

Mis à jour le 27/11/2025

S'inscrire

Formation Elastic Stack ELK : La Suite Elastic

3 jours (21 heures)

Présentation

Notre formation sur la suite complète d'Elastic open source proposée par The Elastic Stack, vous aidera à rechercher des données, les extraire, les analyser et les visualiser pour générer des tableaux de bord en temps réel.

À l'issue de notre cours, vous découvrirez les nombreuses fonctionnalités qu'offre ELK tels que la journalisation centralisée, les multiples options d'hébergement ou l'évolutivité. [ElasticSearch](#) est un puissant moteur de recherche reconnu et utilisé par de grands acteurs internationaux (Sony, IGN, Stackoverflow, github, SoundCloud, Mozilla...). Orienté "document" au sens NoSQL du terme, toutes les données sont stockées sous forme de documents JSON structurés.

ELK possédera un rôle important au sein des infrastructures informatiques de vos entreprises. Vous apprendrez toute l'entièreté de l'écosystème d'ElasticSearch, son rôle ainsi que les cas d'utilisations.

Dans cette formation ELK, vous aborderez l'utilisation d'ELK V9 qui est l'association de 4 outils: Elasticsearch, Logstash, Kibana et Beats.

Vous découvrirez également Beats, qui permet de collecter et d'envoyer simplement des données. Logstash permet d'extraire les logs, les transférer, les parser, et enfin les indexer dans Elasticsearch. Kibana permet d'exploiter les données stockées dans Elasticsearch, de produire des requêtes, d'en faire des tableaux de bord depuis un navigateur web.

Comme dans toutes nos formations, celle-ci vous présentera la toute dernière version d'ELK / Elastic Stack.

Objectifs

- Découvrir Elasticsearch et les dernières nouveautés de la suite Elastic
- Connaissance de la suite ELK (avec Beats ELKB / BELK)

- Alimenter Elasticsearch avec de nombreuses sources de données
- Structurer et enrichir des données hétérogènes
- Transférer des données brutes depuis un fichier ou un broker
- Produire des tableaux de bords / dashboards avec Kibana
- Monitoring système, JMX, Métier et BI
- Administration avancée (Module optionnel)

Public visé

Développeurs, Administrateurs systèmes, DevOps.

Pré-requis

- Connaissances de base d'un système Unix
- [Tester Mes Connaissances](#)

Recommandations de lecture avant et après la formation

- [Un guide de la suite Elastic](#) qui montre les étapes à suivre pour améliorer la pertinence de la recherche
- Le [guide complet](#) sur la suite Elastic

Programme de la formation Elastic Stack ELK

Introduction et vue d'ensemble

- L'écosystème d'Elasticsearch
- Le rôle d'Elasticsearch, Logstash, Kibana et Beats
- Simplifier la gestion des versions avec The Elastic Stack version 9
- Les nouveautés de la version 9
- Principes et fonctionnement
- Exemples d'architectures
- Cas d'utilisations

Elasticsearch - Indexation, Recherche et analyse de données

- Introduction à Elasticsearch
- Indexation et recherche
- Analyse de données
- Mappings et configuration de l'analyse
- Requêtage avec Elasticsearch
- Système de plugins & Configuration
- Queries et Filters
- Agrégations

- Réplication et partitionnement
- TP: Installation et configuration
 - Serveur Elasticsearch
 - Mettre en place un cluster
 - Les rôles des noeuds

Logstash - Transformez et formatez vos données pour les utiliser depuis Elasticsearch

- Concepts : Input, Output, Filter (filtre), Codecs...
- Les Inputs : File, [Redis](#), RabbitMQ...
- Les Filters : Grok, Date, Mutate...
- Les Outputs : File, Elasticsearch, [Redis](#)...
- Threading et haute-disponibilité

Kibana - Visualisez les données d'Elasticsearch et Créez vos rapports

- Installation et configuration
- Découverte des données et construction des requêtes / Queries
- Agrégations et construction de Visualizations
- Panels
- Création des vues
- Mise en place d'un tableau de bord
- TP : Créer un rapport avec une visualisation en temps-réel

Beats - Collectez, Parsez et envoyez simplement vos données

- Introduction aux Data Shippers et au monitoring temps réel
- Monitorer votre réseau grâce à PacketBeat
- Monitorer vos fichiers grâce à FileBeat
- Monitorer vos Windows event logs grâce à WinlogBeat
- Récupérer les métriques importantes de vos serveurs grâce à Metricbeat

Monitoring et analyse

- Mise en pratique
- Monitoring Système
- Monitoring JVM / JMX
- Log As A Service
- Analyse Métier & BI (Business Intelligence)

Modules avancés d'administration (optionnels)

- X-Pack: Sécurisez et protégez vos données et soyez alerté grâce à des rapports sur l'état de santé de vos services Elastic Stack !
- ES-Hadoop

- Elastic Cloud: Elasticsearch as a Service
- Graph
- Tuning et architectures avancés
- Supervision (Kopf, Marvel) et monitoring (Cluster, Nodes, Cat)
- Sauvegardes : Snapshots et Restore

MODULE COMPLÉMENTAIRE EN ANGLAIS SUR DEMANDE (+2 JOURS)

- Training language : English
- Course level : Beginner to intermediate

Cette formation permet de maîtriser les concepts de base de Elasticsearch et d'explorer les principaux composants de "Elastic Stack" : Beats, Logstash, Elasticsearch et Kibana. Elle aborde plusieurs cas d'utilisations et comment définir une architecture adéquate et bien dimensionner les clusters.

Théorie : 60% Pratique : 40%

Audience :

- Data Engineers
- Architects
- System Administrators
- DevOps

Prerequisites :

- Knowledge of REST/HTTP, Json, Yaml are appreciated
- No knowledge required

Elasticsearch : Getting Started

- Elasticsearch Overview
- Keys Features
- Basic Concepts
- Install Elasticsearch
- CRUD Operations
- First steps on Search API

Elasticsearch : Mappings and Templates

- Introduction
- Data Types
- Main parameters
- Mapping API

- Analysis and Inverted Index
- Multi-Fields
- Dynamic Mapping
- Templates

Elasticsearch : Search and Aggregations

- Search API Overview
- Terms, Full Text, and Compound Queries
- Aggregations Overview
- Metrics, Aggregations
- Buckets Aggregations
- Pipelines Aggregations

Elasticsearch : Ingest and Pipelines

- Ingest Node
- Pipelines

Kibana

- Overview
- Management
- Discover
- Visualize and Dashboard
- More Features

Beats

- Overview
- Filebeat
- Metricbeat
- More Beats

Logstash

- Overview
- Pipeline Configuration
- Main settings

Architectures

- Elastic Stack based Architecture
- Elastic Stack and Kafka Integration

- Monitoring using Elastic Stack.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.