

ElasticSearch : infrastructure et administration

Durée: 2 jours

1 180 €

9 au 10 mars

15 au 16 juin

7 au 8 septembre

23 au 24 novembre

Public:

Architectes techniques, ingénieurs système, administrateurs..

Objectifs:

Comprendre le fonctionnement d'Elasticsearch, savoir l'installer et le configurer, gérer la sécurité avec shield, 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 : Shield, Watcher, Marvel, Kibana, Logstash, Beats
Principe : base technique Lucene et apports d'ElasticSearch
Fonctionnement distribué
- Installation et configuration** : Prérequis techniques.
Installation depuis les RPM.
Utilisation de l'interface Marvel.
Premiers pas dans la console Sense.
Etude du fichier : elasticsearch.yml
- L'interface Marvel** : 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, t
Démonstrations.
- 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.

ElasticSearch : infrastructure et administration

- 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
- Sécurisation avec shield** : Présentation des apports de shield : authentification, gestion des accès aux données (rôles), filtrage par adresse IP ;
cryptage des données, contrôle intégrité des données ;
audit d'activité.
Installation du plugin shield.
- 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. Nouveautés de la version 5.
Fonctionnalités à venir.