ELK pour développeurs et analystes

Référence : **PYCB021** Durée : **2 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• 1- Connaissances générales des systèmes d'information, et des systèmes d'exploitation (Linux ou Windows). • 2- Les travaux pratiques sont réalisés sur Linux. • 3- Connaissance d'un langage de programmation structuré.

PROFIL DES STAGIAIRES

• Architectes techniques, développeurs, analystes.

OBJECTIFS

• Comprendre le fonctionnement et les apports d'Elasticsearch dans le traitement de données, et savoir le mettre en oeuvre pour l'analyse de données.

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
- Cas d'usage classiques : analyse de logs et securité, analyse de métriques, recherches web, etc.

Installation et configuration

- Prérequis techniques. Utilisation de l'interface Marvel
- Premiers pas dans la console

Concepts clés

- Présentation des concepts clés d'ElasticSearch : index, types, documents, noeuds, clusters, shards et replica
- Opérations CRUD : exemples d'opérations basiques, création d'index et mappings

Format et stockage des données

- Format des données. Conversion au format JSON des données à traiter.
- Structure des données. Stockage, indexation. Terminologie Elasticsearch : notions de document, type, index.Métadonnées : _index, _type, _ID
- Choix de l'identifiant par l'application avec l'API index, ou genération automatique d'un identifiant
- Indexation inversée

Outils d'interrogation

- API RESTful en HTTP
- Exemples de requêtes simples et plus complexes : recherche de «phrases», extraction de plusieurs documents, etc.
- Notion de pertinence du résultat : «score»

- Requêtes avec Search Lite et avec Query DSL (domain-specific language)
- Utilisation de 'filtre' pour affiner des requêtes
- Aggrégation de résultats

Gestion des accès concurrents

- Utilisation du numéro de version
- Gestion par l'application : différentes méthodes selon les contraintes fonctionnelles
- Utilisation d'un numéro de version externe

Analyse et visualisation de données

- Principes de base de l'analyse de texte
- Recherche dans des données structurées, recherche full text
- Ecriture de requêtes complexes
- Notions d'aggrégations
- Mise en oeuvre : préparation des données, aggregation de mesures, bucket aggregation

Flux logstash et présentation Kibana

- Traitement de logs avec logstash
- Introduction à beats, installation et configuration
- Présentation Kibana et démonstrations
- Fonctionnalités : recherche, visualisation, création de tableaux de bord et graphiques à partir des données fournies par Elacticsearch