

ELASTICSEARCH : INFRASTRUCTURE ET ADMINISTRATION

CODE STAGE : BD022

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.

DURÉE

2 jours

PUBLIC

Architectes techniques, ingénieurs système, administrateurs.

PRÉ-REQUIS

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

PROGRAMME

1- 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

2- Installation et configuration

Prérequis techniques.

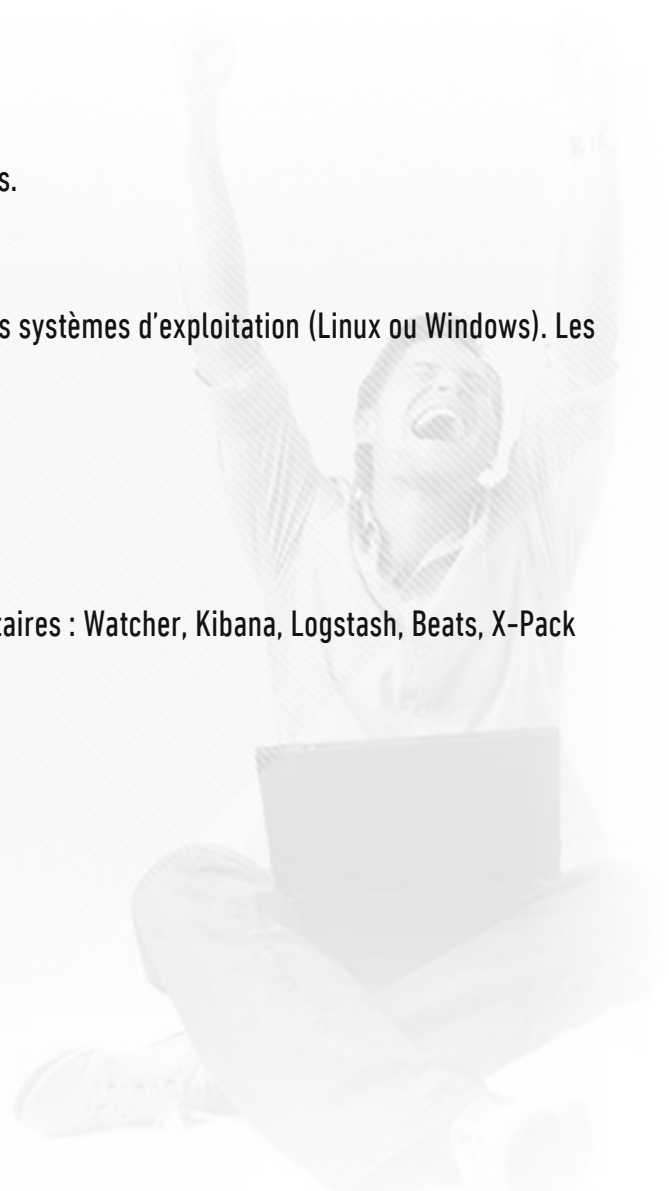
Installation depuis les RPM.


Utilisation de l'interface X-Pack monitoring.

Premiers pas dans la console Sense.

Etude du fichier : elasticsearch.yml

3- 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.

4- Clustering

Définitions : cluster, nœud, sharding

Nature distribuée d'elasticsearch

Présentation des fonctionnalités : stockage distribué, calculs distribués avec Elasticsearch, tolérance aux pannes.

5- Fonctionnement

Notion de nœud maître,

stockage des documents : , shard primaire et répliquet,

routage interne des requêtes.

6- 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

7- Cas d'une panne

Fonctionnement en cas de perte d'un nœud :

élection d'un nouveau nœud maître si nécessaire, déclaration de nouveaux shards primaires

8- Mise en œuvre 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.

9- Exploitation

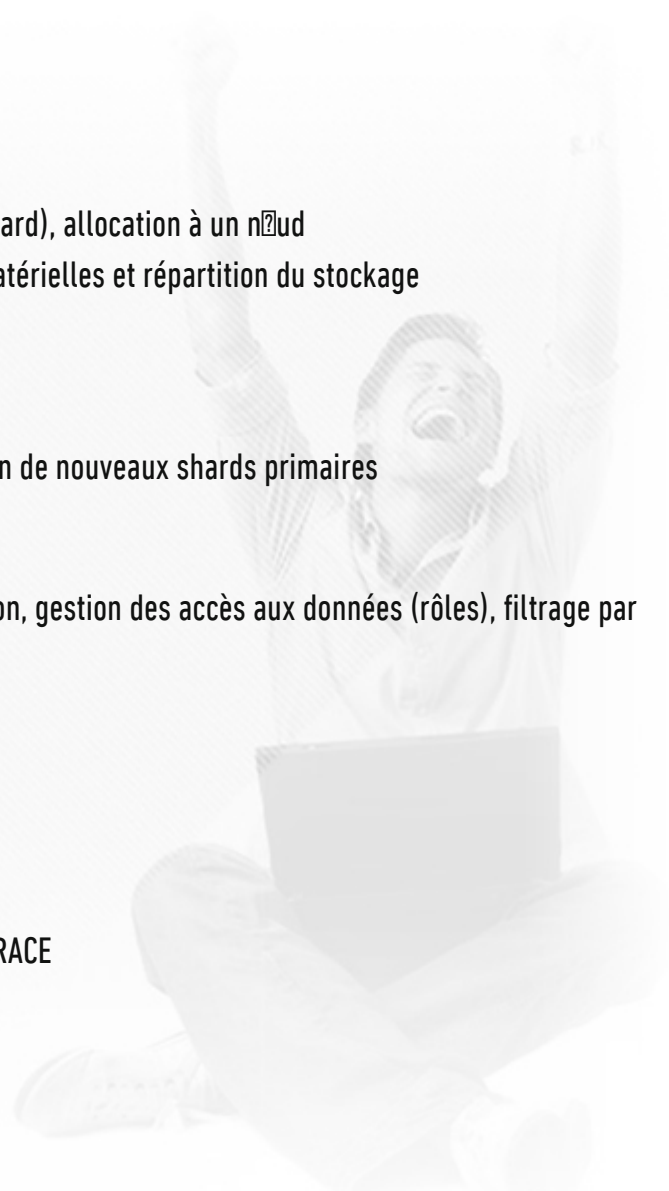
Gestion des logs : `ES_HOME/logs`

Paramétrage de différents niveaux de logs : INFO, DEBUG, TRACE

Suivi des performances.

Sauvegardes avec l'API snapshot.

10- Evolutions



Les différentes versions : fonctionnalités et particularités des versions de 2.0 à 5.0.
Nouveautés de la version 6.0.

