

Formation Stack ELK

Code : SYS-ELK-100 Durée : 2 jours (14 heures)

Public visé

Administrateurs système, Analysts / Engineers Elasticsearch, ingénieurs de développement.

{{< formation-prerequis >}}

Objectifs pédagogiques

À l'issue de cette formation, vous serez capable de :

- Installer et administrer des clusters Elasticsearch
- Configurer et monitorer le cluster Elasticsearch

Programme

Jour 1 - Matin : Introduction

- Présentation de la pile Elastic (Kibana, Logstash, Beats, X-Pack)
- Principe : base technique Lucene et apports d'Elasticsearch
- Fonctionnement distribué
- Cas d'usage classiques (analyse de logs et sécurité, analyse de métriques, recherches Web)

Jour 1 - Après-midi : Installation & Configuration

Installation d'un cluster Elasticsearch

- Cluster : vue d'ensemble
- Prérequis pour l'installation d'un cluster
- Installation de ELK (Elasticsearch, Logstash et Kibana)
- Configuration d'un cluster ELK

Gestion et configuration du cluster

- Fichiers de configuration
- Création du premier noeud (Client, Maître, De données)
- Configuration des nodes et rôles
- Définition des espaces de stockage (shard) et allocation à un noeud

Jour 2 - Matin : Monitoring & Recherche

Monitoring et administration du cluster

- Administration du cluster
- Surveillance des métriques d'index dans Kibana
- Répartition de charge et allocation des nodes
- Gestion des logs et état du bilan de santé
- Principes de sauvegarde et restauration

Elasticsearch : searching

- API RESTful en HTTP
- Recherches simples et complexes
- Recherches avec Bulk
- Pertinence du résultat ("score")
- Query DSL, filtres et agrégation de résultats

Jour 2 - Après-midi : Maintenance & Sécurité

Maintenance du cluster Elasticsearch

- Mise à jour des versions d'Elasticsearch
- Copie instantanée (snapshot) des index
- Utilisation de "Curator" pour automatiser les tâches

Sécurité sur Elasticsearch

- Présentation de X-Pack Security
- Gestion des utilisateurs et rôles
- Prévention des intrusions et falsification de données
- Traçabilité des activités

Modalités d'évaluation des acquis

En cours de formation, par des études de cas ou des travaux pratiques. En fin de formation, par un questionnaire d'auto-évaluation.

{{< formation-require >}}

{{< formation-seealso >}}