Contactez-nous Tél. : +33 (0)1 83 35 34 40
Email inscription@lepont-learning.com
Site web www.lepont-learning.com

ELASTICSEARCH
ElasticStack pour développeurs et analystes

REF : SIHA021

DUREE : 14h

Présentiel Classe virtuelle

PUBLIC

Cette formation s'adresse à des Architectes techniques, développeurs, analystes

Modalités et délais d'accés : les inscriptions sont fernées 24h avant la 1ére journée de formation.

Accessibilité : Si vous avez des contraintes particulières liées à une situation de handicap, veuillez nous contacter au préalable afin que nous puissions, dans la mesure du possible, adapter l'action de formation.

PREREQUIS

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

MODALITES PEDAGOGIQUES

1 poste et 1 support par stagiaire

8 à 10 stagiaires par salle

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

MODALITES D'EVALUATION

Auto-évaluation des acquis par le stagiaire via un questionnaire en ligne

Attestation de fin de stage remise au stagiaire

OBJECTIFS PEDAGOGIQUES

Cette formation vous permet de comprendre le fonctionnement et les apports d'Elasticsearch dans le traitement de données, et savoir le mettre en oeuvre pour l'analyse de données.

PROGRAMME

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.
- Premiers pas dans la console DevTools de Kibana.

Concepts clés

- Présentation des concepts clés d'ElasticSearch :
  - index, types, documents, noeuds, clusters, shards et replica
  - Notions de datatypes et mappings
  - 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 génération 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

Version du : 09/12/2021