Logging Tools

Contents

[Overview 2](#_Toc429407871)

[Use Cases 2](#_Toc429407872)

[Logstash 3](#_Toc429407873)

[Logstash Forwarder 3](#_Toc429407874)

[Logstash Server 3](#_Toc429407875)

[Elastic search 4](#_Toc429407876)

[Kibana 4](#_Toc429407877)

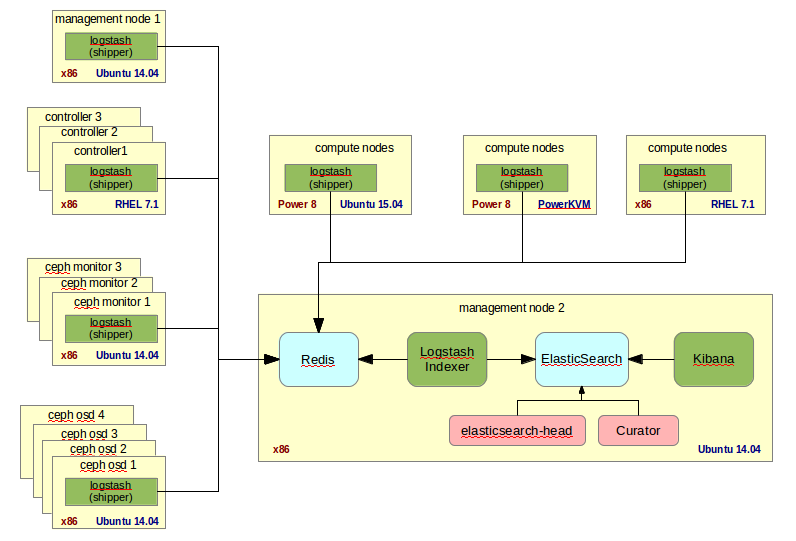
[Packages 4](#_Toc429407878)

[FAQs 5](#_Toc429407879)

[References 5](#_Toc429407880)

# Overview

This document describes Logging tool stack ELK(Elastic search + Logstash + Kibana) as search engine for all the configured log files across all the nodes in the datacenter. Installation and configuration of each comment can be found in the reference section. The figure below describe the components of Logging tool framework, their interactions and deployment model. The logstash client running on client system periodically send the log message of configured files to logstash server. Logstash server aggregates log messages from each client and transmits it to Elastic search. Elastic search does indexing of all the keywords found in the log message and provides REST API for keyword search. Kibana is dashboard for viewing the key word results and visualization of data collected from all the log files.



# Use Cases

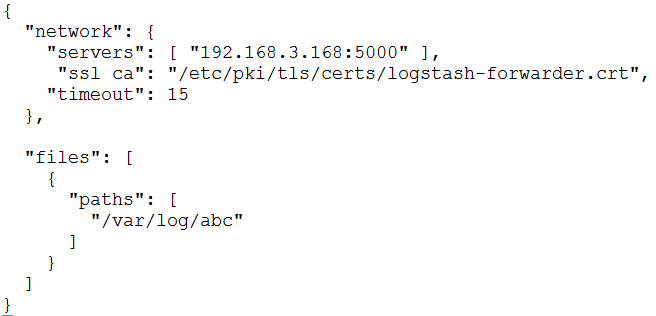
ELK is search and visualization tool for log files spread across hundreds of nodes in datacenter. Listed below are some of the use case of logging tools.

* /var/log/auth.log – logs user login times and failed attempts
  + Any one logged in with root account?
  + Which all system does a user ‘jack’ logged in last week?
  + Failed log in attempt for the a given user
* /var/log/syslog – logs global system message
  + System shutdown and start time
  + Logs critical errors like process crash, disk full, etc
* /var/log/yum.conf, /var/log/apt/history.log – packaged installed info
* Application logs
  + /var/log/apache2 – logs Apache server access details, errors etc
  + /var/log/mysql – logs the mysql errors, users accessing the db

# Logstash

## Logstash Forwarder

Logstash Forwarder or client installed on the nodes, periodically sends the log message to the log server. The log files to be monitored and the log server ip and port details need to be specified in the configuration file /etc/logstash-forwarder.conf. Snapshot of sample configuration file is shown below.



## Logstash Server

Logstash server is centralized server component which aggregates the log messages from all the logstash clients and send them over to elastic search for indexing. Ssl keys need to placed in each logstash client for ssl validation.

