Software Requirement: Windows machine with minimum 8 GB RAM

1. Basic understanding of Elastic search

Understanding Elastic eco system for log collection, aggregation and visualization (ELK stack)

Making your content searchable is not about exposing content to Google for indexing; it's about providing your own tailor made search, within your system to your users. Large players like Twitter and LinkedIn have been using Lucene for years, and today is the day you will see how easy it is to join their club by learning Elasticsearch from the ground up.

ELK Stack: Elastic Search, Log stash and Kibana

Table of Contents

Day 1

* Introduction
  + Elastic Stack Overview
  + Logs and Problems associated with it
* Role of Logstash for performing ETL
  + Logstash Installation and Configuration
  + Understanding and using Inputs, Filters, and Outputs
  + How to apply Conditionals in filters

Elasticsearch

* + Understanding Elastricsearch NoSQL architecture
  + CAP theorm for elasticserch
  + Comparing and contrasting Solr, Lucene and Elasticseach
  + Understanding the Elasticsearch Architecture and different types of Nodes
  + Inside the shards , node and performing cluster installation
  + Installing Elastic search cluster
  + Index Management :
* Multi Tenancy – Multiple indices, index aliases, cross index operations and introduction to data flow
* Elasticsearch Index – Analysis, mappings, index operations, versioning, APIs and settings
* Create  
  Read  
  Update  
  Delete  
  Data Modelling  
  Mapping  
  Aliases
  + Performing different kinds of search : term, terms, match,multi\_match, fuzzy,regexp and wildcard
  + Query DSL  
    Full Text Searches  
    Structured Searches  
    Proximity  
    Partial Matching

Day 2

Aggregations : Performing different kinds of aggregation such as

• percentile\_ranks

• cardinality

• significant\_terms

• top hits

• scripted metric

• filters

• range

• geohash

• terms

• histogram

• date\_histogram

• stats

• extended stats

• min / max

• sum

Suggestions:

• Term suggestion

• Phrase Suggestion

• Completion Suggestion

• Context Suggestion

Logstash :

* + [Installing Logstash](https://www.elastic.co/guide/en/logstash/5.4/installing-logstash.html)
  + [Stashing Your First Event](https://www.elastic.co/guide/en/logstash/5.4/first-event.html)
* [Structure of a Config File](https://www.elastic.co/guide/en/logstash/5.4/configuration-file-structure.html)
* [Accessing Event Data and Fields in the Configuration](https://www.elastic.co/guide/en/logstash/5.4/event-dependent-configuration.html)
* [Using Environment Variables in the Configuration](https://www.elastic.co/guide/en/logstash/5.4/environment-variables.html)
* [Logstash Configuration Examples](https://www.elastic.co/guide/en/logstash/5.4/config-examples.html)
* [Reloading the Config File](https://www.elastic.co/guide/en/logstash/5.4/reloading-config.html)
* [Managing Multiline Events](https://www.elastic.co/guide/en/logstash/5.4/multiline.html)
  + [Glob Pattern Support](https://www.elastic.co/guide/en/logstash/5.4/glob-support.html)
  + [Advanced Pipeline](https://www.elastic.co/guide/en/logstash/5.4/advanced-pipeline.html)
  + [Multiple Output Plugins](https://www.elastic.co/guide/en/logstash/5.4/multiple-input-output-plugins.html)

FileBeat (Advance Topic)

* [Installing Filebeat](https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-installation.html)
* [Configuring Filebeat](https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-configuration.html)
* [Configuring Filebeat to Use Logstash](https://www.elastic.co/guide/en/beats/filebeat/current/config-filebeat-logstash.html)
* [Loading the Index Template in Elasticsearch](https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-template.html)
* [Starting Filebeat](https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-starting.html)
* [Loading the Kibana Index Pattern](https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-index-pattern.html)

Kibana

* + Using Kibana to visualize the ES data
  + Settings
  + Time Picker, Search, and Filters
  + Kibana Discover, Visualization, and Dashboard Interfaces
  + Lab

Day 3

**CORE ELASTICSEARCH: OPERATIONS**

Shards: Filtering, Awareness & Capacity Planning

### **• Filtering (Hot/Cold Architectures)**

### **• Forced Awareness (Data Centre)**

### **• Capacity Planning**

• Time-Based Data Backup: Snapshot and Restore

• High Availability vs. Backup

• Repository, Snapshot, and Restore Internals

### **Repositories:** Shared File System Repository

### **Changing index settings during restore**

### **Restoring to a different cluster**

### **Monitoring snapshot/restore progress**

### **Stopping currently running snapshot and restore operations**

• Lab Production Monitoring:

### **Collecting Data from Particular Indices**

### **Configuring a Tribe Node to Work with Monitoring**

• APIs • Marvel • Alerting Best Practices

• JVM • Query Performance • Thread Pools

• Diagnosing Problems

• Lab Production Operational Best Practices

• Memory • Networking • Disk • Cloud • Security • Cluster Restart (Rolling and Full)

* + Handling Back Pressure in ELK stack
  + Deployment Architectures
  + Hardware Best Practices
* Operation Checklist
  + Debugging and Monitoring