ELK pour administrateurs

Référence : **PYCB022** Durée : **2 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

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

PROFIL DES STAGIAIRES

• Architectes techniques, ingénieurs système, administrateurs.

OBJECTIFS

• Comprendre le fonctionnement d'Elasticsearch, savoir l'installer et le configurer, gérer la sécurité et installer / configurer kibana pour le mapping sur les données Elasticsearch.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Bigdata

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Introduction

- Présentation de la pile elastic
- Positionnement d'Elasticsearch et des produits complémentaires : Watcher, Marvel, Kibana, Logstash, Beats, X-Pack
- Les apports de la version 7.x
- 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 Devtools
- Etude du fichier : elasticsearch.yml

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