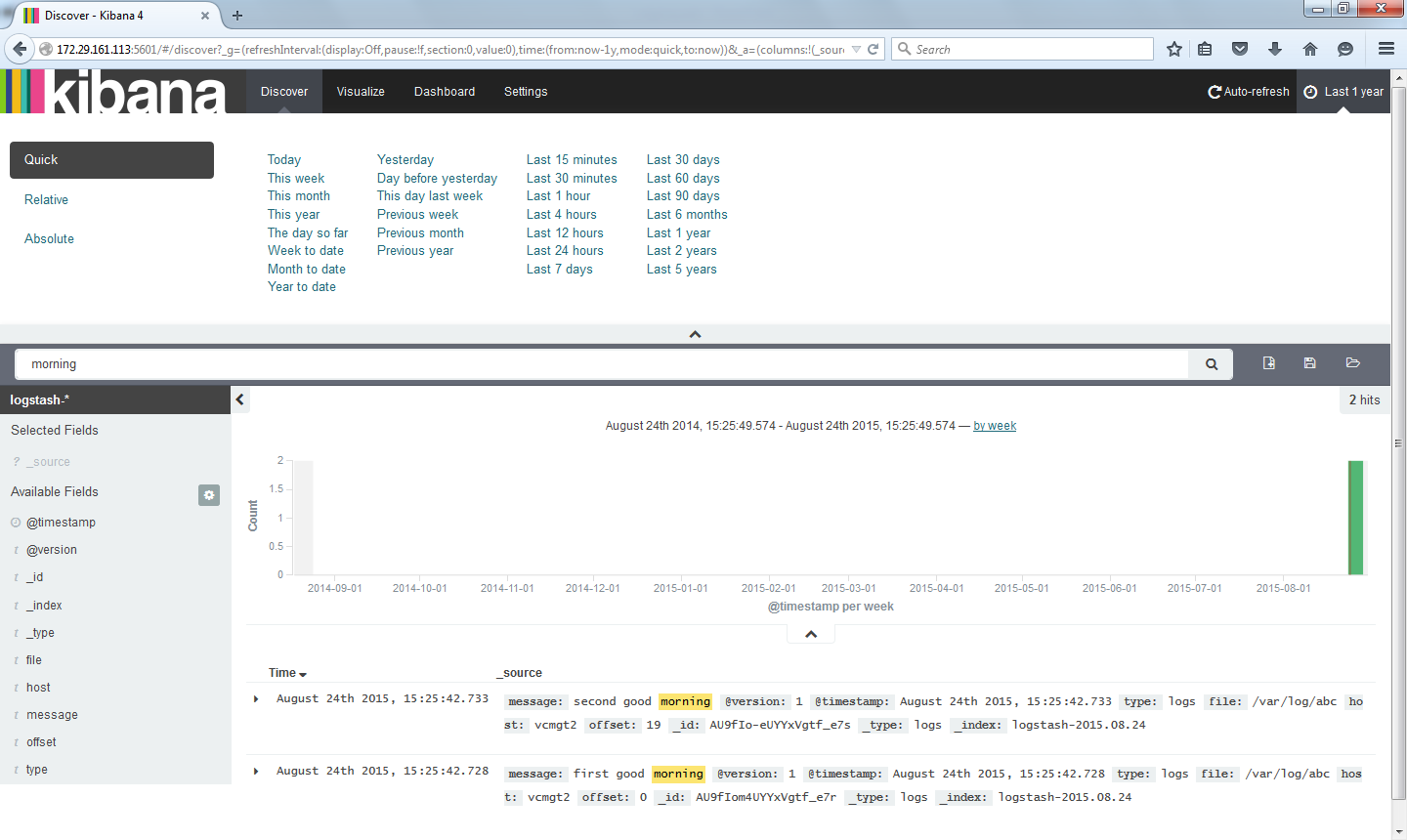


# Elastic search

Elastic search does the indexing of all the log messages received from logstash server. Apart from this it provides REST API’s for performing key word search and other operations for external systems. Curator is command line tool to create, delete indexes in the elastic search. Elastic search-head is web based tool to create and delete indexes.

# Kibana

Kibana is dashboard to explore, visualize data collected from Elastic search. It provides keyword based search on Discover tab, supports pie charts, bar charts to visualize data. Additional functionality includes saved searches, filtering data, and data exports. Sample screen shot of key word search on kibana Discover tab is shown below.



# Packages

Logging tools installation includes server and client components. Server component includes following packages:

1. Logstash Server components
2. Java 8
3. Elastic search
4. Kibana

Client components includes the following:

1. Logstash Forwarder

Packages for x86 system are available publicly through apt or yum repositories. For power ppc64, client packages need to be built from source by installing compilers and other tools.

# FAQs

**Is it possible to create bootable glance image with pre-installed Logstash client, so that VM booting through glance image has Logstash client installed and configured**

Yes, by installing Logstash client and properly configuring the logstash configuration file /etc/logstash-forwarder.conf, it is possible to create pre-installed glance image with logstash client. This can also be achieved through CI/CD tools which will install and configure logstash client post VM creation.

# References

1. ELK installation guide https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-4-on-ubuntu-14-04