Elastic Stack Operations

Description

Elastic Stack is a group of open source products from Elastic designed to help users take data from any type of source and in any format and search, analyze, and visualize that data in real time. The product group was formerly known as ELK Stack, in which the letters in the name stood for the products in the group: Elasticsearch, Logstash and Kibana. A fourth product, Beats, was subsequently added to the stack, rendering the potential acronym unpronounceable.

Elasticsearch is a search and analytics engine. Logstash is a server-side data processing pipeline that ingests data from multiple sources simultaneously, transforms it, and then sends it to a “stash” like Elasticsearch. Kibana lets users visualize data with charts and graphs in Elasticsearch.

The Elastic Stack is the next evolution of the ELK Stack.

This instructor-led course provides information on how to use Elastic Stack and its components in order to turn raw data into valuable business insights.

Delegates will learn how to:

- collect and normalize data using Beats and Logstash
- install, configure, and manage Elasticsearch clusters
- basic data visualization using Kibana In addition to the lectures, the content will be enforced with hands-on labs

Audience

Data Architects, Data Administrators, System Administrators, DevOps

Setup Requirements

- Mac, Linux or Windows
- Latest version of Chrome or Firefox
- SSH Client software (e.g. PuTTY)
- Access to lab servers over TCP/22 and TCP/5601

Outline

Elastic Stack Overview

Installation and Configuration

Ingesting System and Services Metrics

Ingesting File Data

Ingesting Network Monitoring & Tapping

Data Processing

Data Transformation & Enrichment

Working with Nodes

Indexes

Mapping and Analysis

Index Management

Cluster Management

Capacity Planning

Elasticsearch Internals

Monitoring

Production Checklist

Prerequisites

There are no prerequisites