

# Elasticsearch - Infrastructure et administration

2 j (14 heures)

Ref : ESIA

## Public

Architectes techniques, ingénieurs système, administrateurs

## Pré-requis

Avoir des connaissances générales des systèmes d'information et des systèmes d'exploitation (Linux ou Windows)

## Moyens pédagogiques

Formation réalisée en présentiel ou à distance selon la formule retenue  
Exposés, cas pratiques, synthèse, assistance post-formation pendant trois mois  
Un poste par stagiaire, vidéoprojecteur, support de cours fourni à chaque stagiaire

## Modalités de suivi et d'évaluation

Feuille de présence émargée par demi-journée par les stagiaires et le formateur  
Exercices de mise en pratique ou quiz de connaissances tout au long de la formation permettant de mesurer la progression des stagiaires  
Questionnaire d'évaluation de la satisfaction en fin de stage  
Auto-évaluation des acquis de la formation par les stagiaires  
Attestation de fin de formation

## Objectifs

- Comprendre le fonctionnement d'ElasticSearch
- L'installer et le configurer
- Gérer la sécurité avec Shield
- Installer et configurer Kibana pour le mapping sur les données ElasticSearch

## Programme détaillé

### INTRODUCTION

---

- Présentation d'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...
- API d'administration et de supervision
- Stockage dans ElasticSearch et mise à disposition dans une interface Web de graphiques
- Démonstrations

## CLUSTERING

---

- Définitions : Cluster, Nœud, Sharding
- Nature distribuée d'ElasticSearch
- Présentation des fonctionnalités : Stockage distribué, Calculs distribués avec ElasticSearch, Tolérance aux pannes

## FONCTIONNEMENT

---

- Notion de nœud 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 nœud
- Configuration de nouveaux nœuds : Tolérance aux pannes matérielles et répartition du stockage

## CAS D'UNE PANNE - FONCTIONNEMENT EN CAS DE PERTE D'UN NœUD

---

Election d'un nouveau nœud maître si nécessaire

Déclaration de nouveaux shards primaires

## SECURISATION 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 plug-in Shield

Mise en œuvre de l'authentification

Lien avec les annuaires d'entreprise (LDAP, Active Directory)

Définition de rôles : Droits d'accès sur des actions ou des catégories de données, Attribution aux utilisateurs et groupes d'utilisateurs

Configuration de SSL et installation de certificats sur un cluster ElasticSearch

Séparation des communications entre nœuds et clients / nœuds

Configuration du filtrage par adresse IP

## 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 2.0

Fonctionnalités à venir