Elastic Stack

Duration 3 day(s) (ELASTIC-STACK)

Centralize and monitor logs

Description

The Elastic Stack is mainly built around Elasticsearch, Kibana and Logstash even if it is now completed with Beats shipping tools. Elasticsearch is the core element of the stack as the data indexer, storage manager and eventually as a search engine. All projects have to ship and transform datas before sending them to it in a ready to use manner. While shipping can be done with both Beats or Logstash tools, transformation can be done with Ingest Nodes or Logstash binary. Once this is done, you will want an easy to use tool to request/analyze or present your datas with a graphical UI. This is where Kibana gives you the power to build, requests, visualizations and thematic dashboards simply from your preferred web browser.

Goals

- Discover Elasticsearch and its key concepts
- Learn how to transfer and transform data from different sources and using different protocols (brokers, sockets, ...) before sending them to the search engine database
- Learn how to make great interactive dashboards with diagrams, maps and time series compositions

Public

- Architect
- Developer
- Ops

Prerequisites

A minimum knowledge in Web and REST architectures, brokers, development and linux operating system is required.

Structure

50% Theory, 50% Practice

Program

- Elastic stack at a glance
    - New log usages
    - Elasticsearch ecosystem
    - Elasticsearch, Logstash, Beats and Kibana roles
    - Architecture samples
- Introducing Elasticsearch
    - From indexing to search
    - Text Analysis
    - Mappings and analysis configuration
    - Elasticsearch query DSL
    - Queries and Filters
    - Aggregations
    - Replication and sharding
    - Index templates and aliases
    - Data streams
    - ILM and rollover
- Data integration
    - Beats agents
        - The key concepts; Input, Module, Ourput, Processor, ...
        - The Modules
        - The Inputs (with multiline management) and the Outputs
        - The Processors
        - Include / Exclude
        - Command line
    - Ingest pipelines
        - Creation, update and testing
        - Processors, Mustache syntax
        - Error management
        - Usage in Beats agents
    - Logstash
        - The key concepts: Input, Output, Filter, ...
        - The Inputs and Outputs
        - The Filters: Date, Grok, Dissect, Mutate, ...
        - Threading and high availability
        - Persistent queues, dead letter queue
        - Multi pipelines
        - Sending events to index / data stream
    - Fleet
        - Elastic agent
        - Fleet server
        - Integrations
        - Elastic Agent policies
        - Central management
- Kibana
    - Data discovery and queries building
    - Visualizations building using GUI aggregations builder
    - Different types of visualizations
    - Dashboard building and management
    - Canvas to build interactive presentation
    - Sharing et reporting
    - Alerting