par les APIs d'administration et de supervision ;
Stockage dans elasticsearch et mise à disposition dans une interface web de graphiques
Démonstrations.
- Clustering** : Définitions : cluster, noeud, sharding
Nature distribuée d'elasticsearch
Présentation des fonctionnalités : stockage distribué, calculs distribués avec Elasticsearch, tolérance aux pannes.

ElasticSearch : infrastructure et administration

- Fonctionnement** : Notion de noeud maître,
stockage des documents : , shard primaire et réplikat,
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
- Mise en oeuvre X-Pack Security** : Présentation des apports de X-Pack security: authentification,
gestion des accès aux données (rôles), filtrage par adresse IP ;
cryptage des données, contrôle des données;
audit d'activité.
- Exploitation** : Gestion des logs : ES_HOME/logs
Paramétrage de différents niveaux de logs : INFO, DEBUG, TRACE
Suivi des performances.
Sauvegardes avec l'API snapshot.
- Evolutions** : Les différentes versions : fonctionnalités et particularités des versions de 2.0 à 5.0.
Nouveautés de la version 6.0.