Centralized Logging with the Elastic Stack: Getting Started

JP Toto

INFRASTRUCTURE DEVELOPER

@jptoto http://jptoto.jp

What is the Elastic Stack?

Elasticsearch

Logstash

Beats

Kibana

- ✓ Free
- ✓ Open Source
- ✓ Great at full-text searching

Previously Known as the ELK Stack

Elasticsearch

Logstash

Kibana

Elasticsearch Useful for Many Cases

Highly scalable

Built in search, aggregation, and sharding

Used by Microsoft Azure, Wordpress, and Stack Exchange

Your Role Today

DevOps / IT

GLOBOMANTICS

Take monitoring situation from non-existent to fully-fledged enterprise-ready

Web-based monitoring and historical searching

Proactive alerting solution

Elasticsearch

Distributed, fast, highly scalable document database

Created by Shay Banon in 2010

We'll use a simple single node cluster

Getting Started with Elasticsearch for .NET Developers

Administering an Elasticsearch Cluster

Logstash

Aggregates, filters, and supplements log data

Forwards altered logs to Elasticsearch

Sending logs directly to Elasticsearch without Logstash can lead to inconsistent data

Kibana

Web-based front-end

Works easily with Elasticsearch for charts, graphs, and visualizing data

Free from the Elastic company

Beats

Small, lightweight utilities for reading logs from a variety of sources. Usually sends data to Logstash

Filebeat: Text log files

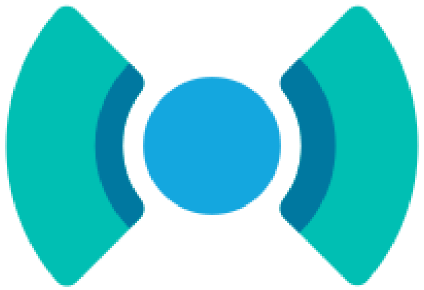
Metricbeat: OS and applications

Packetbeat: Network monitoring

Winlogbeat: Windows Event log

Libbeat: Write your own

Alerting



Helps track conditions based on Elasticsearch data

Continually monitors log data for pre-configured conditions

Send notifications to email, Slack, Hipchat, and PagerDuty out of the box

Summary

Discussed tools needed and how we'll build out the infrastructure

Let's begin building our Elastic Stack and installing software

You should have some experience with Windows & Linux administration to get the most out of the course