ELK Setup

install java sdk

install apache2 for Kibana webserver (could be nxigx)

moved to /var/www/html <<< not sure what this means?

vi /etc/network/interfaces

# The loopback network interface

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet static

address 62.193.8.60

netmask 255.255.255.0

up route add -net 85.15.16.0 netmask 255.255.240.0 gw 62.193.8.1

up route add -net 62.193.13.0 netmask 255.255.255.0 gw 62.193.8.1

auto eth1

iface eth1 inet static

address 62.193.6.50

netmask 255.255.255.0

gateway 62.193.6.254

vi /etc/elasticsearch/elasticsearch.yml

Spots that looks like Ken changed: (only 3 lines uncommented)

# Set a custom port to listen for HTTP traffic:

#

http.port: 443

http.cors.allow-origin: "/.\*/"

http.cors.enabled: true

vi /var/www/html/config.js

elasticsearch: <http://62.193.8.60:443>

vi /var/www/html/index.html.1 << for elastisearch

vi /etc/logstash/conf.d/logstash.conf <<< grok filters go here.

input { stdin { } }

filter {

grok {

match => { "message" => [ "%{SYSLOGLINE}","%{CISCOTIMESTAMP} %{IP} %{NOTSPACE:program} (?m)%{TIMESTAMP\_ISO8601:timestamp}%{SPACE}%{NUMBER:pid}?%{SPACE}?(?<loglevel>AUDIT|CRITICAL|DEBUG|INFO|TRACE|WARNING|ERROR) \[?\b%{NOTSPACE:module}\b\]?%{SPACE}?%{GREEDYDATA:logmessage}?","%{CISCOTIMESTAMP:timestamp} %{IP} %{SYSLOG5424SD} %{GREEDYDATA}%{URIPATHPARAM} %{JAVACLASS:program}%{URIPATHPARAM} %{GREEDYDATA:message}","%{CISCOTIMESTAMP:timestamp} %{IP} %{SYSLOG5424SD} %{GREEDYDATA}%{URIPATHPARAM} %{JAVACLASS}%{GREEDYDATA}%{URIPATHPARAM} %{IP} %{QS}" ] }

add\_field => [ "received\_at", "%{@timestamp}" ]

add\_field => [ "received\_from", "%{host}" ]

overwrite => [ "message" ] # After we've processed the log we dont need the raw message anymore

}

mutate {

gsub => ["timestamp", "\d{3}$", ""]

}

date {

locale => "en"

match => [ "timestamp", "MMM d HH:mm:ss.SSS", "MMM dd HH:mm:ss.SSS" ]

}

}

output {

#stdout { codec => rubydebug }

elasticsearch { host => localhost }

}

62.193.10.10 <- what is this (Piston Openstack Host? Boot node)

Can we change the time on this server?

vi /etc/resolv.conf <<<< added these 2 lines to resolve google.com

nameserver 8.8.8.8

search poc.inin.com

"%{SYSLOGLINE}","%{CISCOTIMESTAMP} %{IP} %{NOTSPACE:program} (?m)%{TIMESTAMP\_ISO8601:timestamp}%{SPACE}%{NUMBER:pid}?%{SPACE}?(?<loglevel>AUDIT|CRITICAL|DEBUG|INFO|TRACE|WARNING|ERROR) \[?\b%{NOTSPACE:module}\b\]?%{SPACE}?%{GREEDYDATA:logmessage}?" ]

Apr 17 19:53:00.587008 62.193.10.22 nova-compute 2015-04-17 19:53:00.586 11959 AUDIT nova.compute.resource\_tracker [-] Free ram (MB): 374272

Parse string #2

%{CISCOTIMESTAMP} %{IP} \[(?m)%{TIMESTAMP\_ISO8601:timestamp}\] %{GREEDYDATA:logmessage}?

Apr 20 13:02:49.574711 62.193.10.27 [2015-04-20 13:02:49.574] 1440/Thread-1 savage.WSGI-FredInterface/INFO: 62.193.10.10 \"GET /private/status HTTP/1.1\" 200 9282\r

<https://grokdebug.herokuapp.com/>

<https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-4-on-ubuntu-14-04>

<https://gist.github.com/ashrithr/c5c03950ef631ac63c43>

<http://christophe.vandeplas.com/2014/06/setting-up-single-node-elk-in-20-minutes.html>

ELK: Automation Tasks

Build KVM VM on INF03

Script to automate ELK build

Notes from Ken:

apt-get update  
apt-get upgrade -y  
wget <https://download.elasticsearch.org/elasticsearch/elasticsearch/elasticsearch-1.2.1.deb>  
dpkg -i elasticsearch-1.2.1.deb  
update-rc.d elasticsearch defaults 95 10  
apt-get install default-jdk  
/etc/init.d/elasticsearch start  
nano /etc/environment  
export no\_proxy=localhost,127.0.0.1  
curl -X GET <http://localhost:9200>  
wget <https://download.elasticsearch.org/logstash/logstash/packages/debian/logstash_1.4.2-1-2c0f5a1_all.deb>  
dpkg -i logstash\_1.4.2-1-2c0f5a1\_all.deb  
wget <https://download.elasticsearch.org/logstash/logstash/packages/debian/logstash-contrib_1.4.2-1-efd53ef_all.deb>  
dpkg -i logstash-contrib\_1.4.2-1-efd53ef\_all.deb  
wget <https://download.elasticsearch.org/kibana/kibana/kibana-3.1.0.tar.gz>  
tar -xvzf kibana-3.1.0.tar.gz  
cd kibana-3.1.0  
# Edit config.js, set hostname  
apt-get install nginx -y  
mkdir /var/www  
mkdir /var/www/kibana  
mv \* /var/www/kibana/  
cd /var/www/kibana  
#Finally we edit edit the /etc/nginx/sites-enabled/default file and find the following:  
#root /usr/share/nginx/www;  
#and change it to read as follows:  
#root /var/www/kibana;