

ELASTICSEARCH

ElasticSearch - ELK pour administrateurs

REF : SIHA022

DUREE : 14h

Présentiel Classe virtuelle

PUBLIC

Cette formation s'adresse à des Architectes techniques, ingénieurs système, administrateurs..

Modalités et délais d'accès : les inscriptions sont fermées 24h avant la 1ère 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.

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 d'Elasticsearch
- Installer et configurer Elasticsearch
- Gérer la sécurité
- Installer et configurer kibana pour le mapping sur les données Elasticsearch.

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

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 répliquet, 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.



