**Overview**

This challenge exercise created a pipeline including log receipt, filtering, normalization, consolidation, and visualization. All items requested in the challenge were completed, including all bonus items EXCEPT for transforming the IP data type in Elastic Search.

**Steps**

Detailed steps describing the installation of each tool described below is located here:

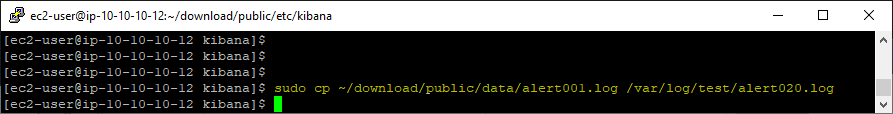
<https://github.com/htstinson/public/blob/master/ChallengeSteps.txt>

**Pipeline - flow**

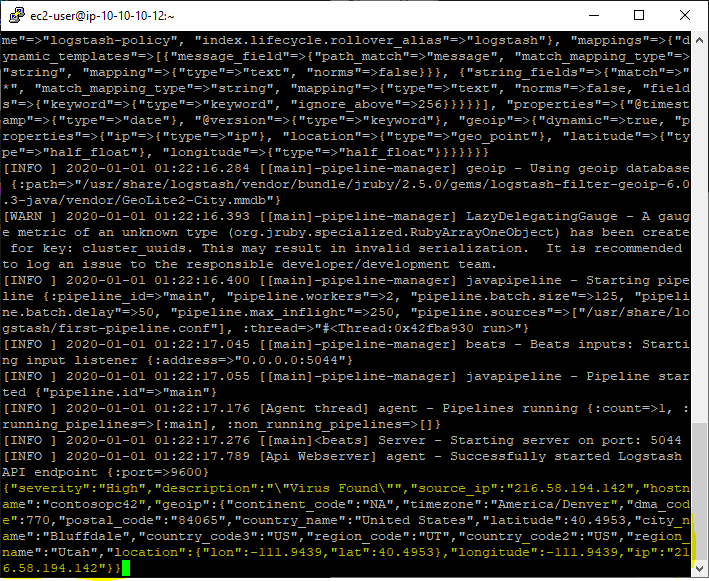
1. Sample log data was added to three files called “alert001.log”, “alert002.log” and “alert003.log”. Each log file differed slightly but had the same layout. These files were deposited in the /var/log/test folder. (Figure A)
2. The Filebeats application monitors the same folder for arriving files with a “log” extension and sends a json object to Logstash for each.
3. Logstash parses each file, adds geo-location data, and replaces numeric severity values with “High”, “Medium” or “Low”. It writes a json object to stdout and sends an object to Elastic Search. It uses the grok, geoip and alter plugins. (Figure B)
4. See Logstash configuration file here: <https://github.com/htstinson/public/blob/master/usr/share/logstash/first-pipeline.conf>
5. Elastic Search consolidates the normalized log entries and provides search functionality. It also provides a source of data for Kibana. (Figure C)
6. Kibana connects to elastic search and offers multiple data visualization tools through a web browser.

**Figure A – Sample Data**

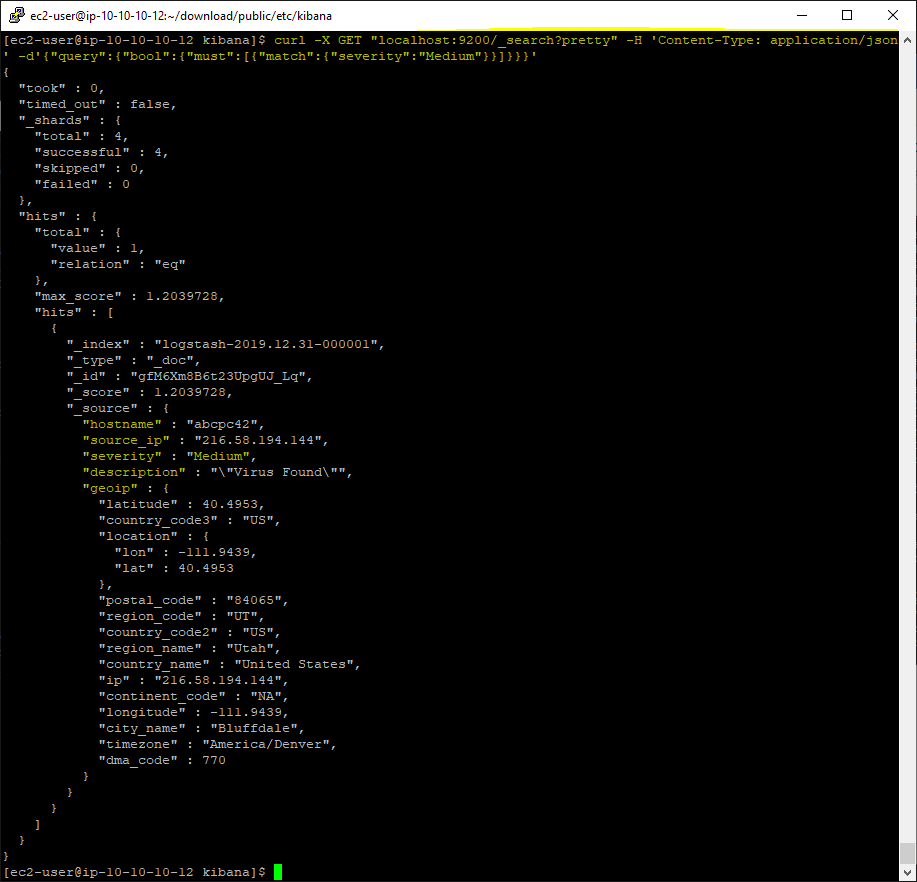
<14>1 2016-12-25T09:03:52.754646-06:00 contosohost1 antivirus 2496 - - alertname="Virus Found" computername="contosopc42" computerip="216.58.194.142" severity="1"



**Figure B – json written to stdout by Logstash**



**Figure C – searching Elastic Search using curl**



**Figure D – Kibana basic table**

