Elastic Stack

Durée 3 jour(s) (ELASTIC-STACK)

Centraliser, explorer, mettre en relief les logs

Description

Elastic Stack est principalement construit autour d'Elasticsearch, Kibana et Logstash même si désormais, les outils Beats viennent les compléter avantageusement. Elasticsearch est la brique fondamentale de la stack en tant que moteur d'indexation des données, base de stockage et finalement comme moteur de recherche. Tous les projets doivent transférer et transformer les données avant de les envoyer vers lui de manière à les rendre utilisables et centralisées. Alors que les outils Beats ou Logstash peuvent transférer les données, la transformation peut être effectuée par les noeuds d'ingestion du cluster Elasticsearch ou bien par les plugins de filtre de Logstash. Il est souhaitable également d'avoir un outil facilitateur nous permettant de requêter/analyser ou représenter nos données avec une interface graphique fluide et confortable. C'est ici que Kibana donne de sa puissance pour créer les requêtes, construire des visualisations ou des tableaux de bords thématiques simplement depuis votre navigateur web préféré.

Formation animée en présentiel

La formation en présentiel se déroule sur des jours consécutifs.

Formation disponible en mode "formation à distance"

La formation à distance peut se dérouler sur des jours consécutifs ou se décomposer en demies journées

Les ressources pédagogiques, la documentation, les slides de formation et les Travaux Pratiques de cette formation sont en anglais.

Précision : nos formateurs dispensent la formation en français et s'appuient sur des supports rédigés en anglais.

Objectifs

- Appréhender Elasticsearch et identifier ses concepts clefs
- Amener et transformer des données brutes via différentes briques technologiques (brokers, sockets...) avant de les envoyer au moteur de recherche Elasticsearch
- Produire des tableaux de bords efficaces avec de nombreux diagrammes, cartes géographiques ou compositions de times series

Public

- Développeur
- Architecte
- Profil orienté Ops

Prérequis

Une connaissance minimum des architectures Web et REST, des brokers de messages, du développement ainsi que du système linux est requise.

Répartition

50% Théorie, 50% Pratique

Evaluations des acquis

L'évaluation des acquis de la formation se fera en séance au travers d'ateliers, d'exercices et/ou de travaux pratiques. Dans le cas d'une formation officielle éditeur, veuillez nous consulter afin que nous vous fassions part des modalités d'évaluation.

A l'issue de la formation, vous sera transmis une évaluation à chaud de l'action de formation qui vous permettra de nous faire part de vos retours quant à votre expérience apprenant avec Zenika.

Ressources pédagogiques

Les ressources pédagogiques proviennent de productions des équipes Zenika et/ou de la documentation éditeur dans le cas d'une formation "Officielle". Les documents sont en français ou en anglais.

RQTH et ma formation Zenika

Si vous êtes sujet à un handicap, prenez contact avec nos équipes pour que nous puissions définir ensemble comment nous pourrons aménager la session afin que vous puissiez vivre une expérience en formation inchangée.

Programme

Vue d'ensemble

- Les nouveaux usages de journalisation
- L'écosystème autour d'Elasticsearch
- Le rôle d'Elasticsearch, Beats, Logstash et Kibana
- Exemples d'architectures

Introduction à Elasticsearch

- De l'indexation à la recherche
- Analyse textuelle
- Mappings et configuration de l'analyse
- Requêtage les possibilités d'Elasticsearch
- Queries et Filters
- Agrégations
- Réplication et partitionnement
- Templates d'index et alias
- Data streams
- ILM et rollover

Intégration des données

- Agents Beats
  - Les concepts clefs: Input, Module, Output, Processor, ...
  - Les Modules
  - les Inputs (avec gestion du multiline) et les Outputs
  - Les Processors
  - Include / Exclude
  - Command line
- Pipelines d'ingestion
  - Création, mise à jour et tests
  - Processors, syntaxe Mustache
  - Gestion des erreurs
  - Utilisation dans les agents Beats
- Logstash
  - Les concepts clefs: Input, Output, Filter, ...
  - Les Inputs et Outputs
  - Les Filters: Date, Grok, Dissect, Mutate, ...
  - Threading et haute-disponibilité
  - Queues persistentes, dead letter queue
  - Multi-pipelines
  - Envoi des données vers des index / data stream
- Fleet
  - Elastic agent
  - Fleet server
  - Intégrations
  - Polices pour les Elastic agent
  - Gestion centralisée

Kibana

- Découverte des données et construction de requêtes
- Agrégations et construction de visualisations
- Les différents types de visualisations
- Assembler des vues en un tableau de bord et l'administrer
- Les Canvas pour construire des présentations interactives

- Partage et export
- Alertes