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 (ELK) même si désormais, les outils Beats viennent les compléter avantageusement. Elasticsearch est la brique fondamentale de la stack en tant qu'indexeur 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.

Objectifs

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

Public

Architecte, Développeur, Ops

Prérequis

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

Répartition

60% Théorie, 40% Pratique

Programme

Vue d'ensemble

- Les nouveaux usages de journalisation
- L'écosystème autour d'Elasticsearch
- Le rôle d'Elasticsearch, 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
- Cas d'usages autour de Logstash(templates d'index, noms dynamiques avec résolution de dates, ...)
- Installation et configuration

Logstash

- Les concepts clefs: Input, Output, Filter...
- Les Inputs: File, Redis, RabbitMQ...
- Les Filters: Grok, Date, Mutate...
- Les Outputs: File, Elasticsearch, Redis...
- Threading et haute-disponibilité

Kibana

- Découverte des données et construction de Queries
- Agrégations et construction de Visualizations
- Compositions de courbes de type 'time series' avec Timelion
- Assembler des vues en un tableau de bord et l'administrer
- Installation et configuration